红茶三杯
Vinsoney

学习 沉淀 成长 分享

数据网络基础 OSI七层模型

红茶三杯 http://weibo.com/vinsoney

Latest update: 2012-08-01

Content

数据网络基础

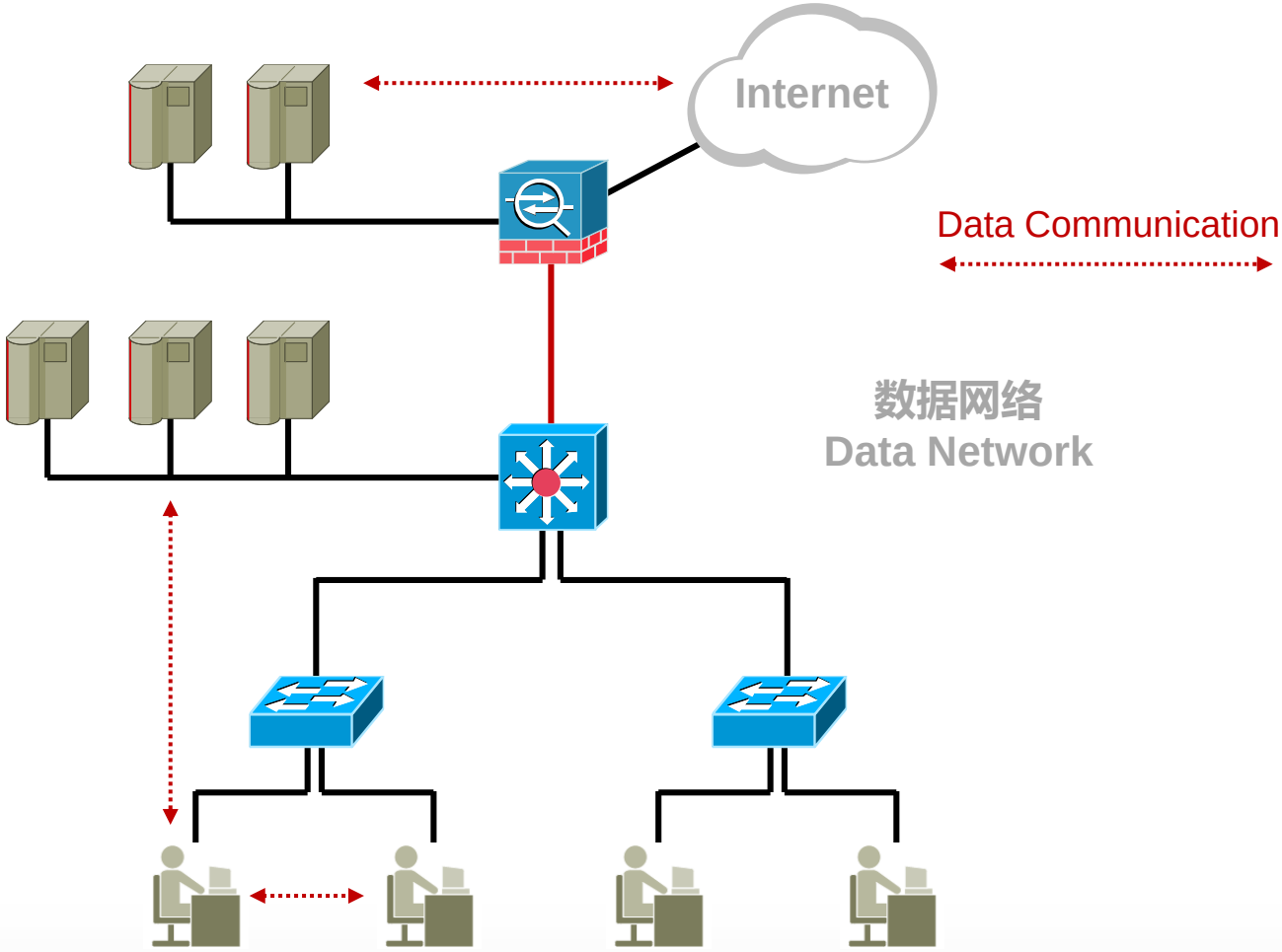
OSI七层模型

红茶三杯
Vinsoney

数据网络基础

- 什么是数据网络
- 什么是网络工程
- 什么是网络工程师

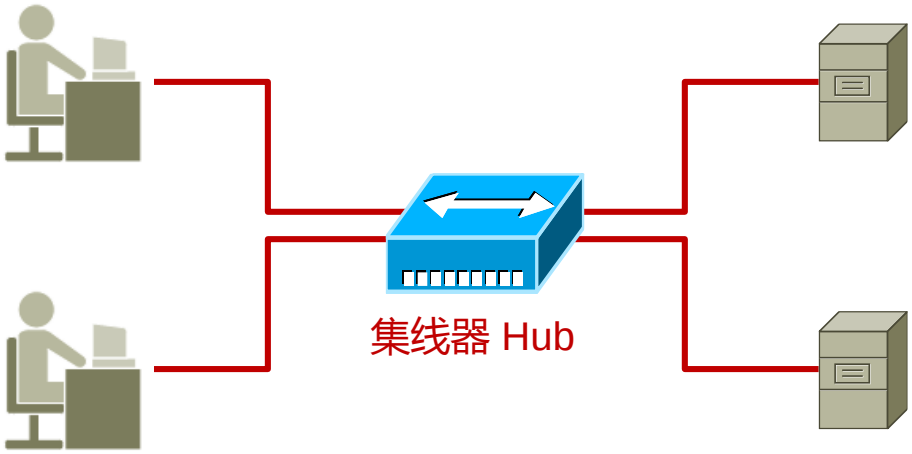
数据通信网络的概念



数据通信网络的概念

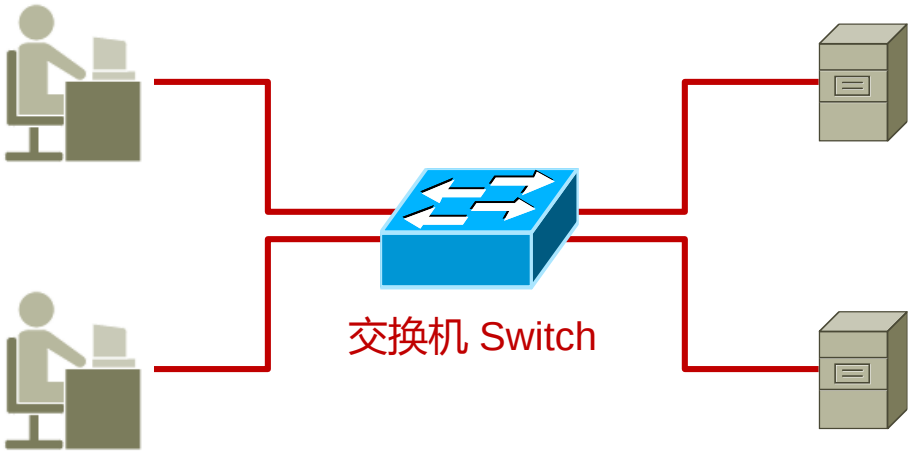
- 数据Data
- 协议Protocols

认识集线器



- 冲突Collision
- 冲突域collision domain

认识交换机

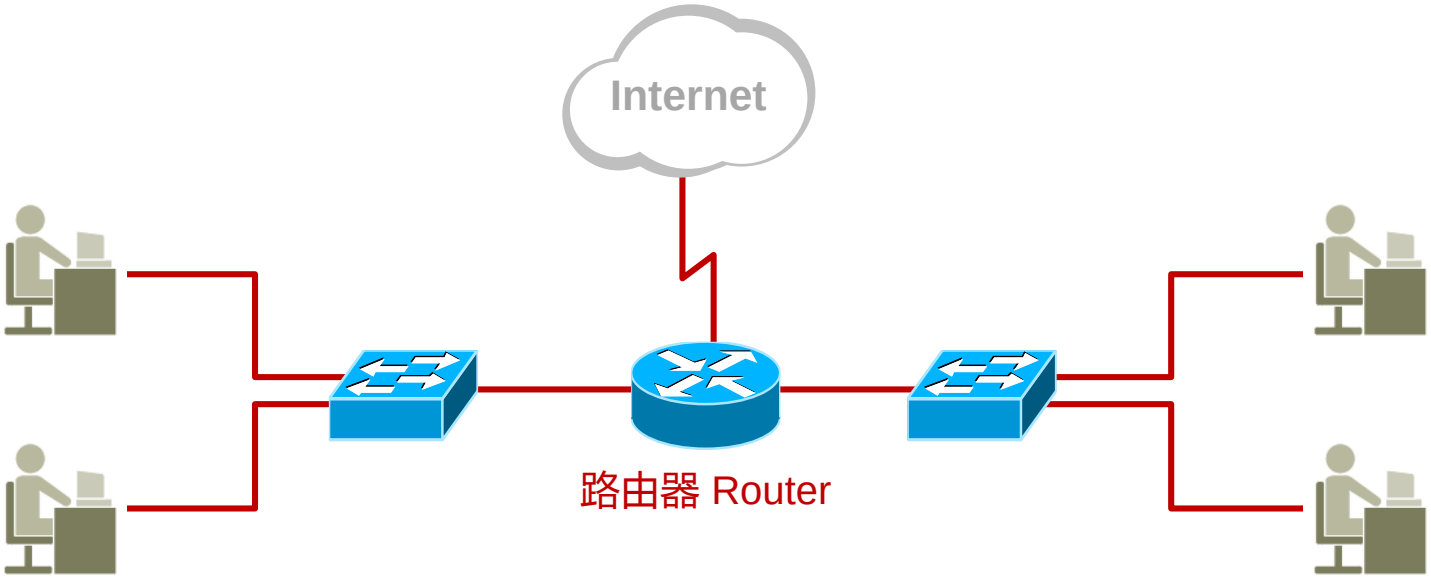


- 交换Switching
- 广播域Broadcast domain
- 单播Unicast
- 组播Multicast
- 广播Broadcast

认识交换机

- 终端设备的接入
- 数据帧的寻址及转发
- 基本的接入安全功能
- 广播域的隔离（VLAN）
- 二层链路的冗余、防环及负载均衡

认识路由器



LAN1

Broadcast Domain1

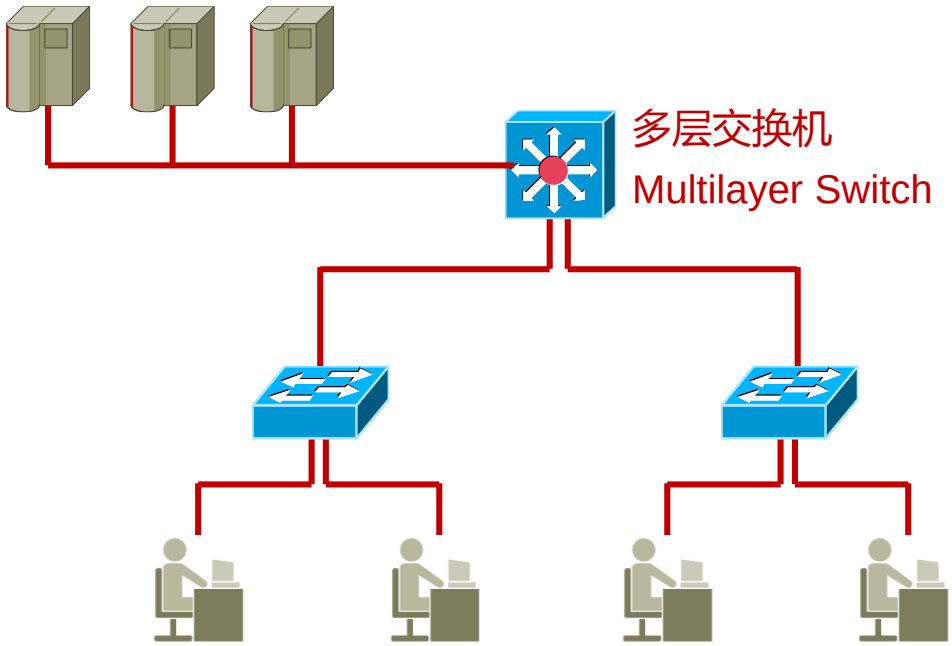
LAN2

Broadcast Domain2

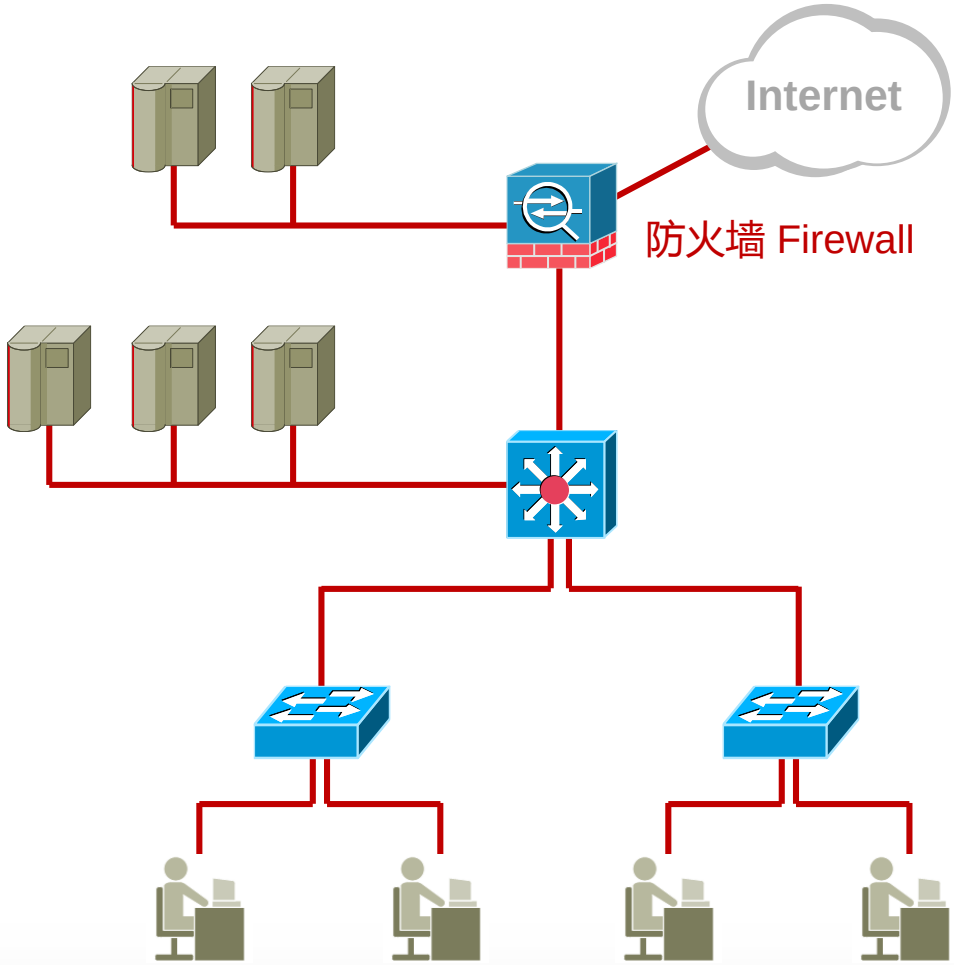
认识路由器

- 隔绝广播
- 路由协议的支持，路由选择
- 网络层寻址及数据转发
- 广域网接入、地址转换及特定的安全功能

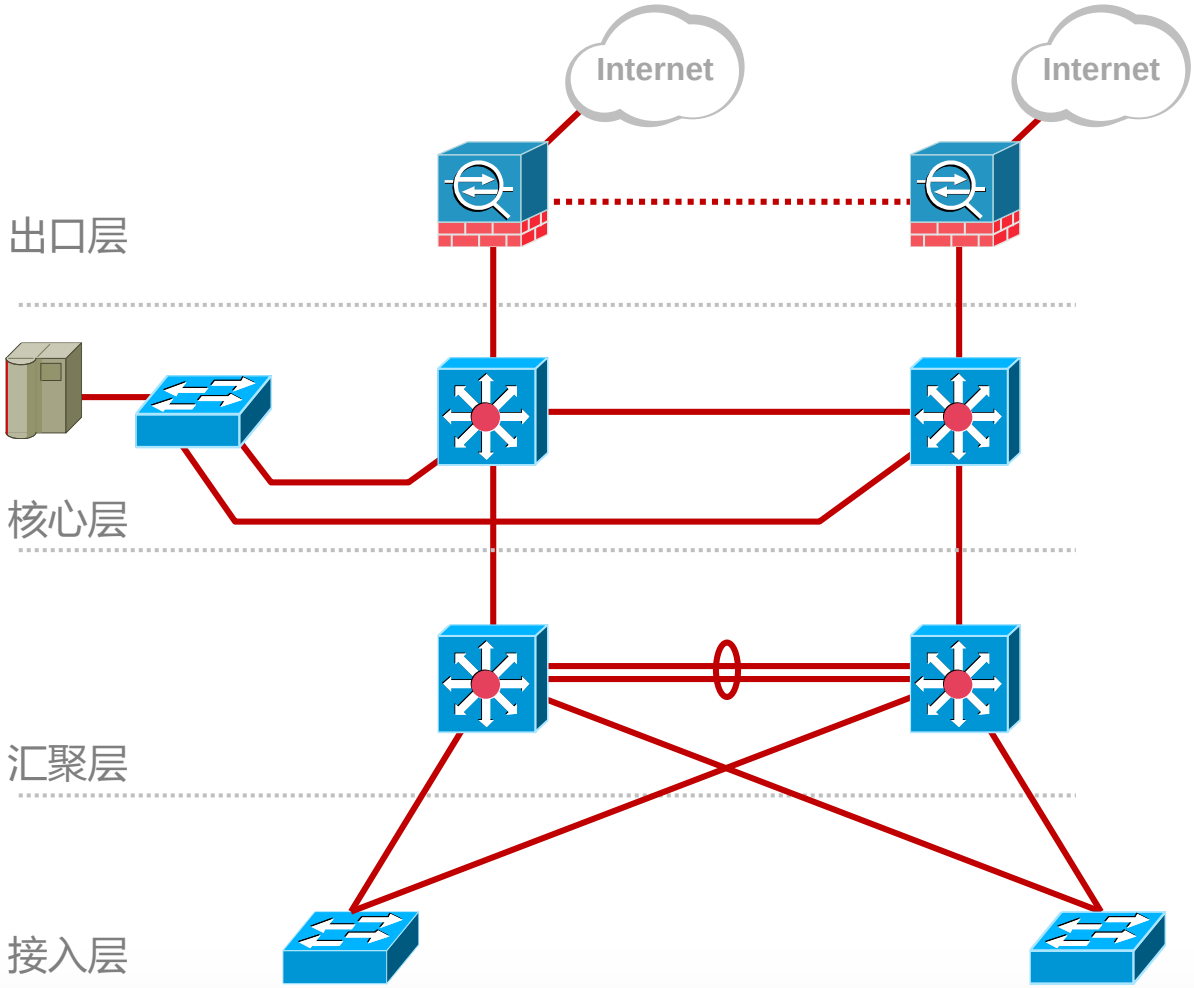
认识多层交换机



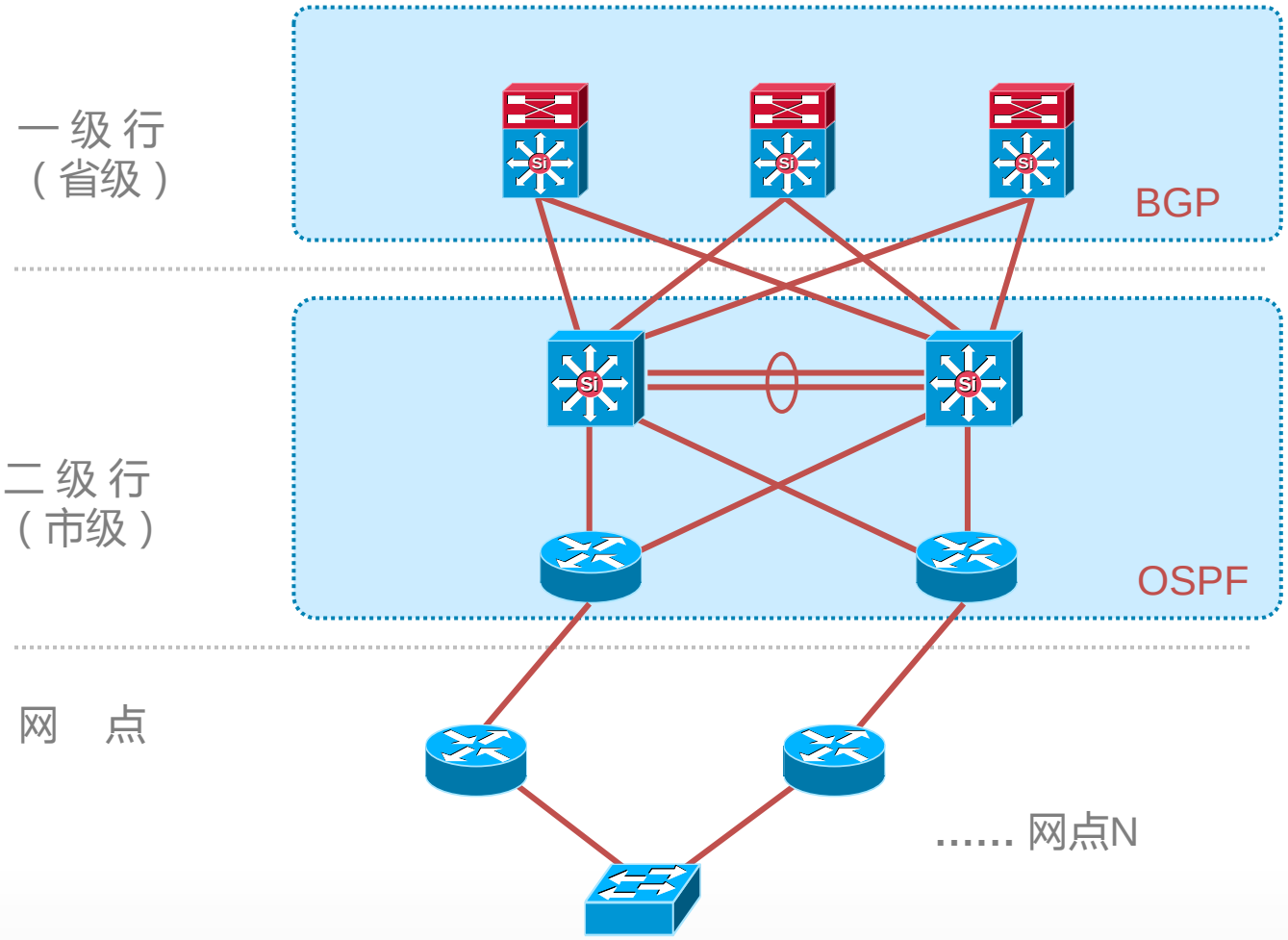
认识防火墙



层次化的园区网

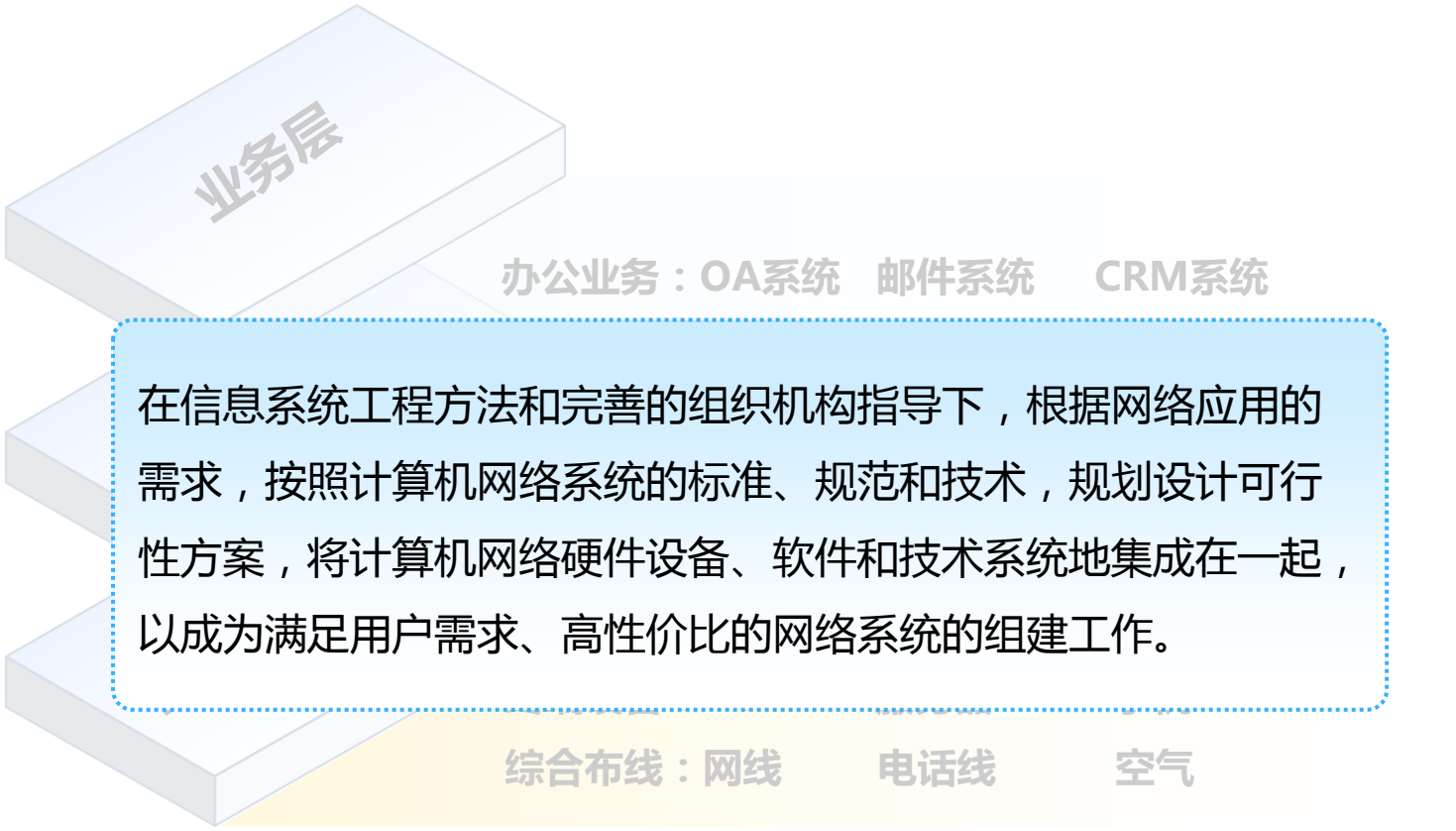


层次化的金融网络



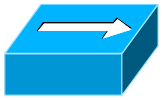
局域网、城域网、广域网

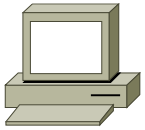
网络工程、数通工程师

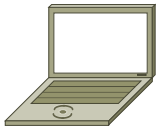


在信息系统工程方法和完善的组织机构指导下，根据网络应用的需求，按照计算机网络系统的标准、规范和技术，规划设计可行性方案，将计算机网络硬件设备、软件和技术系统地集成在一起，以成为满足用户需求、高性价比的网络系统的组建工作。

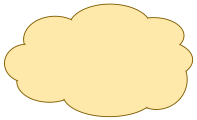
图标约定


100BaseT Hub


PC


Laptop

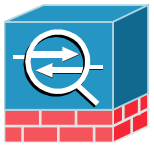

Workgroup Switch

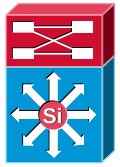

Cloud/Network


Line

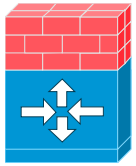

Routers


Access Point


Cisco ASA 5500

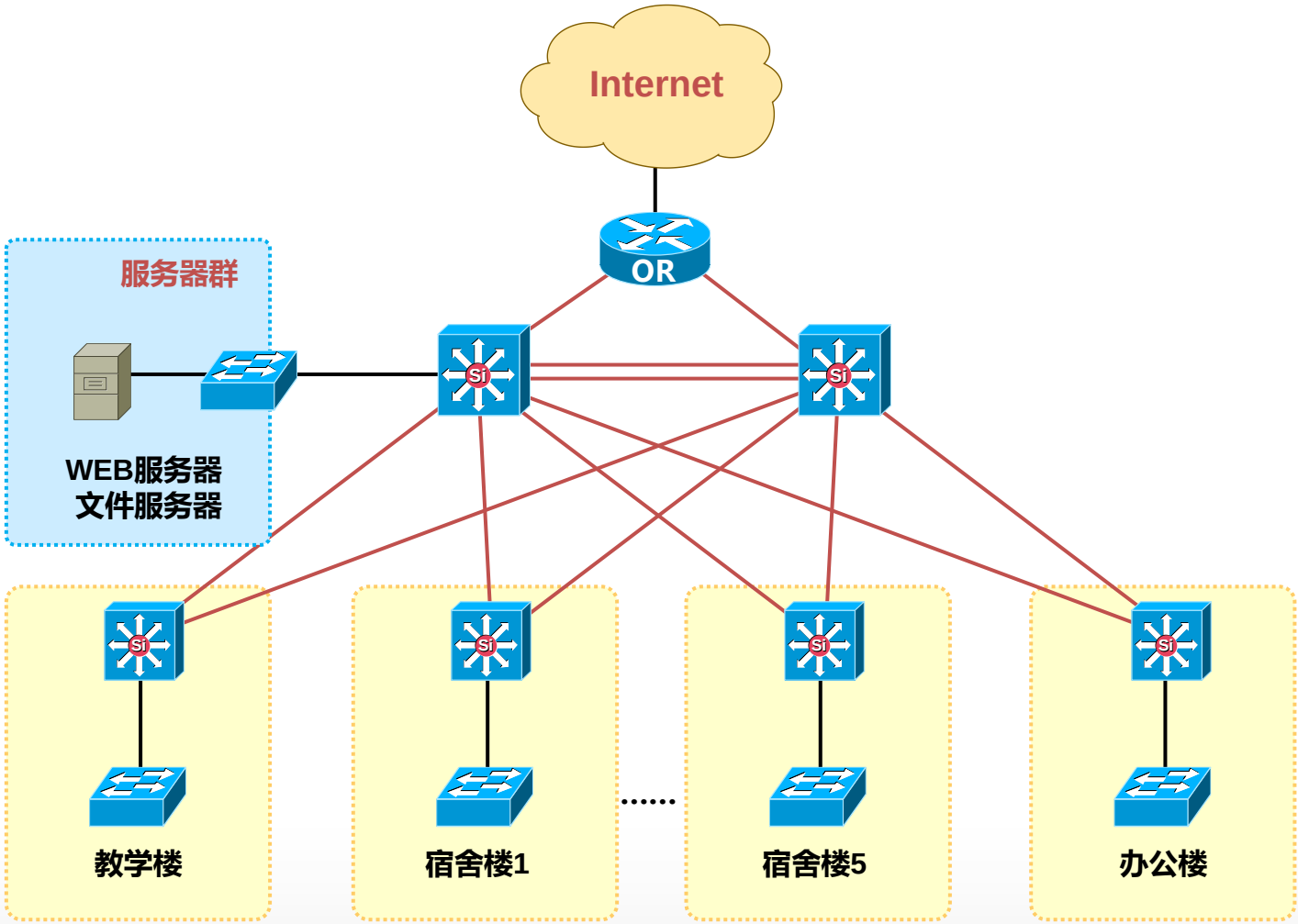


Route/Switch Processor


Cisco IOS Firewall


PIX Firewall

什么是网络拓扑（Topology）



网络技术成长之路

从宏观到微观再回宏观

归施排优	规划、实施、排错、优化；网络实战。
报文及底层	协议的底层工作机制、报文层面的细节。
协议机制	OSPF邻接关系如何建立？STP的详细工作过程如何？
这怎么用	OSPF怎么配置，怎么验证和查看？
这是什么	什么是路由，什么是交换？

红茶三杯
Vinsoney

OSI七层模型

- 什么是OSI七层模型
- OSI每一个层的定义及用途
- 如何使用OSI参考模型分析网络通信过程

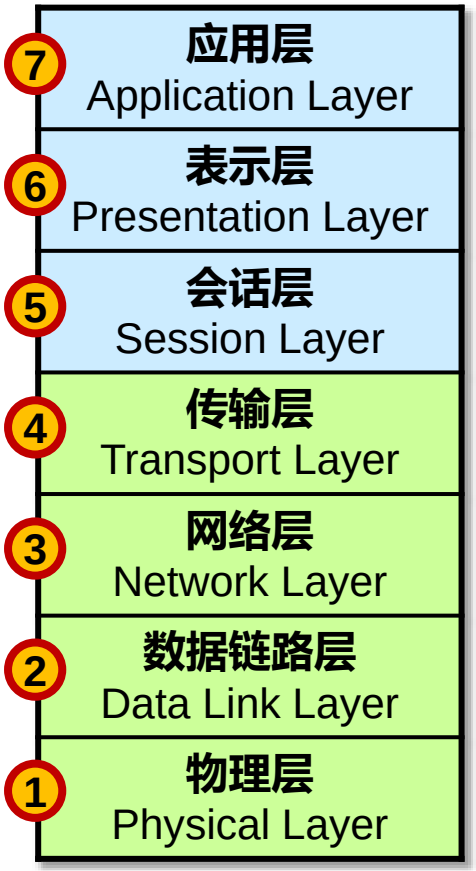
OSI 网际互联

- OSI的概念：
  - Open System Interconnect开放系统互连参考模型，是由ISO（国际标准化组织）定义的。它是个灵活的、稳健的和可互操作的模型。
- OSI模型的目的：
  - 规范不同系统的互联标准，使两个不同的系统能够较容易的通信，而不需要改变底层的硬件或软件的逻辑。
- OSI模型分为七层：
  - OSI把网络按照层次分为七层，由下到上分别为物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。

OSI的优点(不限于)

- 将网络的通信过程划分为小一些、简单一些的部件,因此有助于各个部件的开发、设计和故障排除；
- 通过网络组件的标准化，允许多个供应商进行开发；
- 通过定义在模型的每一层实现什么功能，鼓励产业的标准化；
- 允许各种类型的网络硬件和软件相互通信；
- 防止对某一层所做的改动影响到其他的层，这样就有利于开发。

OSI参考模型



OSI参考模型

各种应用程序协议

数据的格式化、数据加密解密、数据的压缩解压缩

建立、管理、终止实体之间的会话连接

数据的分段及重组；提供端到端的数据服务（可靠或不可靠）

将分组从源端传送到目的端；逻辑寻址；路由选择

将分组数据封装成帧；实现两个相邻结点之间的通信；差错检测

在介质上传输比特；提供机械的和电气的规约

OSI参考模型

特点：

1. OSI模型每层都有自己的功能集；
2. 层与层之间相互独立又相互依靠；
3. 上层依赖于下层，下层为上层提供服务。

第7层：应用层

- 为应用软件提供接口，使应用程序能够使用网络服务。常见的应用层协议：
  - http(80)、ftp(20/21)、smtp(25)、pop3(110)、telnet(23)、dns(53)等

第6层：表示层

- 数据的解码和编码
- 数据的加密和解密
- 数据的压缩和解压缩
- 常见的标准如：
  - ASCII
  - JPEG
  - ……

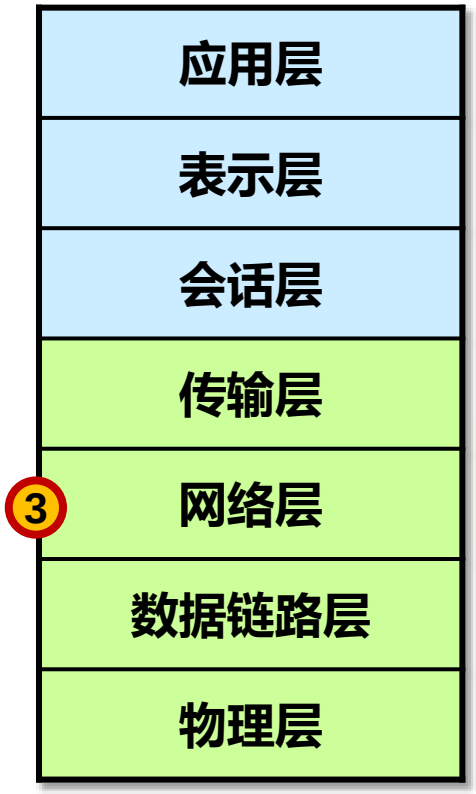
第5层：会话层

- 建立、管理和终止表示层实体之间的会话连接
- 在设各或节点之间提供会话控制
- 它在系统之间协调通信过程,并提供3种不同的方式来组织它们之间的通信:单工、半双工和全双工

第4层：传输层

- 负责建立端到端的连接，保证报文在端到端之间的传输。提供可靠及不可靠的传输机制。
- 服务点编址、分段与重组、连接控制、流量控制、差错控制。

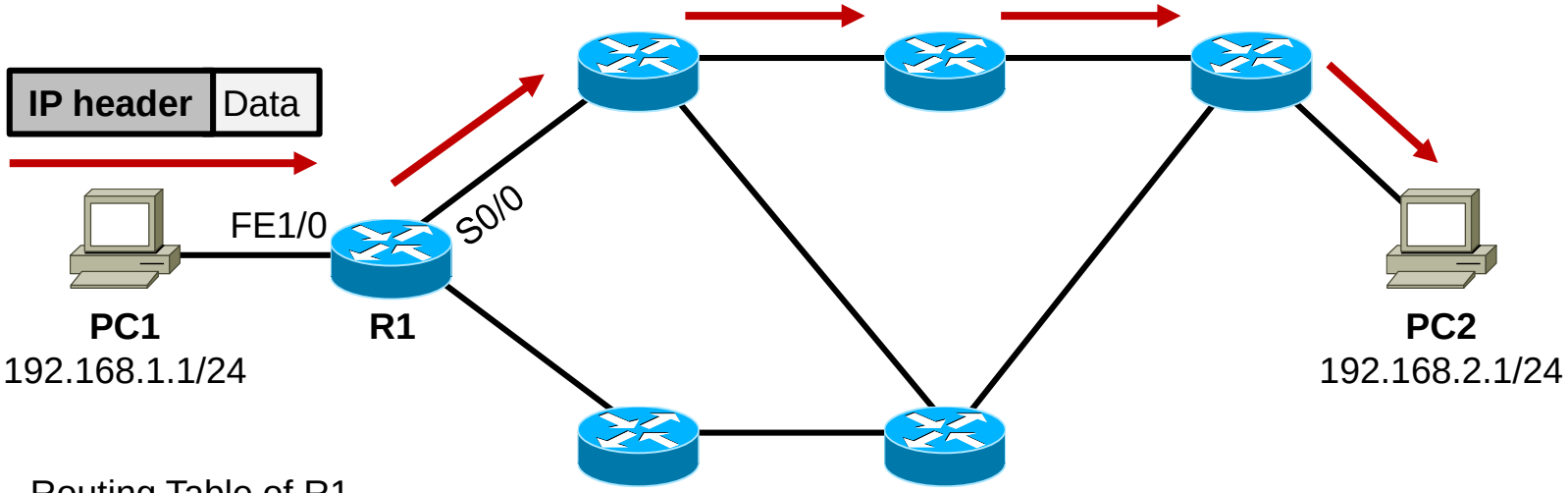
第3层：网络层



- 定义逻辑地址
- 逻辑寻址，将数据分组从源传输到目的
- 路径选择、路由发现、维护路由表

第3层：网络层

- 路由（Routing）



Routing Table of R1

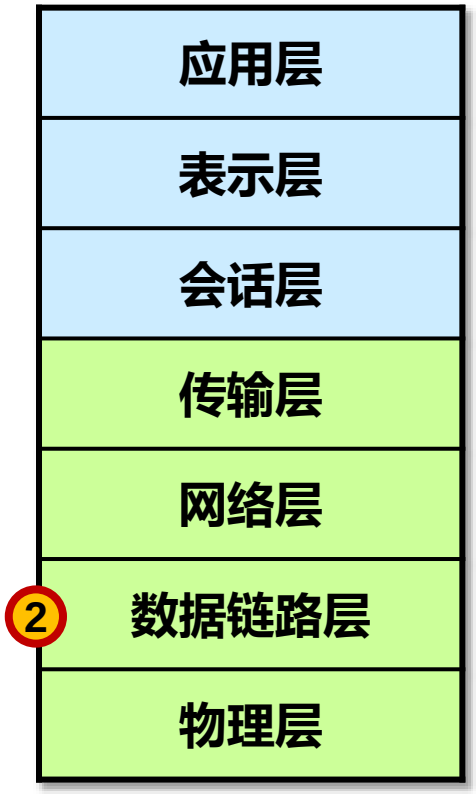
Protocol	Network	Exit Intf
Connected	192.168.1.0/24	FE1/0
Connected	192.168.12.0/24	S0/0
RIP	192.168.2.0/24	S0/0

第3层：网络层

- 工作在第3层的设备：路由器（Router）

- 隔离广播域；隔离广播
- 路由选择；维护路由表
- 寻址及转发
- 流量管理
- 连接广域网(WAN)

第2层：数据链路层

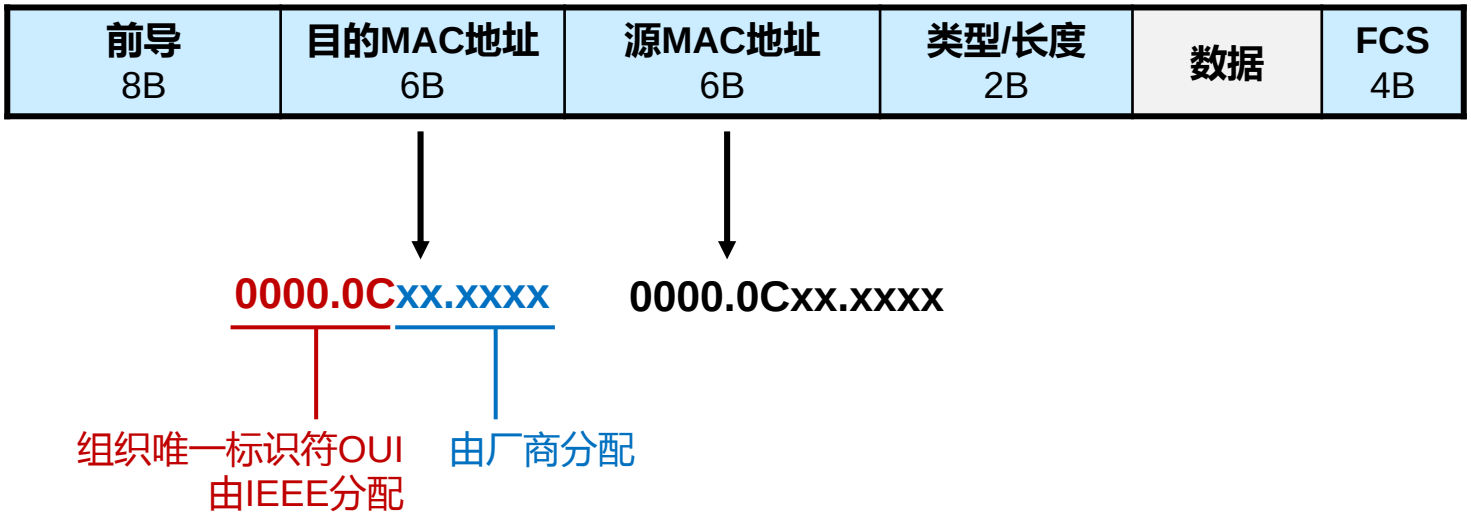


- 组帧、物理编址，将数据帧从链路上的一个节点传递到另一个节点
- 流量控制、差错控制、接入控制

第2层：数据链路层

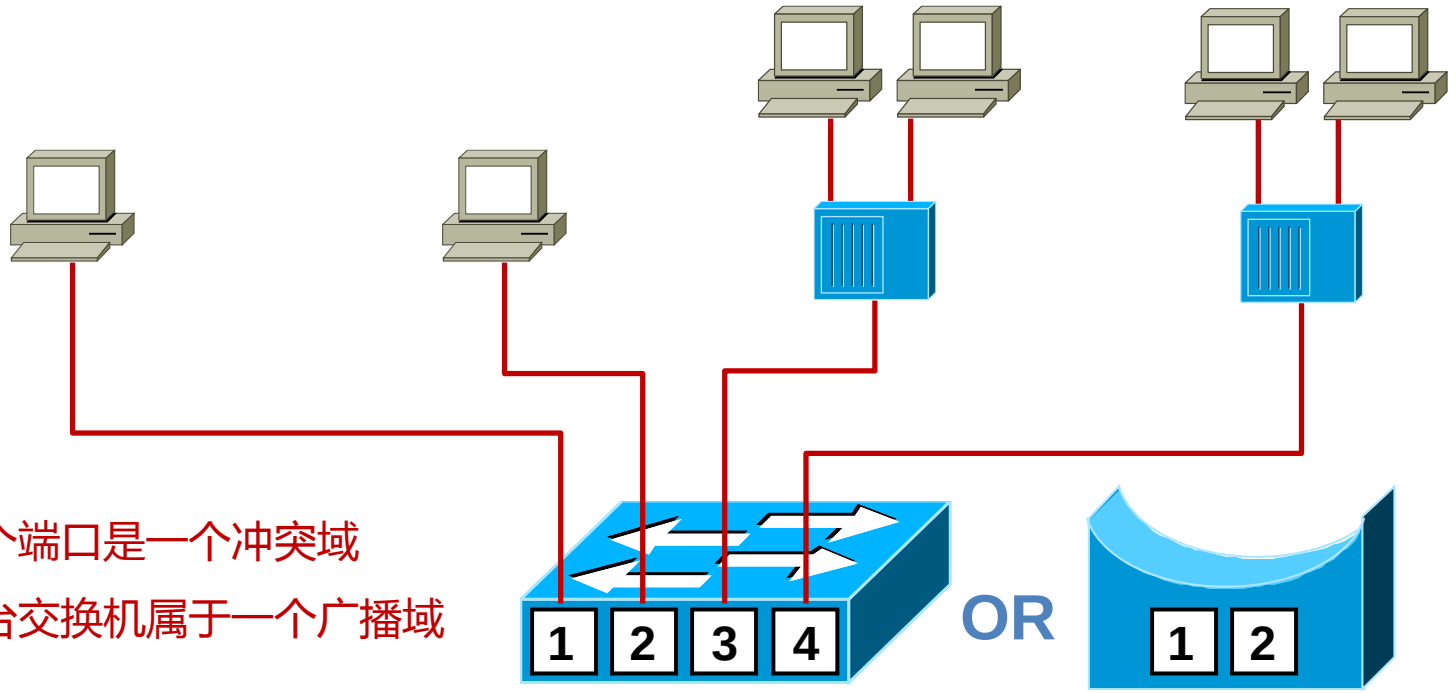
- MAC地址

以太网数据帧格式



第2层：数据链路层

- 工作在OSI 第2层的设备：交换机



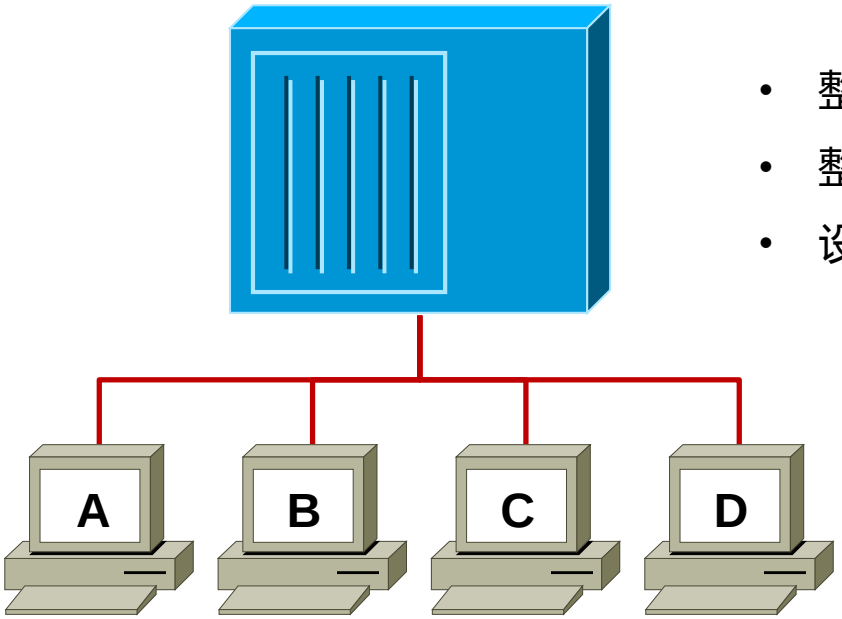
- 每个端口是一个冲突域
- 整台交换机属于一个广播域

第1层：物理层

- 在介质上传递比特流
- 定义接口和媒体的物理特性
- 定义比特的表示、数据传输速率、信号的传输模式（单工、半双工、全双工）
- 定义网络物理拓扑（网状、星型、环型、总线型等）

第1层：物理层

- 设备：Hub集线器



- 整台设备在同一个冲突域 (collision domain)
- 整台设备都在同一个广播域(broadcast domain)
- 设备共享带宽

OSI参考模型

各种应用程序协议

数据的格式化、数据加密解密、数据的压缩解压缩

建立、管理、终止实体之间的会话连接

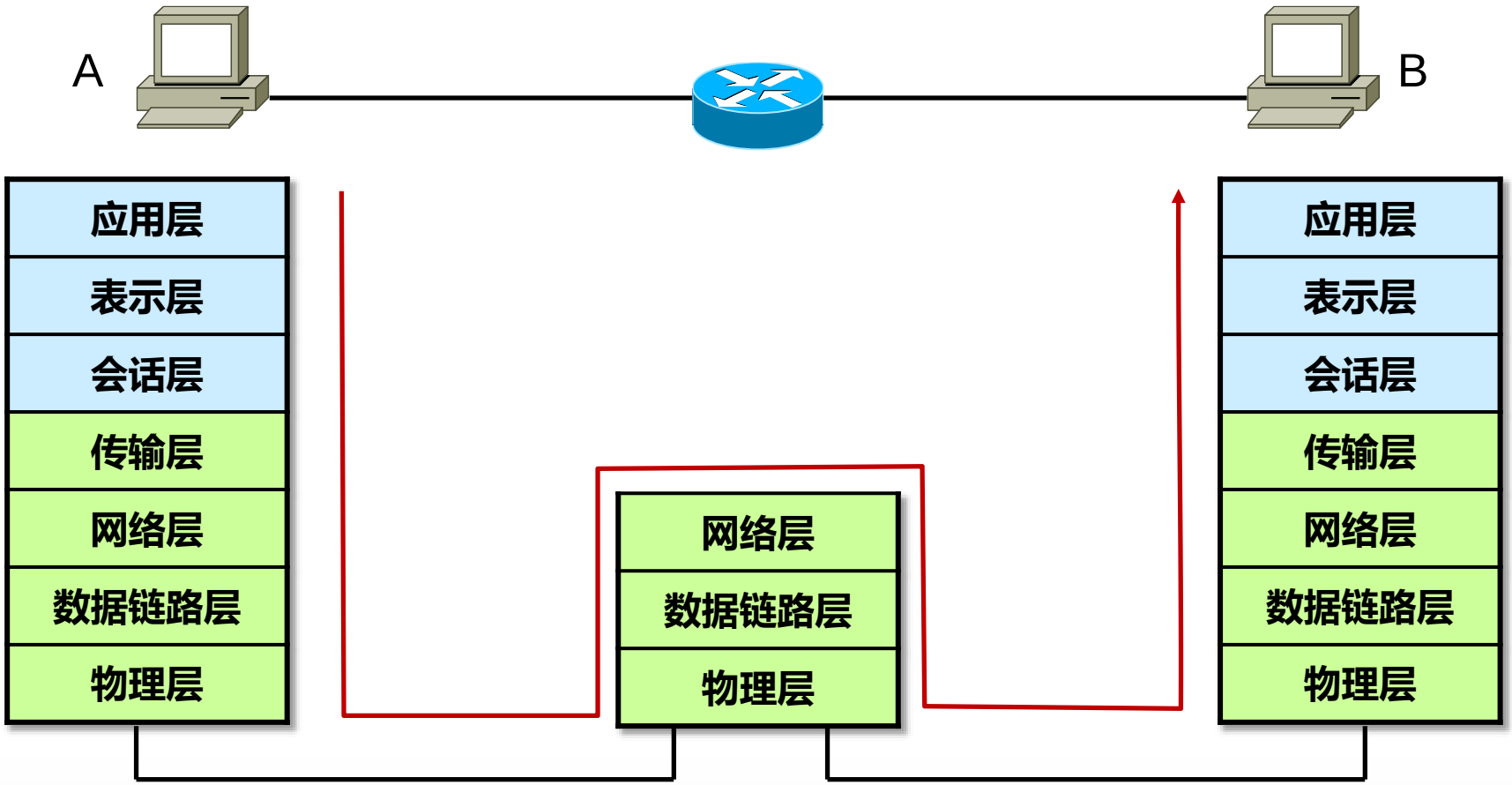
数据的分段及重组；提供端到端的数据服务（可靠或不可靠）

将分组从源端传送到目的端；逻辑寻址；路由选择

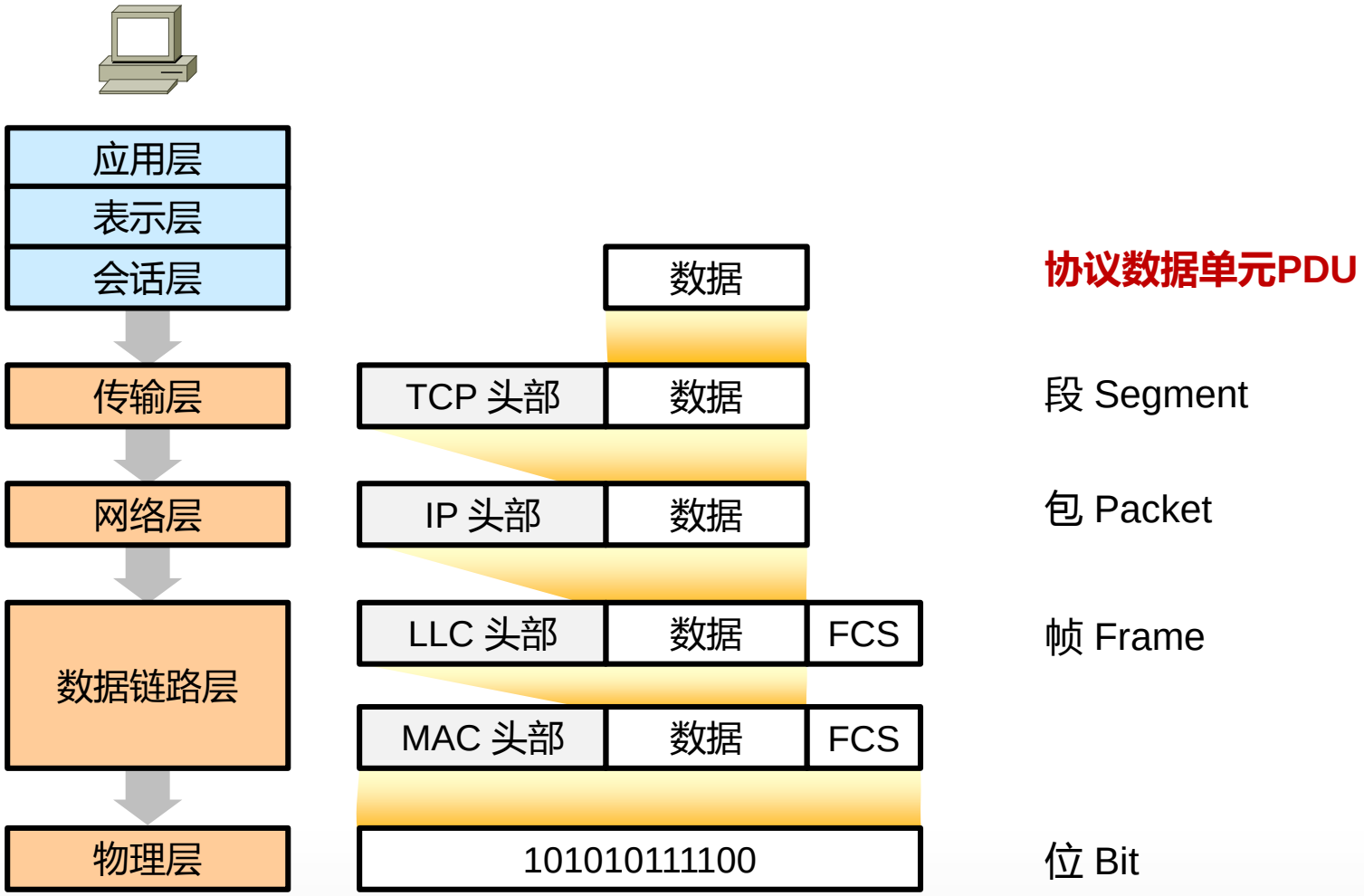
将分组数据封装成帧；实现两个相邻结点之间的通信；差错检测

在介质上传输比特；提供机械的和电气的规约

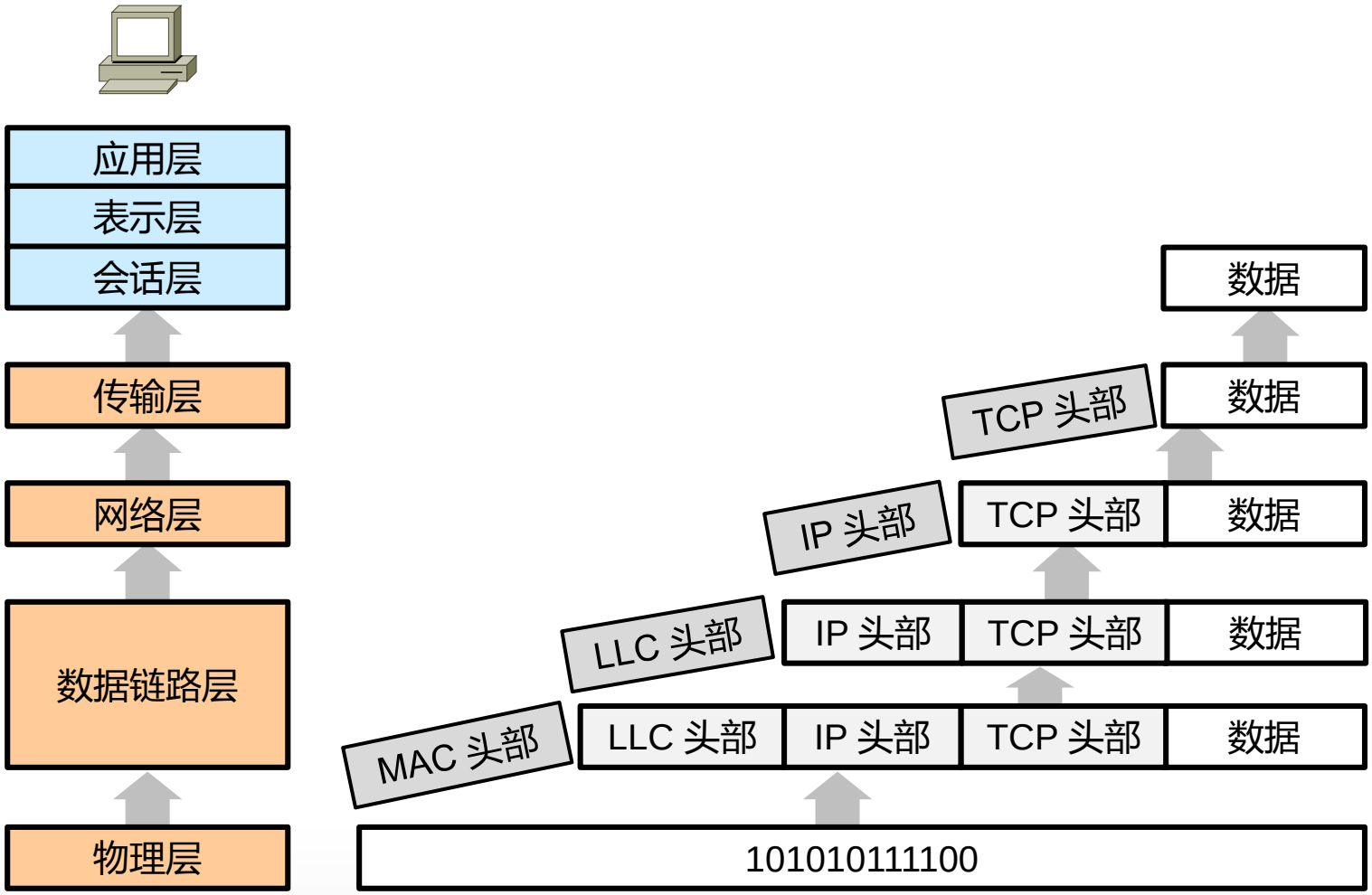
借助OSI模型理解数据传输过程



借助OSI模型理解数据传输过程（封装过程）

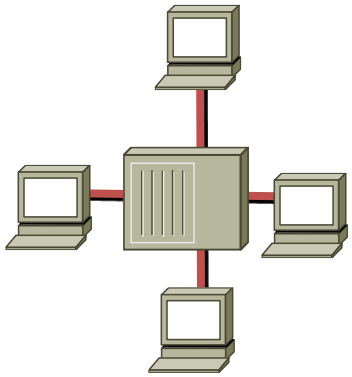


借助OSI模型理解数据传输过程（解封装过程）

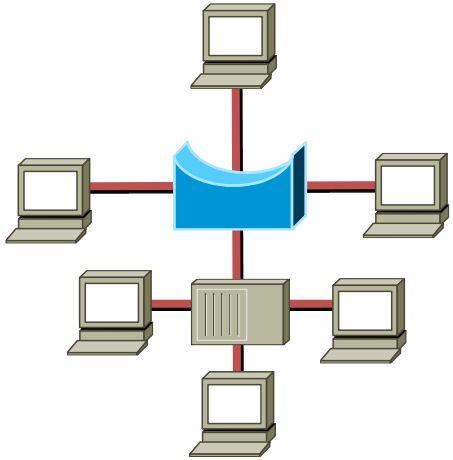


Q&A

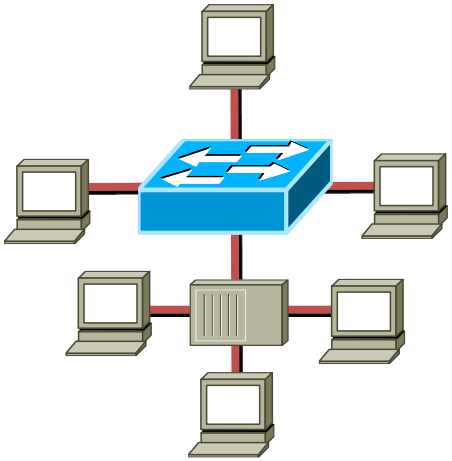
Hub



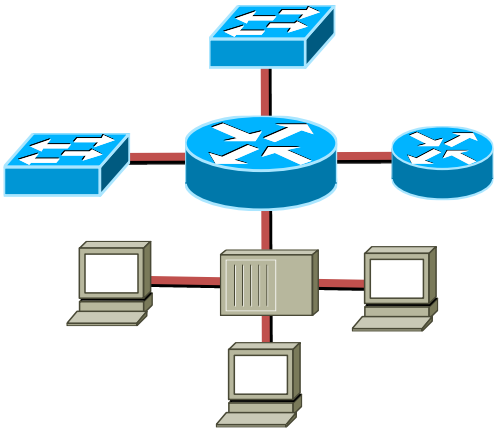
Bridge



Switch



Router



Collision Domains、Broadcast Domains:

红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You

红茶三杯
Vinsoney

学习 沉淀 成长 分享

TCP/IP VLSM

红茶三杯（朱SIR）微博：http://t.sina.com/vinsoney

Latest update: 2012-06-01

Content

TCP/IP

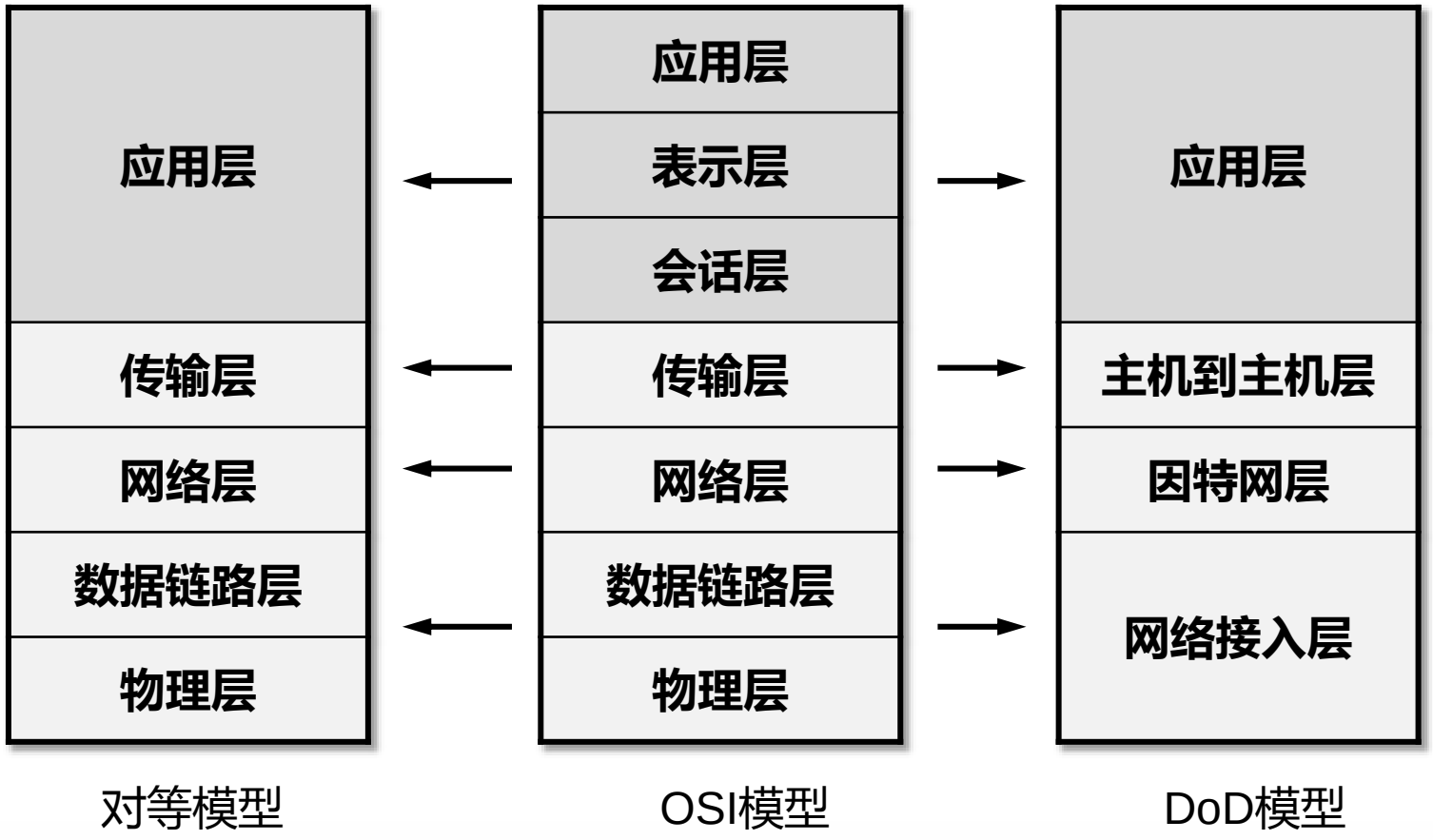
VLSM

红茶三杯
Vinsoney

TCP IP概述

- DoD模型
- TCP、UDP协议概述
- IP、ARP协议概述

TCP/IP参考模型



TCP/IP参考模型

Telnet	FTP	TFTP	SNMP
HTTP	SMTP	NFS	DHCP

TCP	UDP

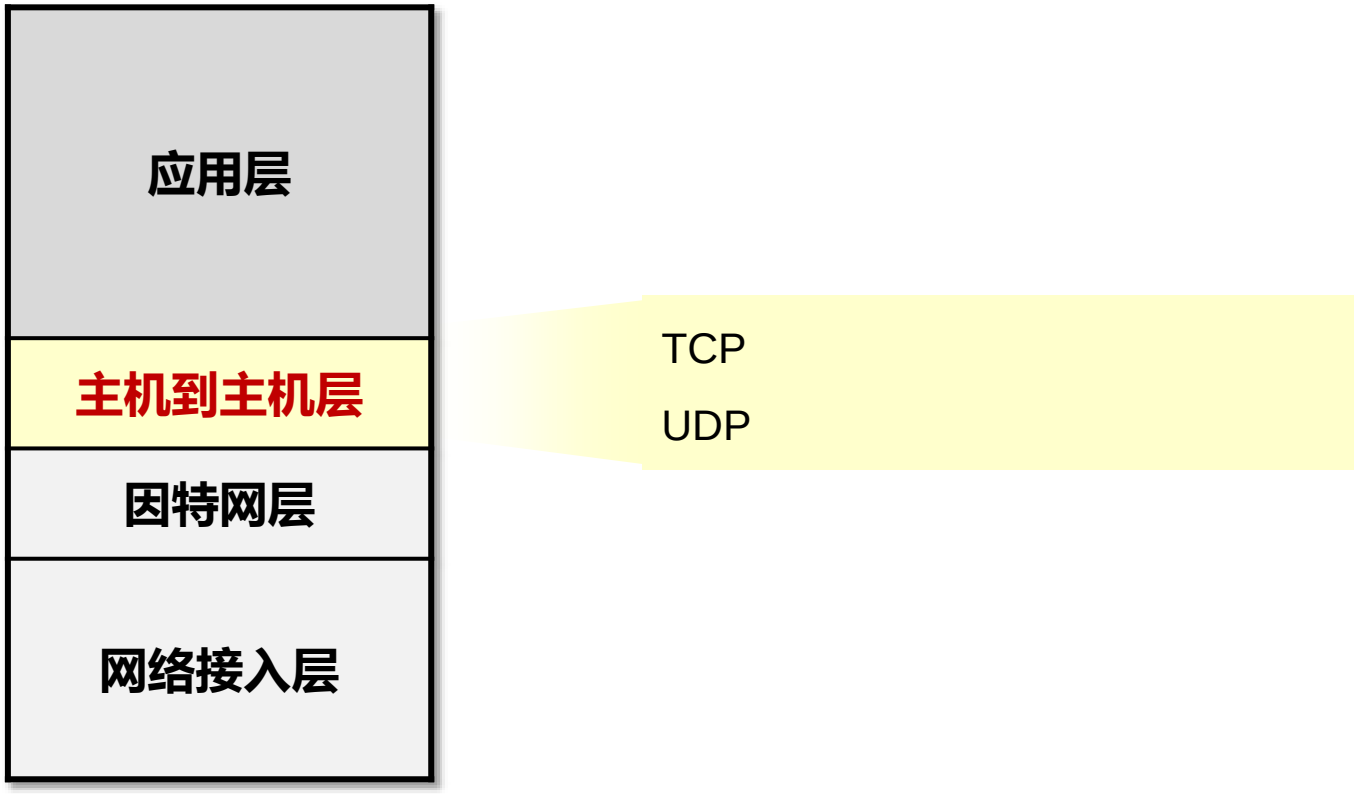
ICMP	IGMP	Routing Prorotocol
IP		

ARP	
Ethernet	Fast Eth

应用层

- HTTP 80
  超文本传输协议，提供浏览网页服务
- Telnet 23
  远程登陆协议，提供远程管理服务
- FTP 20、21
  文件传输协议，提供互联网文件资源共享服务
- SMTP 25
  简单邮件传输协议，提供互联网电子邮件服务
- POP3 110
  邮局协议，提供互联网电子邮件服务
- TFTP 69 (UDP)
  简单文件传输协议，提供简单的文件传输服务

主机到主机层



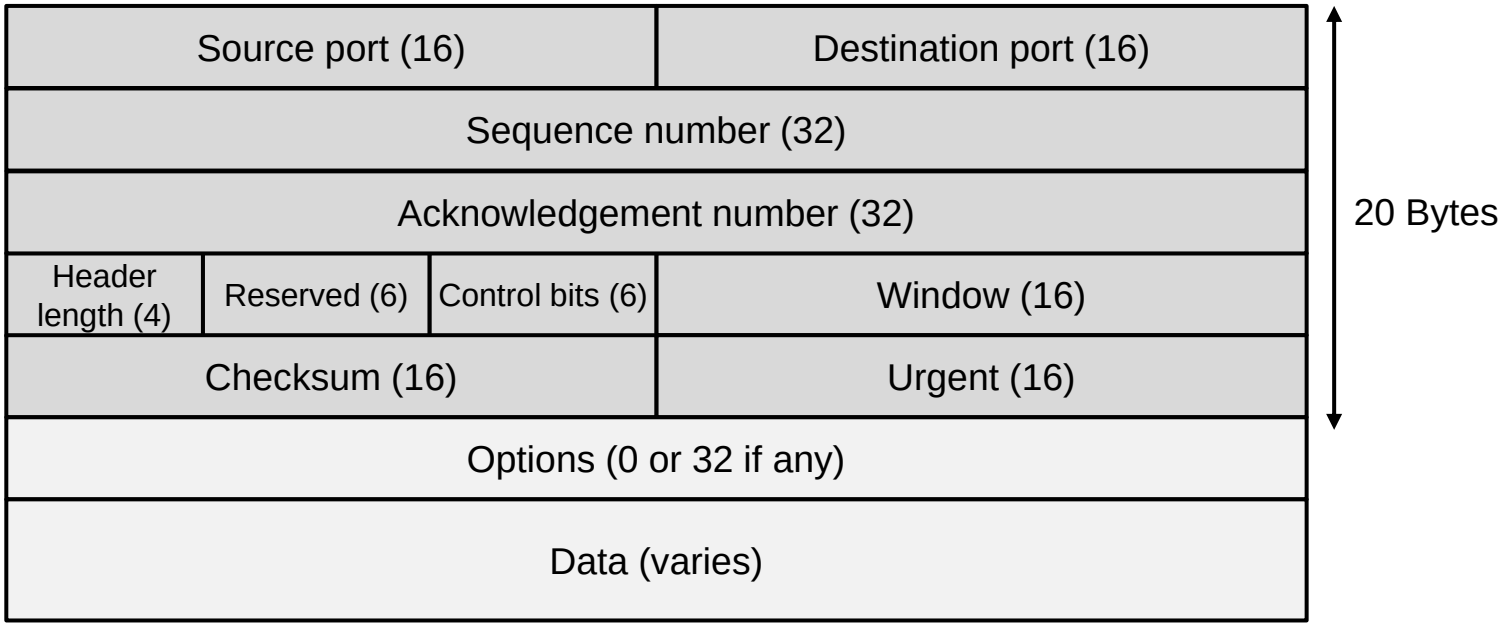
主机到主机层

- TCP与UDP

传输控制协议（TCP）	用户数据报协议（UDP）
面向连接	无连接
可靠传输	尽力而为的传输
支持流控及窗口机制	无流控及窗口机制
HTTP、FTP等	TFTP、DNS、DHCP等

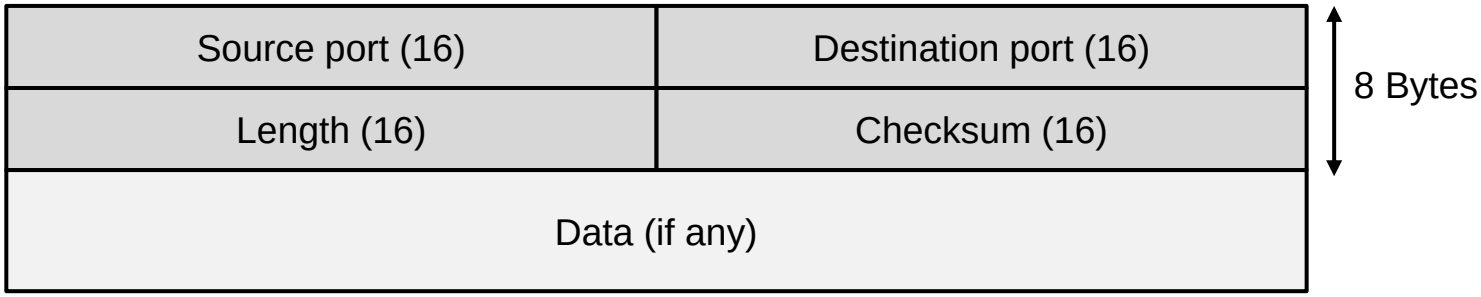
主机到主机层

- TCP Packet



主机到主机层

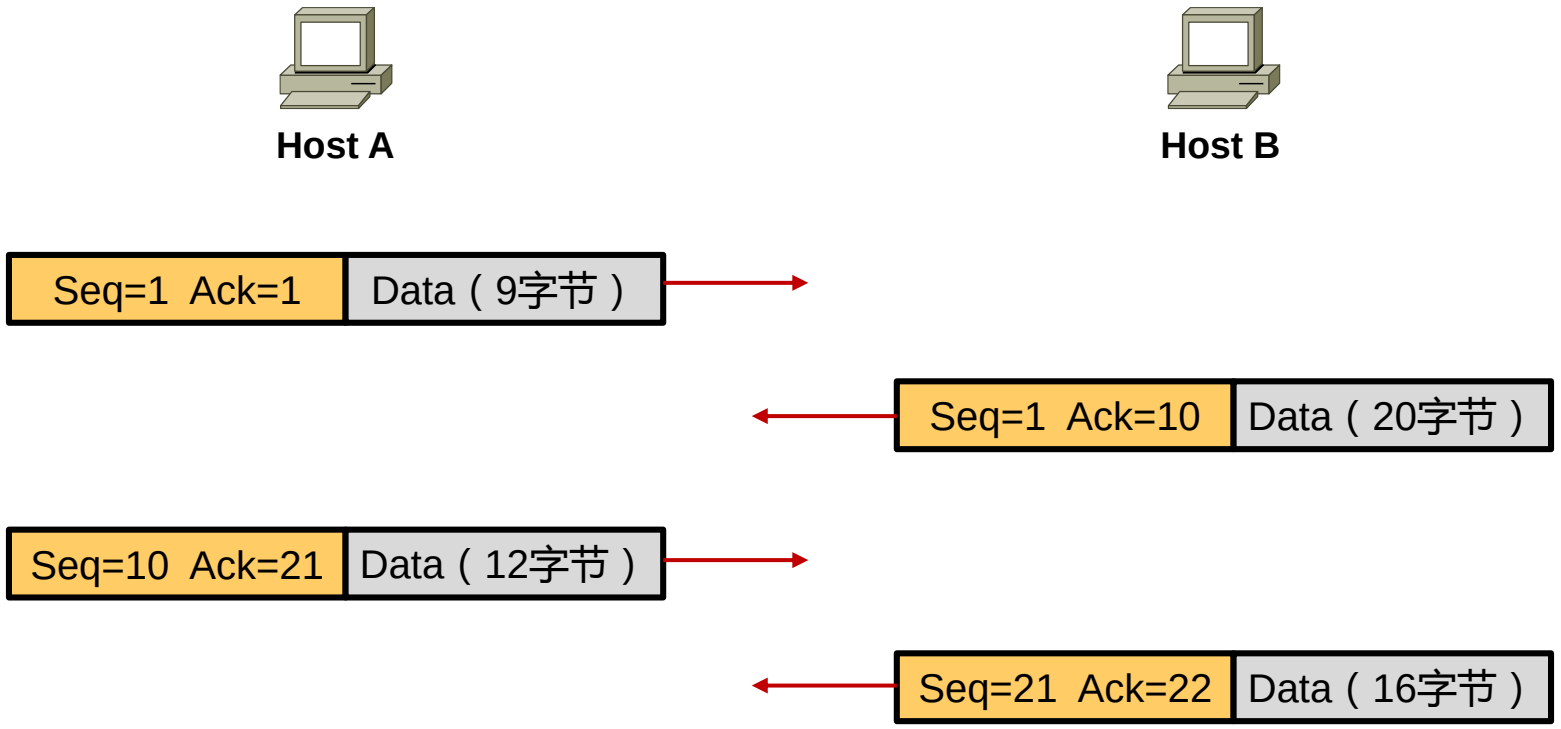
- UDP Packet



No sequence or acknowledgment fields

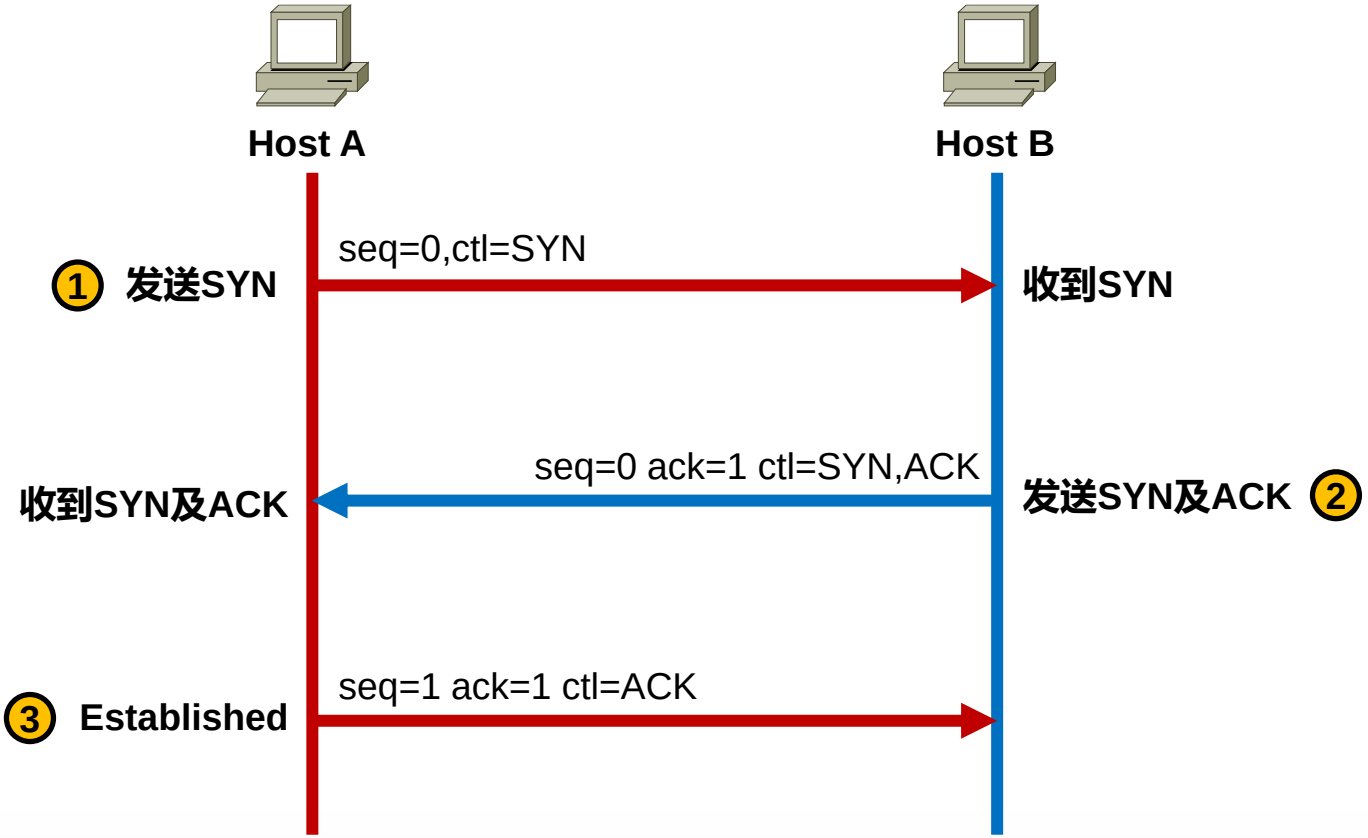
主机到主机层

- TCP序列号及确认号



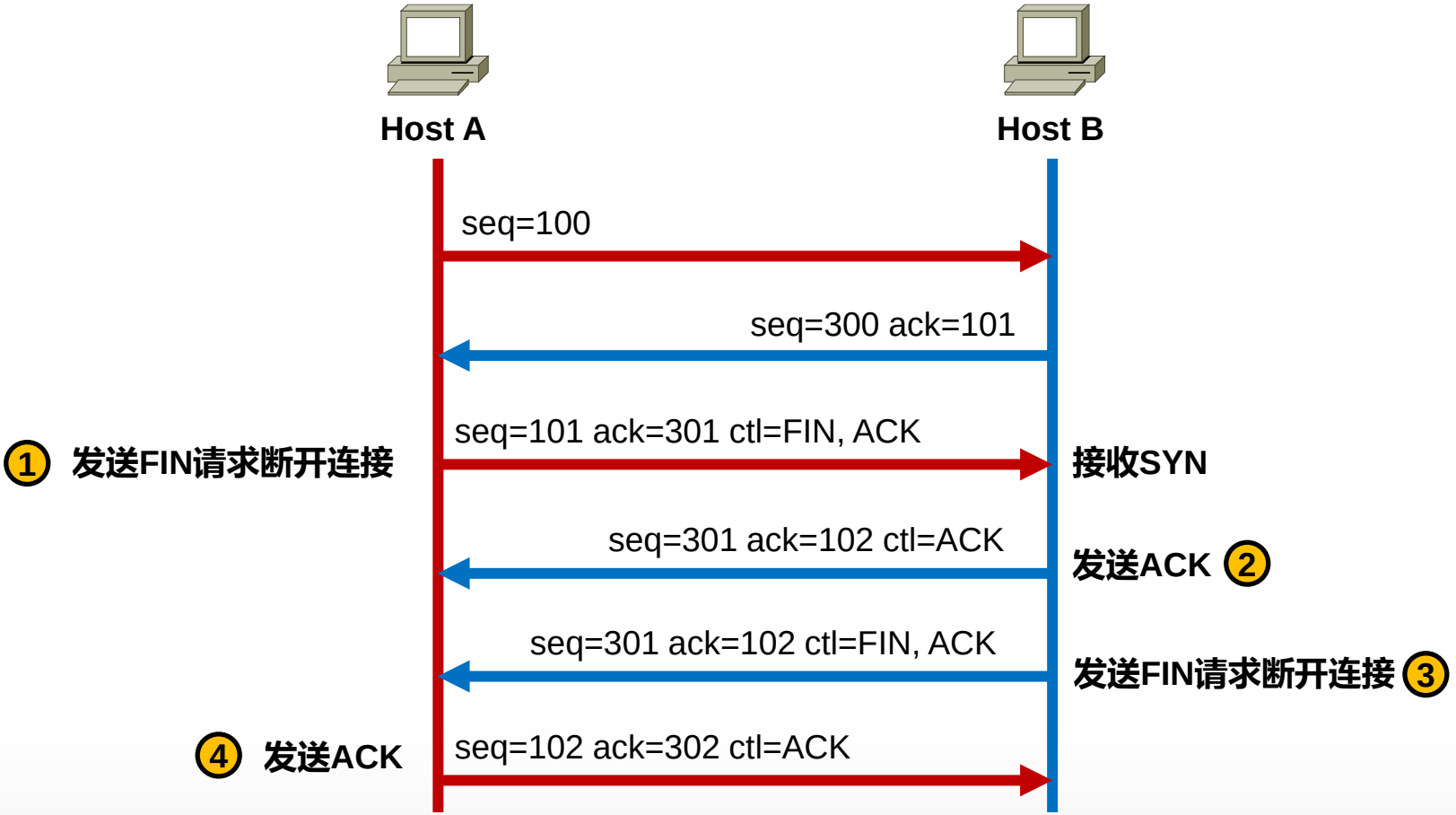
主机到主机层

- TCP三次握手



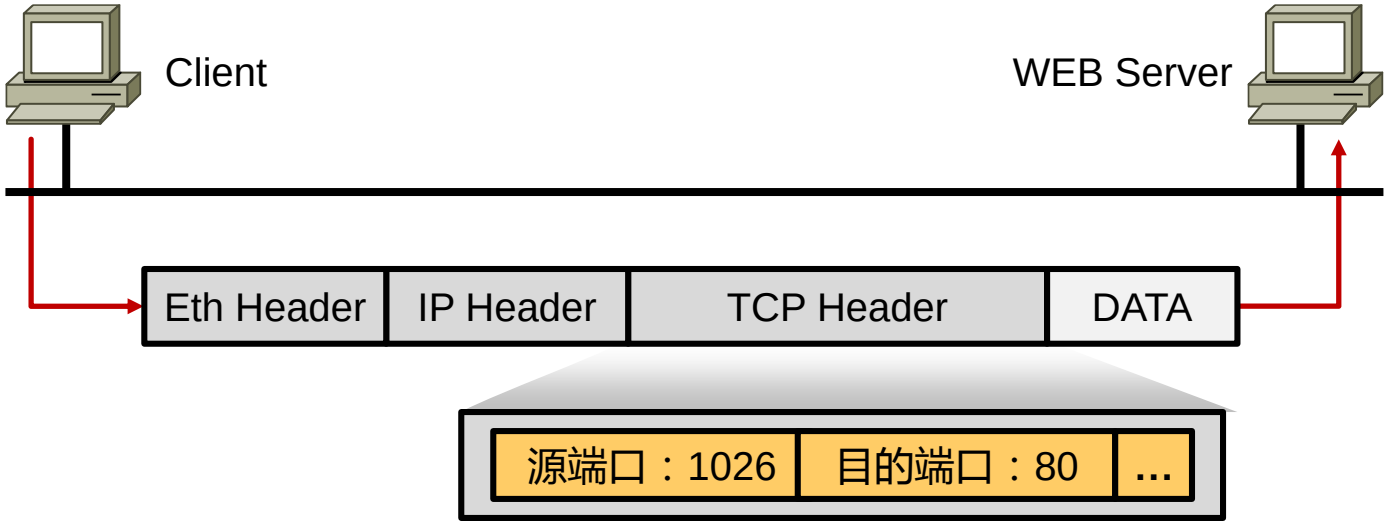
主机到主机层

- TCP四次断开



主机到主机层

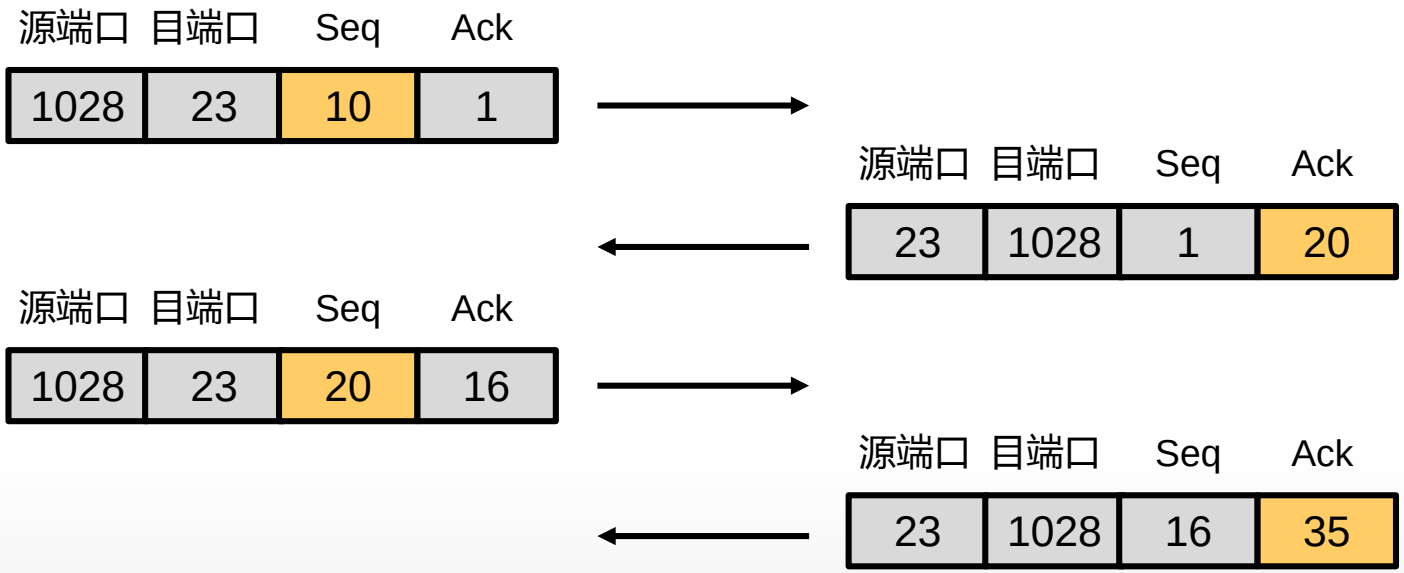
- TCP/UDP端口号



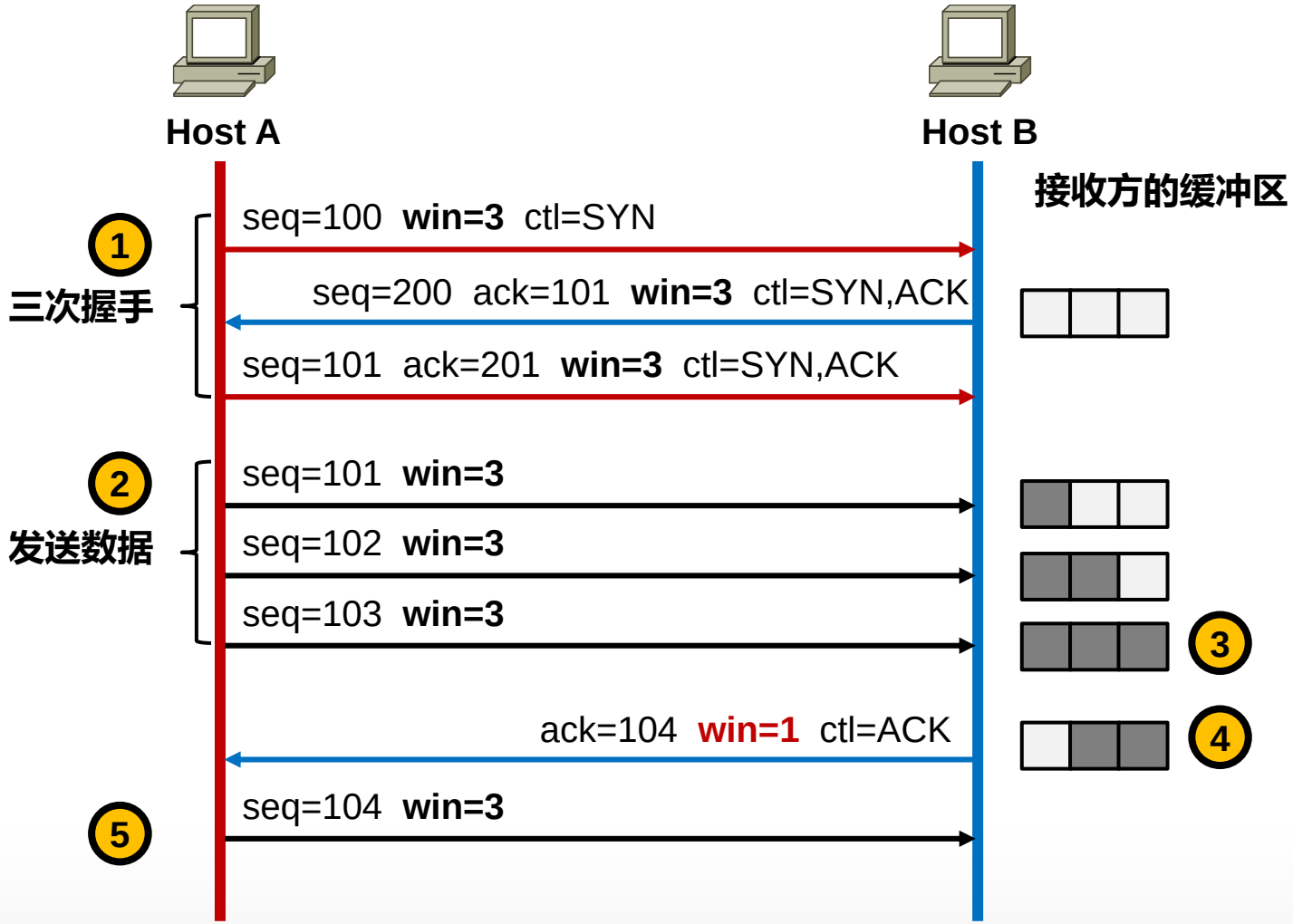
- 源端口随机分配，目标端口使用知名端口（Well-known port）；
- 应用客户端使用的源端口号一般为系统中未使用的且大于1023；
- 目的端口号为服务端开启的服务所侦听的端口，如HTTP缺省使用80。

主机到主机层

- TCP端口号、序列号及确认号



主机到主机层 TCP滑动窗口机制



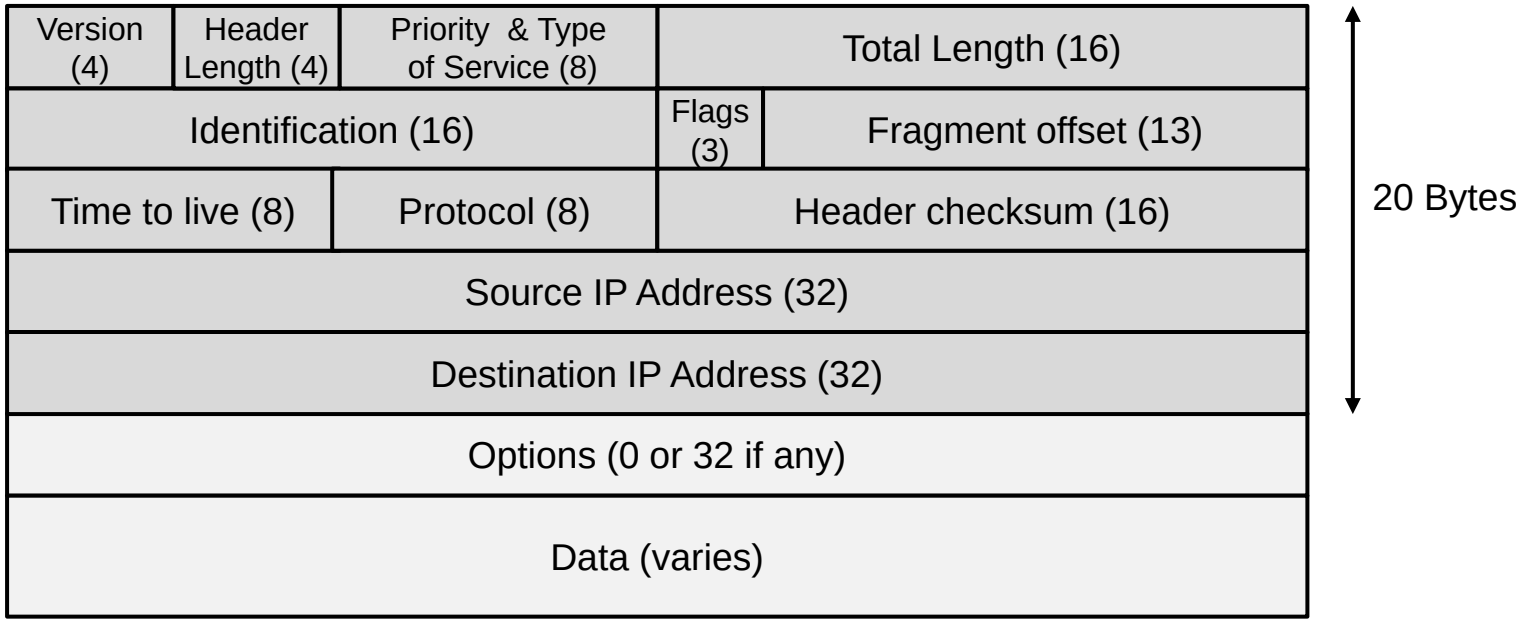
窗口大小 决定了在收到确认前可以发送的字节数

因特网层

- 负责将IP报文从源端发送到目的端
- 定义逻辑地址（IP地址）
- 负责数据包的寻径和转发

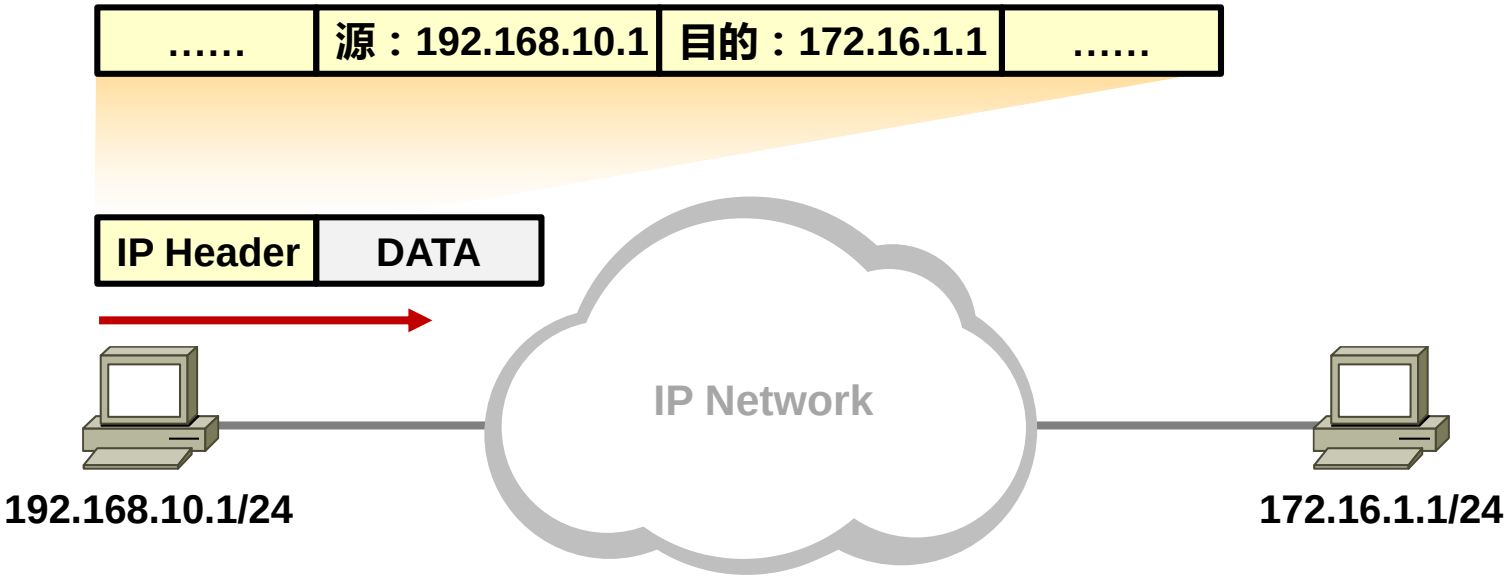
因特网层

- IP Packet



因特网层

- 第3层逻辑地址：IP Address



因特网层

- Address Resolution Protocol
  - 将 IPv4 地址解析为 MAC 地址
  - 维护IP与MAC映射关系的缓存

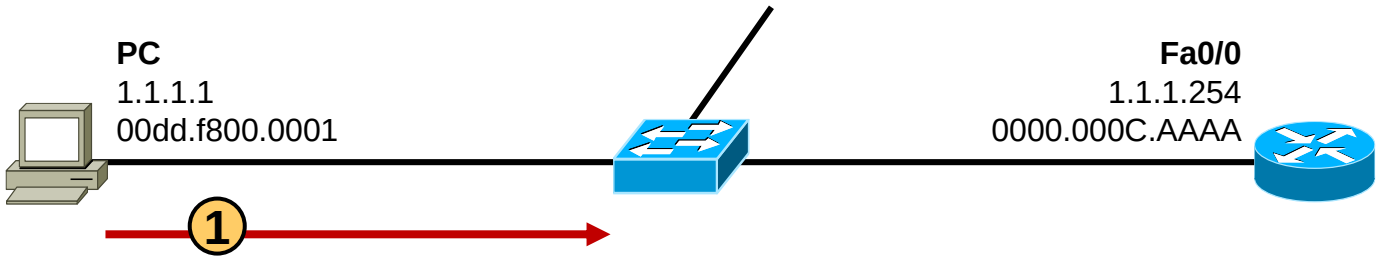
ARP的工作机制 1

PC：arp -a

```
Interface: 1.1.1.1 --- 0x4
Internet Address      Physical Address      Type
```

Router#show arp

```
Protocol  Address     Hardware Addr     Interface
Internet  1.1.1.254   0000.000C.AAAA    FastEthernet0/0
```



Ethernet II Header src 00dd.f800.0001 dst FFFF-FFFF-FFFF	
Arp Request	
SenderMac	00dd.f800.0001
SenderIP	1.1.1.1
TargetMac	00-00-00-00-00-00
TargetIP	1.1.1.254

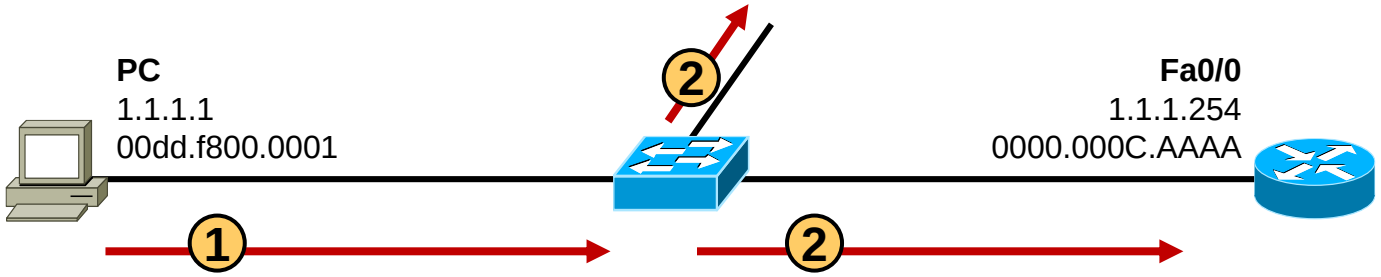
ARP的工作机制 2

PC：arp -a

```
Interface: 1.1.1.1 --- 0x4
Internet Address      Physical Address      Type
```

Router#show arp

```
Protocol  Address     Hardware Addr     Interface
Internet  1.1.1.254   0000.000C.AAAA    FastEthernet0/0
```



Ethernet II Header src 00dd.f800.0001 dst FFFF-FFFF-FFFF	
Arp Request	
SenderMac	00dd.f800.0001
SenderIP	1.1.1.1
TargetMac	00-00-00-00-00-00
TargetIP	1.1.1.254

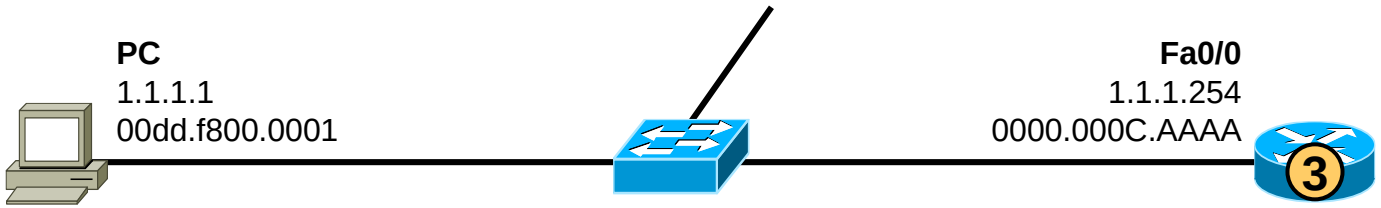
ARP的工作机制 3

PC：arp -a

```
Interface: 1.1.1.1 --- 0x4
Internet Address      Physical Address      Type
```

Router#show arp

Protocol	Address	Hardware Addr	Interface
Internet	1.1.1.254	0000.000C.AAAA	FastEthernet0/0
Internet	1.1.1.1	00dd.f800.0001	FastEthernet0/0



Ethernet II Header src 00dd.f800.0001 dst FFFF-FFFF-FFFF	
Arp Request	
SenderMac	00dd.f800.0001
SenderIP	1.1.1.1
TargetMac	00-00-00-00-00-00
TargetIP	1.1.1.254

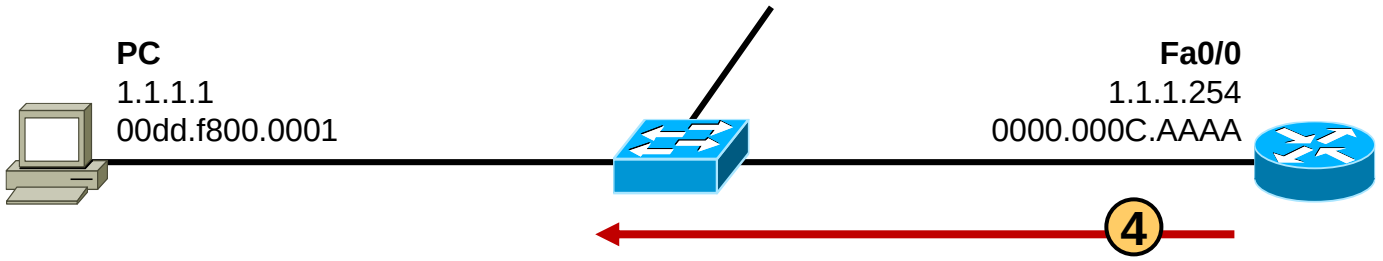
ARP的工作机制 4

PC：arp -a

```
Interface: 1.1.1.1 --- 0x4
Internet Address      Physical Address      Type
```

Router#show arp

Protocol	Address	Hardware Addr	Interface
Internet	1.1.1.254	0000.000C.AAAA	FastEthernet0/0
Internet	1.1.1.1	00dd.f800.0001	FastEthernet0/0



Ethernet II Header src 0000.000C.AAAA dst 00dd.f800.0001	
Arp Reply	
SenderMac	0000.000C.AAAA
SenderIP	1.1.1.254
TargetMac	00dd.f800.0001
TargetIP	1.1.1.1

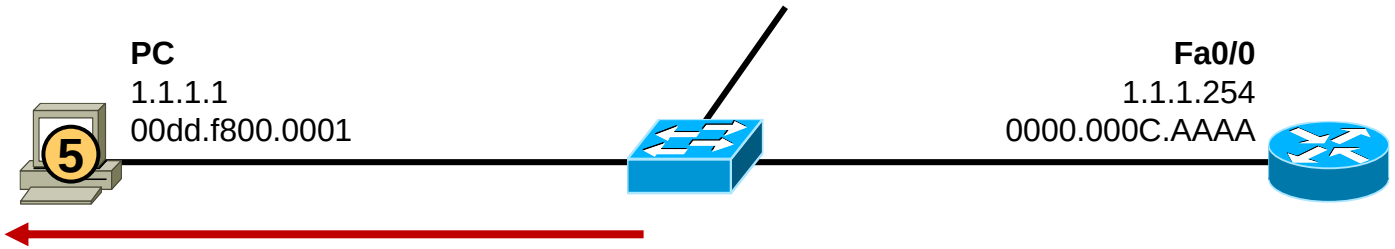
ARP的工作机制 5

PC：arp -a

```
Interface: 1.1.1.1 --- 0x4
Internet Address      Physical Address      Type
1.1.1.254             0000.000C.AAAA        dynamic
```

Router#show arp

```
Protocol  Address      Hardware Addr     Interface
Internet  1.1.1.254    0000.000C.AAAA    FastEthernet0/0
Internet  1.1.1.1      00dd.f800.0001    FastEthernet0/0
```

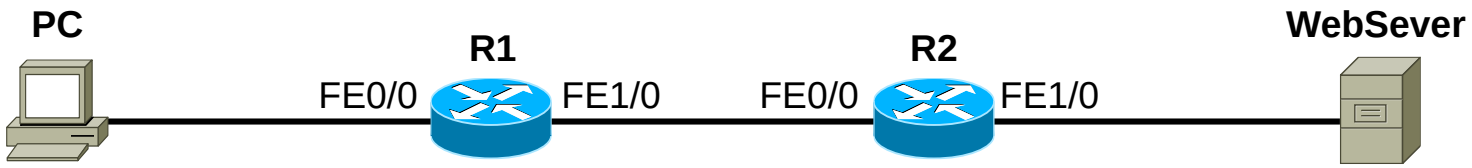


Ethernet II Header src 0000.000C.AAAA dst 00dd.f800.0001	
Arp Reply	
SenderMac	0000.000C.AAAA
SenderIP	1.1.1.254
TargetMac	00dd.f800.0001
TargetIP	1.1.1.1

因特网层常用工具

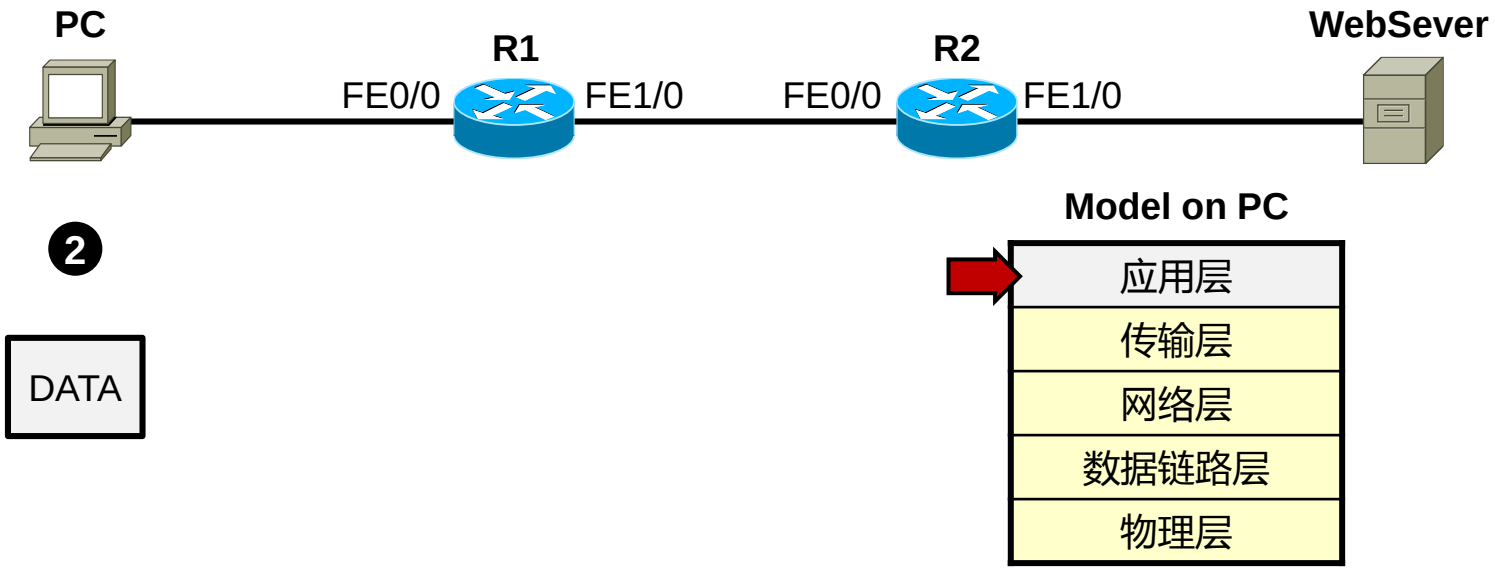
- **Ping（ICMP)**
- **Traceroute/Tracert**

利用TCP/IP参考模型分析数据传输过程



设备	接口	IP	MAC
PC	网卡	192.168.1.1/24	00DD.F800.0001
R1	F0/0	192.168.1.254/24	0000.AAAA.0001
R1	F1/0	192.168.12.1/24	0000.AAAA.0002
R2	F0/0	192.168.12.2/24	0000.BBBB.0001
R2	F1/0	192.168.2.254/24	0000.BBBB.0002
Server	网卡	192.168.2.1/24	00DD.F800.000F

利用TCP/IP参考模型分析数据传输过程



利用TCP/IP参考模型分析数据传输过程

❷

TCP 头部	DATA

传输层头部

源端口号：1026 目的端口号：80	**DATA** HTTP荷载

Model on PC

应用层
传输层
网络层
数据链路层
物理层

利用TCP/IP参考模型分析数据传输过程

❸

IP 头部	TCP 头部	DATA

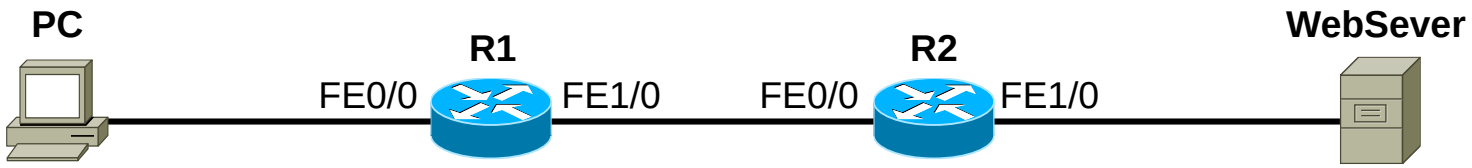
IP头部

源IP：192.168.1.1 目IP：192.168.2.1 协议号：6	源端口号：1026 目的端口号：80	**DATA** HTTP荷载

Model on PC

应用层
传输层
网络层
数据链路层
物理层

利用TCP/IP参考模型分析数据传输过程



❹

以太网头部	IP头部	TCP头部	DATA

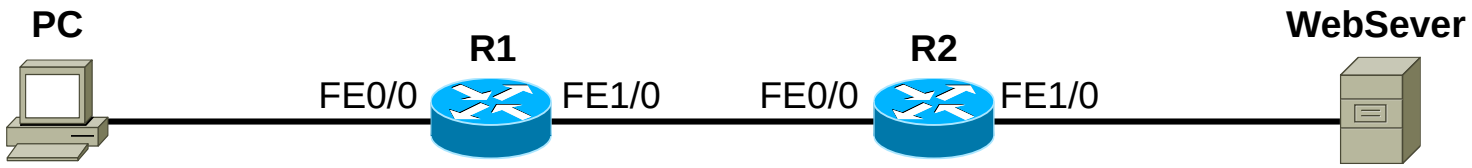
Model on PC

应用层
传输层
网络层
数据链路层
物理层

以太网头部

源MAC：00DD.F800.0001 目MAC：0000.AAAA.0001 类型：0x0800	源IP：192.168.1.1 目IP：192.168.2.1 协议号：6	源端口号：1026 目的端口号：80	**DATA** HTTP荷载

利用TCP/IP参考模型分析数据传输过程

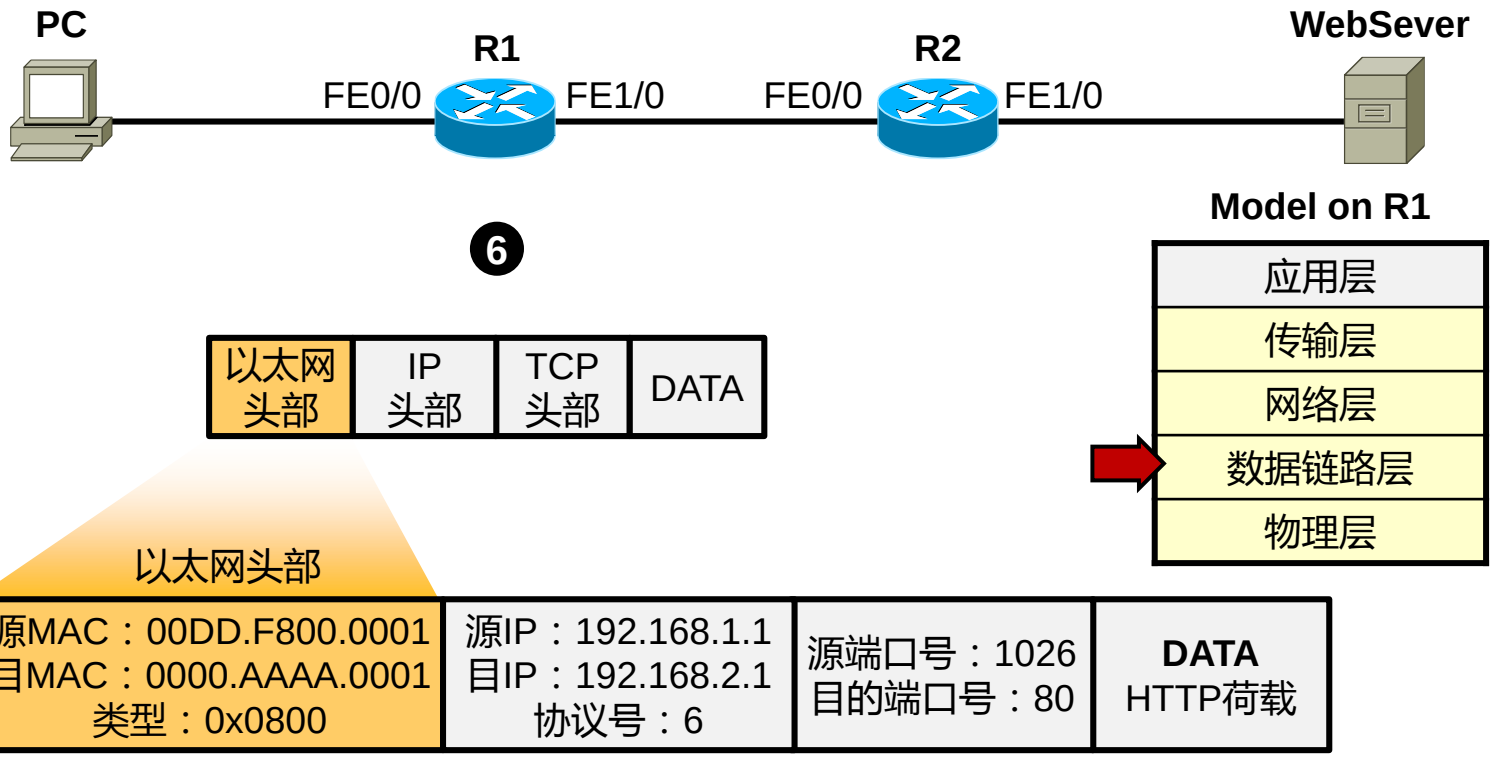


以太网头部	IP头部	TCP头部	DATA

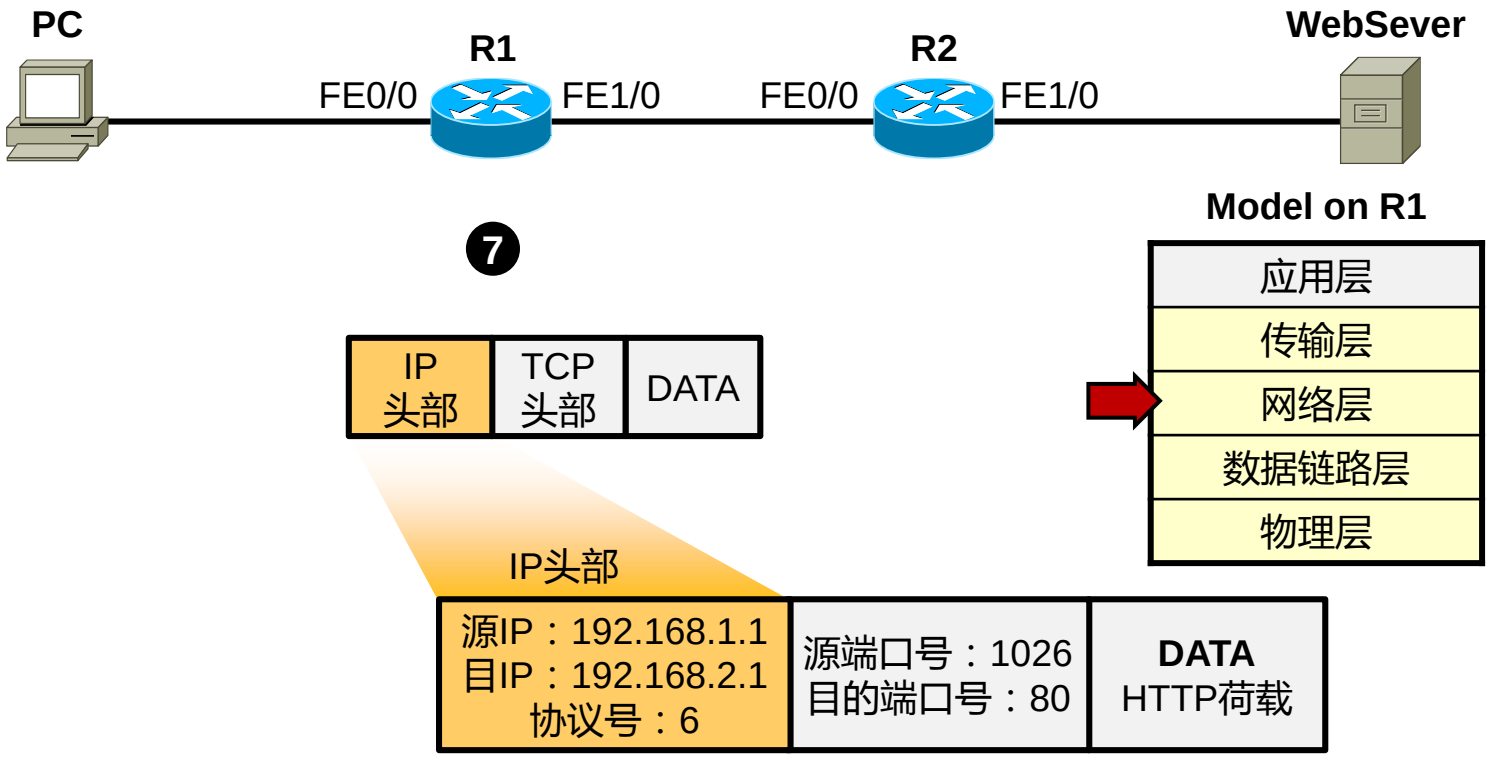
Model on PC

应用层
传输层
网络层
数据链路层
物理层

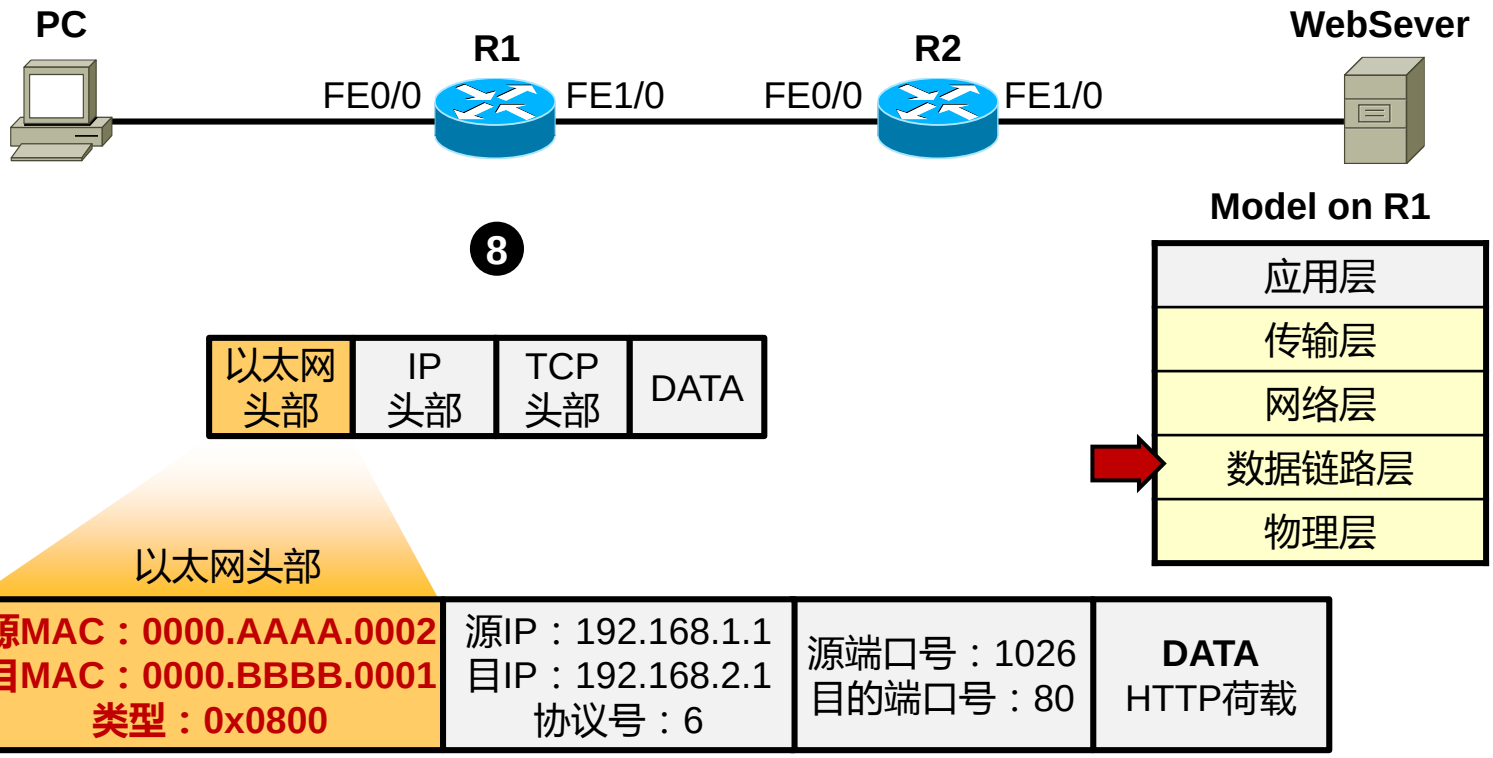
利用TCP/IP参考模型分析数据传输过程



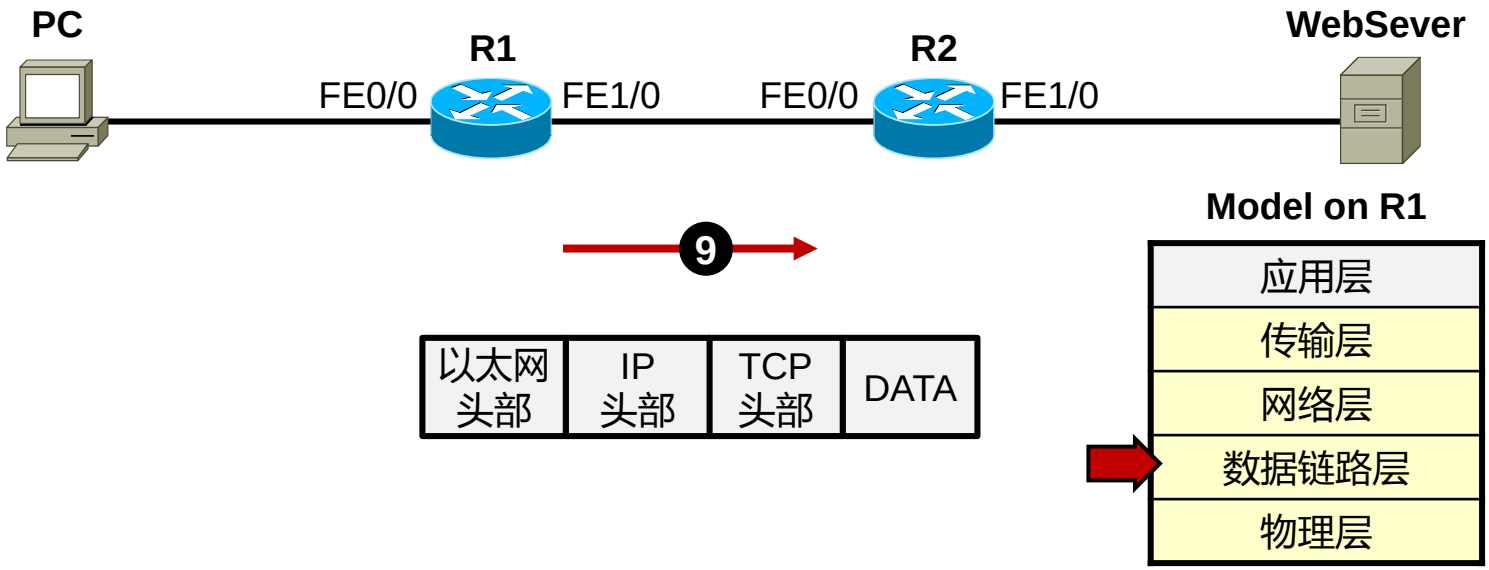
利用TCP/IP参考模型分析数据传输过程



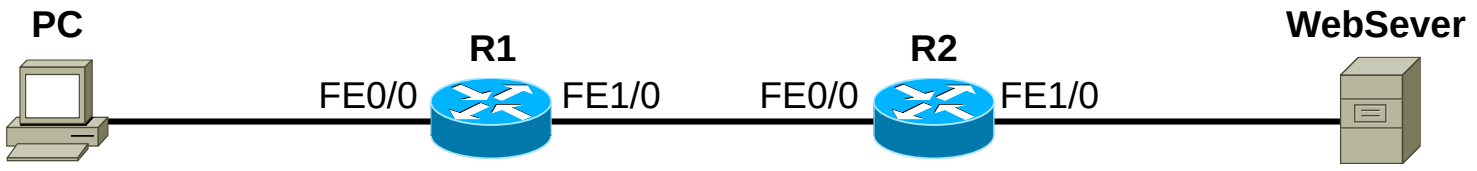
利用TCP/IP参考模型分析数据传输过程



利用TCP/IP参考模型分析数据传输过程



利用TCP/IP参考模型分析数据传输过程



Model on R2

应用层
传输层
网络层
数据链路层
物理层

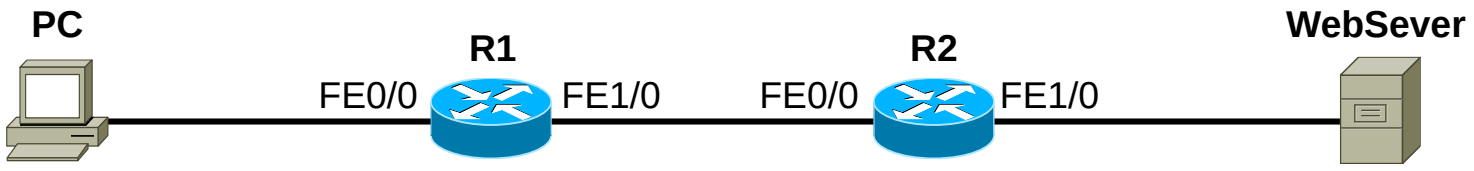
10

以太网头部	IP头部	TCP头部	DATA

以太网头部

源MAC：0000.AAAA.0002 **目MAC：0000.BBBB.0001** **类型：0x0800**	源IP：192.168.1.1 目IP：192.168.2.1 协议号：6	源端口号：1026 目的端口号：80	**DATA** HTTP荷载

利用TCP/IP参考模型分析数据传输过程



Model on R1

应用层
传输层
网络层
数据链路层
物理层

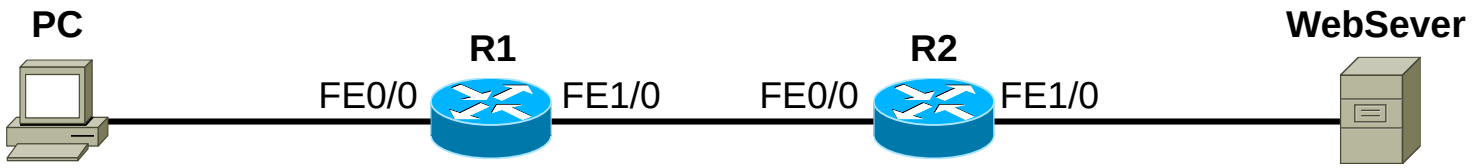
11

IP 头部	TCP 头部	DATA

IP头部

源IP：192.168.1.1 目IP：192.168.2.1 协议号：6	源端口号：1026 目的端口号：80	**DATA** HTTP荷载

利用TCP/IP参考模型分析数据传输过程



Model on R1

应用层
传输层
网络层
数据链路层
物理层

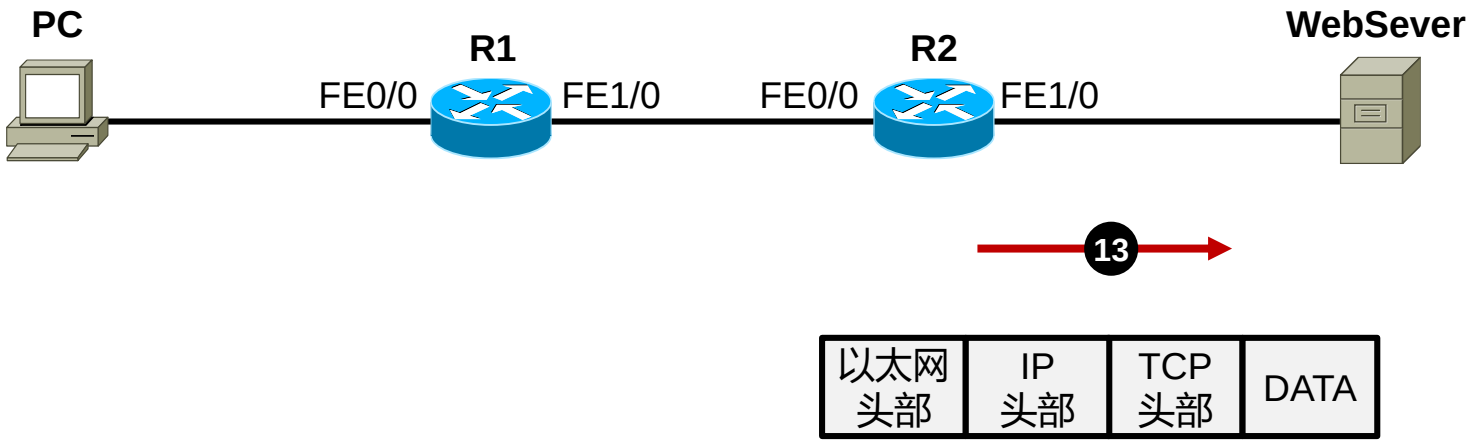
12

以太网头部	IP头部	TCP头部	DATA

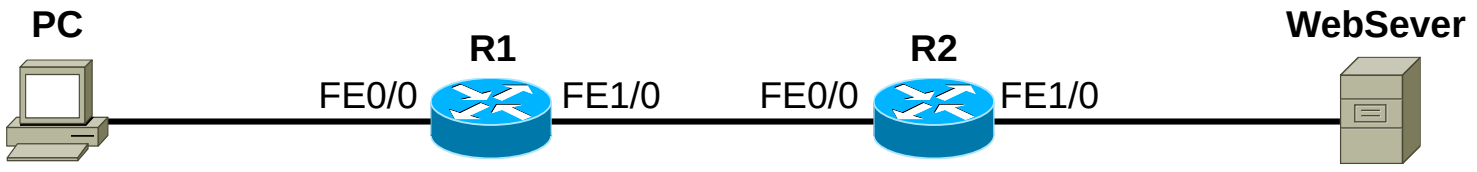
以太网头部

源MAC：0000.BBBB.0002 目MAC：00DD.F800.000F 类型：0x0800	源IP：192.168.1.1 目IP：192.168.2.1 协议号：6	源端口号：1026 目的端口号：80	**DATA** HTTP荷载

利用TCP/IP参考模型分析数据传输过程



利用TCP/IP参考模型分析数据传输过程



Model on R1

应用层
传输层
网络层
数据链路层
物理层

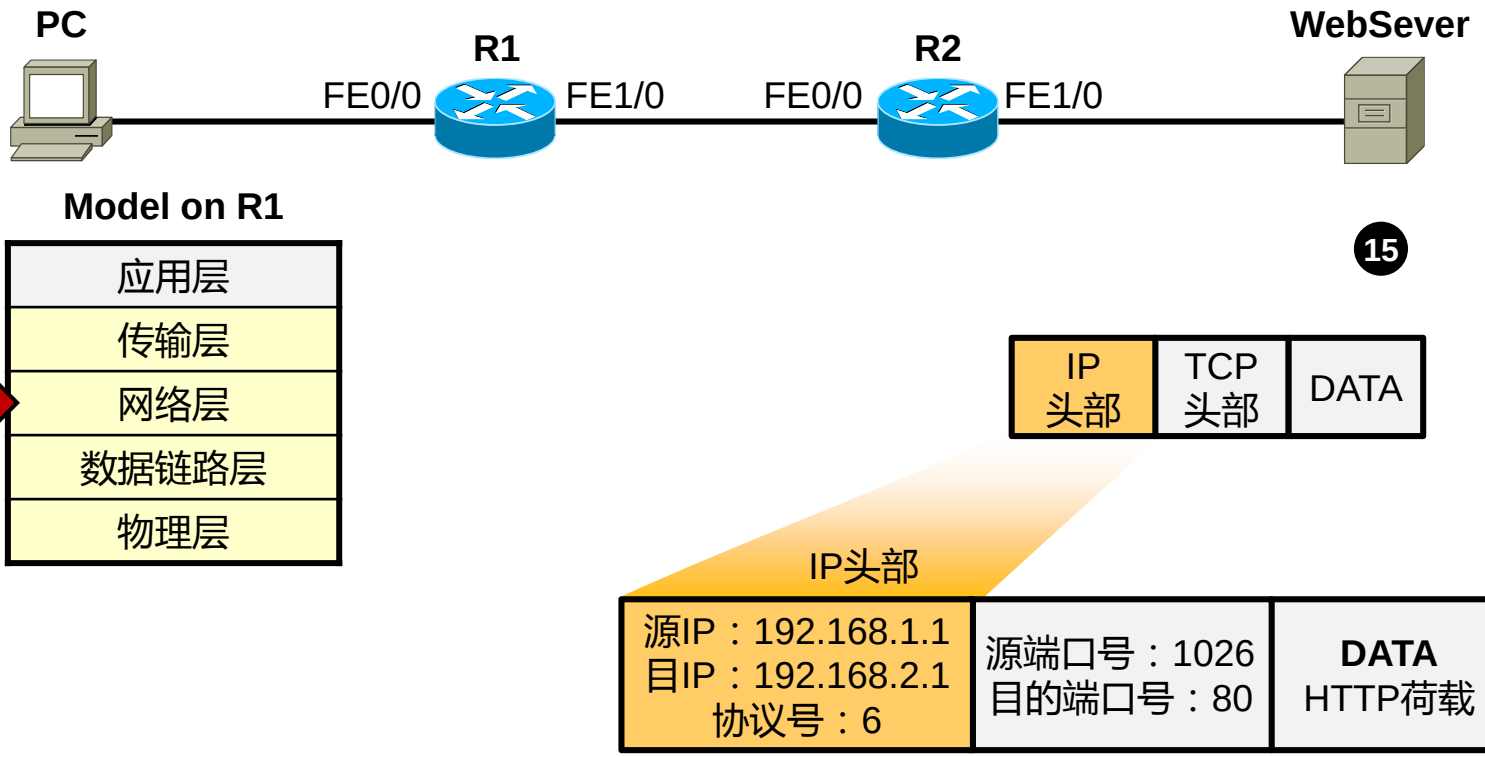
14

以太网头部	IP头部	TCP头部	DATA

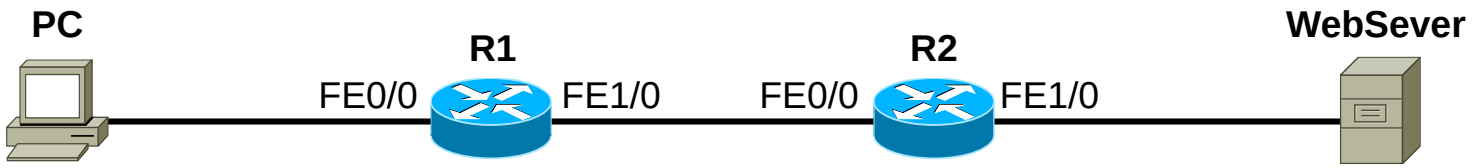
以太网头部

源MAC：0000.BBBB.0002 目MAC：00DD.F800.000F 类型：0x0800	源IP：192.168.1.1 目IP：192.168.2.1 协议号：6	源端口号：1026 目的端口号：80	**DATA** HTTP荷载

利用TCP/IP参考模型分析数据传输过程



利用TCP/IP参考模型分析数据传输过程



Model on R1

应用层
传输层
网络层
数据链路层
物理层

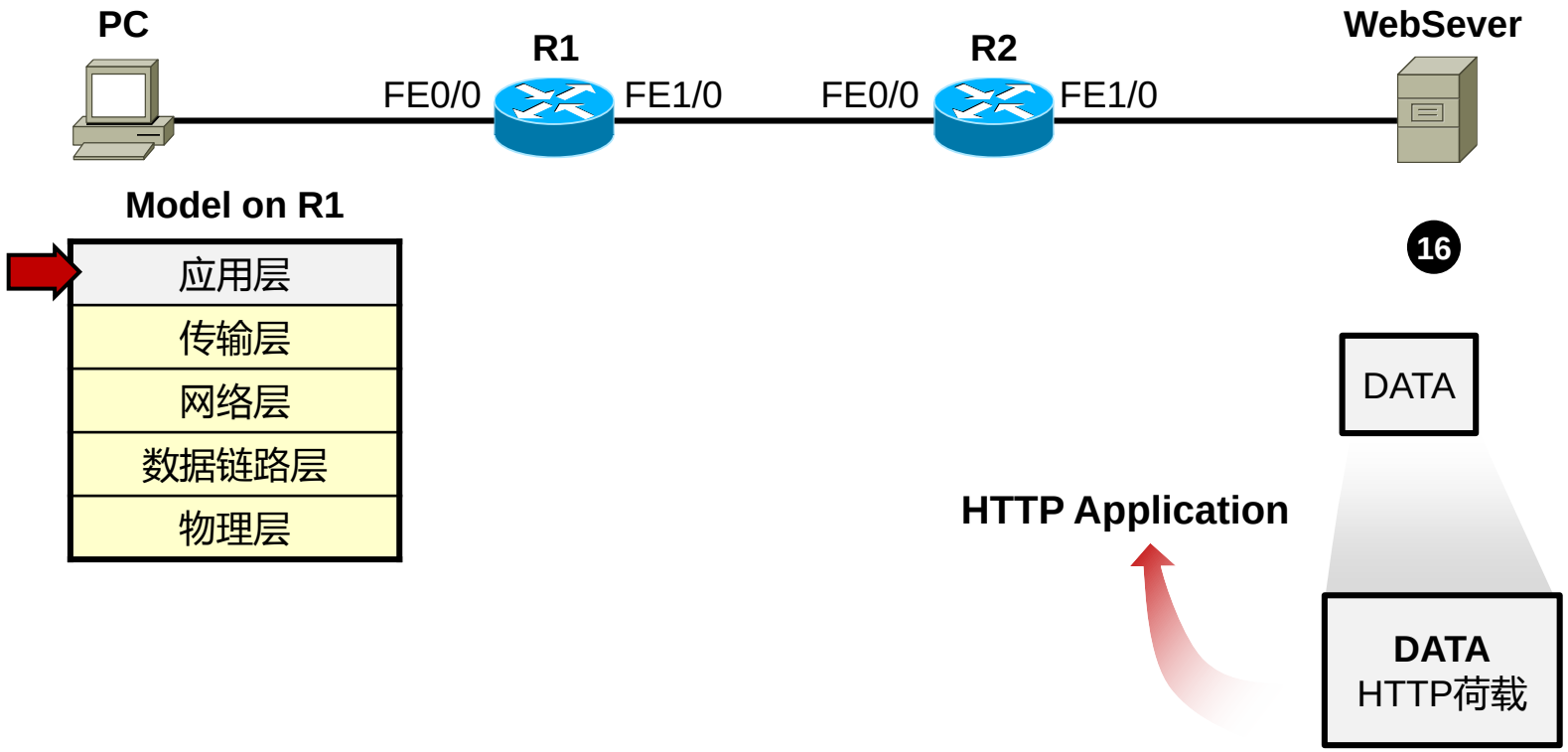
16

TCP 头部	DATA

TCP头部

源端口号：1026 目的端口号：80	**DATA** HTTP荷载

利用TCP/IP参考模型分析数据传输过程



红茶三杯
Vinsoney

VLSM

- IP地址的概念
- IP地址的类别
- 网络掩码的作用
- IP地址的类型（主机、广播、网络号）
- VLSM可变长子网掩码

什么是IP地址

- 在IP网络中，通信节点需要有一个唯一的IP地址；
- IP地址用于IP报文的寻址以及标识一个节点；
- IPv4地址一共32bits，使用点分十进制的形式表示；

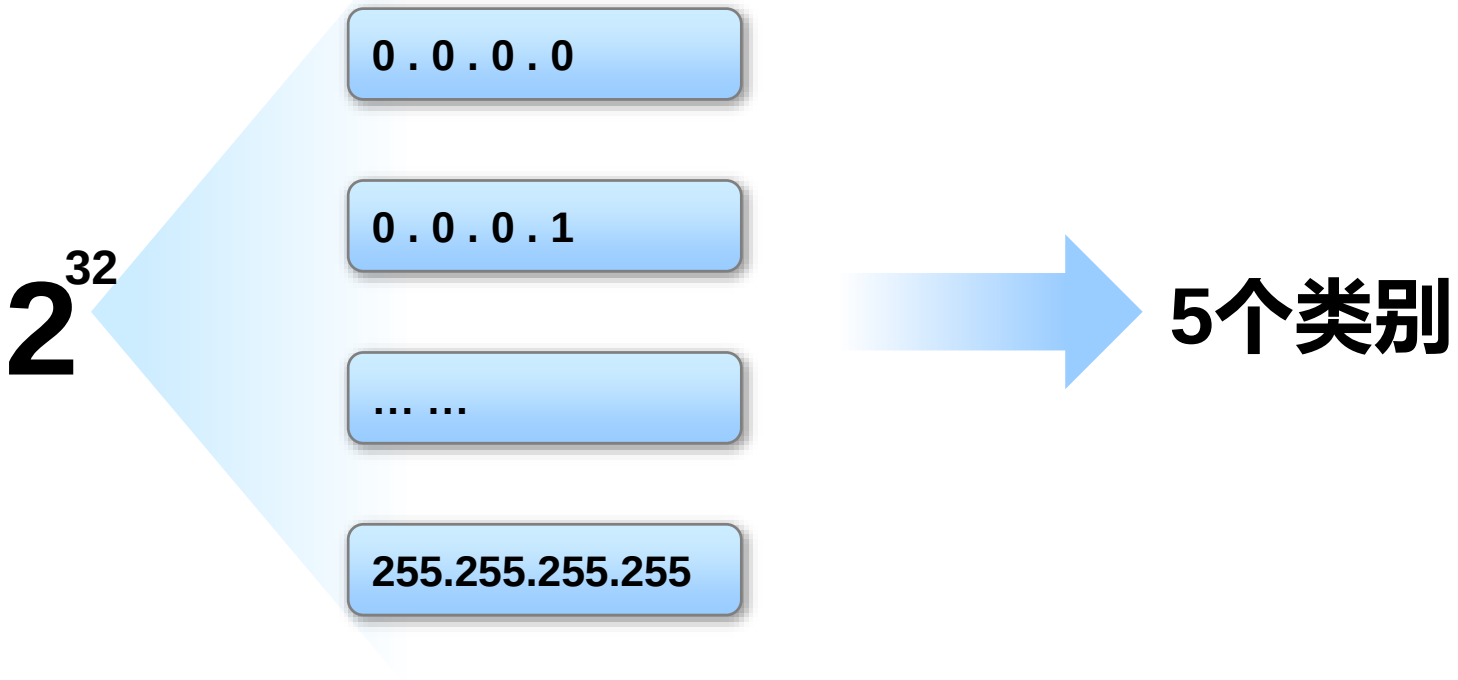
十进制	**192.**	**168.**	**10.**	**1**
二进制	11000000	10101000	00001010	00000001

十进制与二进制的转换

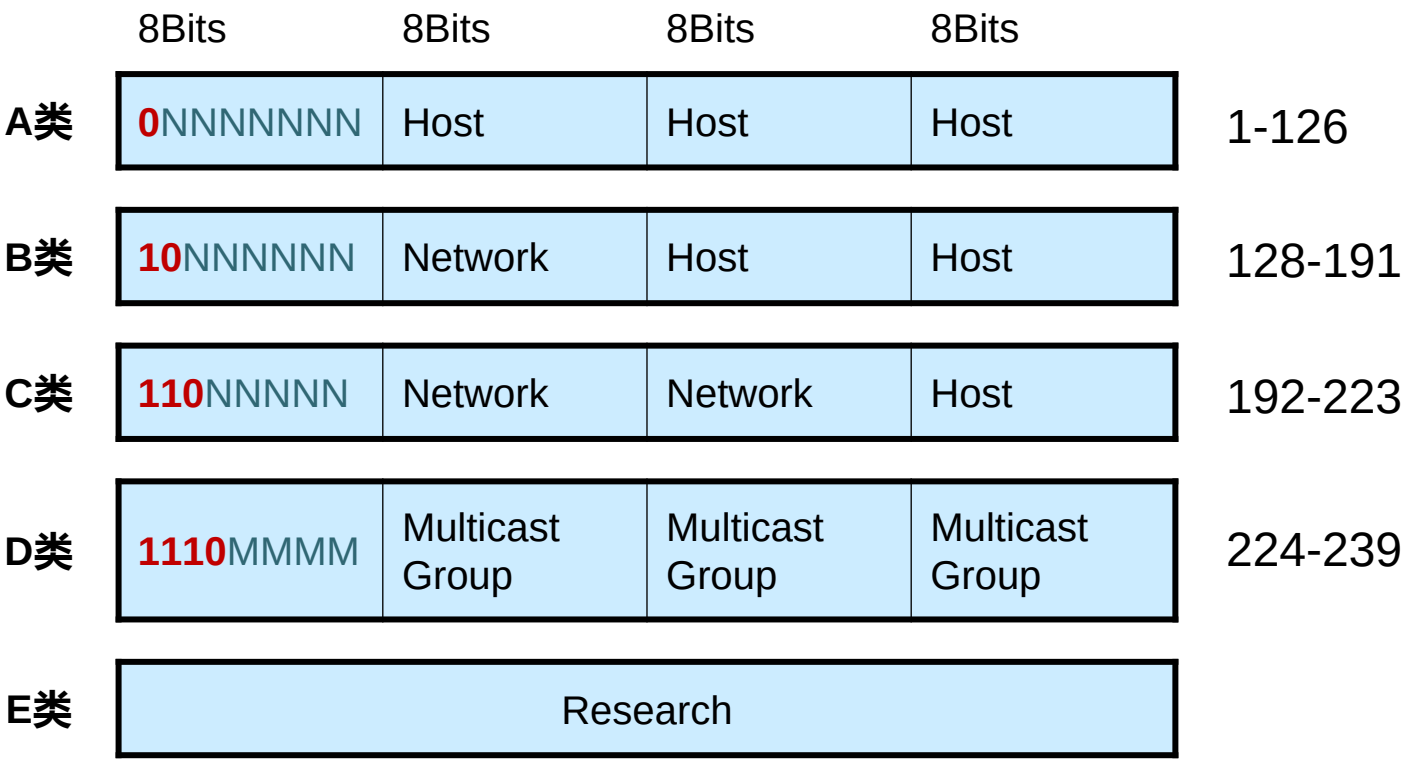
幂	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
	128	64	32	16	8	4	2	1
位	1	1	0	0	0	0	0	0

= 128 + 64 = 192

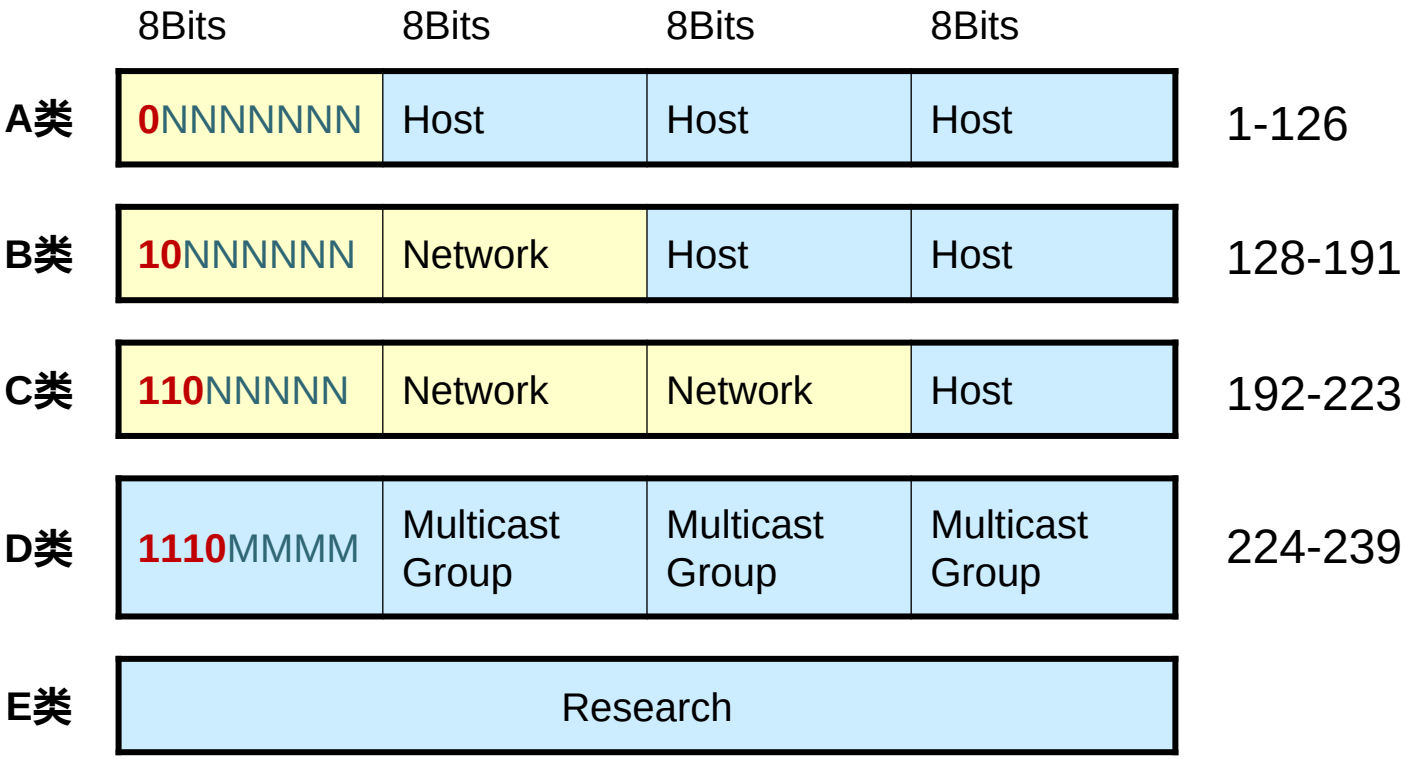
IP地址的类别



IP地址的类别

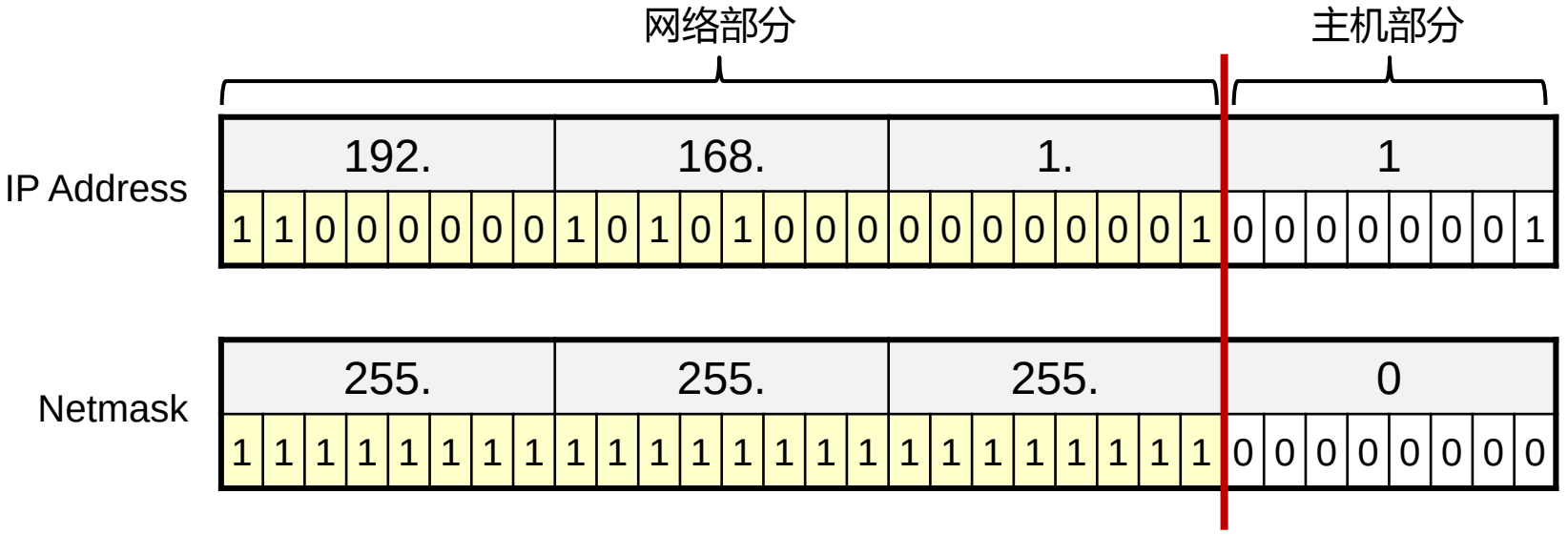


IP地址的类别（网络部分、主机部分）



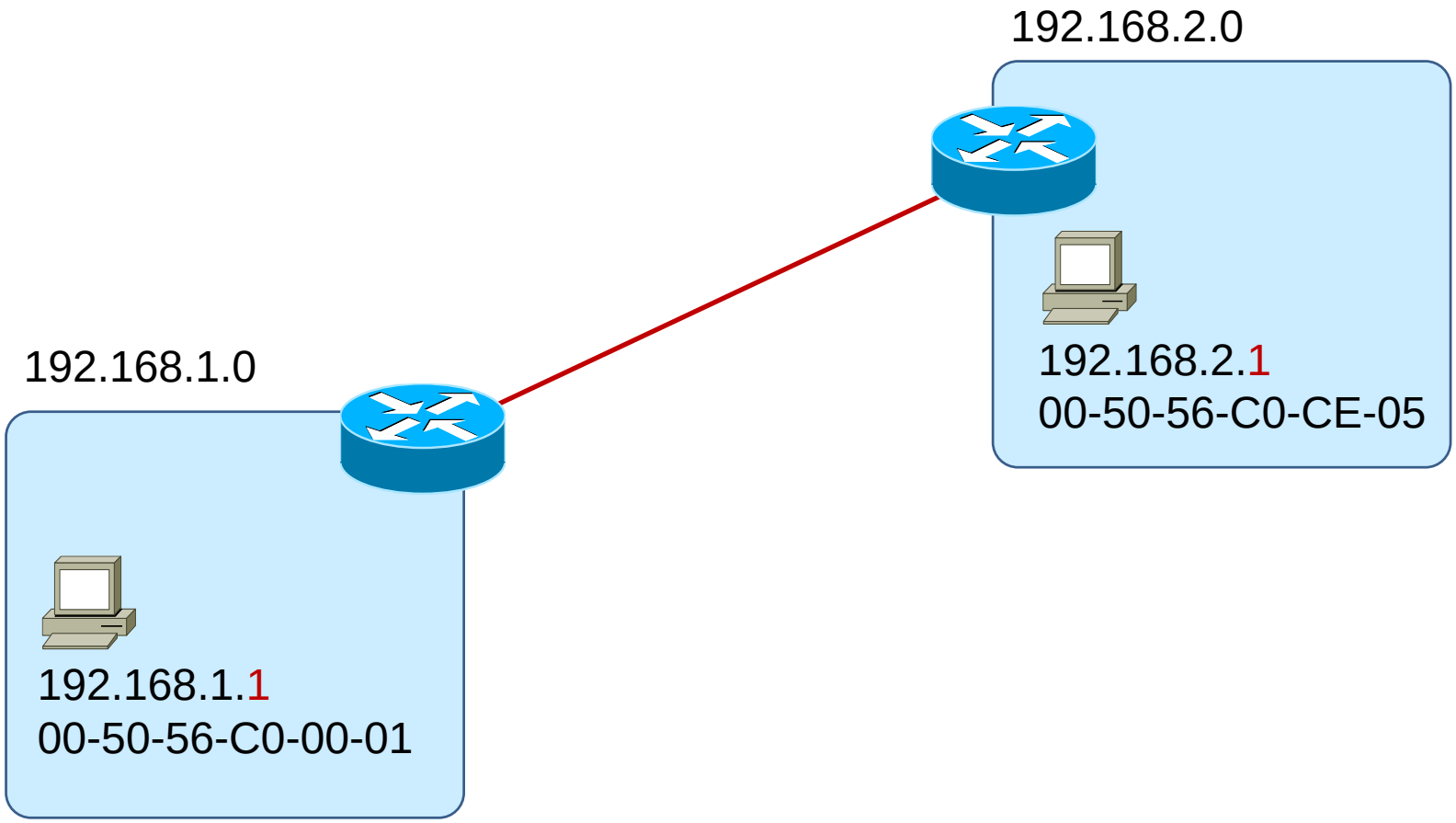
网络掩码 Netmask

- 网络掩码与IP地址搭配使用，用于描述一个IP地址中的网络部分及主机部分。
- 网络掩码32bits，与32bits的IP地址一一对应，掩码中为1的位对应IP地址中的网络位，掩码中为0的位对应IP地址中的主机位。



可使用掩码长度的呈现方式：192.168.1.0/24

网络掩码 Netmask

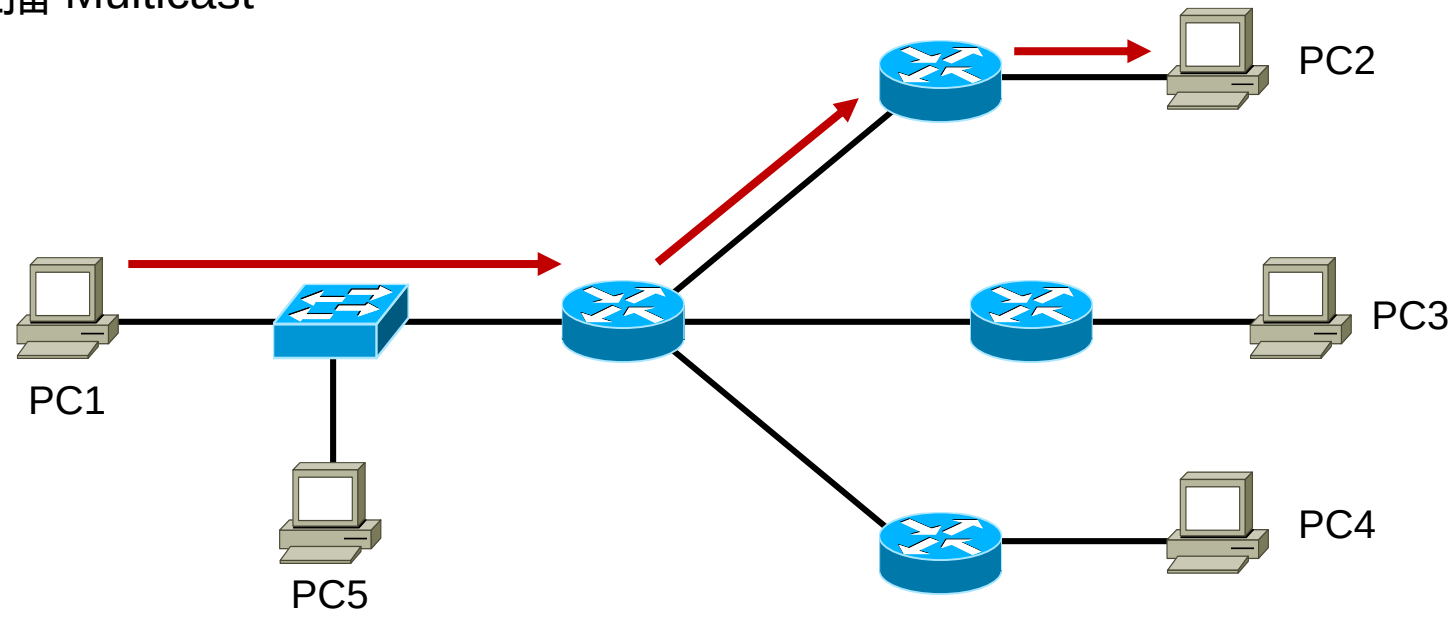


Test

Address	Class	Network	Host
10.2.1.1	A	10.0.0.0	1.1
128.63.2.100	B	128.63.0.0	2.100
201.222.5.64			
192.6.141.2			
256.241.201.1			

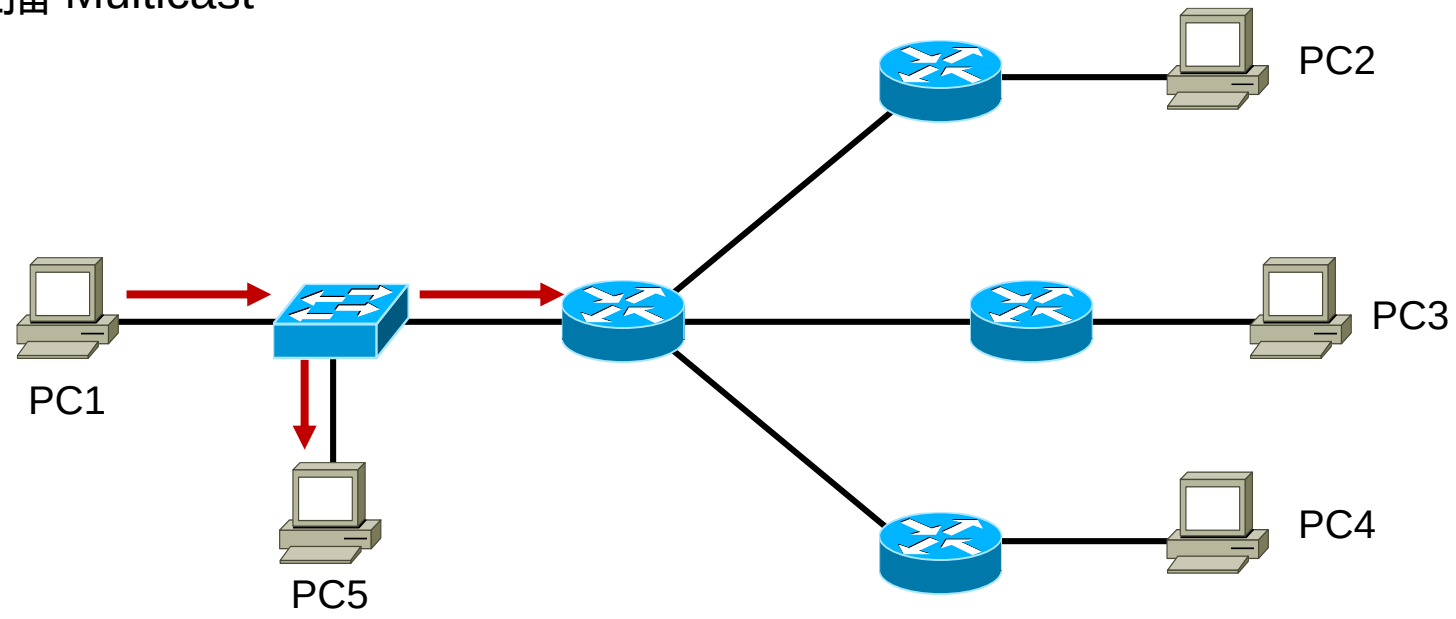
IP网络通信类型

- 单播 Unicast
- 广播 Broadcast
- 组播 Multicast



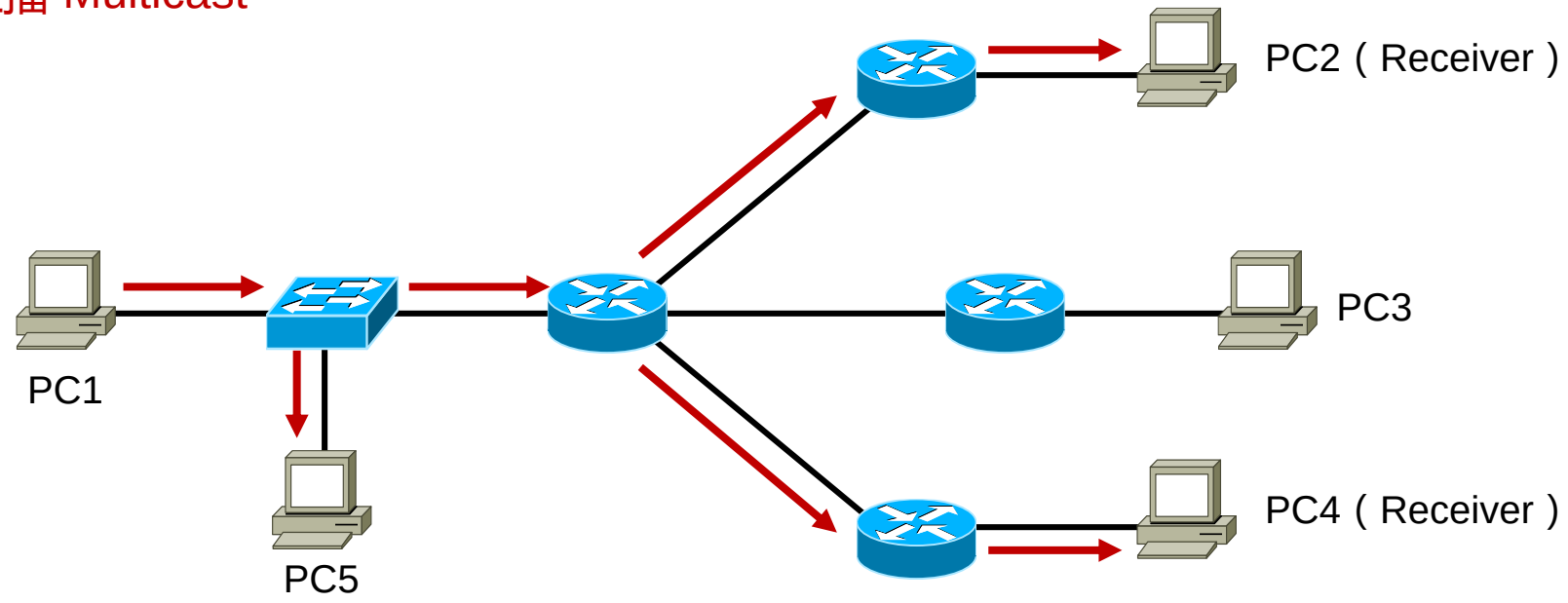
IP网络通信类型

- 单播 Unicast
- 广播 Broadcast
- 组播 Multicast



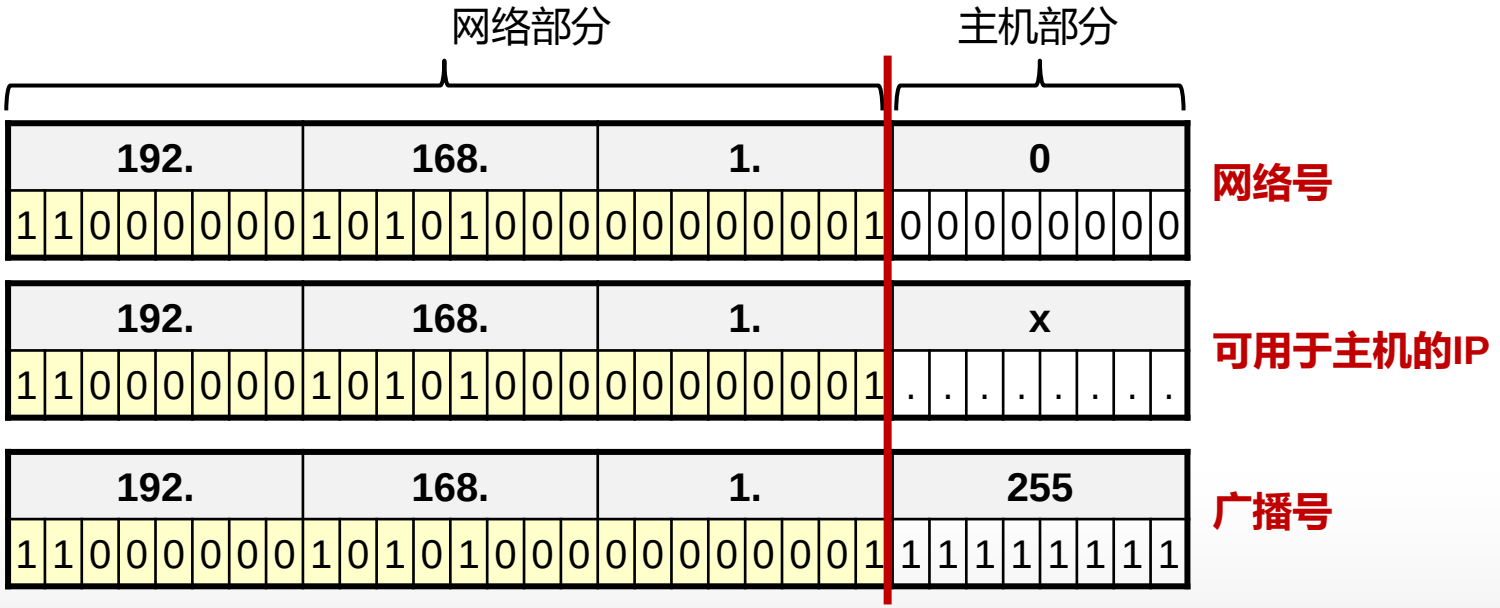
IP网络通信类型

- 单播 Unicast
- 广播 Broadcast
- 组播 Multicast

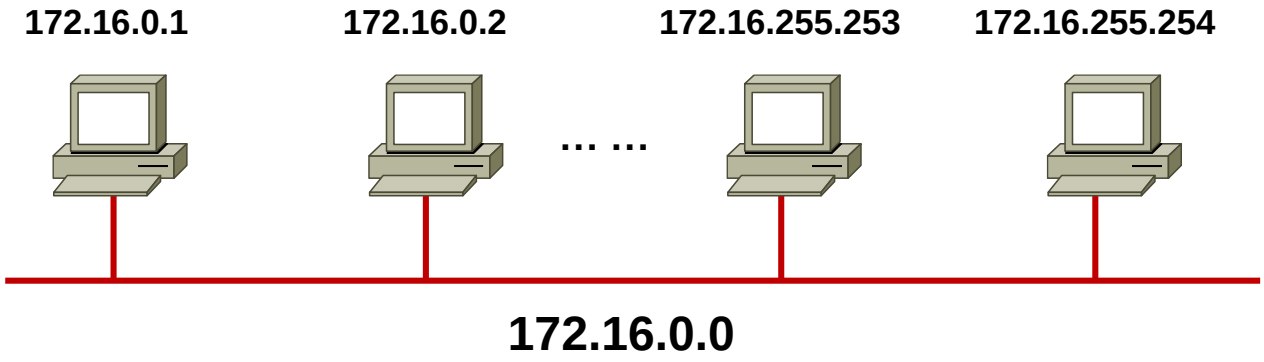


IP地址类型

- 网络地址：指代网络的地址。在网络的 IPv4 地址范围内，最小地址保留为网络地址。此地址的主机部分的每个主机位均为0。
- 广播地址：用于向网络中的所有主机发送数据的特殊地址。广播地址使用该网络范围内的最大地址。即主机部分的各比特位全部为1的地址。
- 主机地址：可分配给网络中终端设备的地址。

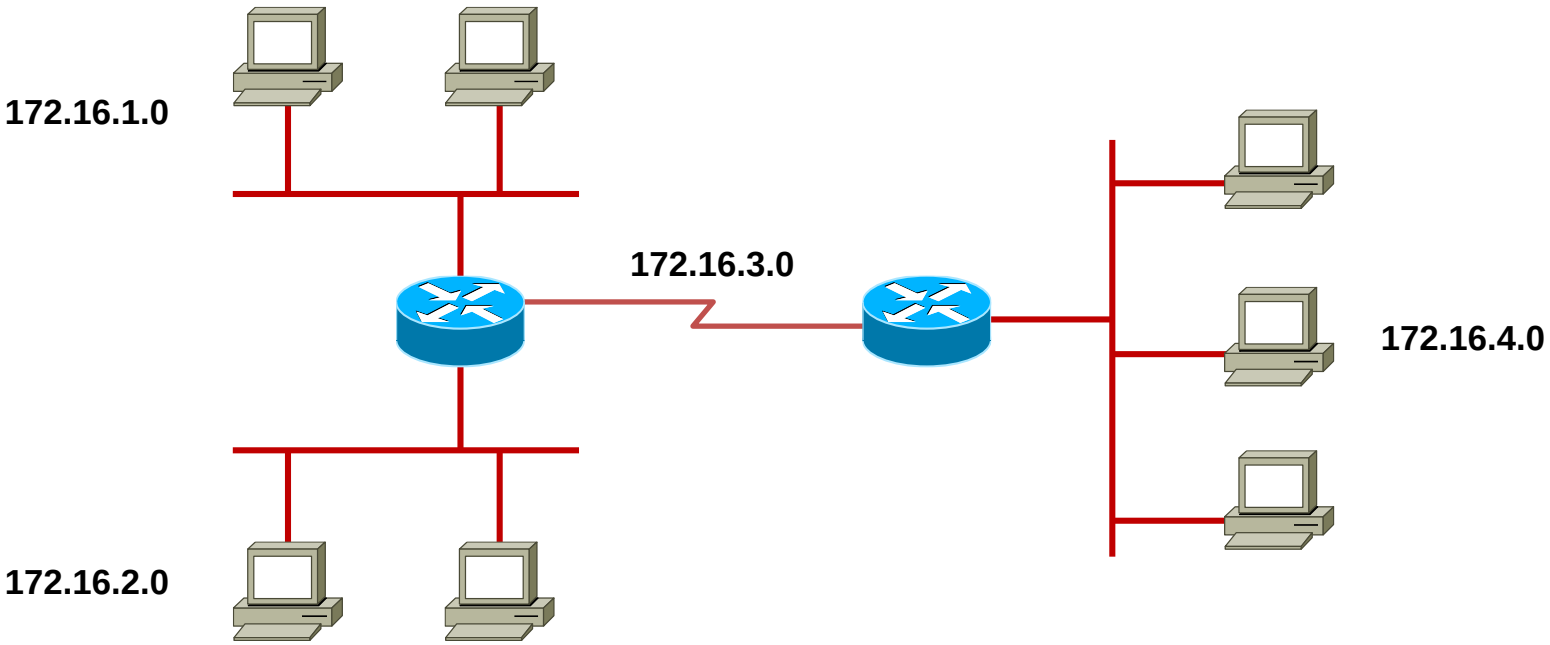


为什么要划分子网？



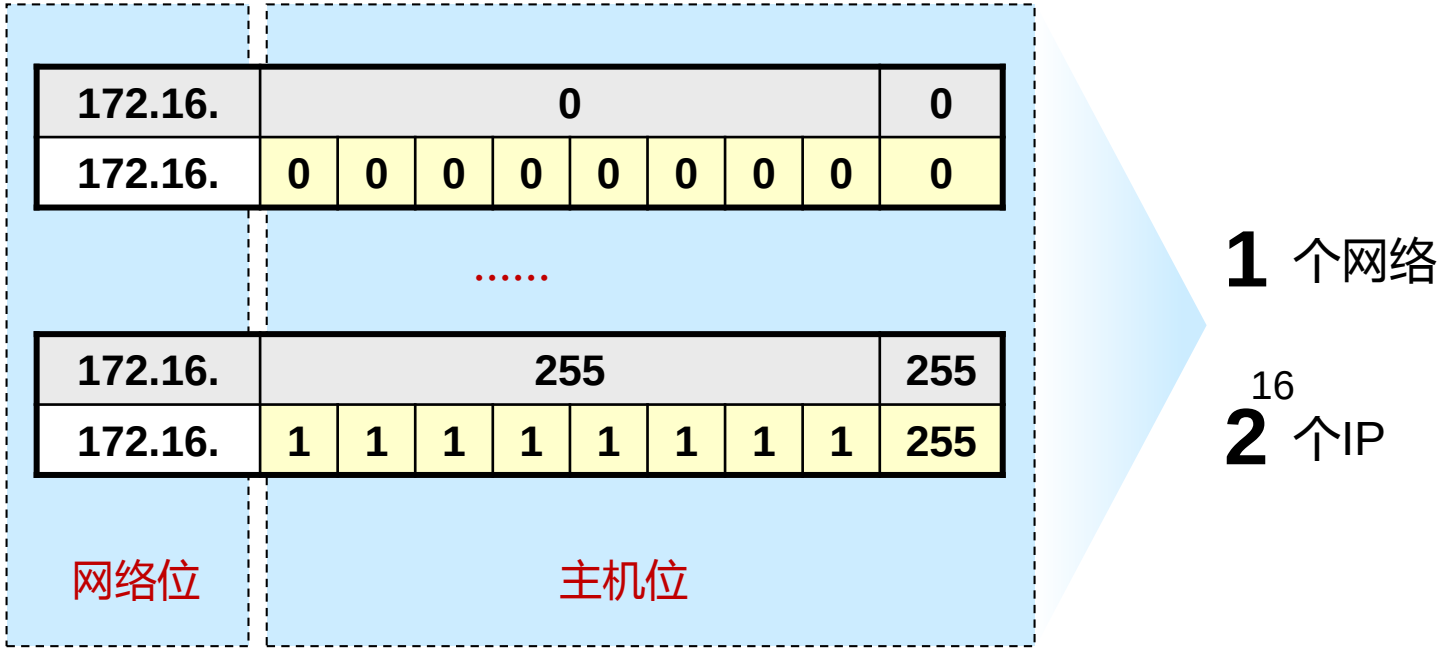
- IP地址空间只能按照默认的类别使用，例如一个B类地址，默认掩码为255.255.0.0，意味着这个地址空间里有2的16次方个IP，并且该网络号只能用于一个广播域；
- IP地址空间的极大浪费；
- 一个广播域中PC数量过于庞大，网络可能被广播报文消耗大量的资源。

为什么要划分子网？



如何进行子网划分

假设你有一个B类地址：172.16.0.0/16

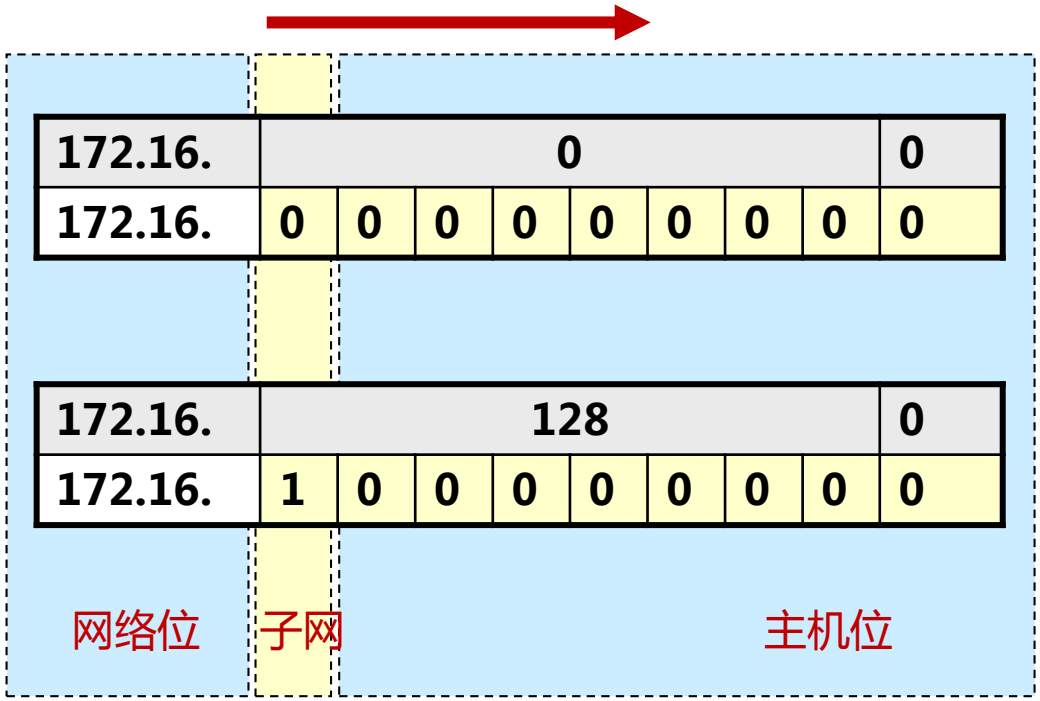


1 个网络

2^{16} 个IP

如何进行子网划分

网络位向主机位借位，从而使得网络部分的位数加长：

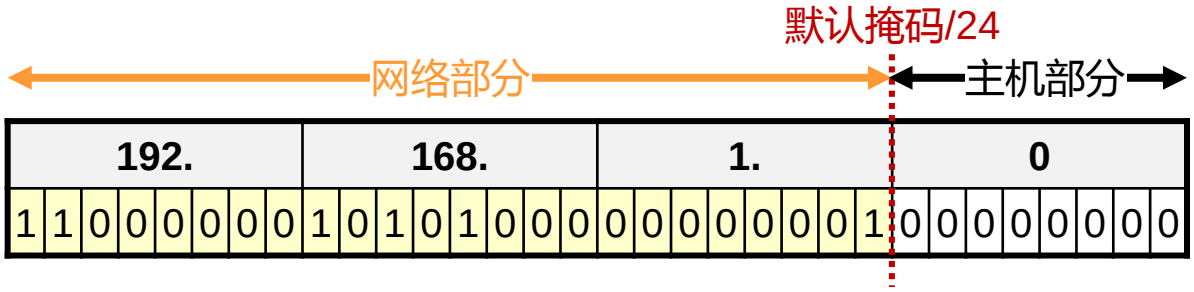


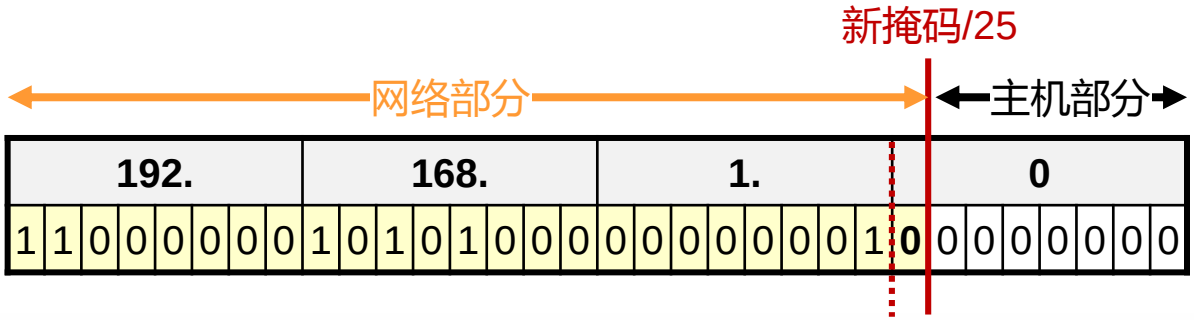
子网：172.16.0.0
掩码：255.255.128.0
主机：172.16.0.1 – 172.16.127.254

子网：172.16.128.0
掩码：255.255.128.0
主机：172.16.128.1 – 172.16.255.254

子网划分示例1

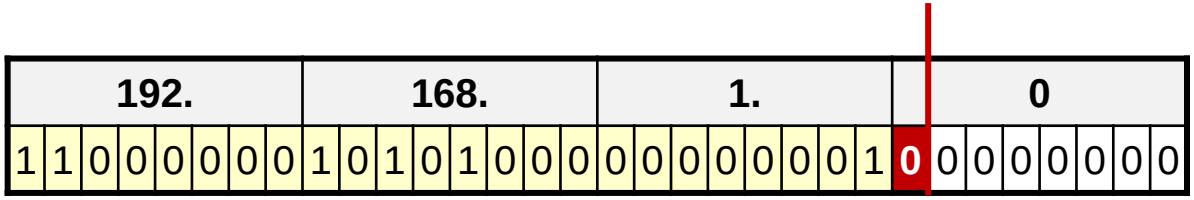
- 将192.168.1.0/24这个C类地址进行子网划分，网络位向主机位借1位



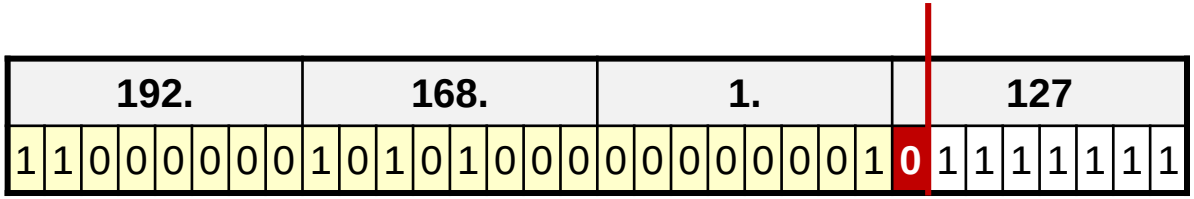


子网划分示例1

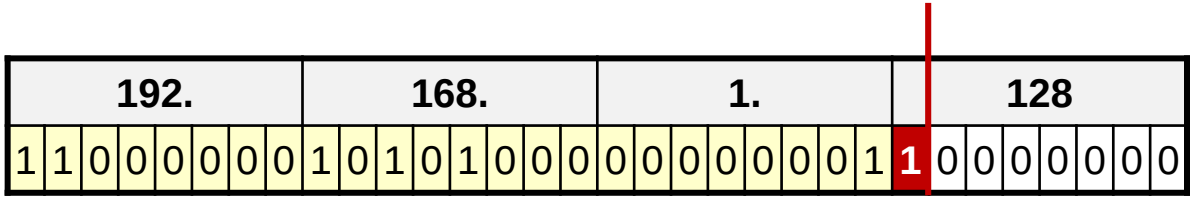
- 将192.168.1.0/24这个C类地址进行子网划分，网络位向主机位借1位



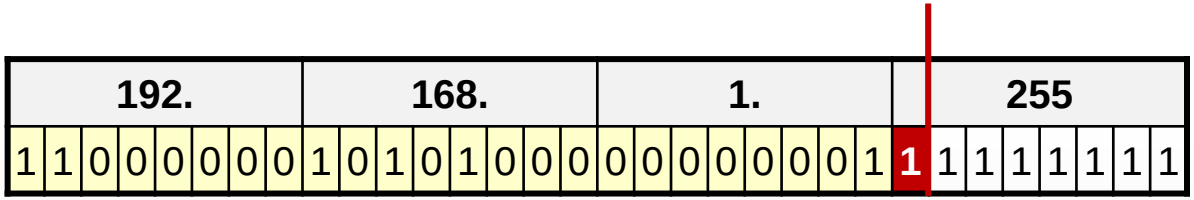
子网1
网络号：192.168.1.0/25



子网1
广播号：192.168.1.127



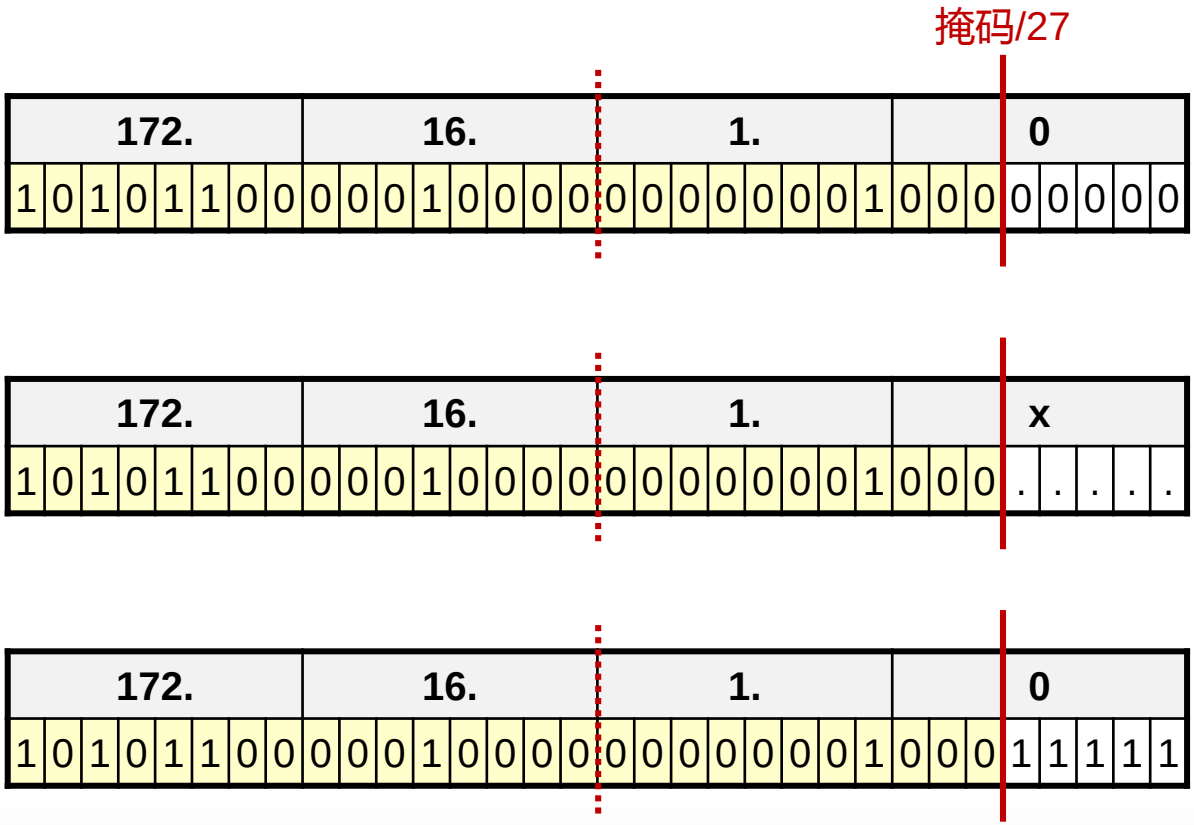
子网2
网络号：192.168.1.128/25



子网2
广播号：192.168.1.255

子网划分示例2

- 计算一下172.16.1.0/27这个子网的网络号、广播号，及可用IP地址



计算产生的子网及每个子网的主机数量

2^m = 向主机位借位后产生的子网个数

m为所借的位数

2^n-2 = 向主机位借位后产生的每个子网中可用主机IP数

n为原主机位剔除被借位后的剩余位数

-2的原因是，每个子网中的网络号及广播号不可用

公有IP及私有IP

IPv4地址空间中有一部分特殊的地址，成为私有IP地址，私有IP地址不能直接访问公网（Internet）的IP，只能在本地使用。

私有IP地址空间	地址范围
10.0.0.0/8	10.0.0.0 到 10.255.255.255
172.16.0.0/12	172.16.0.0 到 172.31.255.255
192.168.0.0/16	192.168.0.0 到 192.168.255.255

红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You

红茶三杯
Vinsoney

学习 沉淀 成长 分享

设备管理及CISCO IOS基础配置

红茶三杯（朱SIR）微博：http://t.sina.com/vinsoney

Latest update: 2012-06-01

Content

CISCO路由器及启动过程

设备管理及CISCO IOS介绍

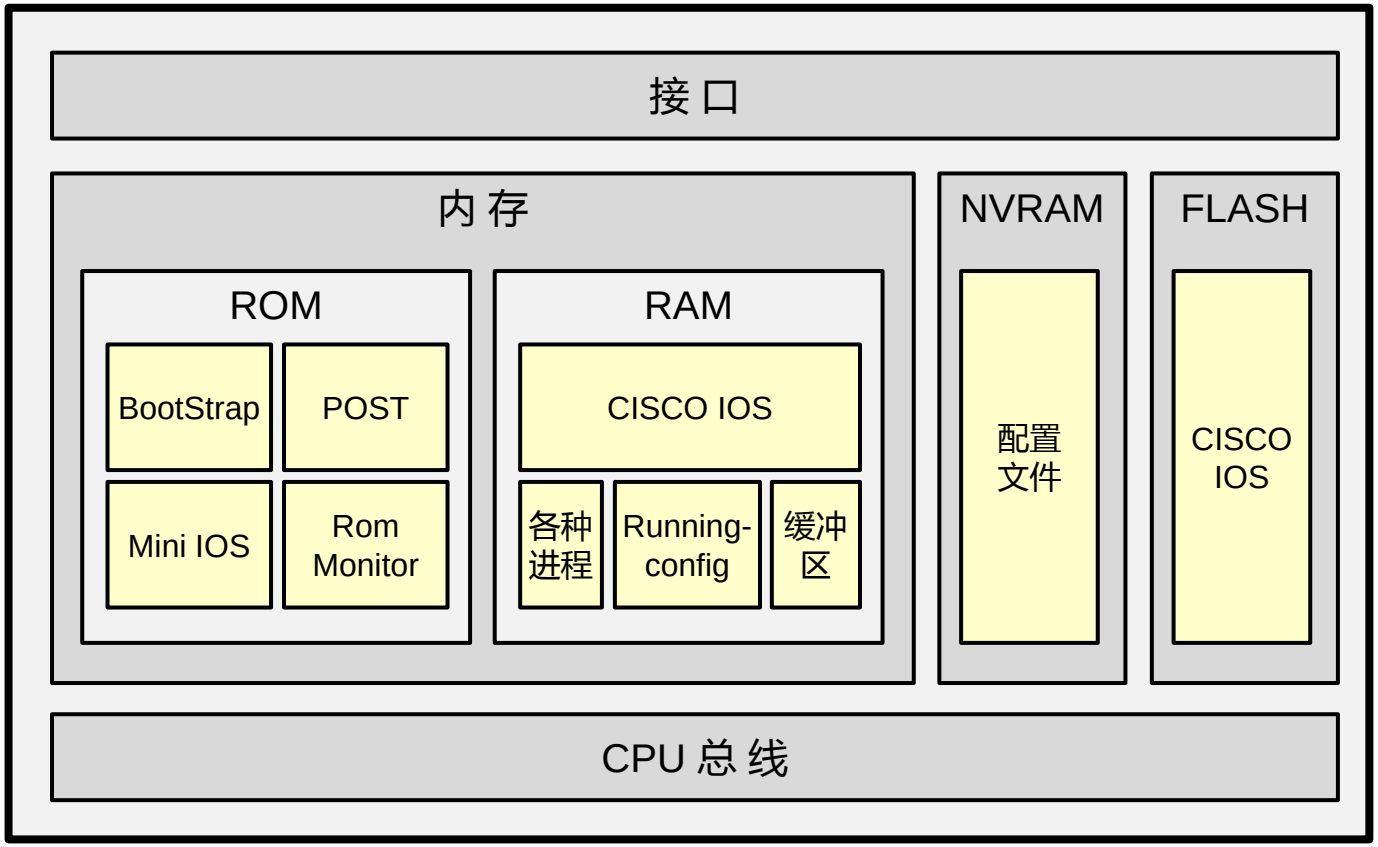
CISCO IOS路由器基础实验

红茶三杯
Vinsoney

CISCO路由器及启动过程

- 路由器组件
- 路由器启动过程

路由器组件



路由器组件及功能

- **CPU**
  - 执行操作系统的指令，中央处理器
- **随机访问存储器（RAM）– RAM中存储的信息在设备断电后会丢失**
  - 当前运行中的操作系统镜像（CISCO IOS）
  - 当前运行的配置文件（Running-configuration）
  - IP路由表（IP Routing-Table）
  - ARP表（ARP cache）
  - 数据包缓存区

路由器组件及功能 (cont.)

- **只读存储器（ROM）**
  - 启动引导程序（BOOTSTRAP）
  - 基本的自检软件（POST）
  - Mini IOS（用于紧急恢复）
- **非易失性存储器（NVRAM）**
  - 存储启动配置（Startup-configuration）
- **FLASH**
  - CISCO IOS
- **Interfaces**

Cisco路由器的启动步骤

- **检测路由器硬件**
  - Power-On Self Test（POST）
  - 执行Bootstrap
- **定位加载 Cisco IOS 软件**
  - 定位 IOS
  - 加载 IOS
- **定位加载启动配置文件或进入配置模式**
  - 启动程序搜寻配置文件

红茶三杯
Vinsoney

设备管理及CISCO IOS介绍

- 通过Console接口管理网络设备
- CISCO IOS概述
- CISCO IOS命令行界面
- CISCO IOS基础配置命令

Cisco IOS简介

- **Cisco Internetwork Operating System（CISCO IOS）**
  - Cisco互联网络操作系统，Cisco私有的网络设备操作系统。它是Cisco 的一项核心技术，该操作系统应用于Cisco路由器、局域网交换机、小型无线接入点等设备。
- **Cisco IOS 可为设备提供下列网络服务：**
  - 基本的路由和交换功能
  - 安全可靠地访问网络资源
  - 网络可伸缩性

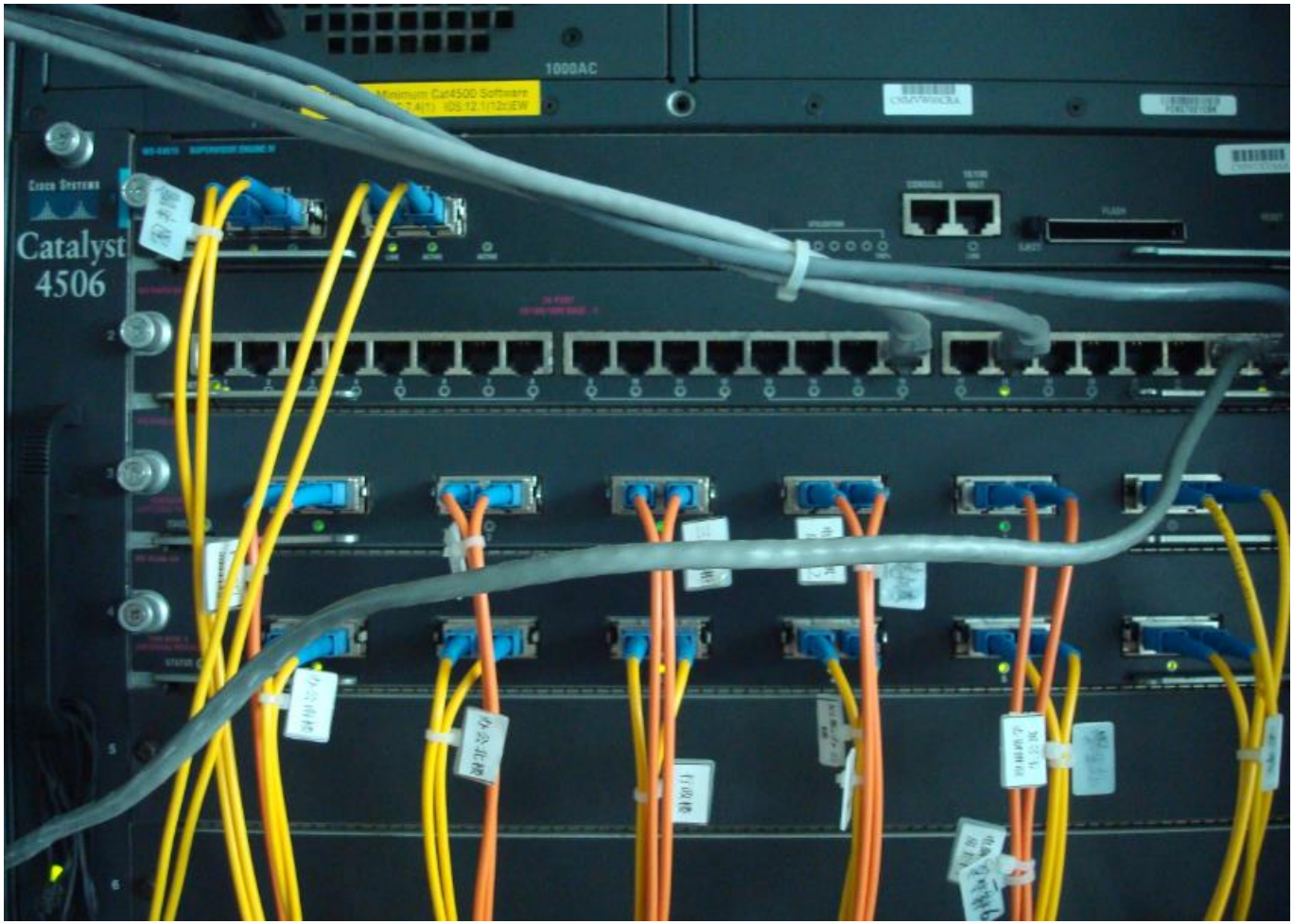
设备管理方法

- 可以通过多种方法访问 CLI 环境。最常用的方法有：
  - 通过Console接口管理设备
  - 通过Telnet或SSH远程管理设备
  - 辅助端口

通过Console线管理设备

COM口

Console Port

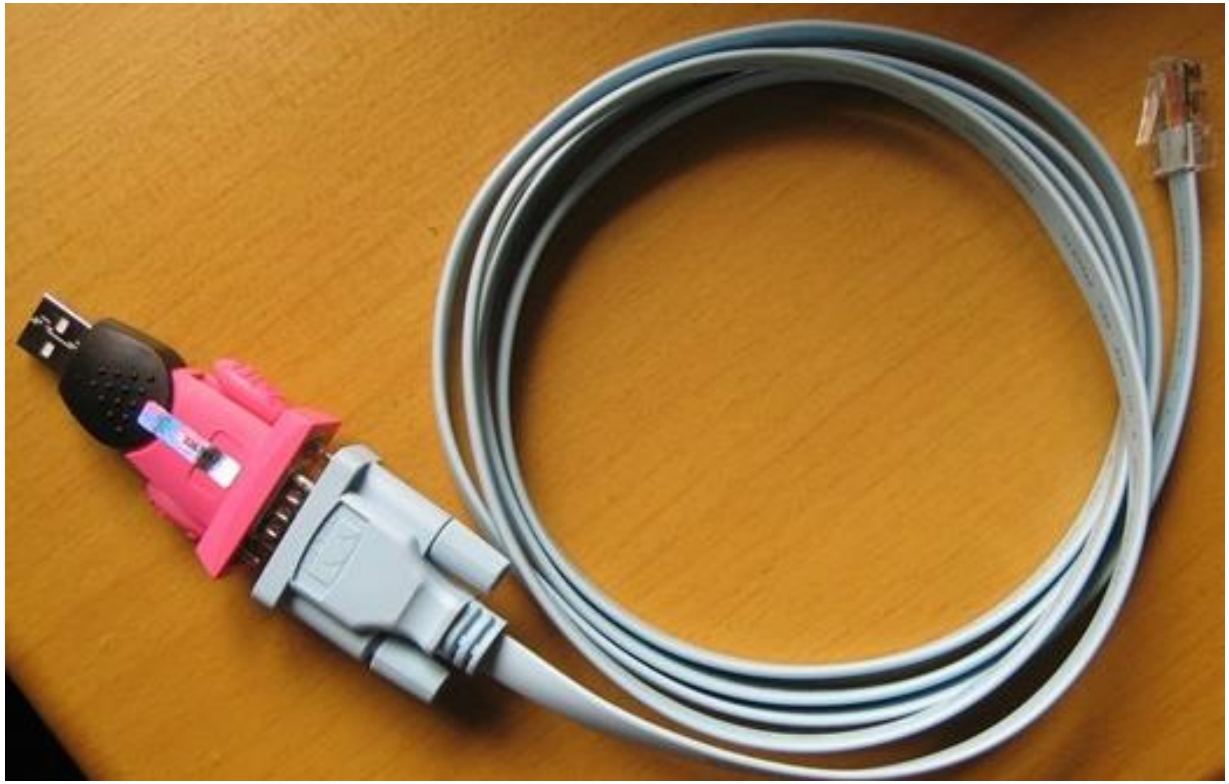


认识相关线缆

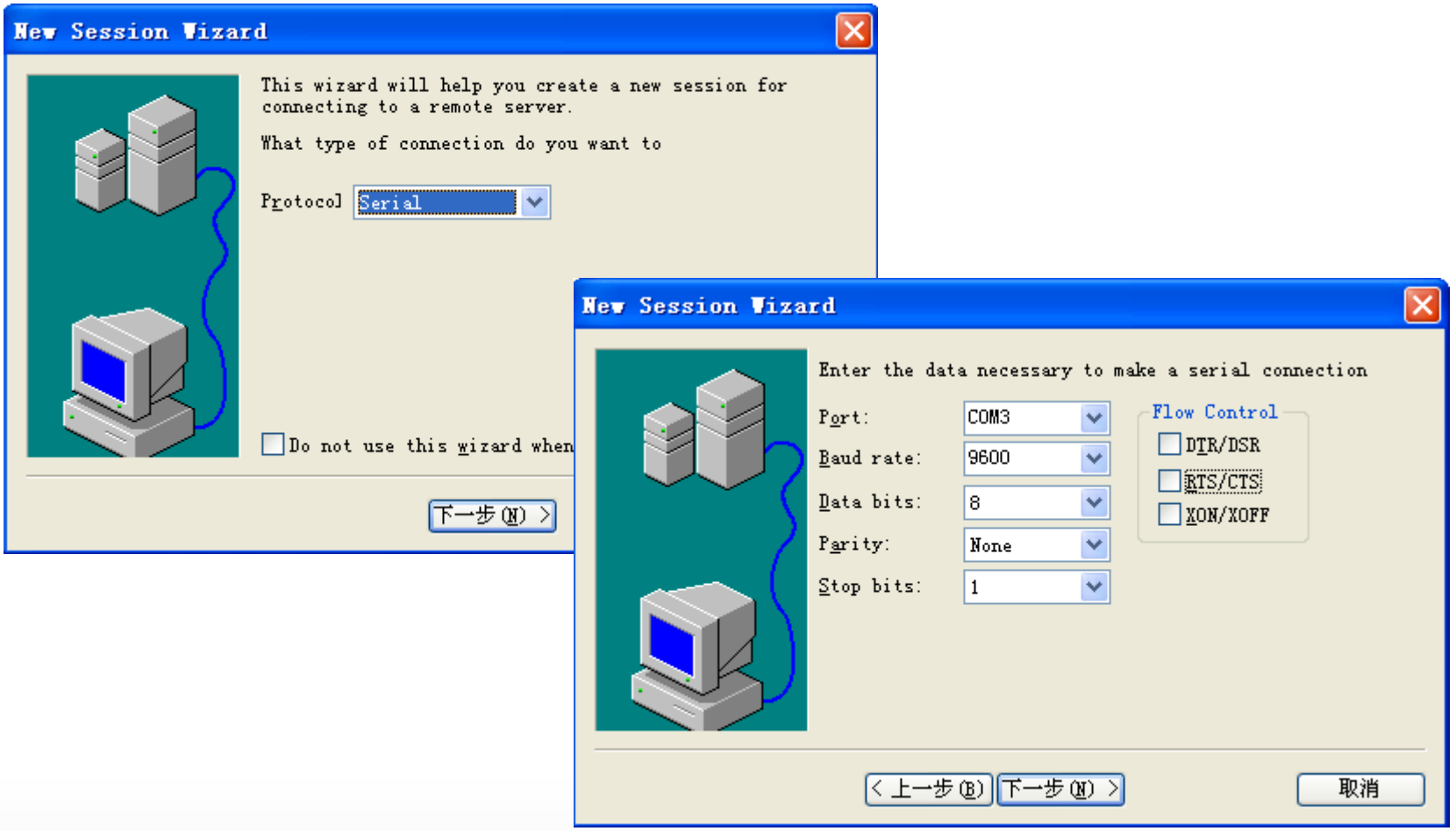
USB-RS232

Console线

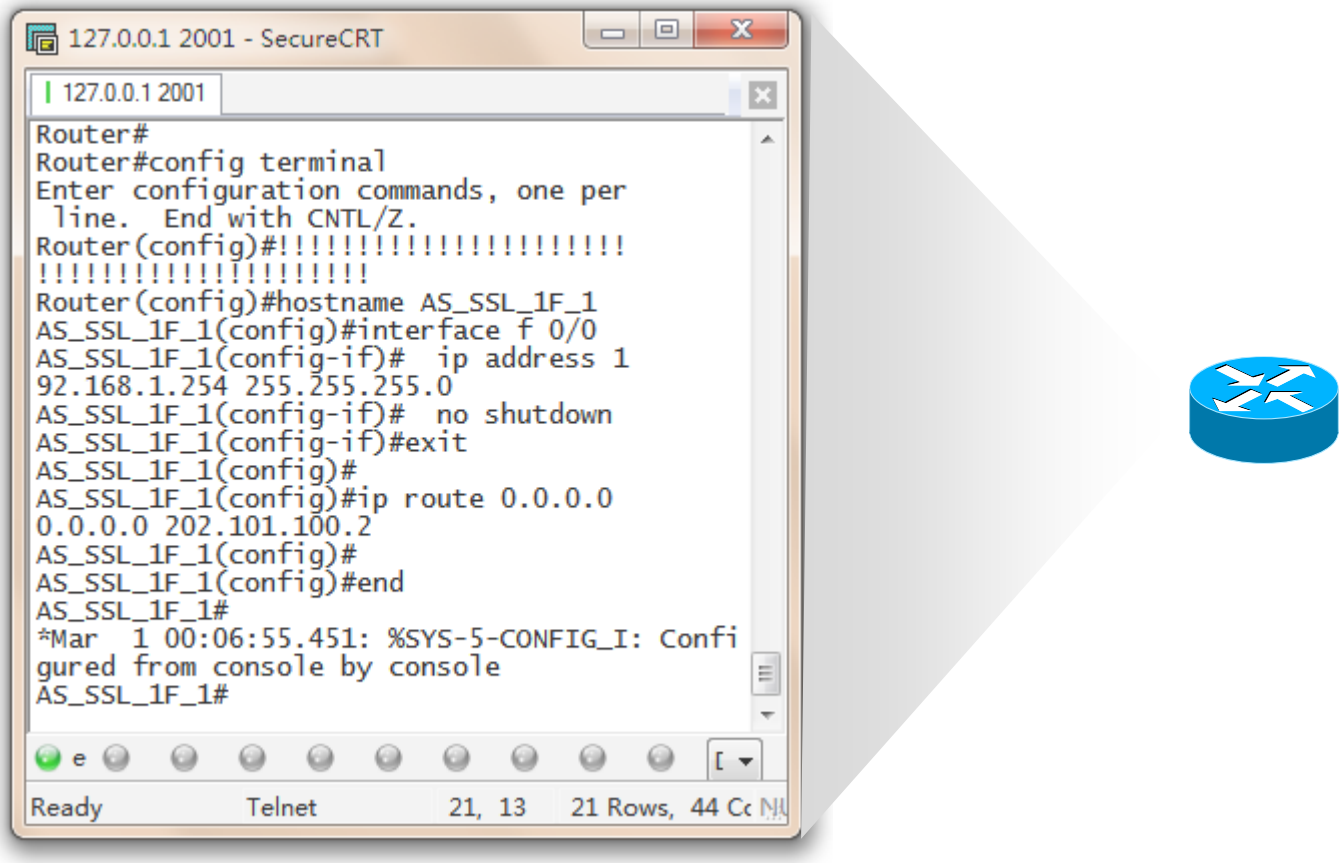
认识相关线缆



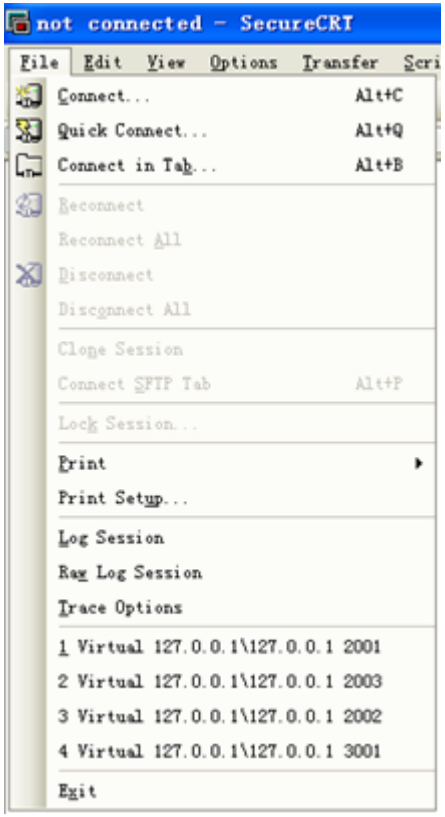
SecureCRT软件的设置及使用

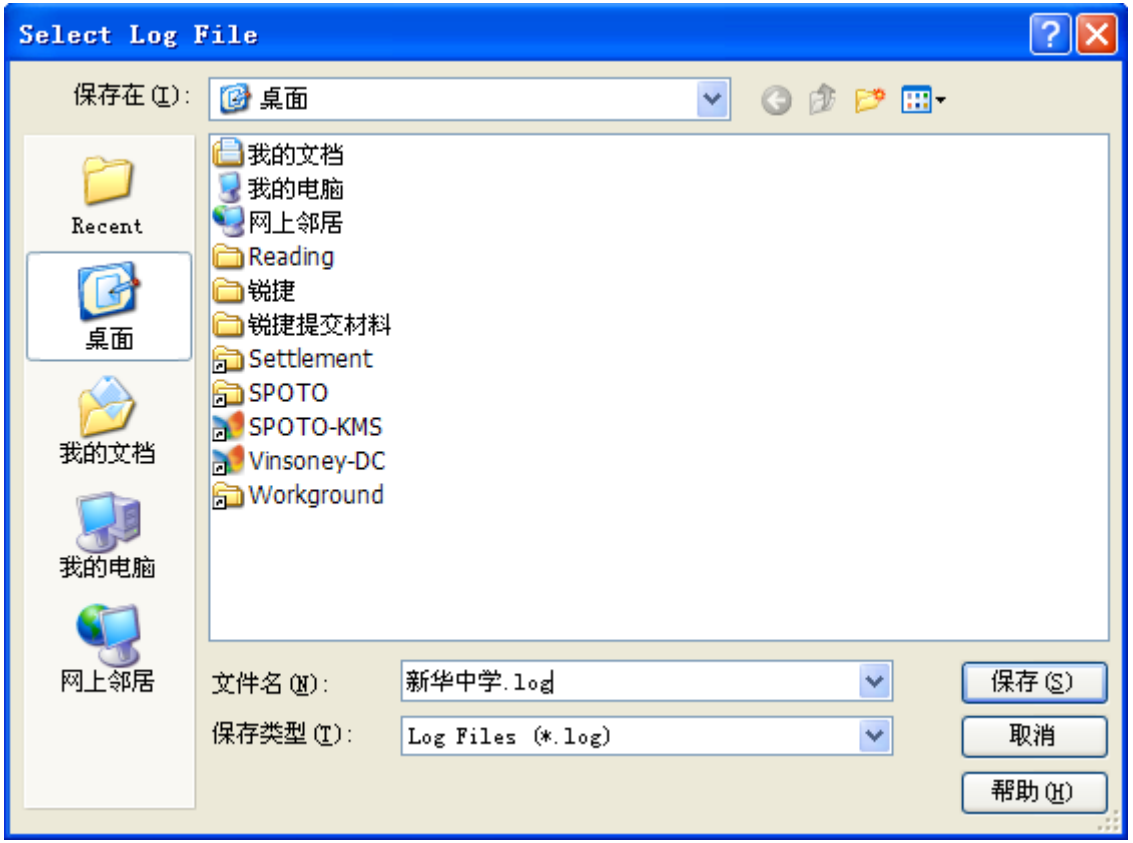


SecureCRT软件的设置及使用



SecureCRT软件的设置及使用（Log Session）





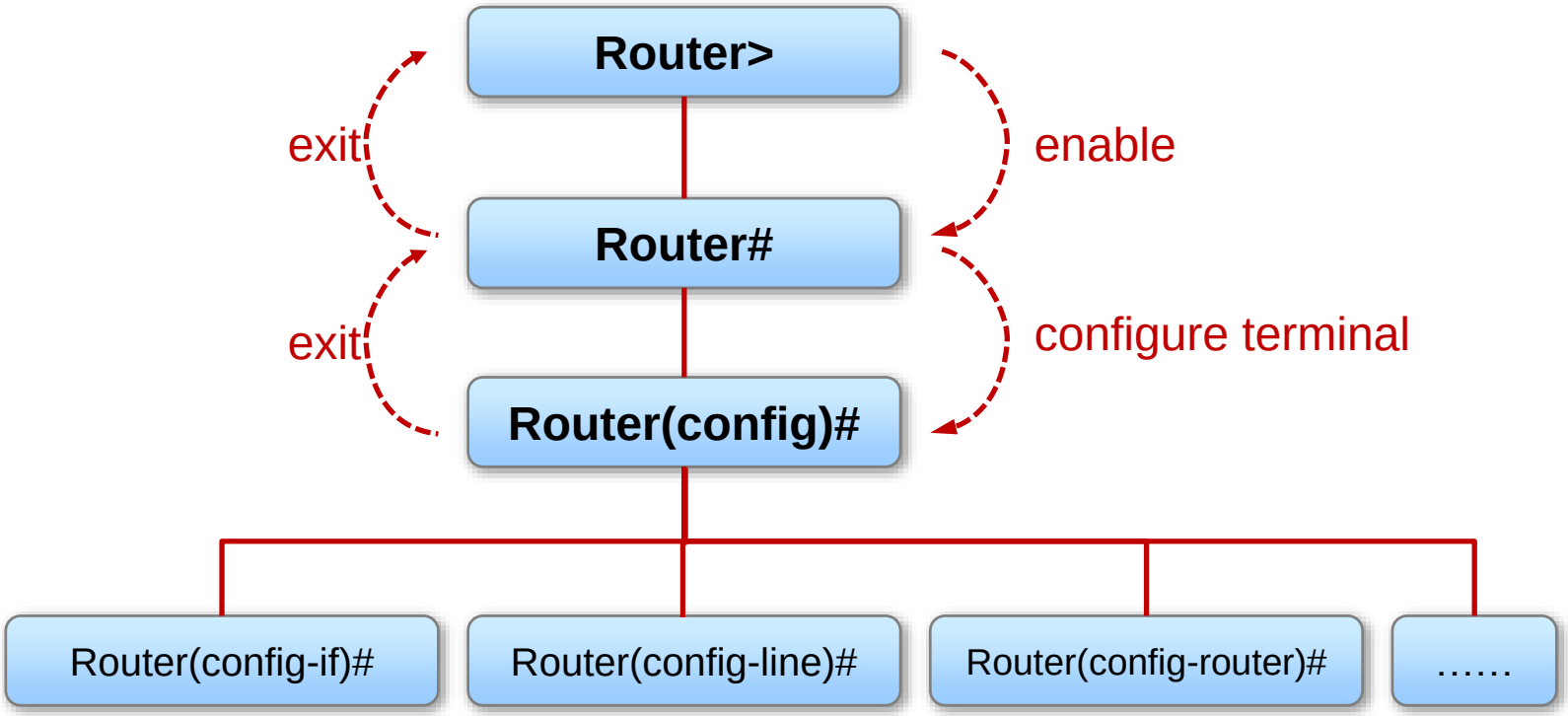
Cisco IOS配置模式

- **用户模式 cisco>**
  - 正常登陆设备CLI后的第一个配置模式，只具备最基本的查看权限
- **特权模式 cisco#**
  - 从用户模式通过认证后即可进入特权模式
- **全局配置模式**
  - 可配置设备全局参数，开启或关闭设备全局特性或功能；
  - 从全局配置模式可进入多种不同的其他子配置模式。

Cisco IOS配置模式

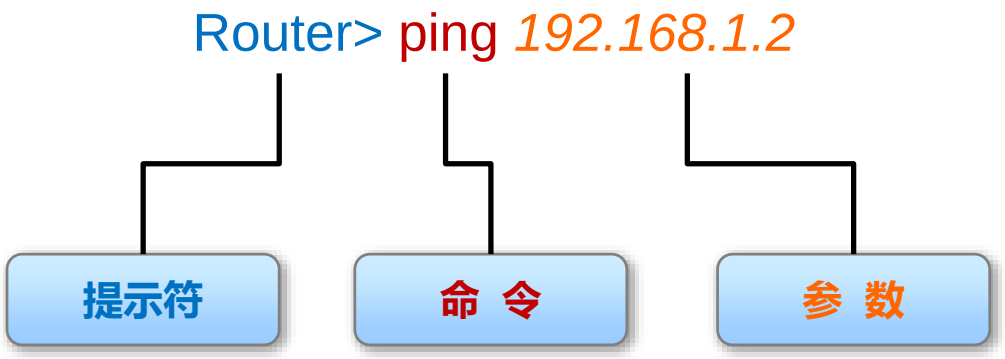
- **接口模式**
  - 用于配置设备的接口
- **线路模式**
  - 用于配置一条线路（实际线路或虚拟线路）（例如控制台、AUX 或 VTY 等等）
- **路由进程配置模式**
  - 用于配置一个路由协议进程

Cisco IOS配置模式的切换



基本IOS命令结构

- 每个 IOS 命令都具有特定的格式或语法，并在相应的提示符下执行。
- 常规命令语法为命令后接相应的关键字和参数。
- 某些命令包含一个关键字和参数子集，此子集可提供额外功能。



使用CLI的帮助

- 命令提示及补全
- 命令语法检查
- 热键和快捷方式

使用CLI的帮助

- **命令提示及补全**

```
R1(config)#rout?
  route-map  router
R1(config)#router ?
  bgp       Border Gateway Protocol (BGP)
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis      ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile    Mobile routes
  odr       On Demand stub Routes
  ospf      Open Shortest Path First (OSPF)
  rip       Routing Information Protocol (RIP)
```

使用CLI的帮助

- **命令提示及补全**

```
R1#conf t<tab>
R1#configure terminal
```

使用CLI的帮助

- **命令语法检查**

```
R1(config)#router ospf
% Incomplete command.                    // 命令不完整
```

```
R1(config)#router ospd 1
                           ^
% Invalid input detected at '^' marker.  // 箭头所指字符无法识别
```

```
R1(config)#s
% Ambiguous command:  "s"                // 未知的输入
```

使用CLI的帮助

- **热键和快捷方式**

- Tab	填写命令或关键字的剩下部分。
- Ctrl-R	重新显示一行
- Ctrl-Z	退出配置模式并返回到执行模式
- 向下箭头	用于在前面用过的命令的列表中向前滚动
- 向上箭头	用于在前面用过的命令的列表中向后滚动
- Ctrl-Shift-6	用于中断诸如 ping 或 traceroute 之类的 IOS 进程
- Ctrl-C	放弃当前命令并退出配置模式

CISCO IOS基础配置

- **配置设备名称**

```
Router(config)# hostname  AS_SSL_1F_S3640
AS_SSL_1F_S3640(config)#
```

CISCO IOS基础配置

- **配置用户登录密码**
  - Console Password：用于限制人员通过控制台（Console）连接访问设备
  - Enable Password：用于限制人员访问特权执行模式
  - Enable Secrect：经加密，用于限制人员访问特权执行模式
  - VTY Password：用于限制人员通过 Telnet 访问设备

```
R1(config)#line console 0
R1(config-line)#password spoto
R1(config-line)#login                    !! Enable password checking
```

CISCO IOS基础配置

- **配置用户登录密码**
  - 控制台口令 — 用于限制人员通过控制台连接访问设备
  - 使能口令 — 用于限制人员访问特权执行模式
  - 使能加密口令 — 经加密，用于限制人员访问特权执行模式
  - VTY 口令 — 用于限制人员通过 Telnet 访问设备

```
Router(config)#enable password spoto
Router(config)#enable secret spoto
```

CISCO IOS基础配置

- **配置用户登录密码**
  - 控制台口令 — 用于限制人员通过控制台连接访问设备
  - 使能口令 — 用于限制人员访问特权执行模式
  - 使能加密口令 — 经加密，用于限制人员访问特权执行模式
  - VTY 口令 — 用于限制人员通过 Telnet 访问设备

```
Router(config)#line vty 0 4
Router(config-line)#password password
Router(config-line)#login
```

CISCO IOS基础配置

- 管理配置文件

将当前配置写入启动配置文件

```
R1# write
R1# copy running-config startup-config
```

删除启动配置文件

```
R1# erase startup-config
R1# delete flash:config.text
```

CISCO IOS基础配置

- 接口配置

进入接口


```
R1(config)# interface ethernet 0/0
R1(config-if)#
```

为接口配置IP地址

```
R1(config-if)# ip address 192.168.1.1 255.255.255.0
```

激活接口

```
R1(config-if)# no shutdown                    //CISCO设备接口默认shutdown状态
```

CISCO IOS基础配置

- 接口配置（cont.）

配置serial接口

```
R1(config)# interface serial 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# clock rate 64000          // 在DCE端配置时钟信号
```

CISCO IOS基础配置

- Line接口配置

配置telnet密码

```
R1(config)# line vty 0 4
R1(config-line)# password spoto
R1(config-line)# login
```

CISCO IOS基础配置

- **show命令**

show ?	
show version	查看当前操作系统版本
show running-config	查看运行配置
show startup-config	查看启动配置
show flash	查看FLASH
show cpu	查看CPU利用率
show memory	查看内存使用情况
show interface	查看端口

配置文件

write 或 copy running-config startup-config

Running-config

- 运行中的配置文件，存储在RAM中
- 对设备进行配置时，配置信息将写入该配置文件，对运行中的设备产生直接影响
- 该配置信息在设备掉电后将丢失，如果需保存当前运行的配置，使用write命令
- 使用show running-config命令查看

Startup-config

- 保存的配置文件，存储在Flash中
- 该文件由于保存在Flash中，因此设备重启该配置不丢失
- 设备启动过程中，会加载该配置文件，将配置信息拷贝到running-config后运行
- 使用show startup-config命令查看
- 使用erase startup-config命令删除

CISCO IOS基础配置

- **验证配置**

ping

```
Ping 192.168.1.2
```

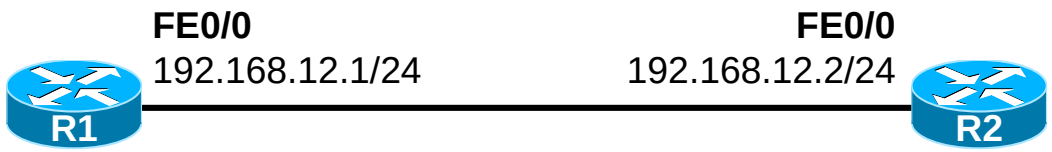
traceroute

```
traceroute 2.2.2.2
```

红茶三杯
Vinsoney

CISCO IOS 路由器基础实验

Topology




```
Router# configure terminal
Router(config)# hostname R1
R1(config)# interface fastethernet 0/0
R1(config-if)# ip address 192.168.12.1 255.255.255.0
R1(config-if)# no shutdown
```

```
Router# configure terminal
Router(config)# hostname R2
R2(config)# interface fastethernet 0/0
R2(config-if)# ip address 192.168.12.2 255.255.255.0
R2(config-if)# no shutdown
```

红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You

红茶三杯
Vinsoney

学习 沉淀 成长 分享

IP路由基础

红茶三杯（朱SIR）微博：http://t.sina.com/vinsoney

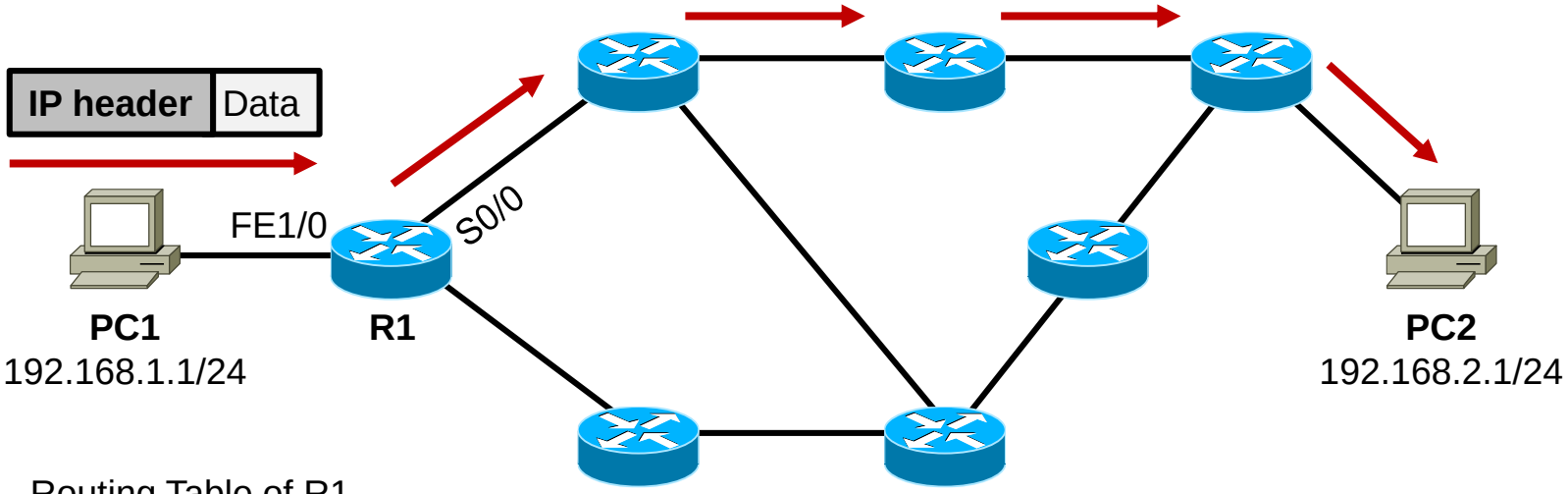
Latest update: 2012-06-01

Content

路由的基本概念

- 什么是IP路由
- 学会查看路由表
- 路由条目的获取来源

路由的概念



Routing Table of R1

Protocol	Network/Mask	NextHop	Interface
Connected	192.168.1.0/24	-	FE1/0
Connected	192.168.12.0/24	-	S0/0
RIP	192.168.2.0/24	192.168.12.2	S0/0

路由表 Routing Table

- 每一台路由器都会维护一个路由表，在路由表中包含着路由器发现的路由（路由条目、路由表项）；
- 路由表相当于路由器的地图，路由器能够正确转发IP报文的前提是在其路由表中存在匹配该数据包目的IP地址的路由条目；
- 路由表中的路由条目获取来源有多种：直连路由、静态路由及动态路由协议。

查看路由表 show ip route

R1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.12.0/24 is directly connected, Serial0/0
S 192.168.23.0/24 [1/0] via 192.168.12.2

路由条目的获取来源（路由协议类型）

查看路由表 show ip route

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.12.0/24 s directly connected, Serial0/0
S    192.168.23.0/24 [1/0] via 192.168.12.2
```

目的网络号/掩码长度

查看路由表 show ip route

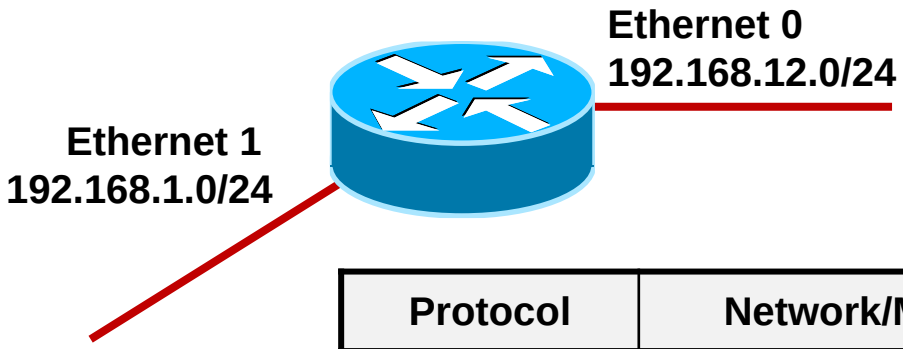
```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.12.0/24 is directly connected, Serial0/0
S    192.168.23.0/24 [1/0] via 192.168.12.2
```

去往该目的网络的出接口或需经的下一跳IP或

IP路由表



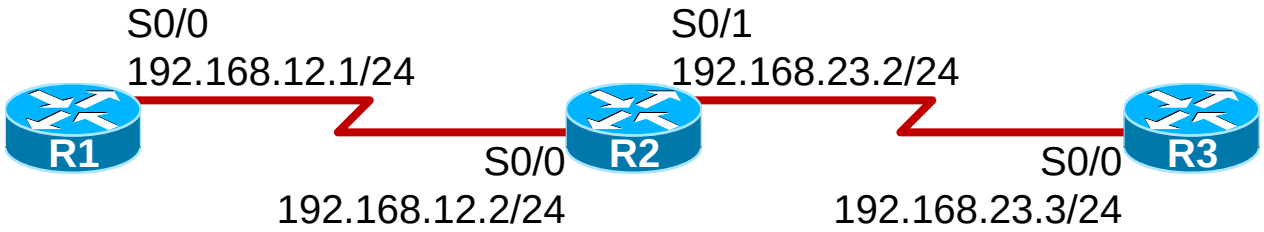
Protocol	Network/Mask	Interface
Connected	192.168.1.0/24	E0
Connected	192.168.12.0/24	E1

- 初始化情况下，路由器所知的网络只有其直连接口所在网络；
- 直连路由在路由表中的标记为C（Connected）；
- 直连路由被加载到路由表中的前提是该网络的接口物理状态、协议状态均为UP。

路由信息的来源

- 直连路由：路由器的直连接口所在网络。
- 静态路由：手工为路由器配置的路由条目。
- 动态路由：路由器动态学习到的路由。

直连路由



R2#show ip route

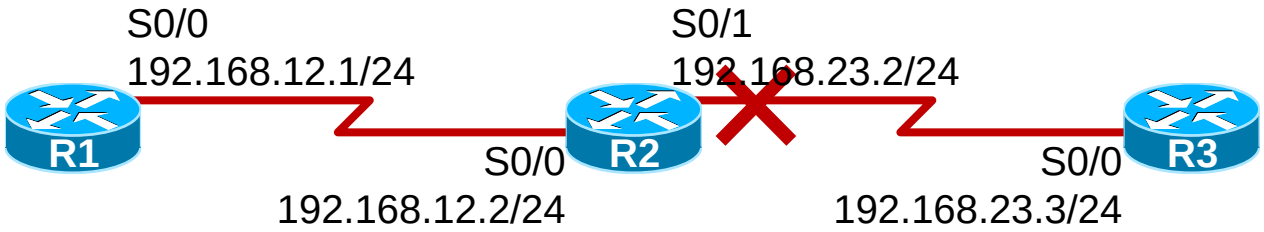
Codes: **C - connected**, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.12.0/24 is directly connected, Serial0/0

C 192.168.23.0/24 is directly connected, Serial0/1

直连路由



R2#show ip route

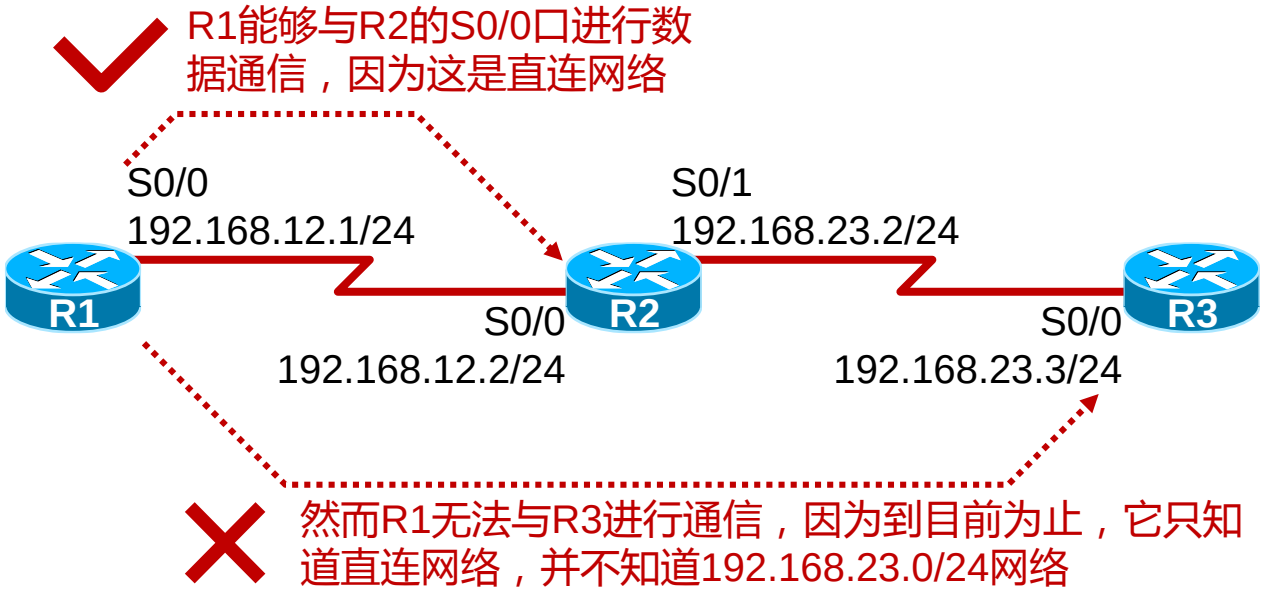
Codes: **C - connected**, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.12.0/24 is directly connected, Serial0/0

~~**C** 192.168.23.0/24 is directly connected, Serial0/1~~

直连路由

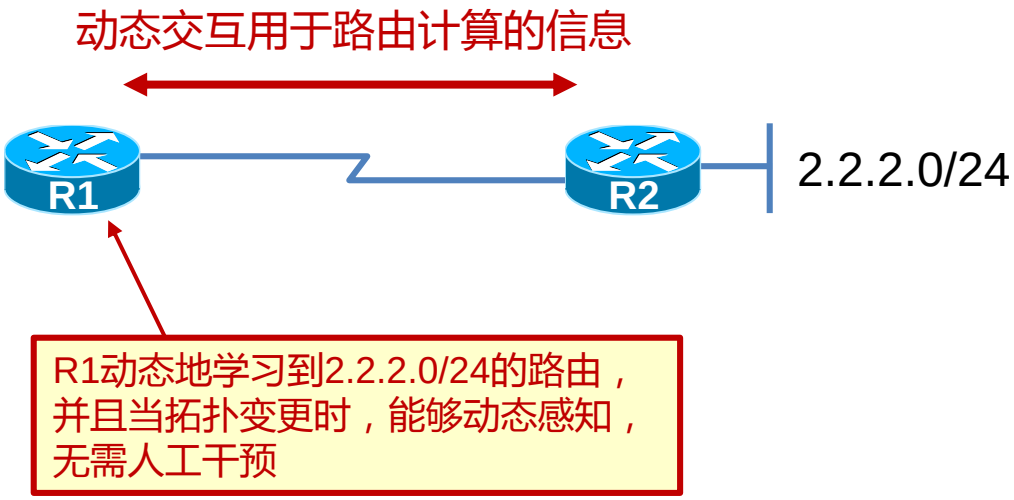


静态路由

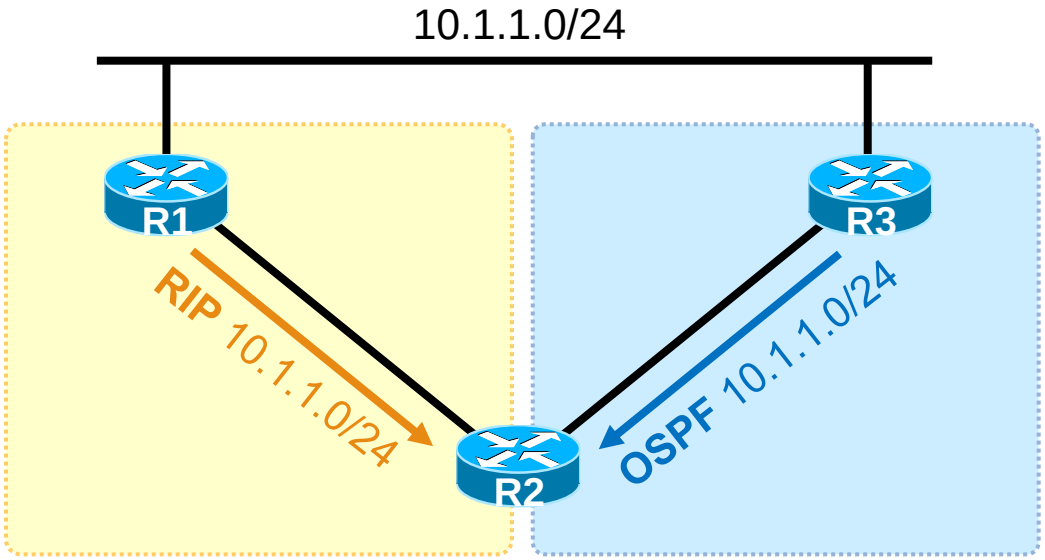
- 手工为路由器添加的路由条目。

动态路由协议

- 通过在路由器上运行动态路由协议，使得路由器之间能够交互“用于路由计算的信息”，从而路由器动态的“学习”到网络中的路由。



管理距离 Administrative Distance



R2同时从RIP及OSPF学习到
10.1.1.0/24的路由，它将如何优选？

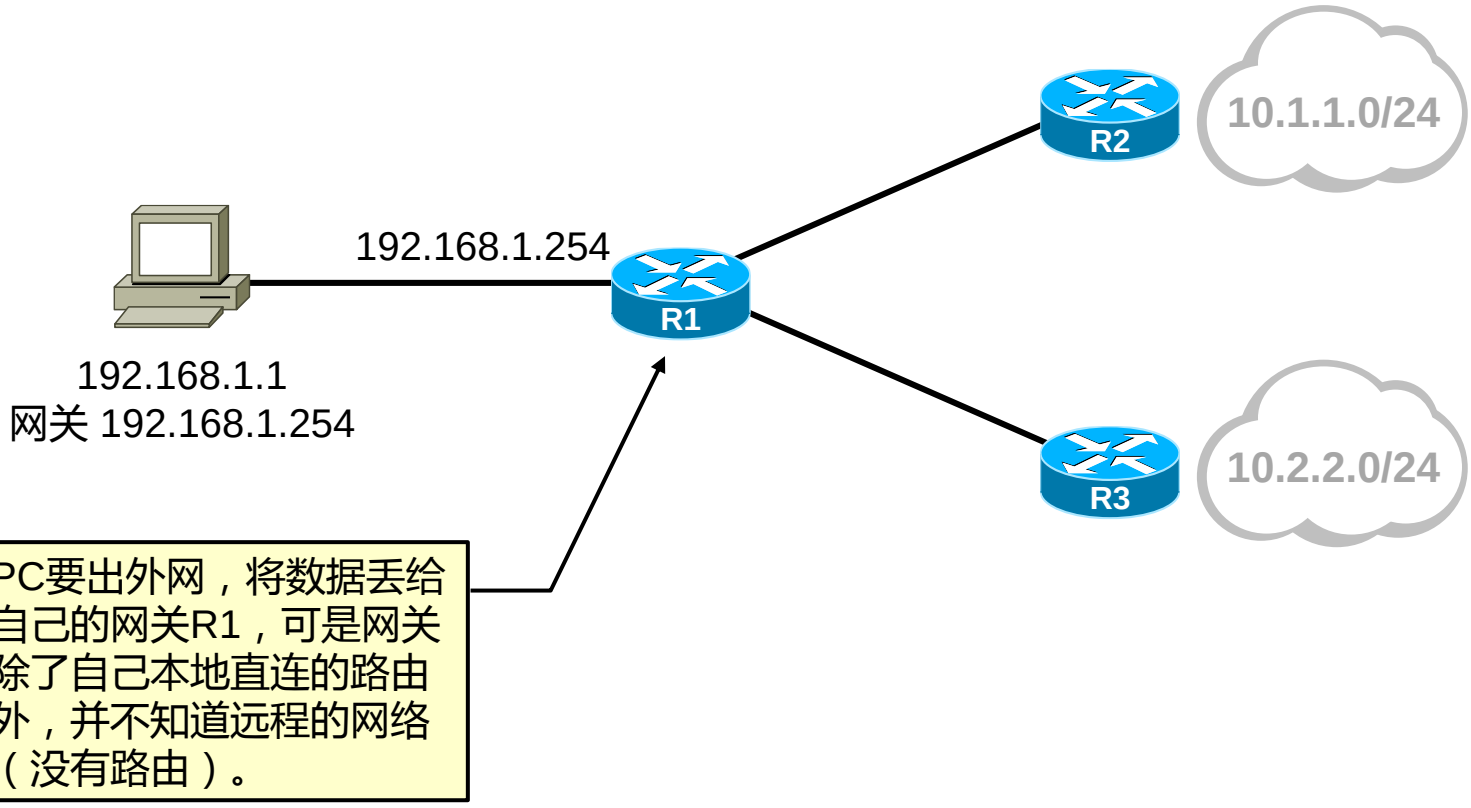
AD值越小越优先

Routing Protocols	AD	备注
直连接口	0	
关联出接口的静态路由	1	Metric =0
关联下一跳的静态路由	1	Metric =0
EIGRP 汇总路由	5	
外部 BGP	20	
内部EIGRP	90	
IGRP	100	
OSPF	110	
RIPv1、v2	120	
外部EIGRP	170	
内部BGP	200	

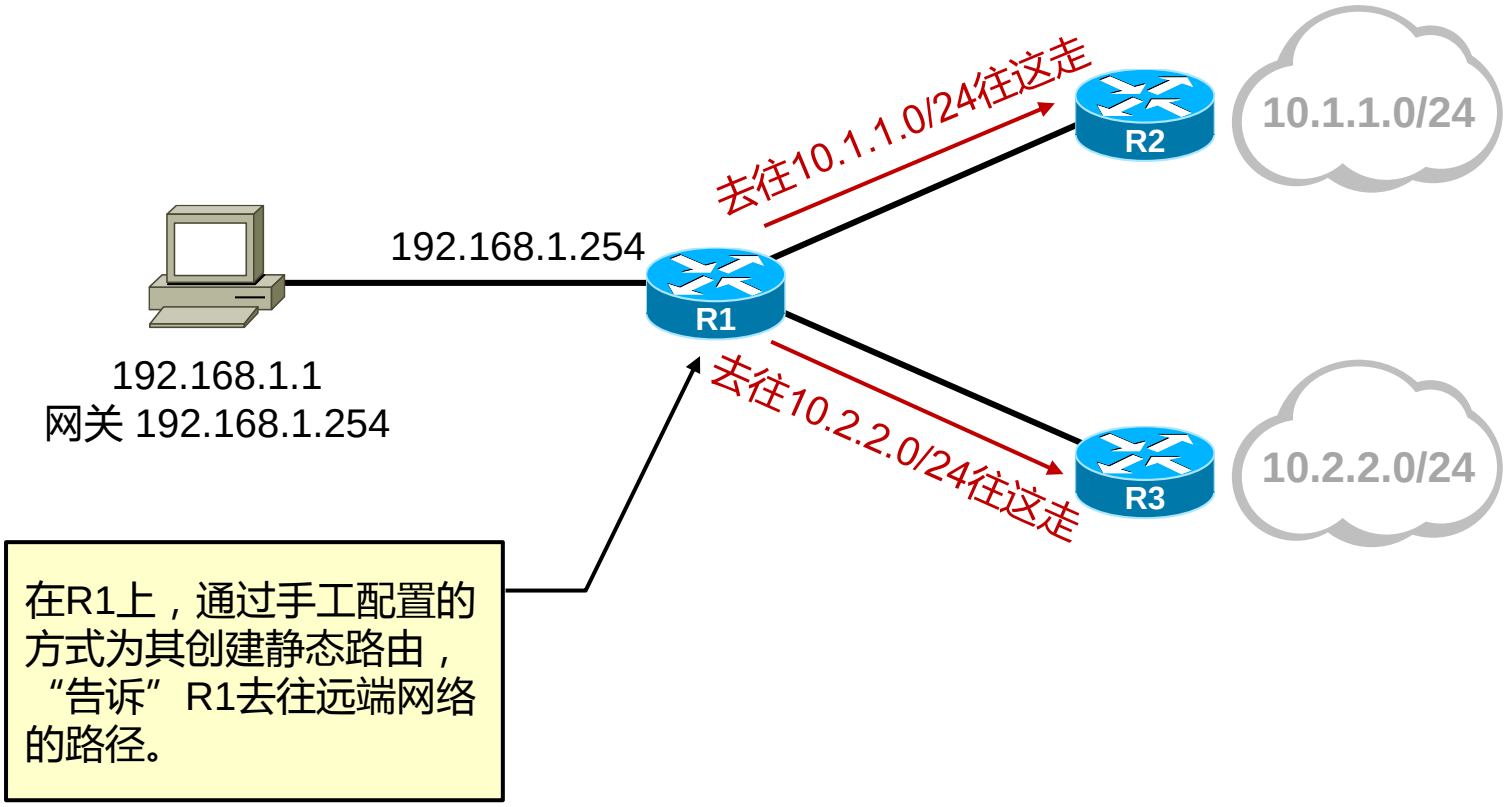
静态路由

- 静态路由的概念
- 静态路由的配置
- 缺省路由
- 静态路由配置示例及解析

什么是静态路由


10.1.1.0/24
R2
192.168.1.254
R1
192.168.1.1
网关 192.168.1.254
R3
10.2.2.0/24
PC要出外网，将数据丢给自己的网关R1，可是网关除了自己本地直连的路由外，并不知道远程的网络（没有路由）。

什么是静态路由


去往10.1.1.0/24往这走
R2
10.1.1.0/24
192.168.1.254
R1
192.168.1.1
网关 192.168.1.254
去往10.2.2.0/24往这走
R3
10.2.2.0/24
在R1上，通过手工配置的方式为其创建静态路由，“告诉”R1去往远端网络的路径。

静态路由的特点

- 需要通过手工的方式进行添加及维护；
- 适用于组网规模较小的场景，如果网络规模较大，则配置及维护的成本就会很高；
- 无法根据拓扑的变化进行动态的响应（各厂商开发了扩展特性，以便弥补静态路由在这点上的不足）；
- 在大型的网络中，往往采用动、静态路由结合的方式进行部署。

静态路由的配置

静态路由配置命令：

R1(config)# ip route *network-address subnet-mask {ip-add | exit-interface}*

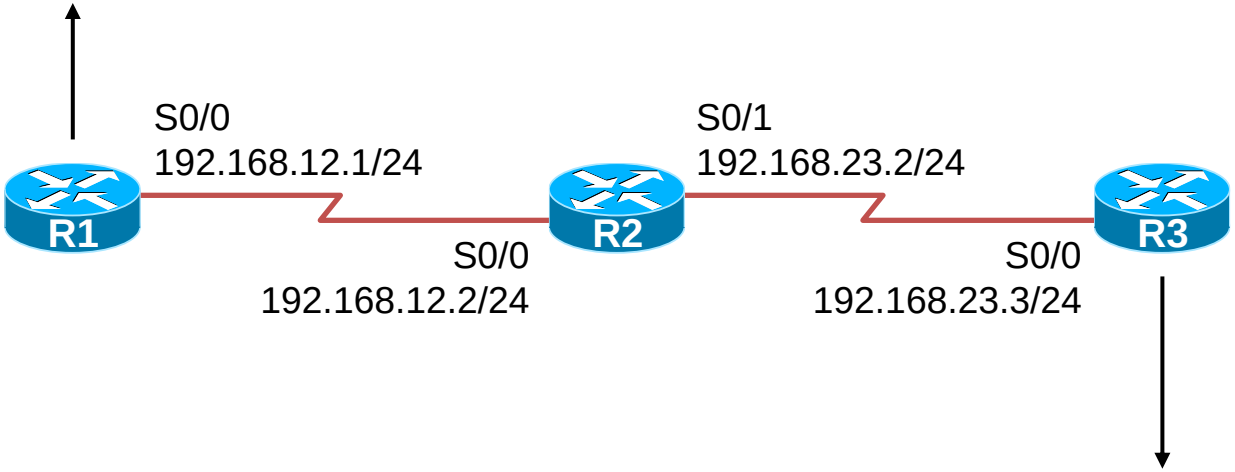
配置示例：

R1(config)# ip route *192.168.1.0 255.255.255.0 192.168.12.2*

R1(config)# ip route *192.168.1.0 255.255.255.0 serial 0*

静态路由的配置

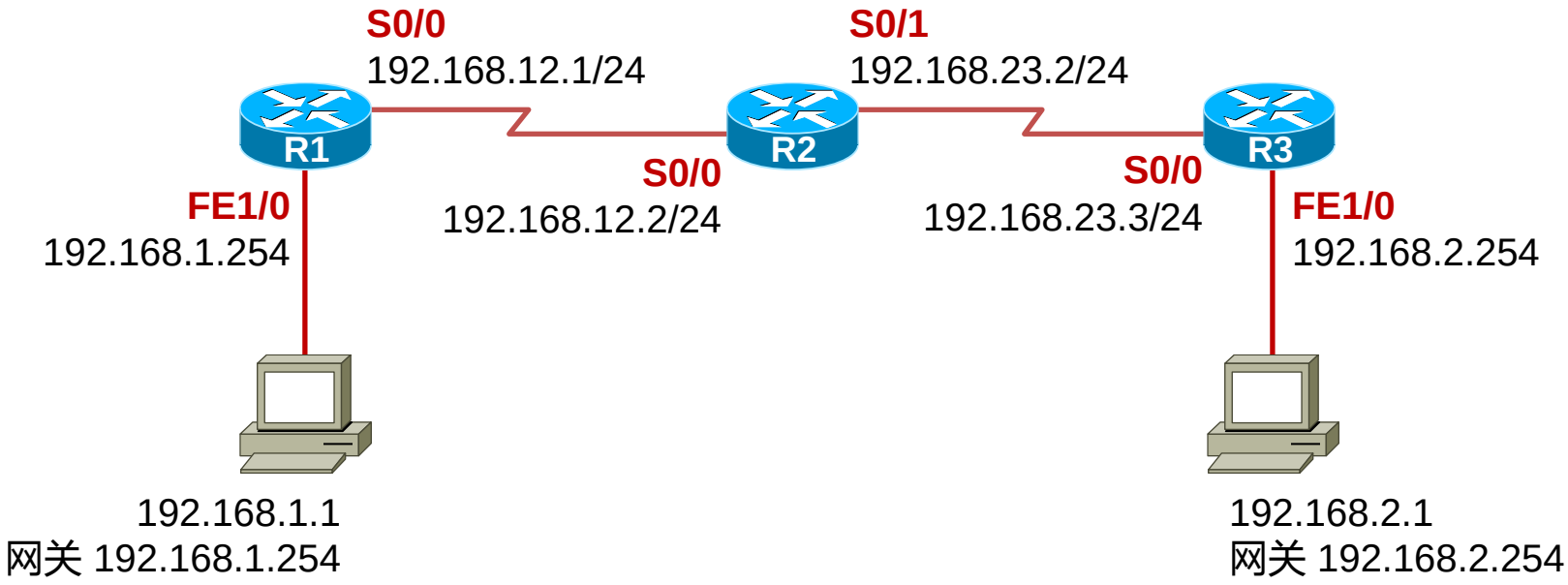
R1(config)# ip route 192.168.23.0 255.255.255.0 192.168.12.2



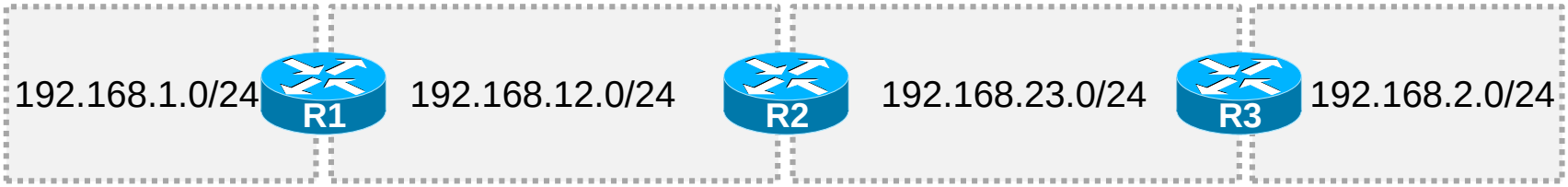
R3(config)# ip route 192.168.12.0 255.255.255.0 serial0/0

注意：通信是双向的，因此要留意往返流量（的路由）

静态路由的配置及解析



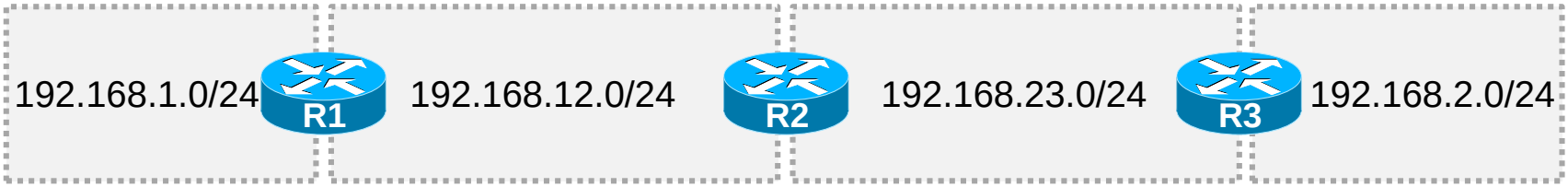
静态路由的配置及解析



协议	目的网络号	出接口	下一跳
C	192.168.1.0/24	FE1/0	-
C	192.168.12.0/24	S0/0	-

怎么去192.168.23.0及2.0？

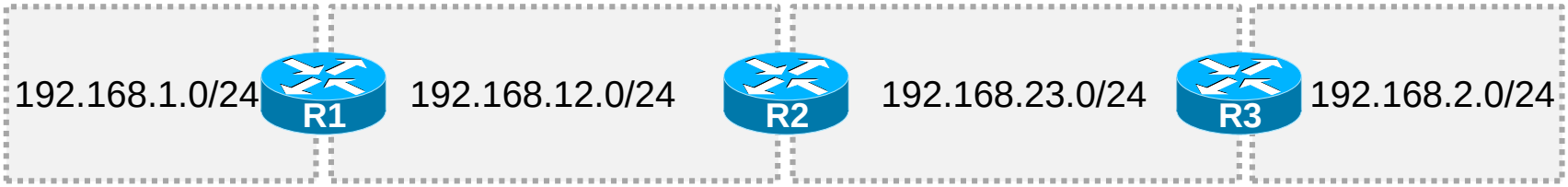
静态路由的配置及解析



协议	目的网络号	出接口	下一跳
C	192.168.1.0/24	FE1/0	-
C	192.168.12.0/24	S0/0	-
S	192.168.23.0/24	S0/0	192.168.12.2
S	192.168.2.0/24	S0/0	192.168.12.2

通过静态路由，告诉R1
该如何去往这两个网段

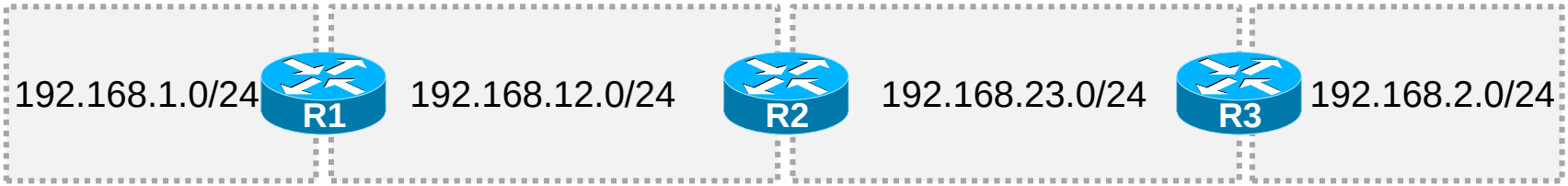
静态路由的配置及解析



协议	目的网络号	出接口	下一跳
C	192.168.12.0/24	S0/0	-
C	192.168.23.0/24	S0/1	-
S	192.168.1.0/24	S0/0	192.168.12.1
S	192.168.2.0/24	S0/1	192.168.23.3

通过静态路由，告诉R2
该如何去往这两个网段

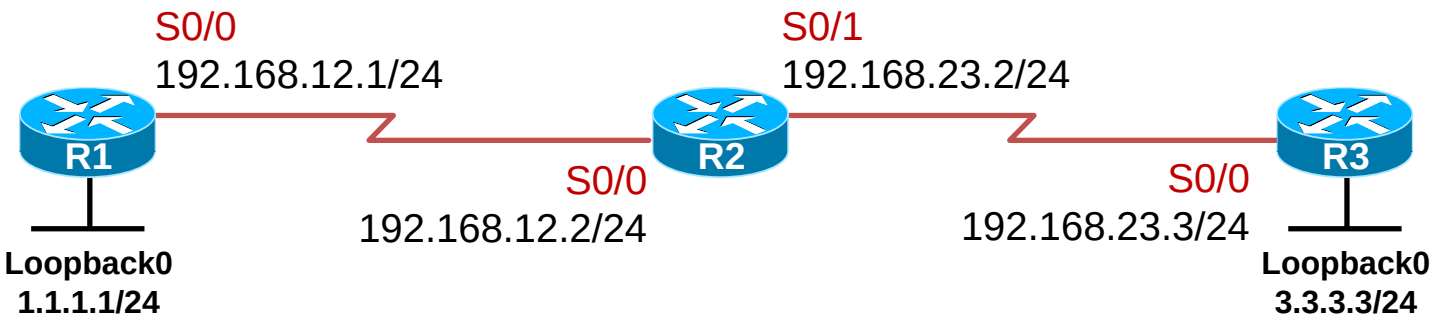
静态路由的配置及解析



通过静态路由，告诉R3
该如何去往这两个网段

协议	目的网络号	出接口	下一跳
C	192.168.2.0/24	FE1/0	-
C	192.168.23.0/24	S0/0	-
S	192.168.12.0/24	S0/0	192.168.23.2
S	192.168.1.0/24	S0/0	192.168.23.2

Loopback接口

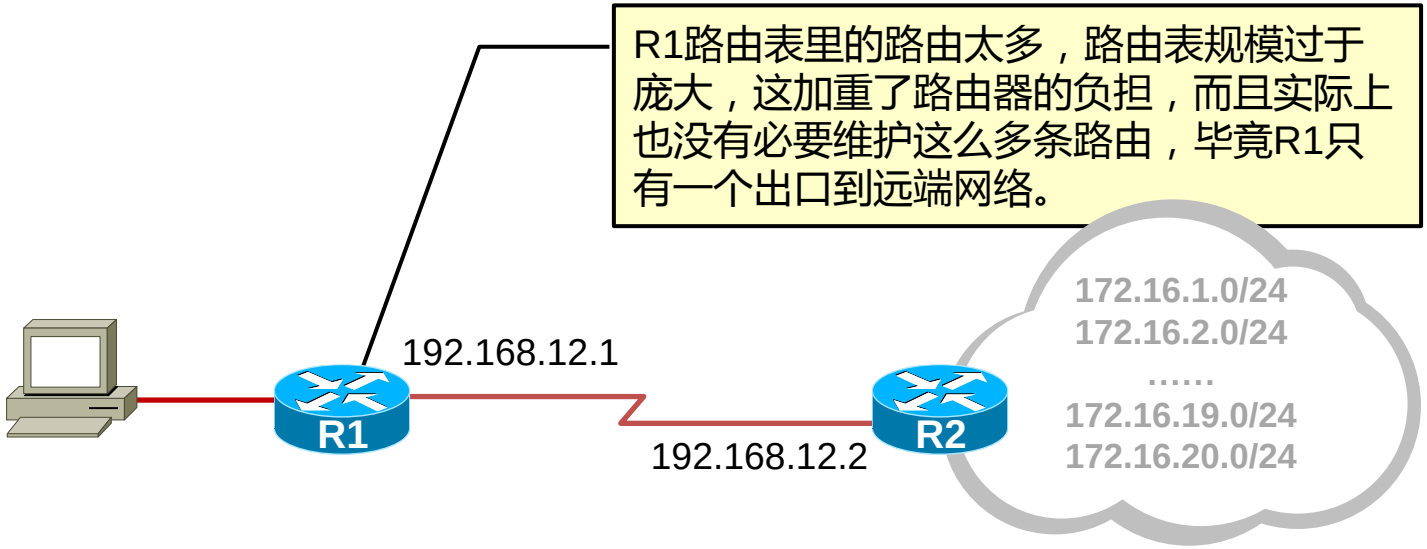



```
Interface loopback 0
 ip address 1.1.1.1 255.255.255.0
```

Loopback接口

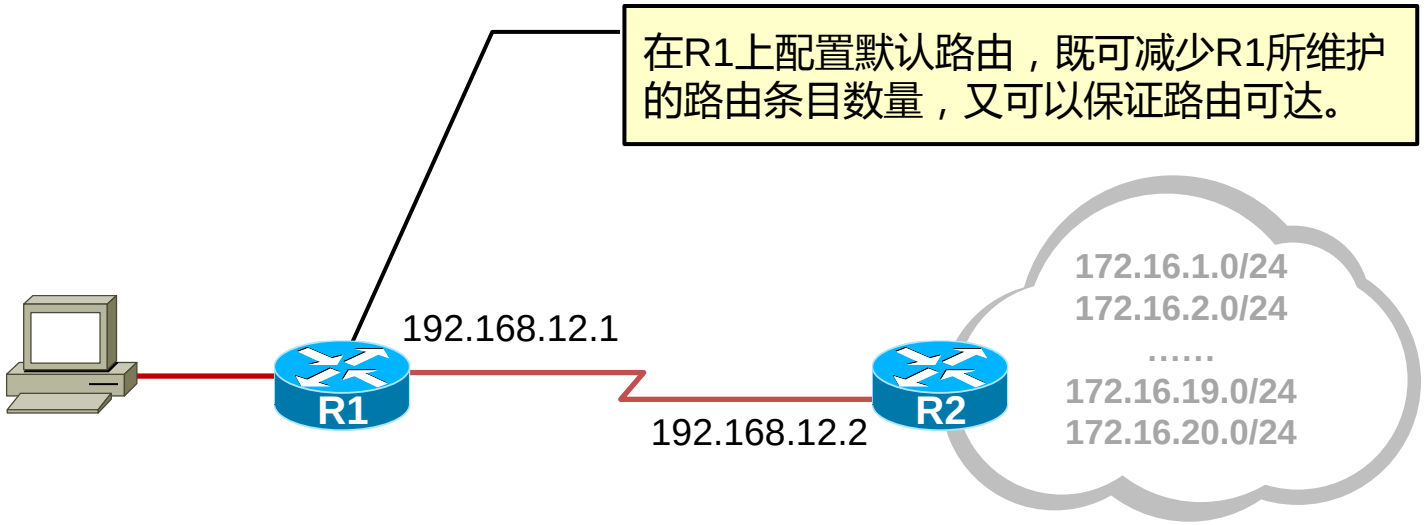
- Loopback接口，也叫环回口，是一个逻辑的、虚拟的接口；
- 使用全局配置命令 interface loopback 加上接口编号可创建一个Loopback接口，创建完成后即可为接口配置IP地址；
- Loopback接口在手工创建后，除非人为shutdown，否则不会DOWN掉；
- Loopback接口常用于：
  - 模拟路由器的直连网段，可用于测试；
  - 可用于设备管理（Loopback接口比较稳定）；
  - 供其他协议使用，例如OSPF、BGP、MPLS等；
  - SNMP Traps消息的源地址；
  - 其他用途（Loopback接口的用途十分广泛）。

缺省路由（默认路由）




```
R1(config)# ip route 172.16.1.0 255.255.255.0 192.168.12.2
R1(config)# ip route 172.16.2.0 255.255.255.0 192.168.12.2
R1(config)# …
R1(config)# ip route 172.16.20.0 255.255.255.0 192.168.12.2
```

缺省路由（默认路由）



R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.12.2

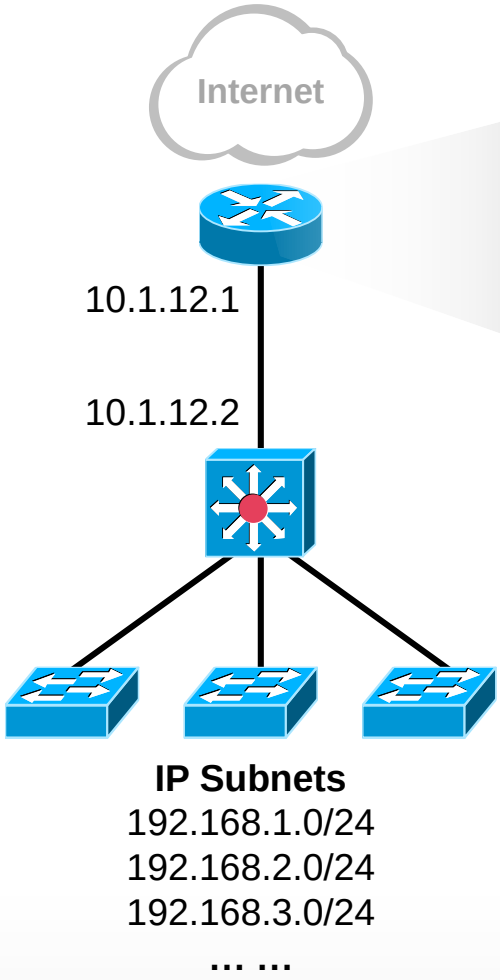
维护及故障排查常用命令

- Ping– 测试连通性
- Traceroute– 追踪到达目标沿途中的每一跳
- Show ip route– 显示路由表
- Show ip interface brief– 接口消息IP信息摘要
- Show cdp neighbors detail– 用于搜集CDP邻居信息

红茶三杯
Vinsoney

路由汇总

技术背景



Ip route 0.0.0.0 0.0.0.0 202.101.100.2

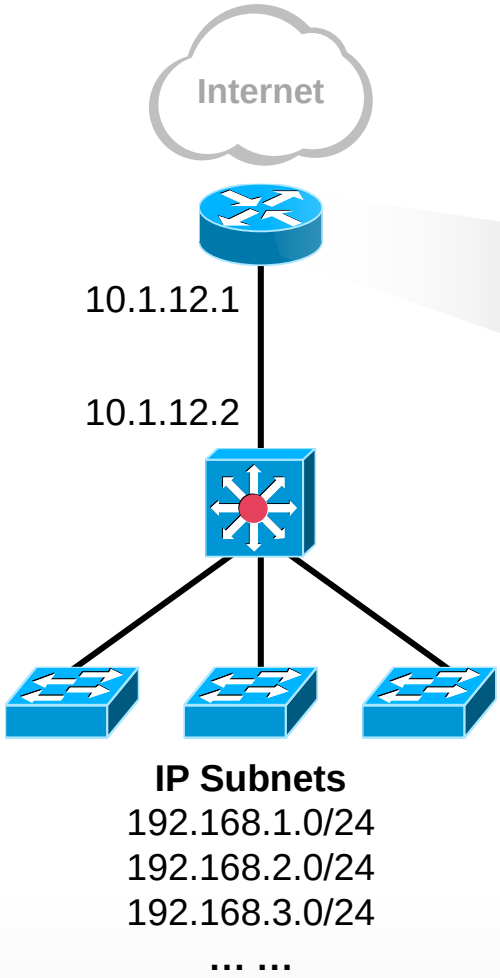
Ip route 192.168.1.0 255.255.255.0 10.1.12.2

Ip route 192.168.2.0 255.255.255.0 10.1.12.2

Ip route 192.168.3.0 255.255.255.0 10.1.12.2

路由表条目太多，这些路由前缀是有“共性”的，而且下一跳地址都相同，有何办法优化?

路由汇总 Route Summarization

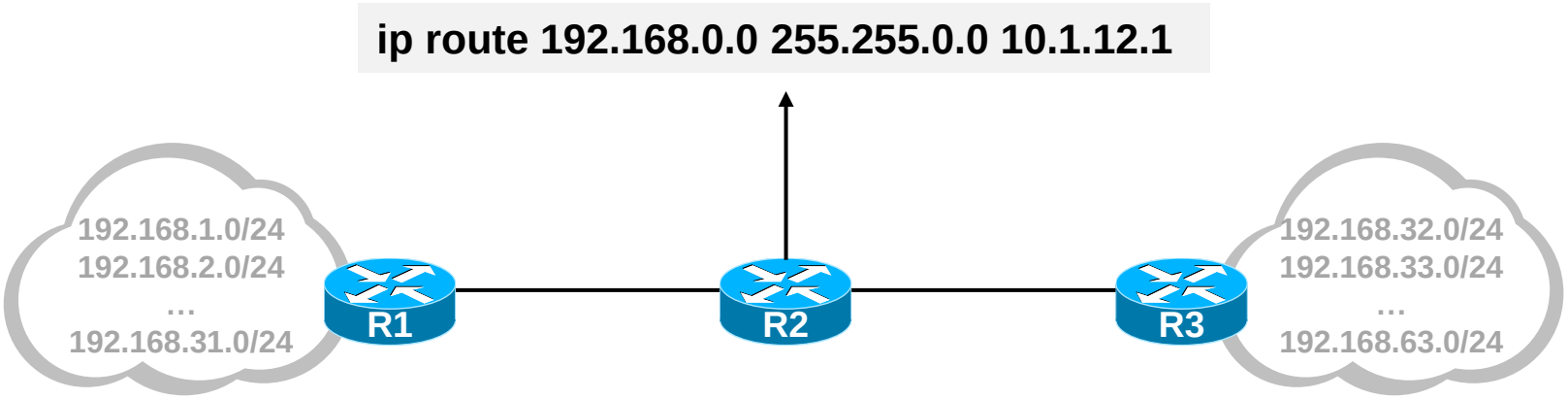


Ip route 0.0.0.0 0.0.0.0 202.101.100.2

Ip route 192.168.0.0 255.255.0.0 10.1.12.2

使用路由汇总之后，网络可达性满足的情况下，路由表的条目数量也大大减少了，路由器的资源消耗也就更小

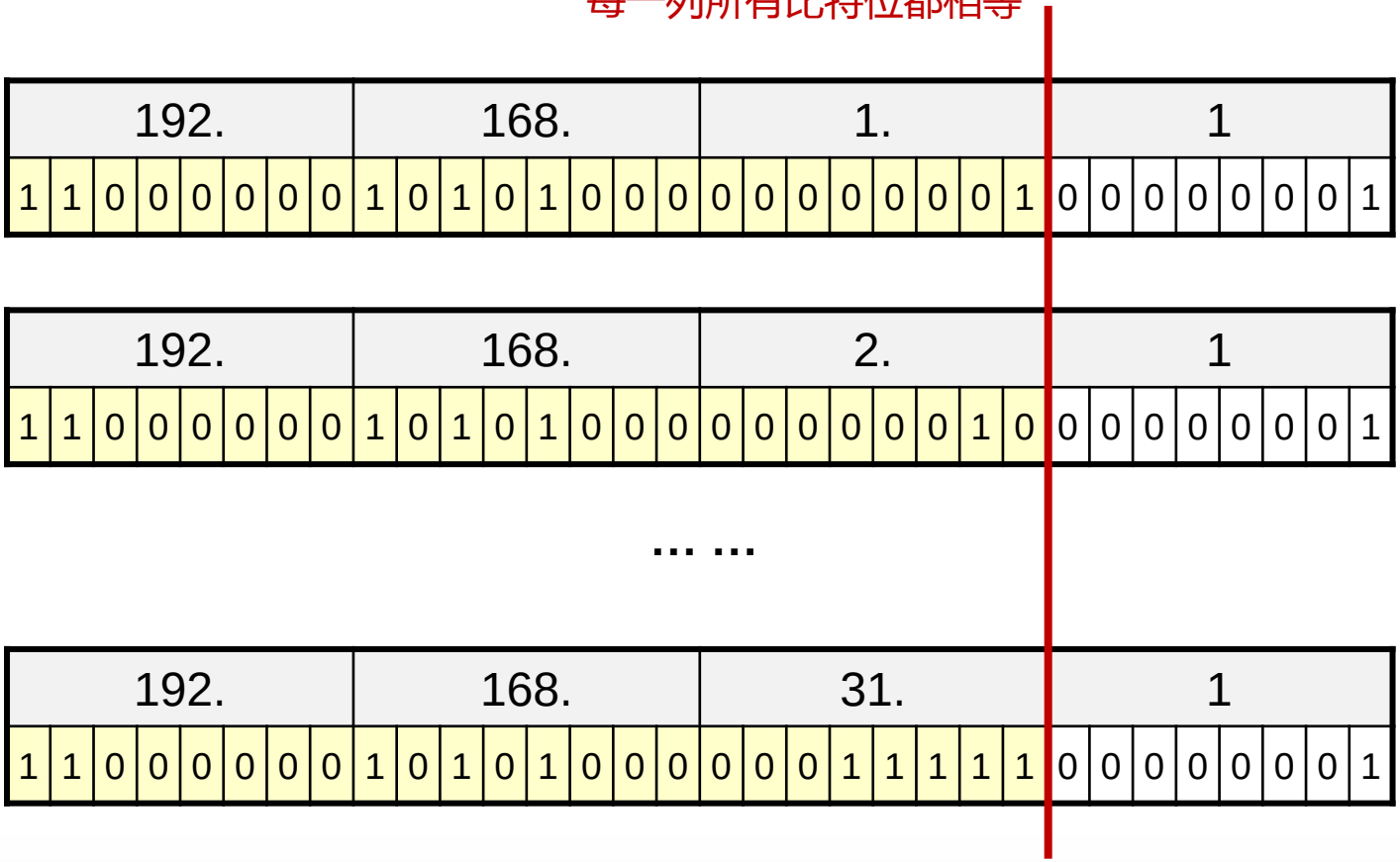
路由汇总的原则



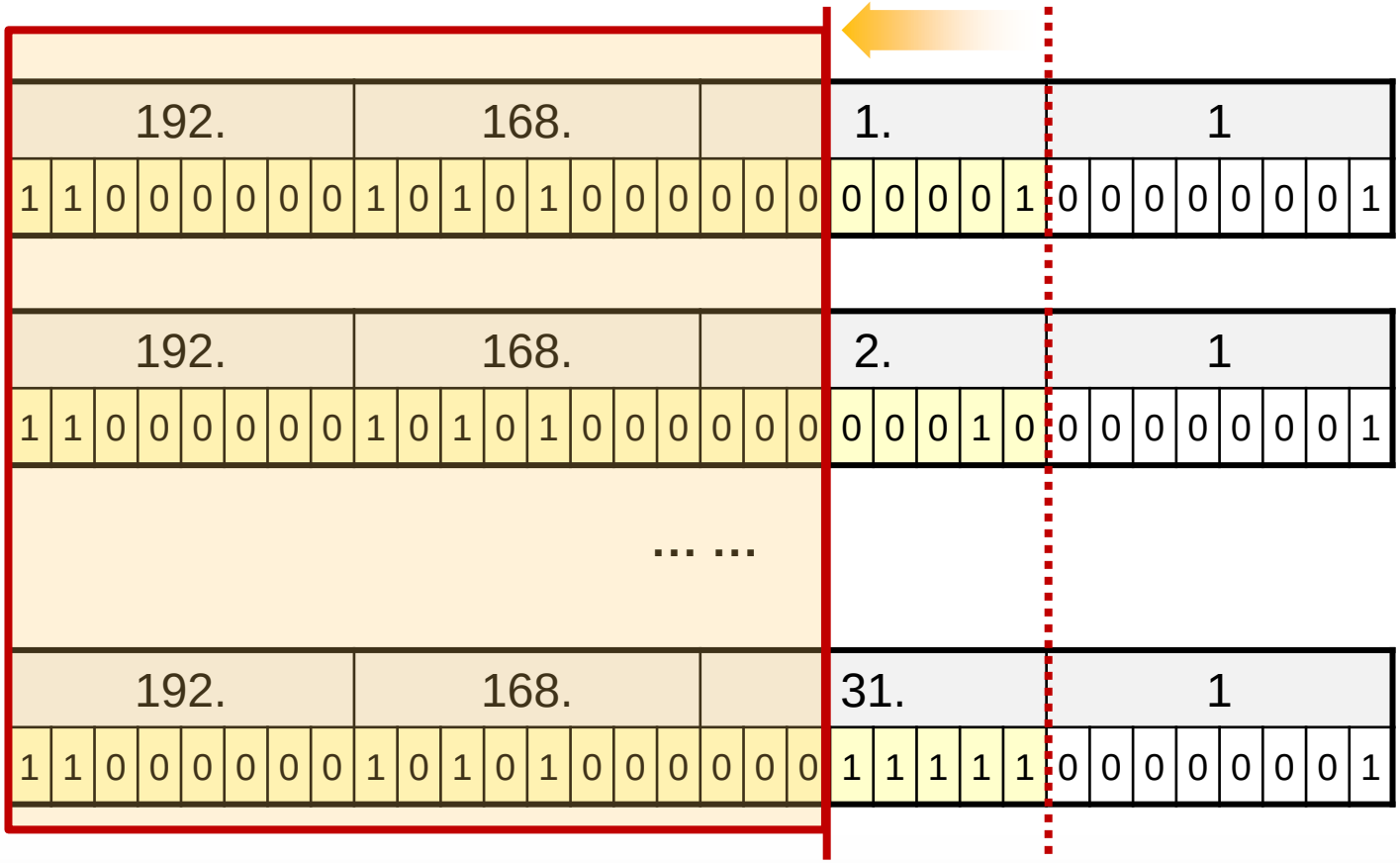
R2的这条汇总路由太“粗犷”，将R3这一侧的网络也“囊括”在内，这可能导致数据的转发出现问题。因此汇总路由的书写需紧凑、精确。

汇总路由的计算

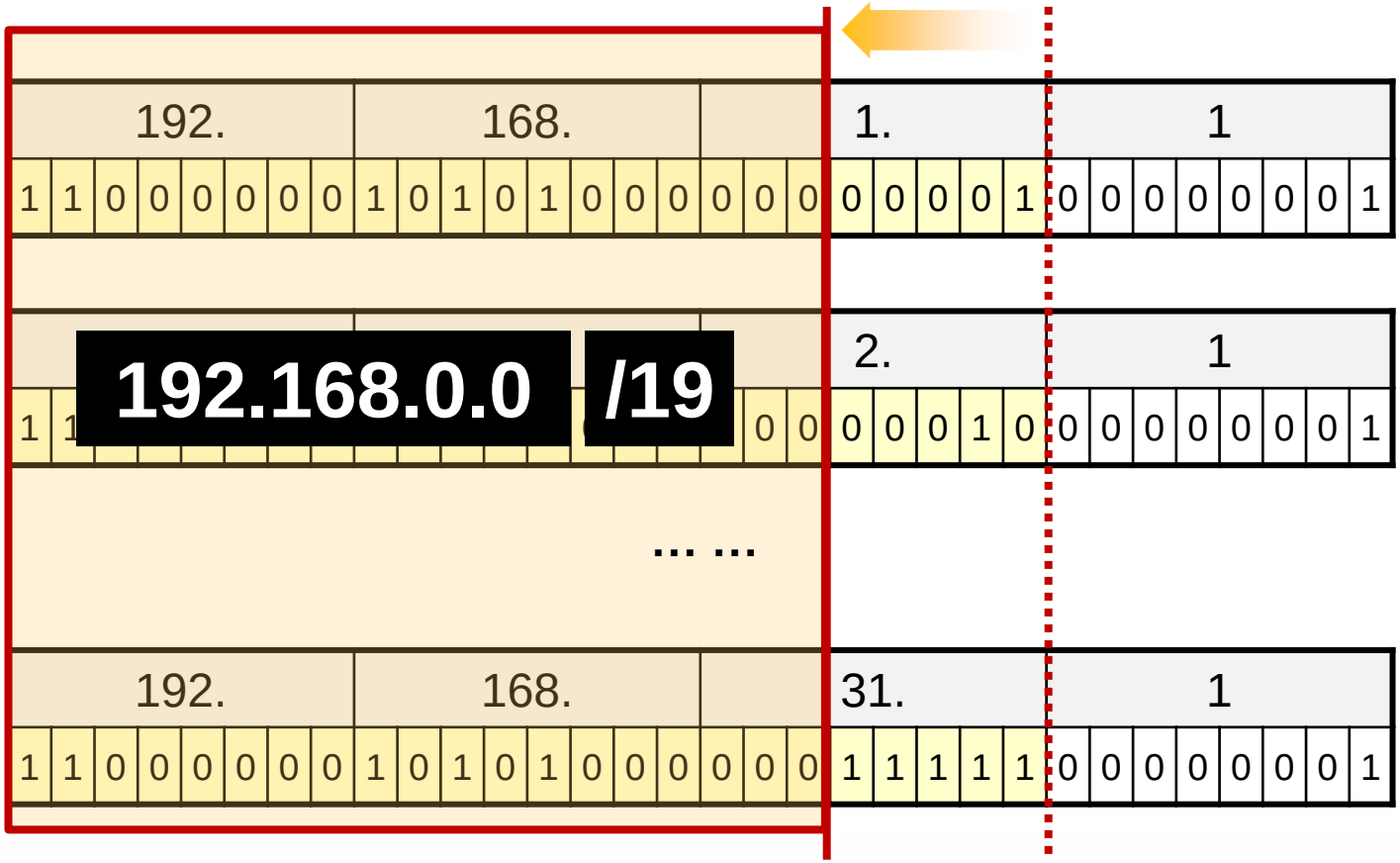
从默认掩码/24开始，向左移，直到分割线左侧的每一列所有比特位都相等



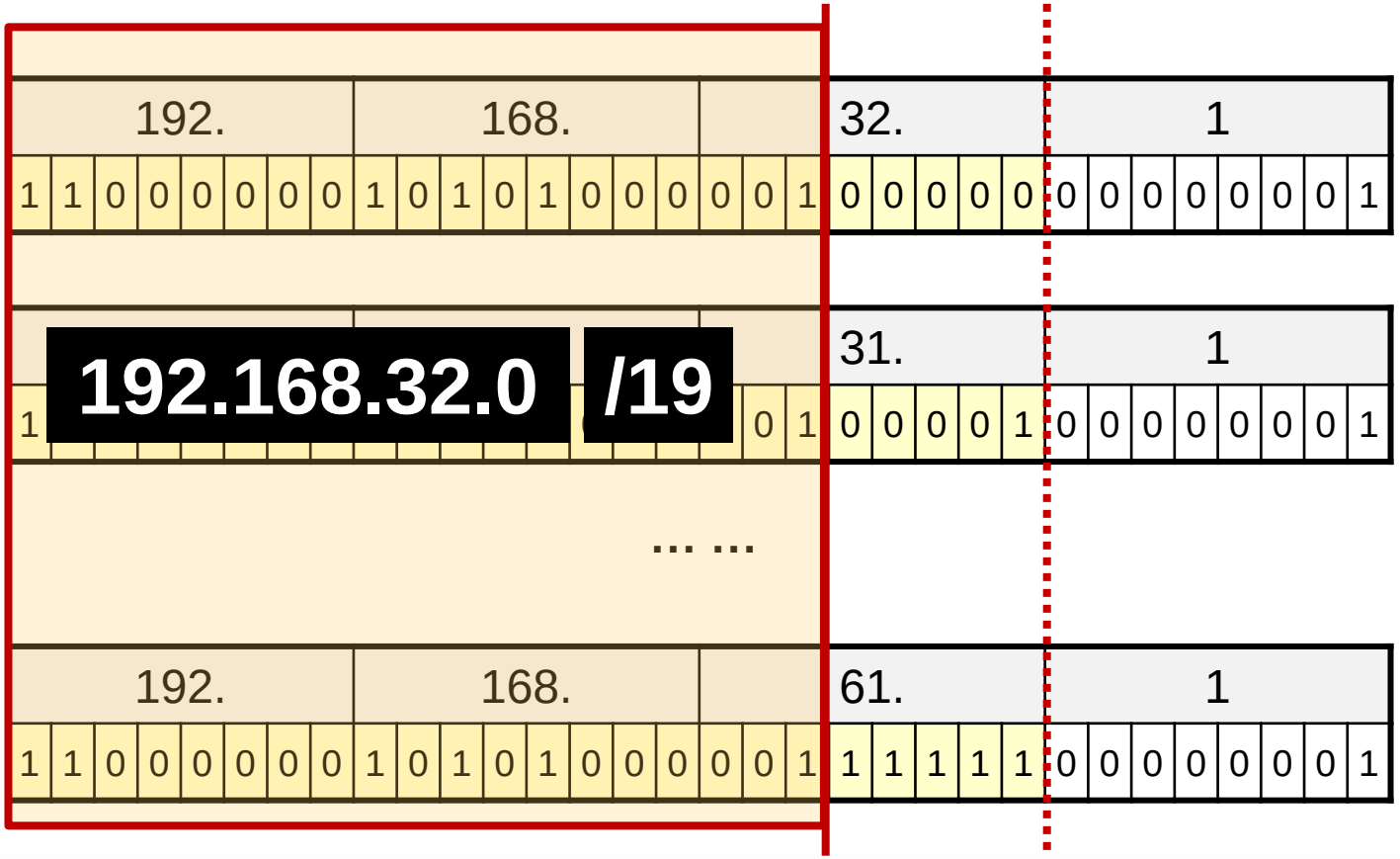
汇总路由的计算



汇总路由的计算



练习 192.168.32.0/24 至 192.168.63.0/24



路由汇总小结

- 路由汇总作为一种网络优化手段被广泛运用在各种网络中
- 在网络设备上部署路由汇总既能保证网络的可达性，同时减少设备为维护庞大路由表、以及路由计算所消耗的资源
- 路由汇总其实是网络号与网络掩码的技巧
- 在实际组网中往往是根据明细子网的需求反推汇总路由。也就是说路由汇总在网络规划阶段就应该考虑，而不是网络组建完成后
- 部署路由汇总时需谨慎，否则容易产生数据环路

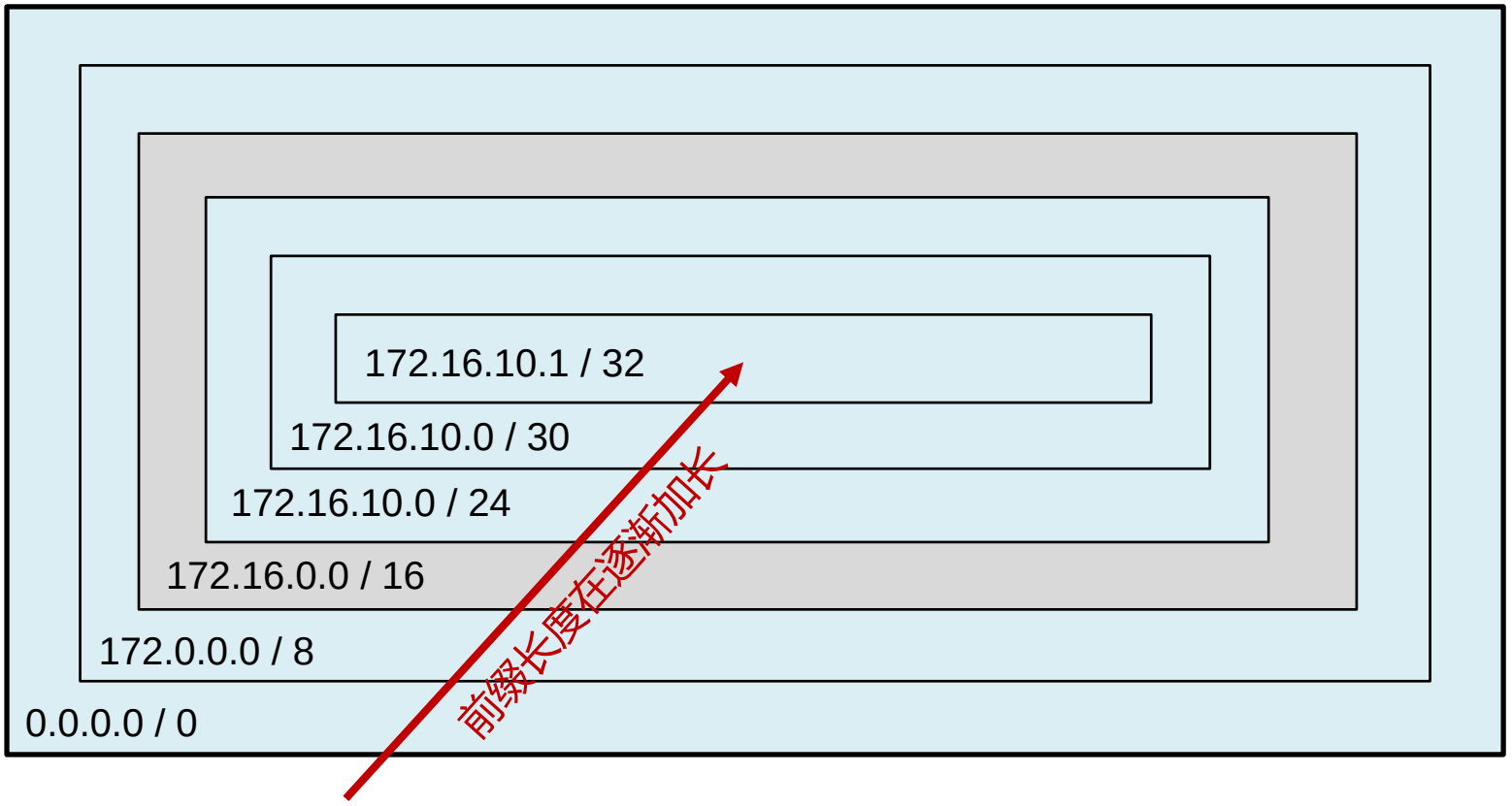
最长匹配原则

几种类型的路由

- 主机路由
- 子网路由
- 汇总路由（一组子网）
- 主类网络号
- 超网（CIDR）
- 缺省路由（默认路由）

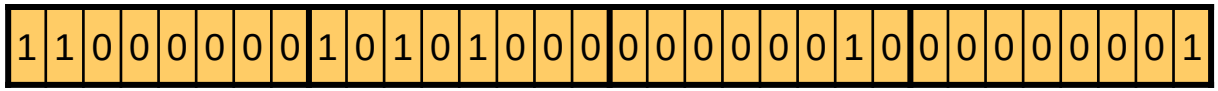
192.168.1.0 **/24**

最长匹配原则

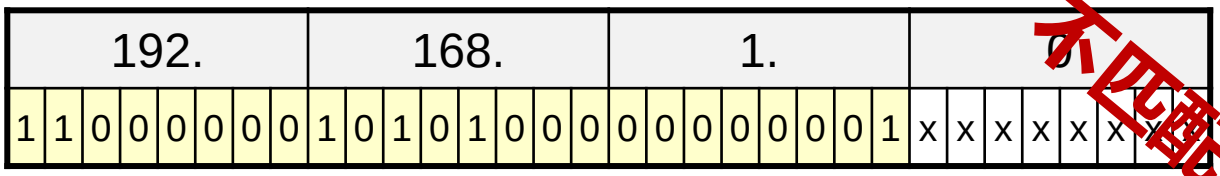

172.16.10.1 / 32
172.16.10.0 / 30
172.16.10.0 / 24
172.16.0.0 / 16
172.0.0.0 / 8
0.0.0.0 / 0
前缀长度在逐渐加长

最长匹配原则

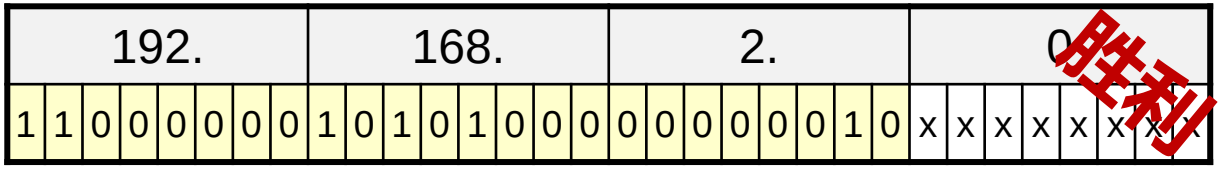
数据包目的IP：192.168.2.1



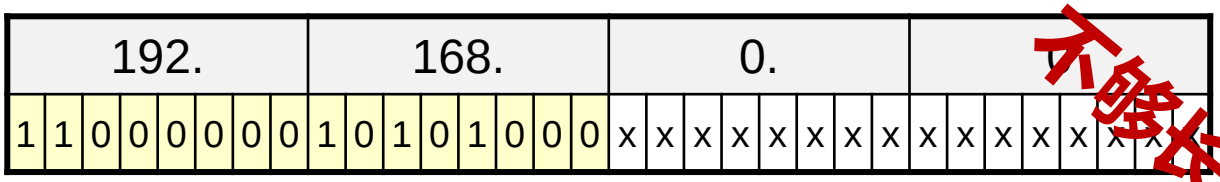
路由前缀1
192.168.1.0/24



路由前缀2
192.168.2.0/24



路由前缀3
192.168.0.0/16



小结

- 路由条目包括目的网络号及掩码，两者缺一不可，网络号或者掩码不相同，则为不同的路由条目；
- 一般来说，当路由器同时从多种不同的途径获取到去往同一个目的网络的路由，则先比较这些路由来源的AD值（管理距离），优选AD值最小路由，如果路由来自相同的途径（例如来自同种路由协议），则再比较度量值；
- 默认情况下，路由的查询遵循最长匹配原则；
- 路由查询的行为是逐跳的，到目标网络的沿途每个路由器都必须有关于该目标网段的路由信息；
- 绝大部分数据通信行为是双向的，考虑流量的时候，要关注流量的往返。

红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You

红茶三杯
Vinsoney

学习 沉淀 成长 分享

动态路由协议、RIP

红茶三杯（朱SIR）微博：http://t.sina.com/vinsoney

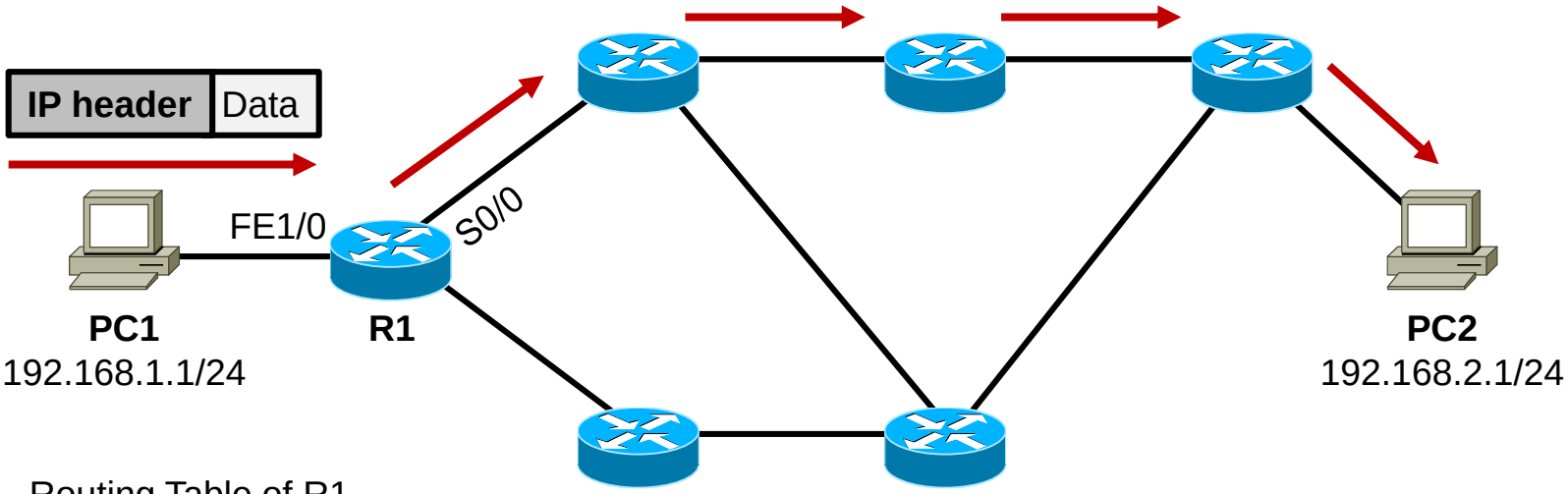
Latest update: 2012-06-01

Content

动态路由协议概述

- 什么是路由
- 什么是动态路由协议
- 动态路由协议的分类

什么是路由



Routing Table of R1

Protocol	Network	Exit Intf
Connected	192.168.1.0/24	FE1/0
Connected	192.168.12.0/24	S0/0
RIP	192.168.2.0/24	S0/0

什么是路由

> 当路由器（或其他三层设备）收到一个IP数据包时，会在路由表中查询数据包的目的IP地址，在找到最匹配的路由表项后，将数据包按照这个表项所指示的下一跳IP地址或出接口去转发。

查看IP路由表

R1# show ip route

Gateway of last resort is not set

2.0.0.0/24 is subnetted, 1 subnets

O 2.2.2.0 [110/65] via 9.9.12.2, 00:00:02, Serial0/0

9.0.0.0/24 is subnetted, 1 subnets

C 9.9.12.0 is directly connected, Serial0/0

路由协议的分类

静态路由

根据数据访问需求手工在每台设备上进行静态路由条目的创建。

动态路由协议

路由器自动进行路由或用于路由计算的相关信息的更新和同步，并且当网络拓扑变更时，能够动态收敛。

```
R1# show ip route
2.0.0.0/24 is subnetted, 1 subnets
O       2.2.2.0 [110/65] via 9.9.12.2, 00:00:02, Serial0/0
        9.0.0.0/24 is subnetted, 1 subnets
C       9.9.12.0 is directly connected, Serial0/0
```

动态路由协议的分类

按工作区域分类

IGP (Interior Gateway Protocols)
内部网关协议

RIP | OSPF | EIGRP | IS-IS

EGP (Exterior Gateway Protocols))
外部网关协议

BGP

按工作机制及算法分类

(Distance Vector Routing Protocols)
距离矢量路由协议

RIP | IGRP | EIGRP (高级)

(Link-State Routing Protocol)
链路状态路由协议

OSPF | IS-IS

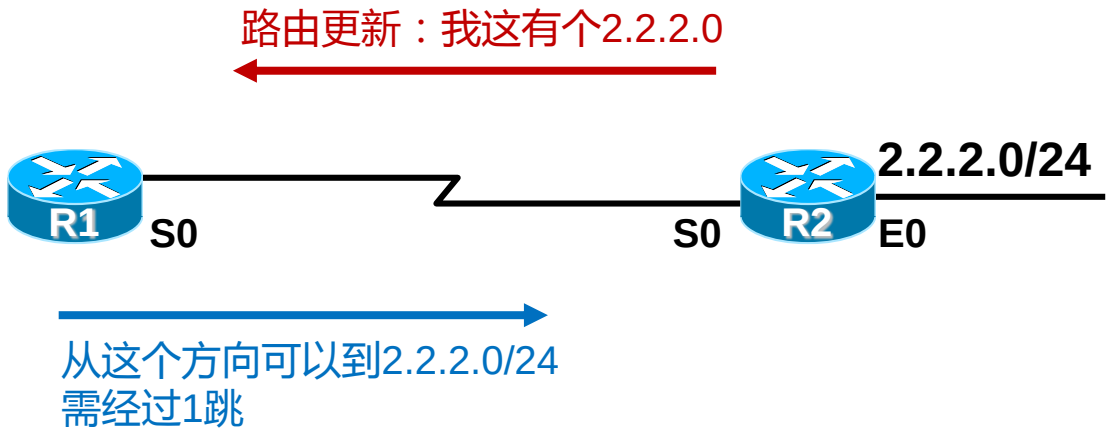
红茶三杯
Vinsoney

RIP

- 距离矢量路由协议概述
- RIP概述
- RIP路由更新过程
- 路由环路的产生及避免
- RIP基本配置

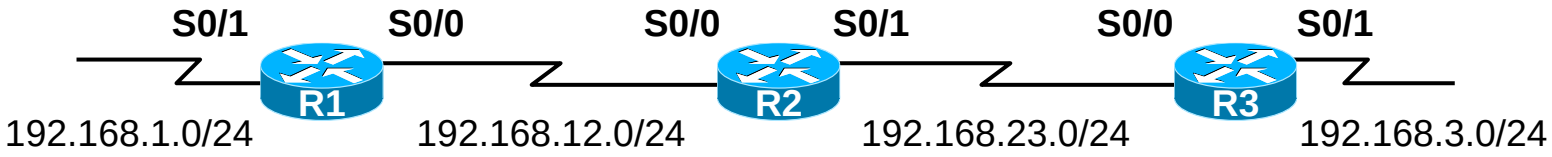
距离矢量路由选择协议

- 使用距离矢量路由协议的路由器并不了解网络的拓扑。该路由器只知道：
  - 自身与目的网络之间的距离
  - 应该往哪个方向或使用哪个接口转发数据包



距离矢量路由选择协议

- **直连路由写入路由表**



R1的路由表

192.168.12.0/24	S0/0	0
192.168.1.0/24	S0/1	0

R2的路由表

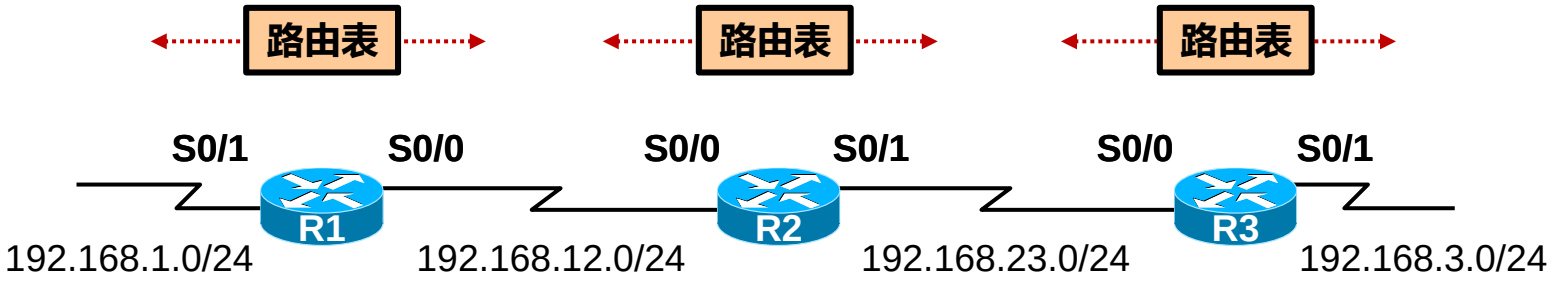
192.168.12.0/24	S0/0	0
192.168.23.0/24	S0/1	0

R3的路由表

192.168.23.0/24	S0/0	0
192.168.3.0/24	S0/1	0

距离矢量路由选择协议

- **初次路由信息交换**



R1的路由表

192.168.12.0/24	S0/0	0
192.168.1.0/24	S0/1	0
192.168.23.0/24	S0/0	1

R2的路由表

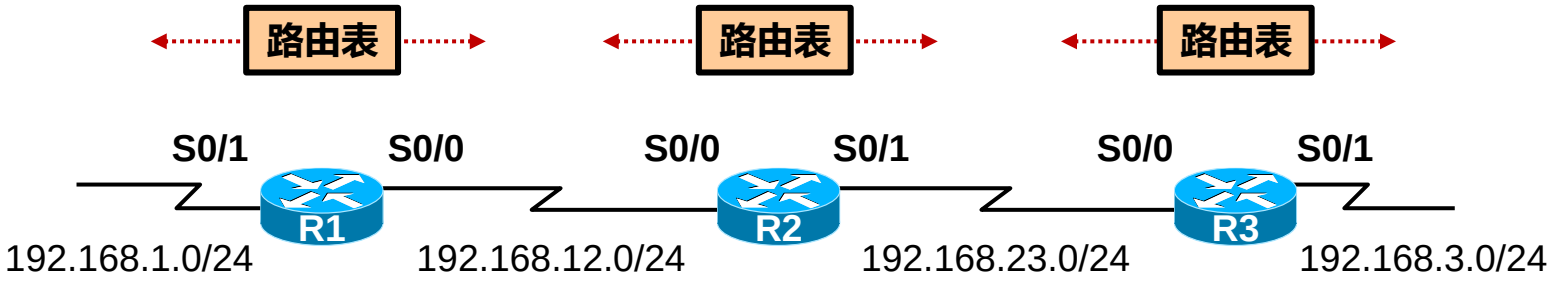
192.168.12.0/24	S0/0	0
192.168.23.0/24	S0/1	0
192.168.1.0/24	S0/0	1
192.168.3.0/24	S0/1	1

R3的路由表

192.168.23.0/24	S0/0	0
192.168.3.0/24	S0/1	0
192.168.12.0/24	S0/0	1

距离矢量路由选择协议

- **下一个更新周期到来**



R1的路由表

192.168.12.0/24	S0/0	0
192.168.1.0/24	S0/1	0
192.168.23.0/24	S0/0	1
192.168.3.0/24	S0/0	2

R2的路由表

192.168.12.0/24	S0/0	0
192.168.23.0/24	S0/1	0
192.168.1.0/24	S0/0	1
192.168.3.0/24	S0/1	1

R3的路由表

192.168.23.0/24	S0/0	0
192.168.3.0/24	S0/1	0
192.168.12.0/24	S0/0	1
192.168.1.0/24	S0/0	2

距离矢量路由选择协议

- **路由器收敛完成**
  - 当所有路由表包含相同网络可达性信息
  - 网络（路由）进入一个稳态
- **路由器继续交换路由信息**
  - 当无新路由信息被更新时收敛结束
  - 网络在达到收敛前无法完全正常工作

Routing Information Protocols

- RIP是应用及开发较早的路由协议，是典型的距离矢量路由协议
- 适用于小型网络，最大跳数15跳（16跳视为不可达）
- RIP是基于UDP的，使用端口号520
- 在CISCO IOS平台上的管理性距离为120

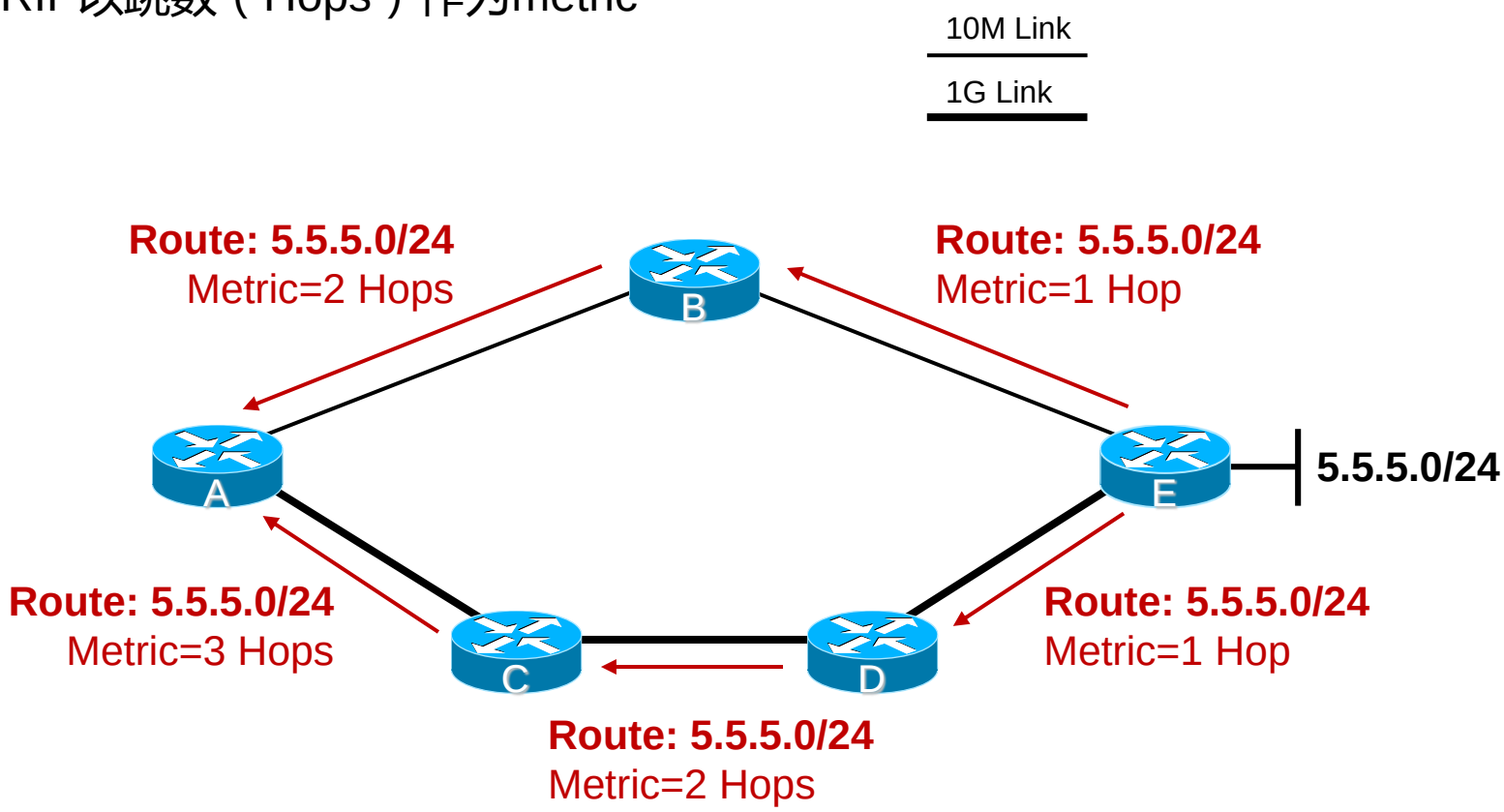
RIP versions

RIPv1	RIPv2
使用广播更新路由表	使用组播更新路由表
有类路由协议	无类路由协议
不支持VLSM	支持VLSM
没有认证功能	有认证功能
不支持手工汇总	支持手工汇总
不支持路由标记（Tag）	支持路由标记功能
更新消息中的路由条目没有Next-hop信息	更新消息中的路由条目含有Next-hop信息

- RIPng是IPv6的RIP

Metric 路由度量值

- RIP以跳数（Hops）作为metric



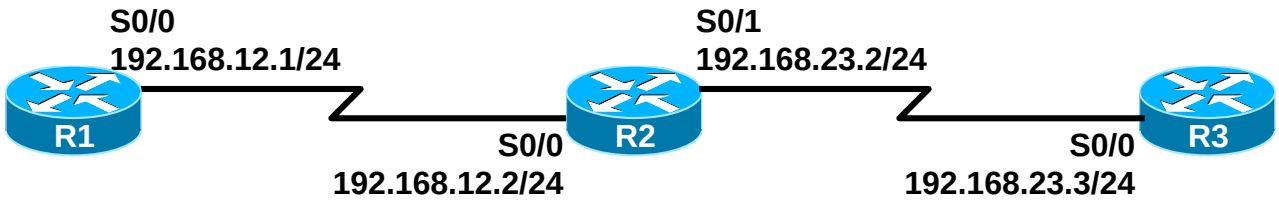
Metric 路由度量值

- RIP度量值的查看

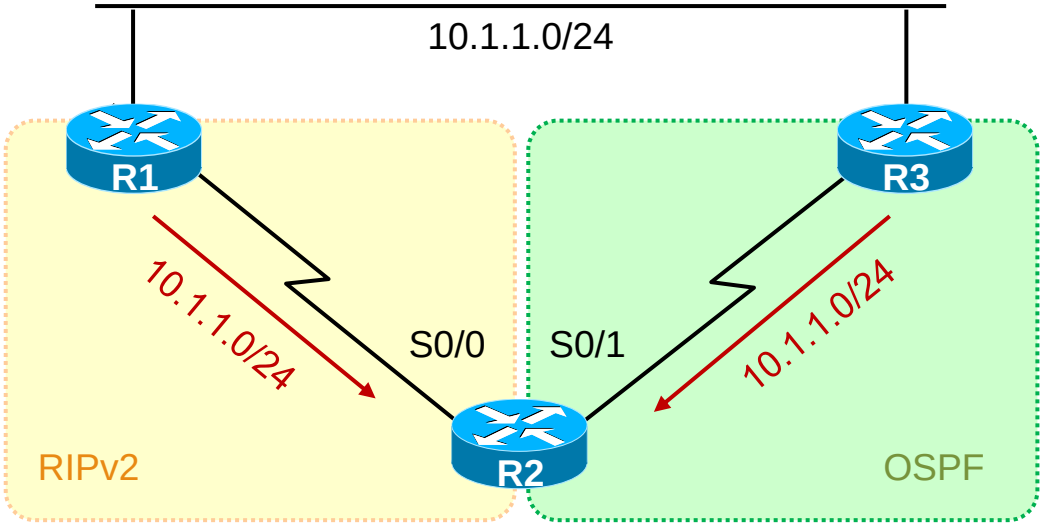
R1# show ip route

```
C    192.168.12.0/24 is directly connected, Serial0/0
R    192.168.23.0/24 [120/1] via 192.168.12.2, 00:00:08, Serial0/0
```

Metric = 1跳



Administrative Distance 管理距离



R2的路由表

Protocol	Network	AD	Exit Intf
OSPF	10.1.1.0/24	110	S0/1

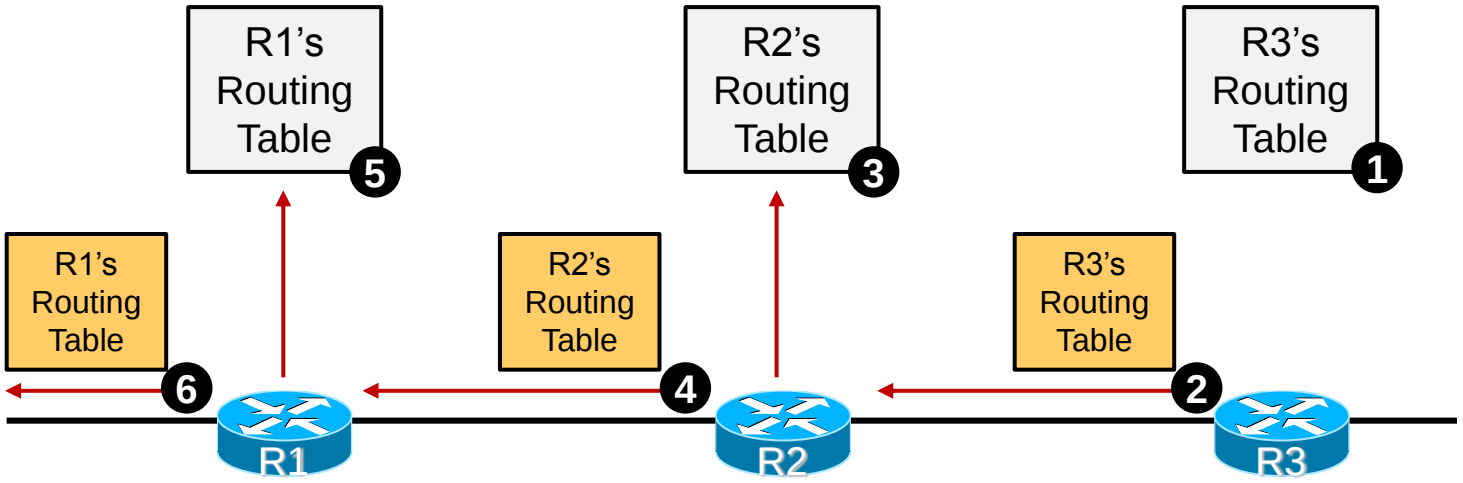
Administrative Distance 管理距离

- 常见的路由协议及其对应的AD值（On Cisco IOS Platform）

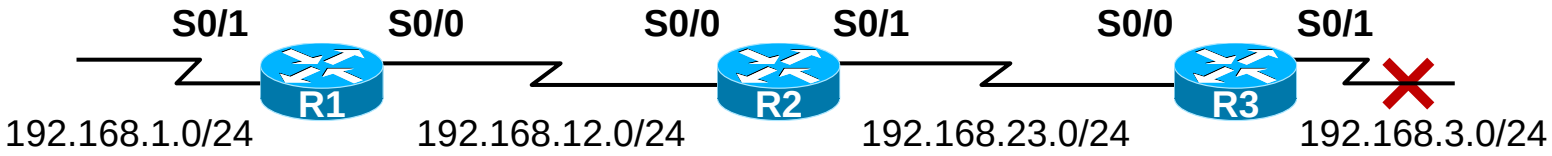
Routing Protocols	AD	备注
直连接口	0	
关联出接口的静态路由	1	Metric =0
关联下一跳的静态路由	1	Metric =0
EIGRP 汇总路由	5	
外部 BGP	20	
内部EIGRP	90	
IGRP	100	
OSPF	110	
RIPv1、v2	120	
外部EIGRP	170	
内部BGP	200	

距离矢量路由选择协议

- 周期性泛洪整张路由表
- 依照传闻的更新
- 逐跳更新



环路的产生



R1的路由表

192.168.12.0/24	S0/0	0
192.168.1.0/24	S0/1	0
192.168.23.0/24	S0/0	1
192.168.3.0/24	S0/0	2

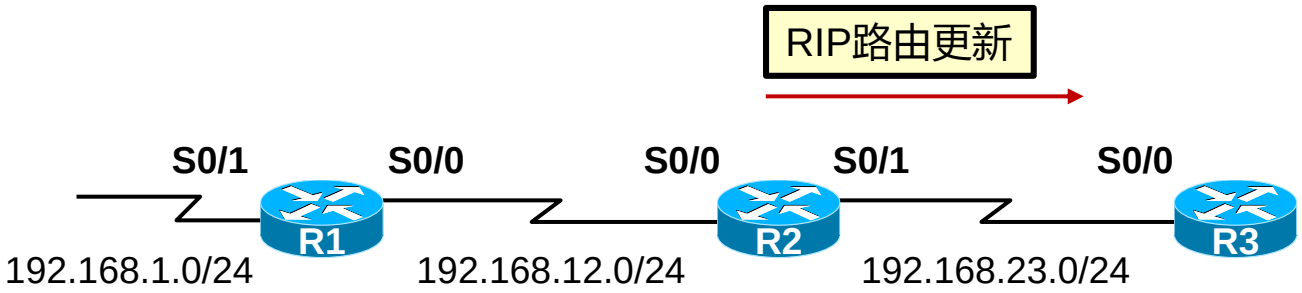
R2的路由表

192.168.12.0/24	S0/0	0
192.168.23.0/24	S0/1	0
192.168.1.0/24	S0/0	1
192.168.3.0/24	S0/1	1

R3的路由表

192.168.23.0/24	S0/0	0
~~192.168.3.0/24~~	~~S0/1~~	~~0~~
192.168.12.0/24	S0/0	1
192.168.1.0/24	S0/0	2

环路的产生



R1的路由表

192.168.12.0/24	S0/0	0
192.168.1.0/24	S0/1	0
192.168.23.0/24	S0/0	1
192.168.2.0/24	S0/0	2

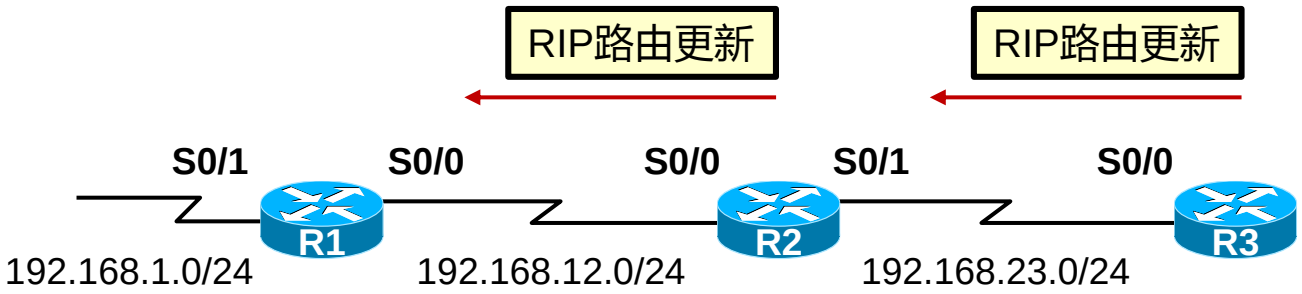
R2的路由表

192.168.12.0/24	S0/0	0
192.168.23.0/24	S0/1	0
192.168.1.0/24	S0/0	1
192.168.2.0/24	S0/1	1

R3的路由表

192.168.23.0/24	S0/0	0
192.168.3.0/24	S0/0	2
192.168.12.0/24	S0/0	1
192.168.1.0/24	S0/0	2

环路的产生



R1的路由表

192.168.12.0/24	S0/0	0
192.168.1.0/24	S0/1	0
192.168.23.0/24	S0/0	1
192.168.3.0/24	S0/0	4

R2的路由表

192.168.12.0/24	S0/0	0
192.168.23.0/24	S0/1	0
192.168.1.0/24	S0/0	0
192.168.3.0/24	S0/1	3

R3的路由表

192.168.23.0/24	S0/0	0
192.168.3.0/24	S0/0	2
192.168.12.0/24	S0/0	1
192.168.1.0/24	S0/0	2

有多种机制可以消除路由环路。这些机制包括：

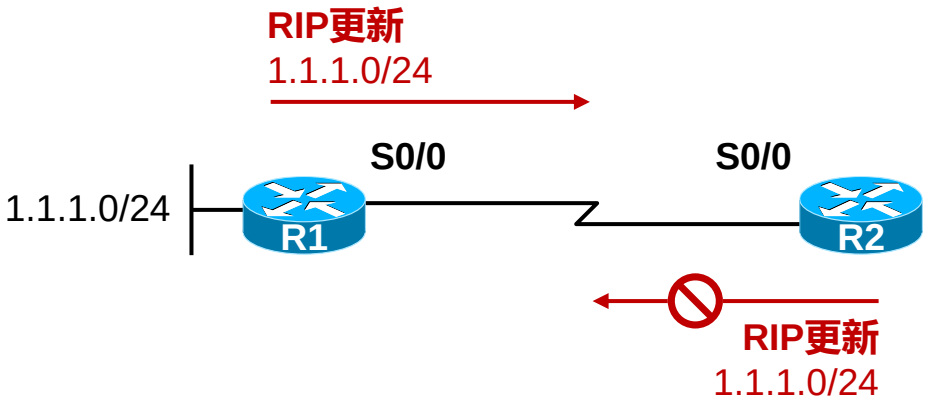
- 定义最大跳数
- 水平分割
- 毒性路由
- 毒性逆转
- 抑制计时器
- 触发更新

定义最大跳数（16跳为不可达）

- RIP定义跳数最大值为15条，也就意味着16跳被视为不可达
- 通过定义最大跳数可以很好的防止路由度量值计数到无穷大
- RIP最大跳数的定义极大程度上限制了RIP所能支持的网络规模

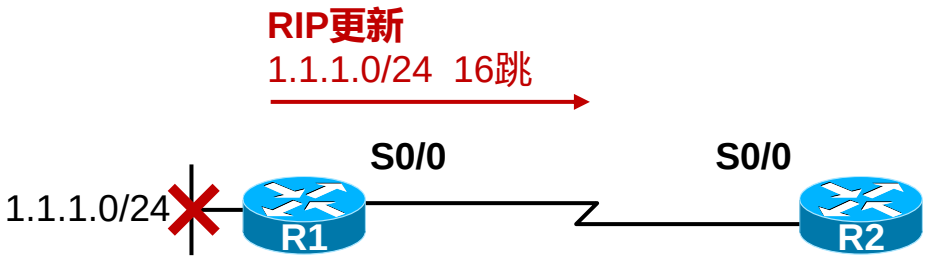
水平分割 Split Horizon

- RIP路由器不会将在某个接口上收到的RIP路由再从这个接口更新出去，这就是水平分割规则。



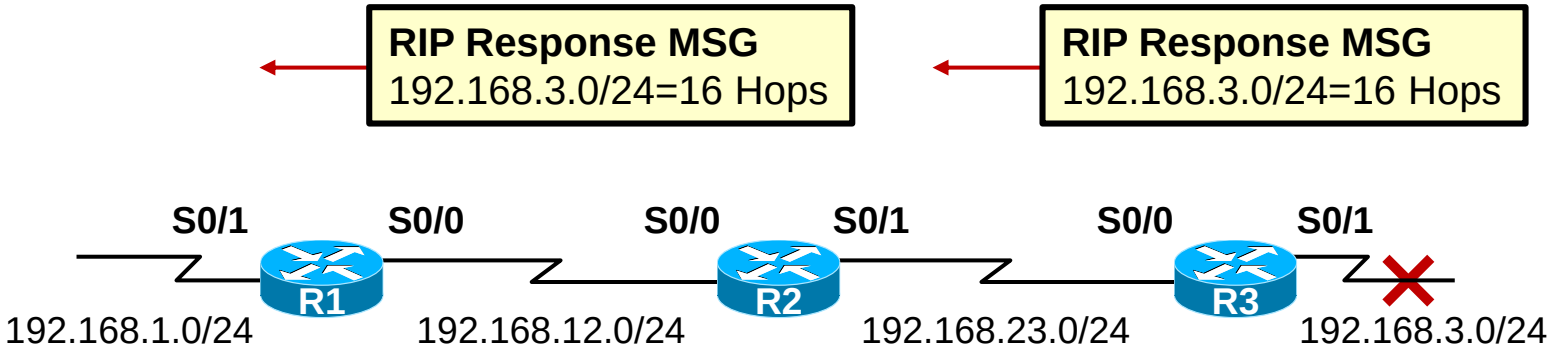
毒性路由 RoutePoisoning

- 当路由器感知到某个网段发生故障，可以立即泛洪该网段的路由（将其跳数设置为16跳，也就是不可达），以此来快速刷新网络中其他路由器的路由表。



触发更新 Triggered Update

- 拓扑发生变更时，路由器立即发送更新消息，而不等更新计时器超时



RIP的配置

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

- 激活RIP路由进程

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

- 在指定的网段上激活RIP
- RIP只支持主类网络宣告

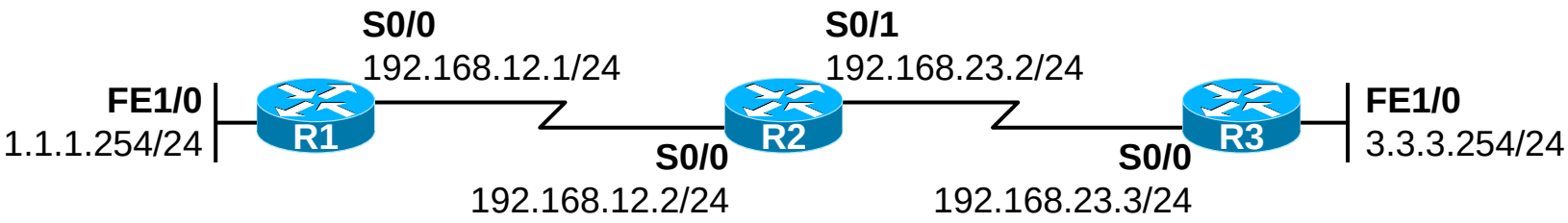
```
Router(config-router)# version 1/2
```

- 指定RIP的版本

红茶三杯
Vinsoney

RIP基础实验

RIPv2基础实验



R1的配置：

```
router rip
  version 2
  network 1.0.0.0
  network 192.168.12.0
```

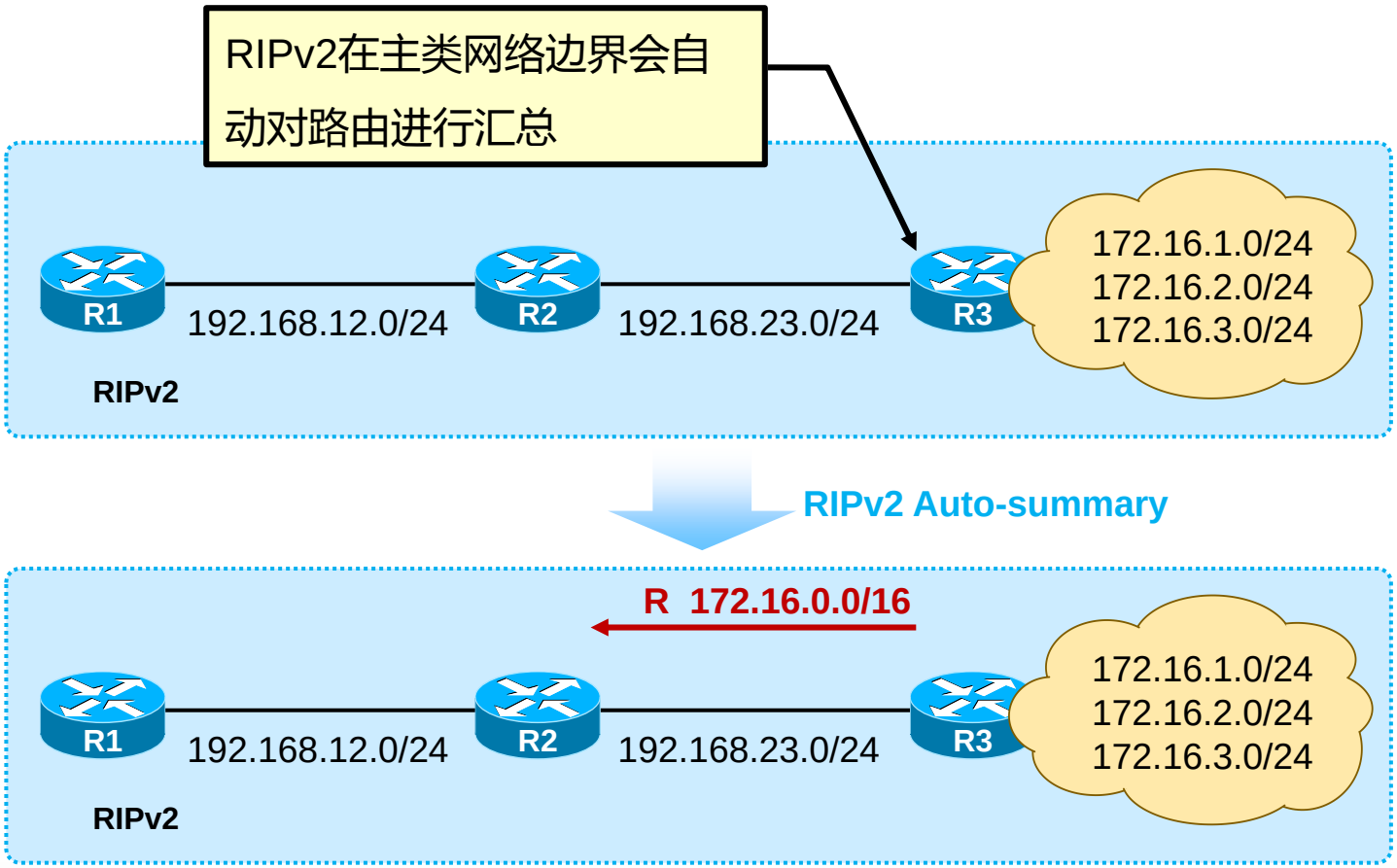
R2的配置：

```
router rip
  version 2
  network 192.168.12.0
  network 192.168.23.0
```

R3的配置：

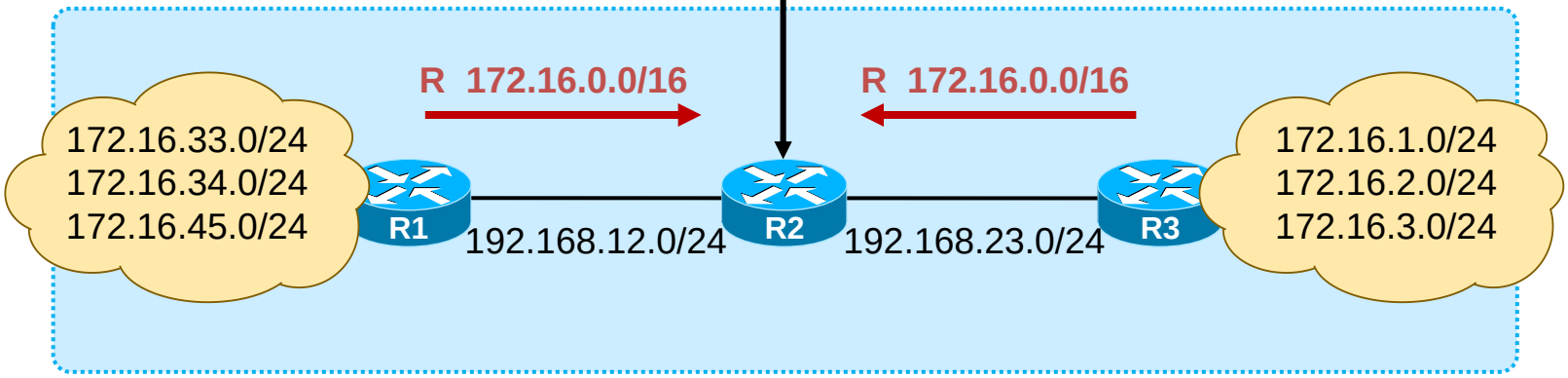
```
router rip
  version 2
  network 192.168.23.0
  network 3.0.0.0
```

RIPv2的自动汇总

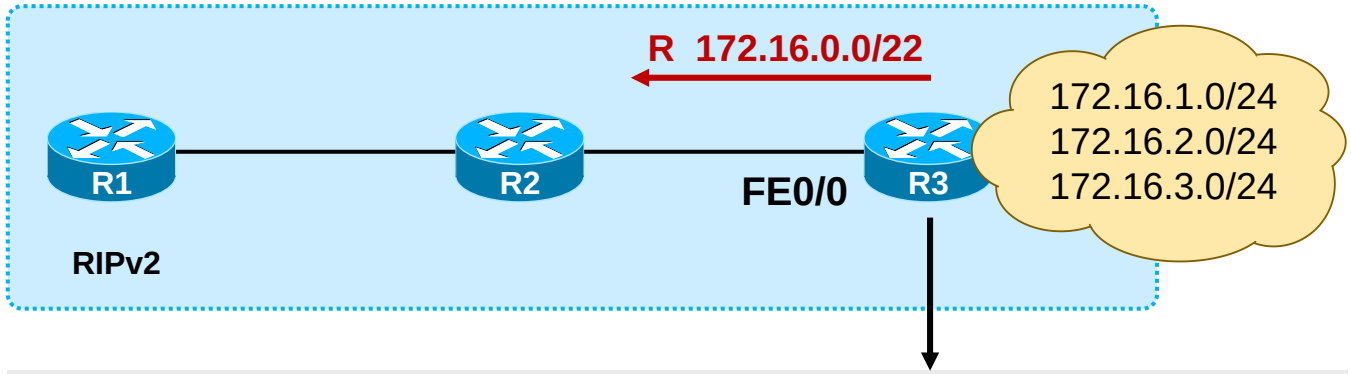


RIPv2的自动汇总

R1、R3都处于主类网络边界，因此都将172的明细路由汇总为172.16.0.0传递给R2，此时R2上172.16.0.0/16的路由将出现等价负载均衡。



RIP的手工汇总




```
router rip
  version 2
  no auto-summary                          !! 先关闭自动汇总
interface fastethernet0/0
  ip summary-address rip 172.16.0.0 255.255.252.0
```

RIP路由汇总存在什么问题？

RIPv2的手工路由汇总不支持CIDR（超网）

FAQ

- 什么是RFC

红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You

红茶三杯
Vinsoney

学习 沉淀 成长 分享

EIGRP

红茶三杯（朱SIR）微博：http://t.sina.com/vinsoney

Latest update: 2012-06-01

课程目标

EIGRP协议基础

EIGRP基础配置

红茶三杯
Vinsoney

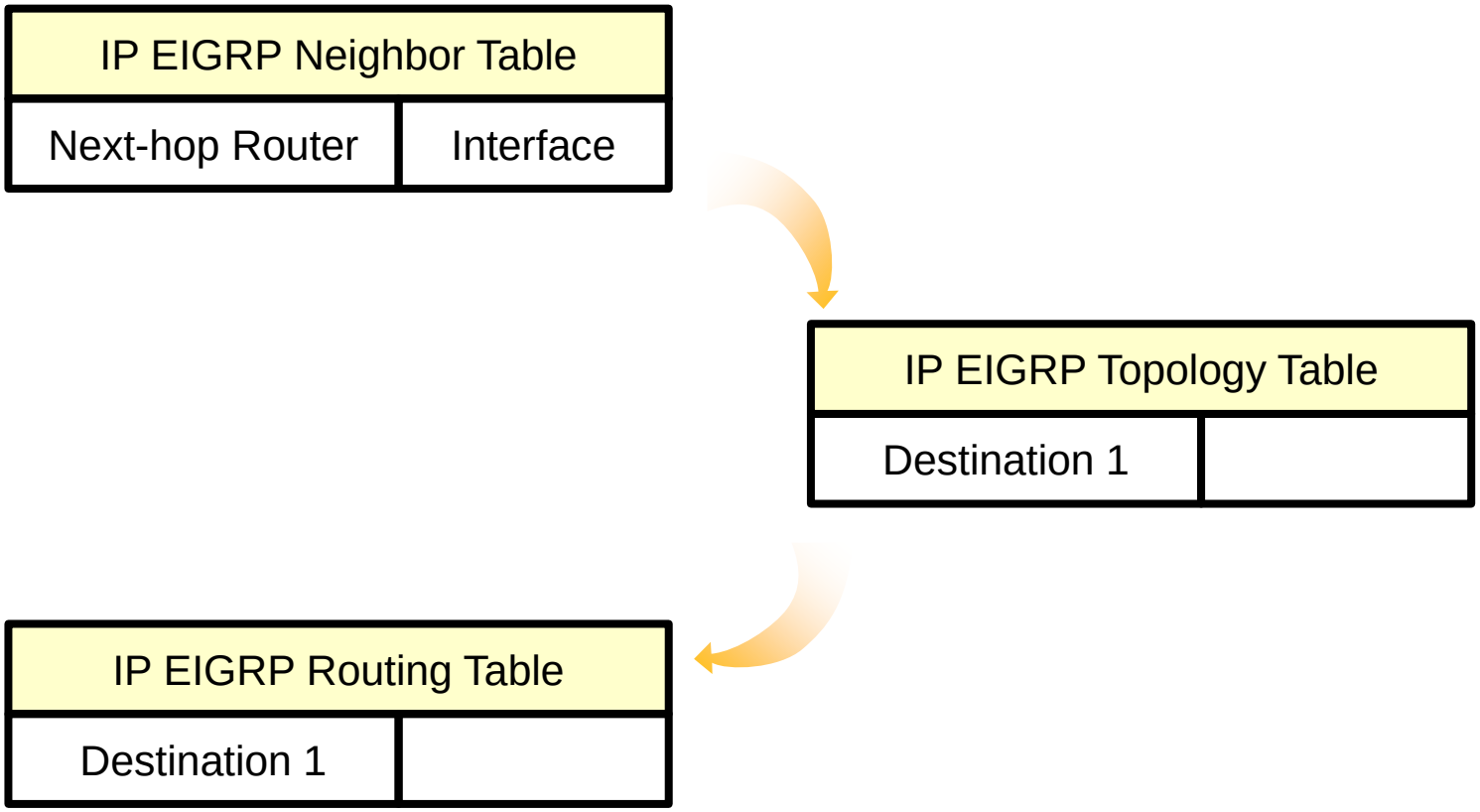
EIGRP协议基础

- EIGRP的协议特点
- EIGRP的三张表
- EIGRP数据包
- 初始路由发现
- EIGRP metric
- DUAL算法

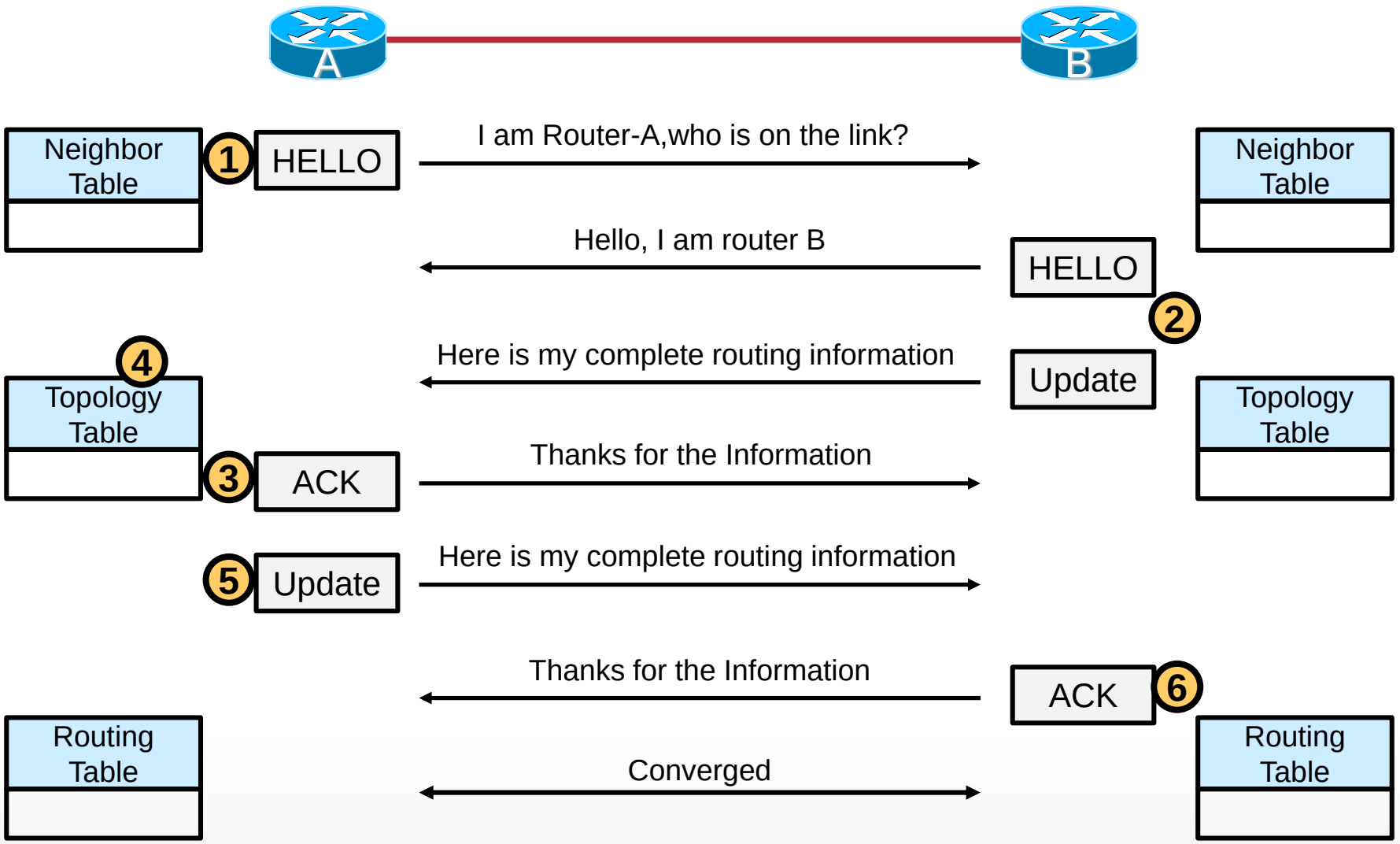
EIGRP的协议特点

- CISCO私有的高级距离矢量协议；
- 无类路由协议，支持VLSM；
- DUAL算法，EIGRP的核心，形成无环路由；
- 快速收敛，后继及可行后继；
- 低路由更新开销，支持组播及单播的方式发送协议数据；
- 支持自动及手工路由汇总；
- 支持等价及非等价负载均衡；
- 支持多种网络层协议（IP、IPX、Appletalk，etc.）。

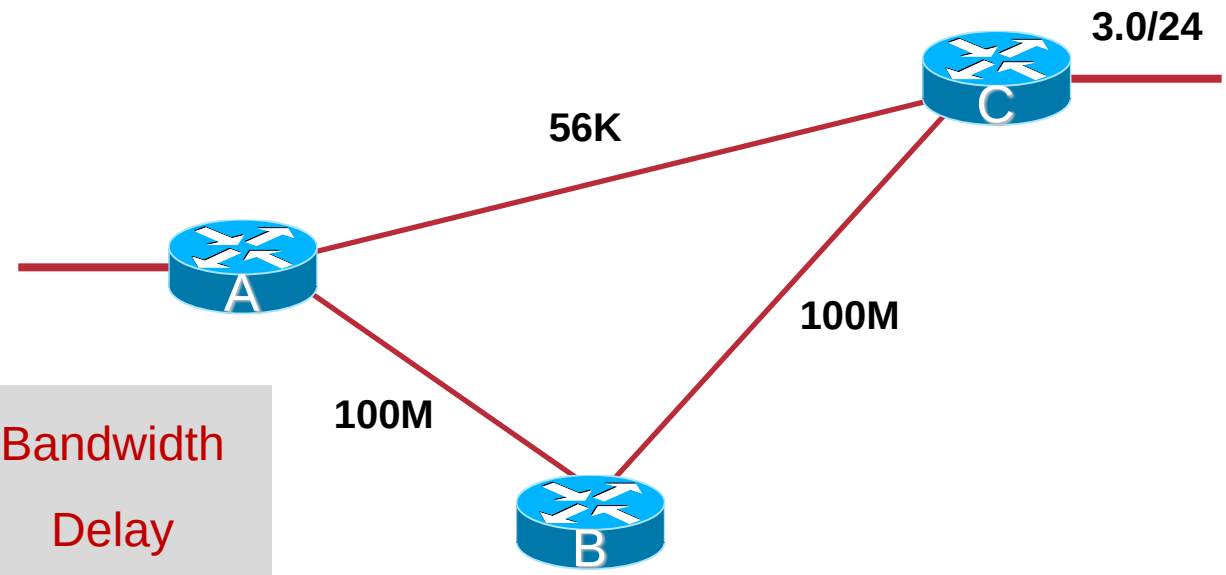
EIGRP的三张表


IP EIGRP Neighbor Table
Next-hop Router
Interface
IP EIGRP Topology Table
Destination 1
IP EIGRP Routing Table
Destination 1

初始路由发现



EIGRP的Metric



Bandwidth

Delay

Reliability

Loading

MTU

EIGRP的Metric

R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.12.0/24 is directly connected, FastEthernet1/0
C 192.168.13.0/24 is directly connected, Serial0/0
D 3.0.0.0/8 **[90/158720]** via 192.168.12.2, 00:01:10, FastEthernet1/0
D 192.168.23.0/24 **[90/30720]** via 192.168.12.2, 00:01:23, FastEthernet1/0

EIGRP的Metric计算

$$BW = \frac{10^7}{\text{接口最小带宽kbit/s}} \times 256 \quad (kbit/s)$$

接口最小带宽指的是沿着路由学习过来的方向所有入站接口带宽中最小值

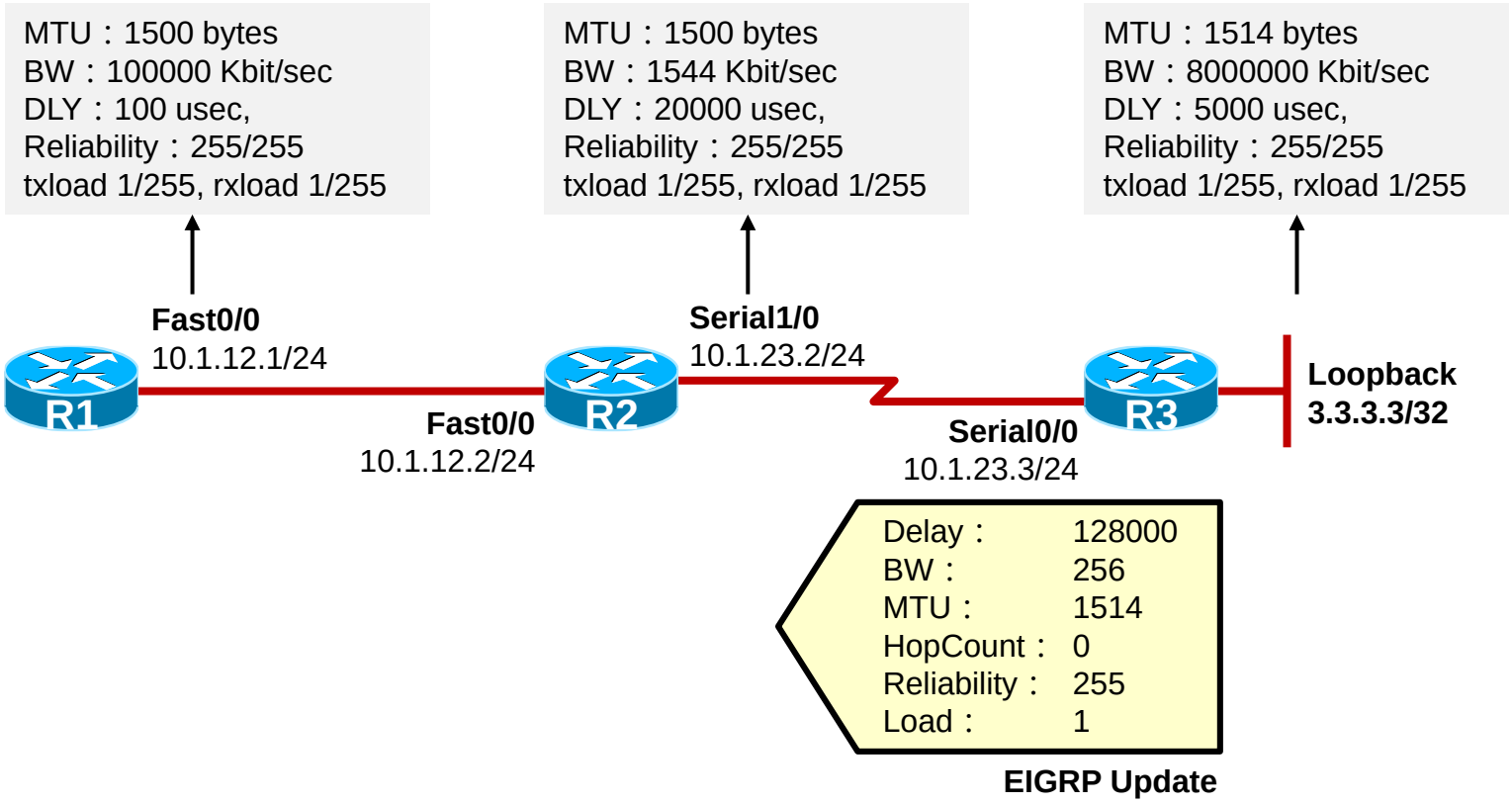
$$DLY = \frac{\text{延迟(us)}}{10} \times 256 \quad (us)$$

沿着路由学习过来的方向所有入站接口的延迟累加

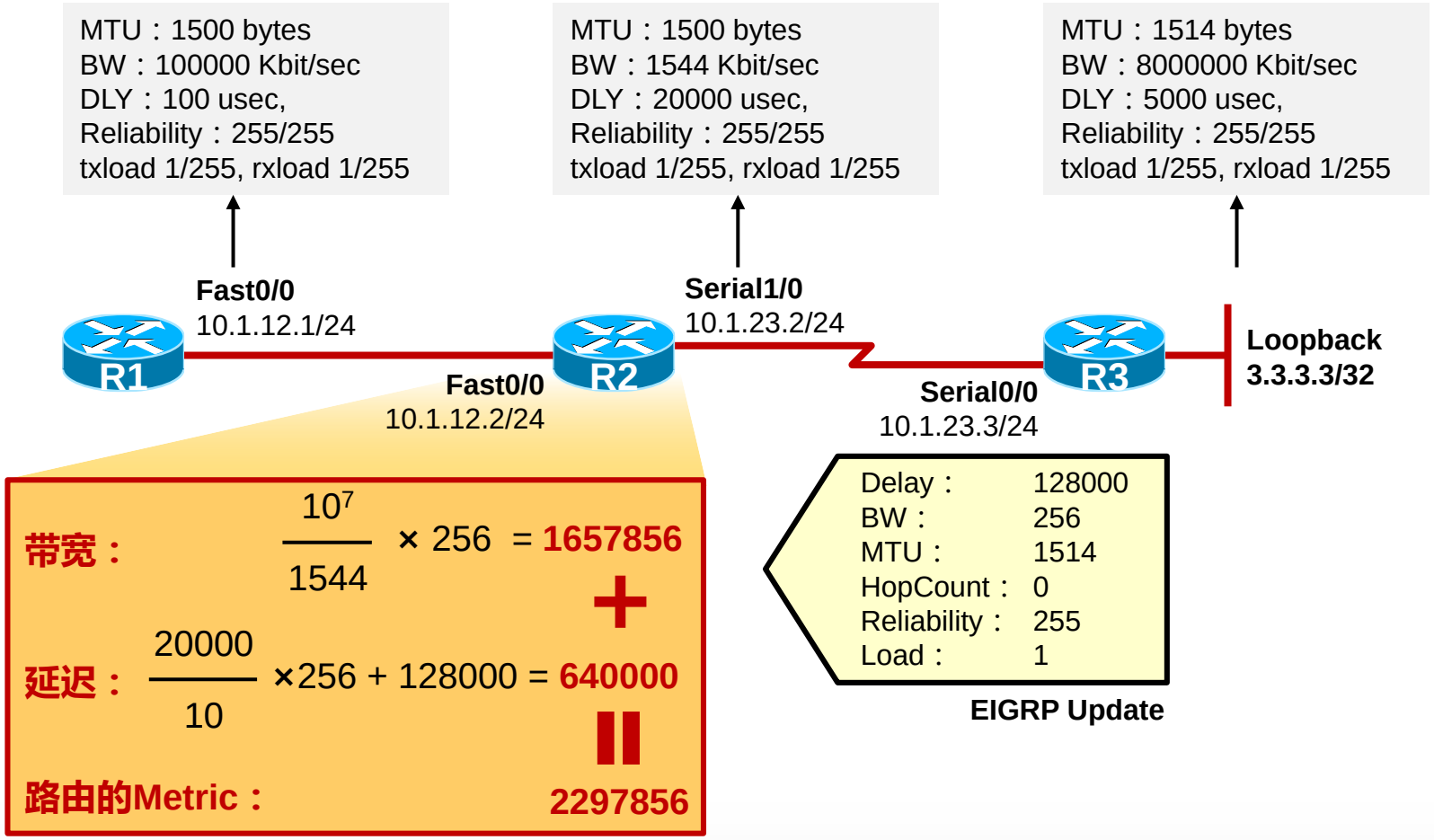
$$Metric = \left[K1 \times BW + \frac{K2 \times BW}{256 - LOAD} + K3 \times DLY \right] \times \left[\frac{K5}{RELIA + K4} \right]$$

- 默认 K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0
- EIGRP路由metric默认为 **延迟+带宽**

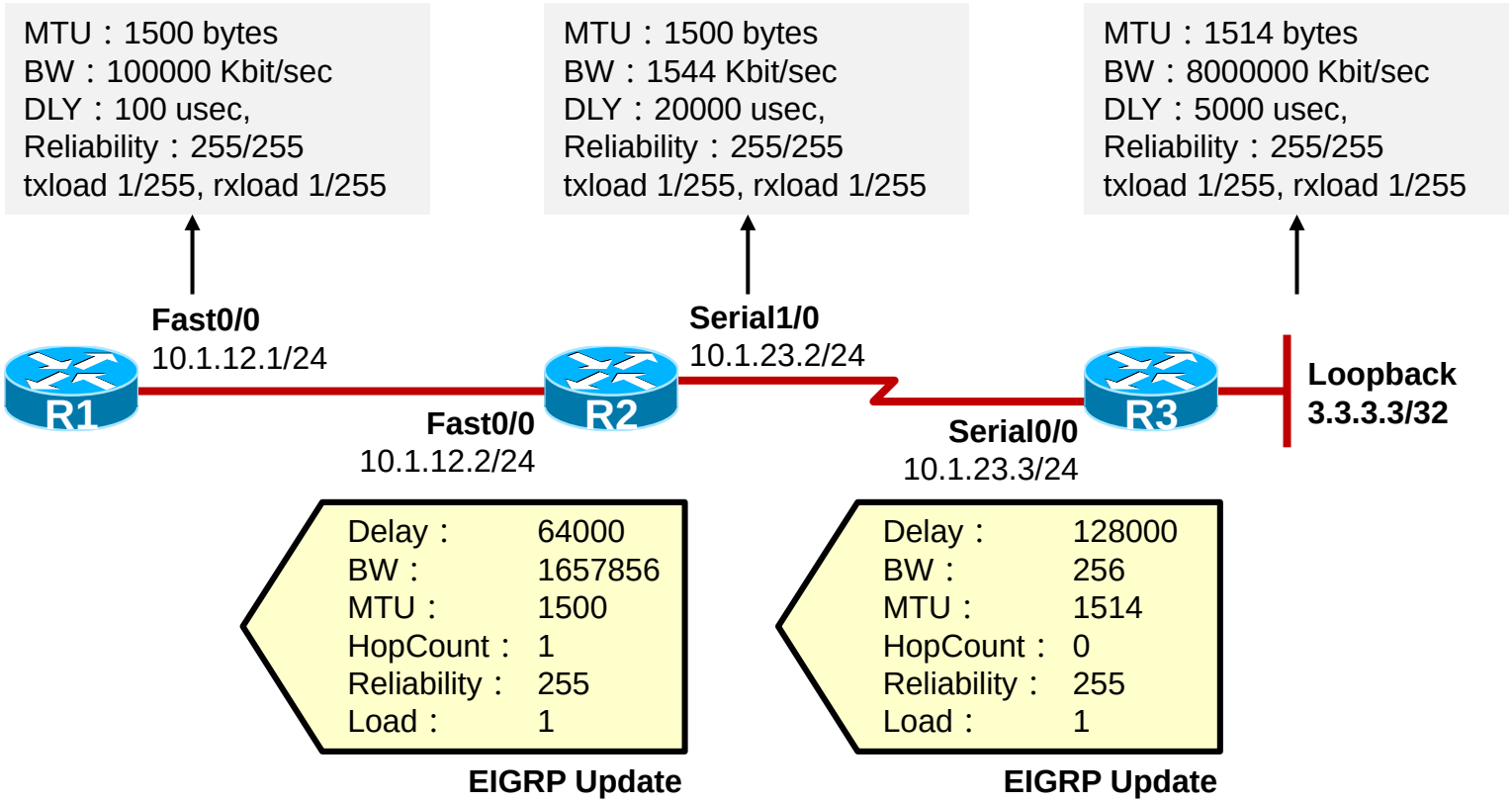
EIGRP的Metric计算



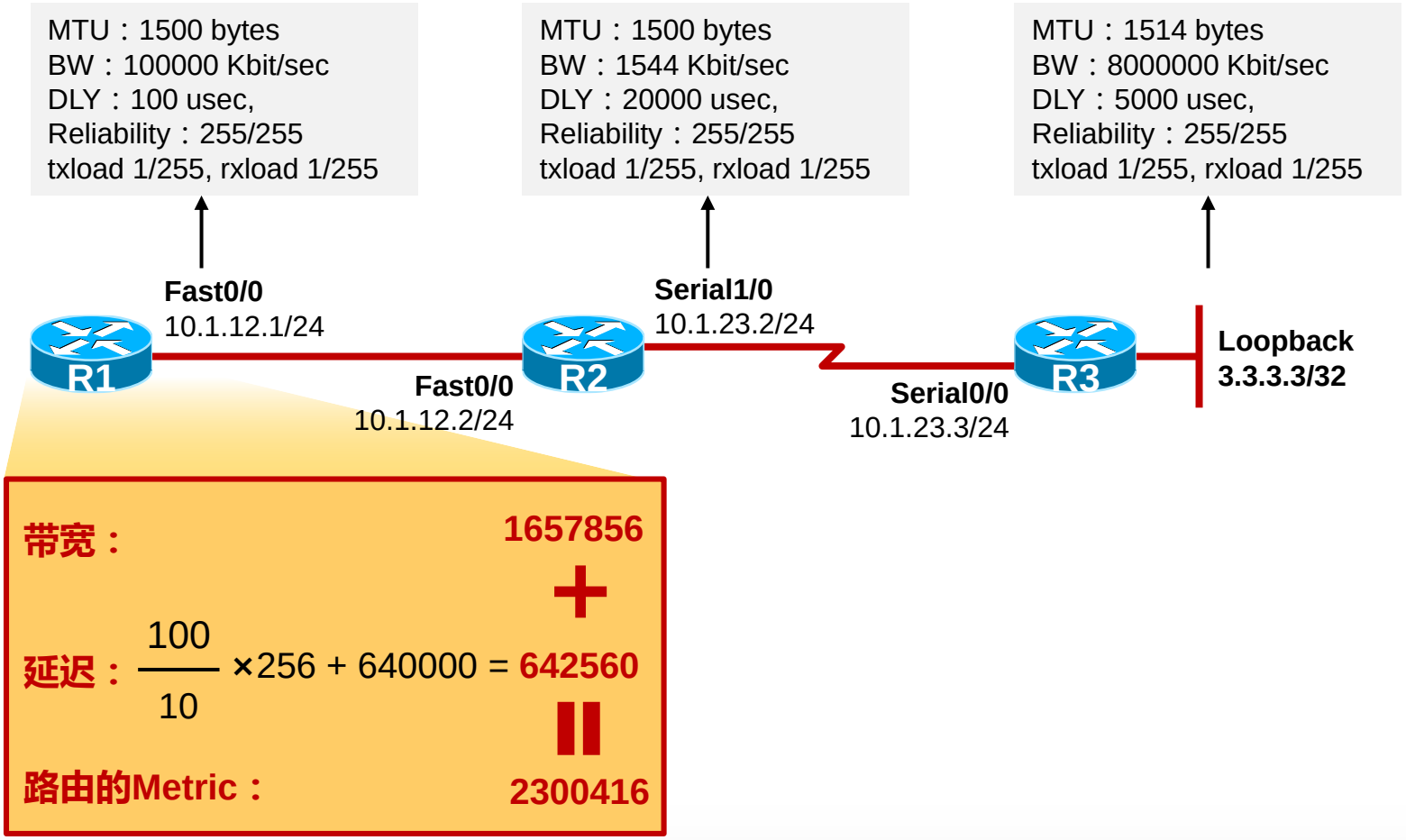
EIGRP的Metric计算



EIGRP的Metric计算



EIGRP的Metric计算

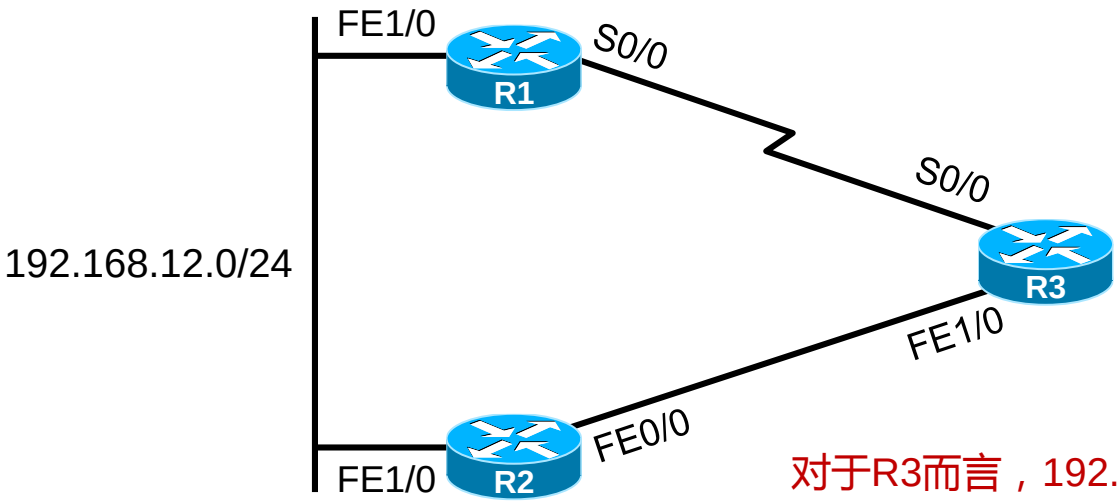


DUAL算法

- Diffusing Update Algorithm，简称DUAL，扩散更新算法
- 用于计算最佳无环路径和备用路径
- 特点：
  - 无环拓扑
  - 可立即使用的无环备用路径
  - 快速收敛
  - 低带宽利用率（通过限定更新实现）

Successor, Fessible Successor

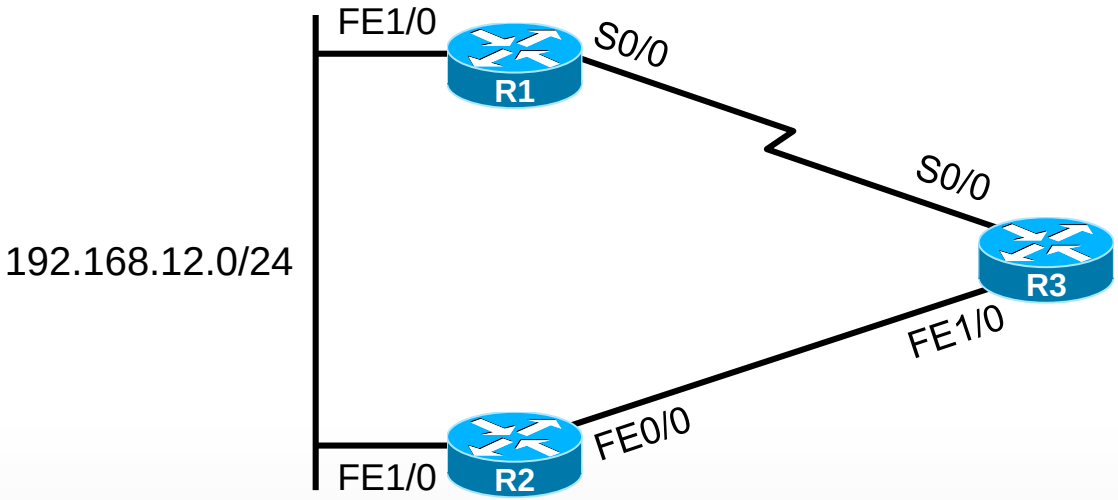
- Successor 后继：被实际选中作为到达目标网络所使用的下一跳路由器。
- Fessible Successor 可行后继：到达该目标网络的备份下一跳路由器（必须满足FC）。



对于R3而言，192.168.12.0/24路由的Successor是R2

Feasible Distance, Advertised Distance

- Advertised Distance 通告距离：邻居到达目标网络的度量值。
- Feasible Distance 可行距离：邻居到达目标网络的度量值（AD）加上本路由器到达该邻居的度量值 。
- Feasible Condition 可行性条件：邻居到达目标网络的度量值（AD）小于本路由器的FD时，则认为该邻居通告的路径满足FC。



后继、可行后继路由器、FD及AD

R3#show ip eigrp topology

```
IP-EIGRP Topology Table for AS(1) / ID (192.168.23.3)

Codes:   P - Passive, A - Active, U - Update, Q - Query, R - Reply,
         r - reply Status, s - sia Status

  P  192.168.12.0/24, 1 successors, FD is 30720
         via 192.168.23.2 ( 30720 / 28160 ), FastEthernet1/0
         via 192.168.13.1 ( 2172416 / 28160 ), Serial0/0
```

后继Successor

FD

AD

可行后继FS

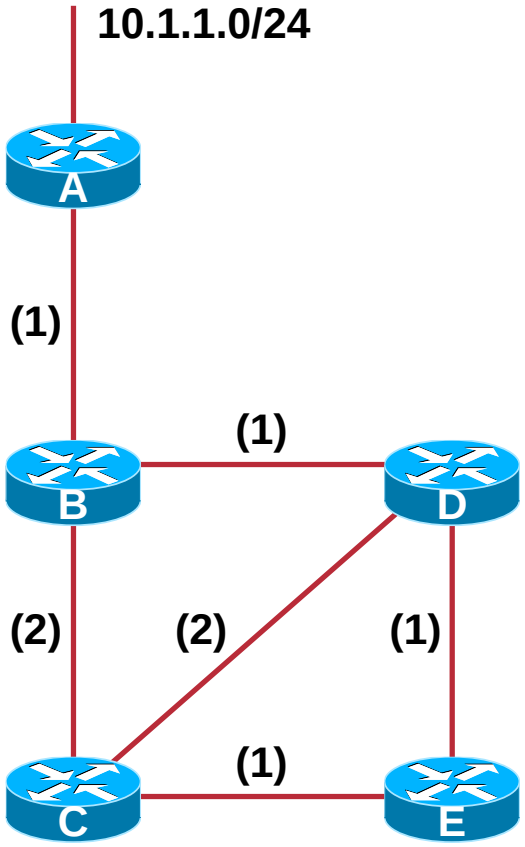
R3#show ip route

FD

后继Successor

```
D    192.168.12.0/24 [90/30720] via 192.168.23.2, 00:10:23, FastEthernet1/0
```

DUAL算法



C的拓扑表

		FD	AD	
(1.0)		3		(FD)
	via B	3	1	(Successor)
	via D	4	2	(FS)
	via E	4	3	

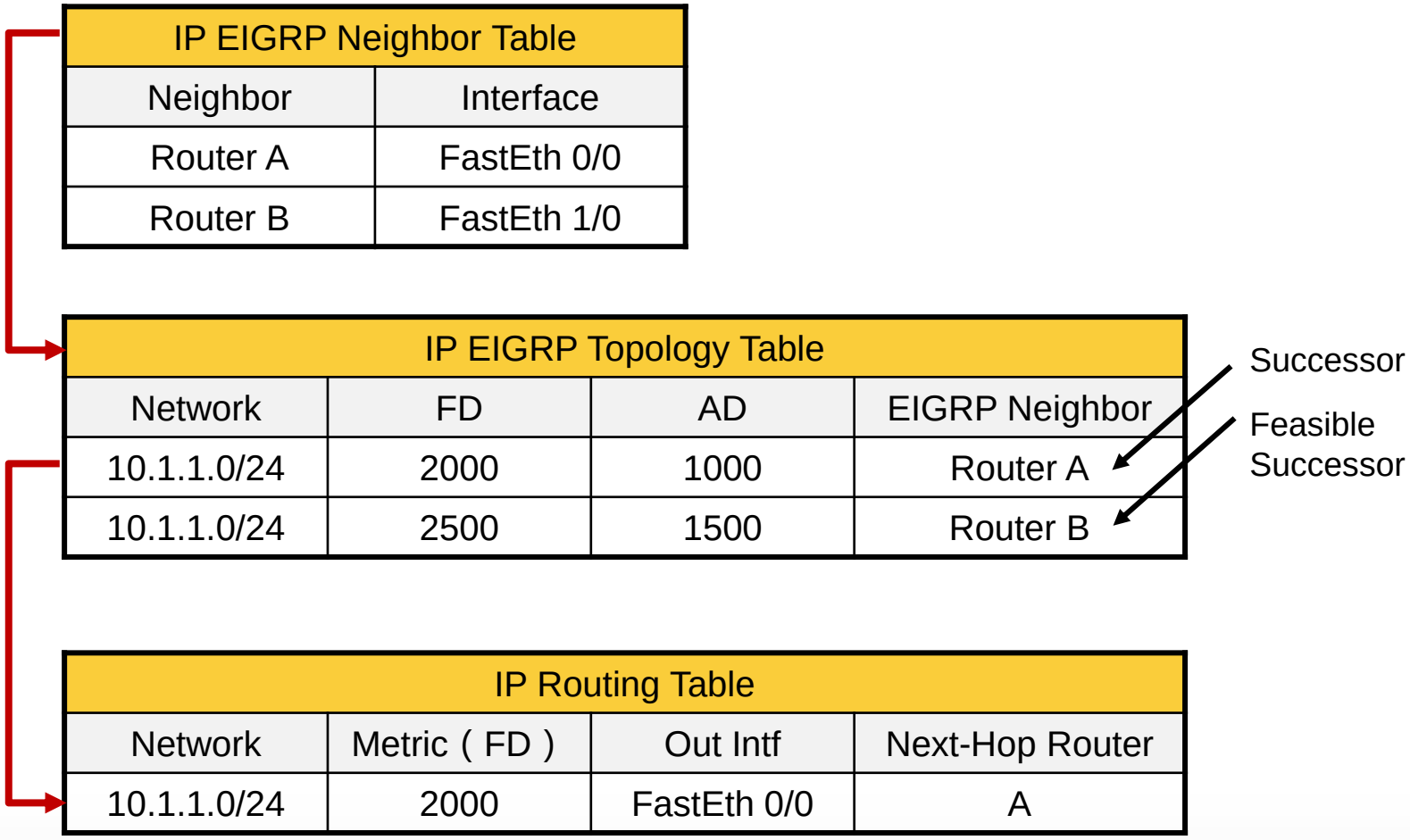
D的拓扑表

		FD	AD	
(1.0)		2		(FD)
	via B	2	1	(Successor)
	via C	5	3	

E的拓扑表

		FD	AD	
(1.0)		3		(FD)
	via D	3	2	(Successor)
	via C	4	3	

DUAL算法



红茶三杯
Vinsoney

EIGRP的配置及验证

基础配置

- **创建EIGRP进程，并进入路由进程的配置模式**

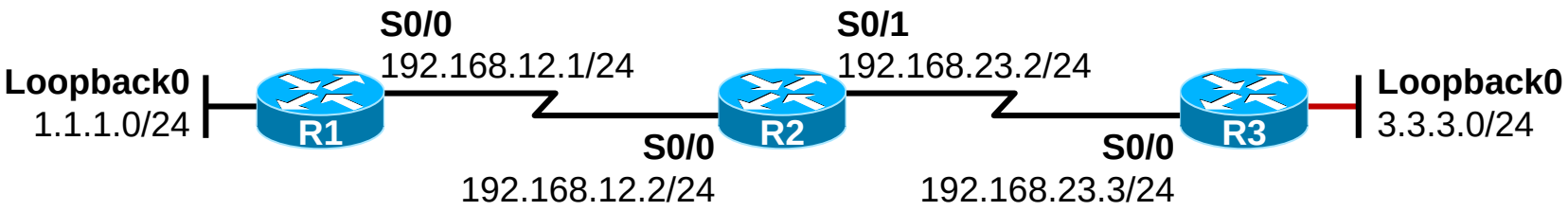
```
Router(config)# router eigrp autonomous-system-num
```

- **在指定的接口上激活EIGRP**

```
Router(config-router)# network network [wildcard-mask]
```

  - 如果不加通配符掩码，则自动识别为主类通告，也就是如果键入network 10.1.1.0，实际为network 10.0.0.0

基础配置示例



R1

```
router eigrp 1
  network 1.0.0.0
  network 192.168.12.0
```

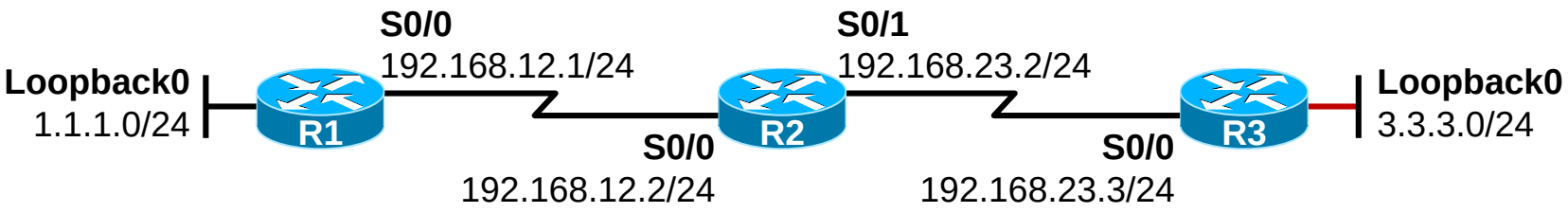
R2

```
router eigrp 1
  network 192.168.12.0
  network 192.168.23.0
```

R3

```
router eigrp 1
  network 192.168.23.0
  network 3.0.0.0
```

基础配置示例



R2#show ip route

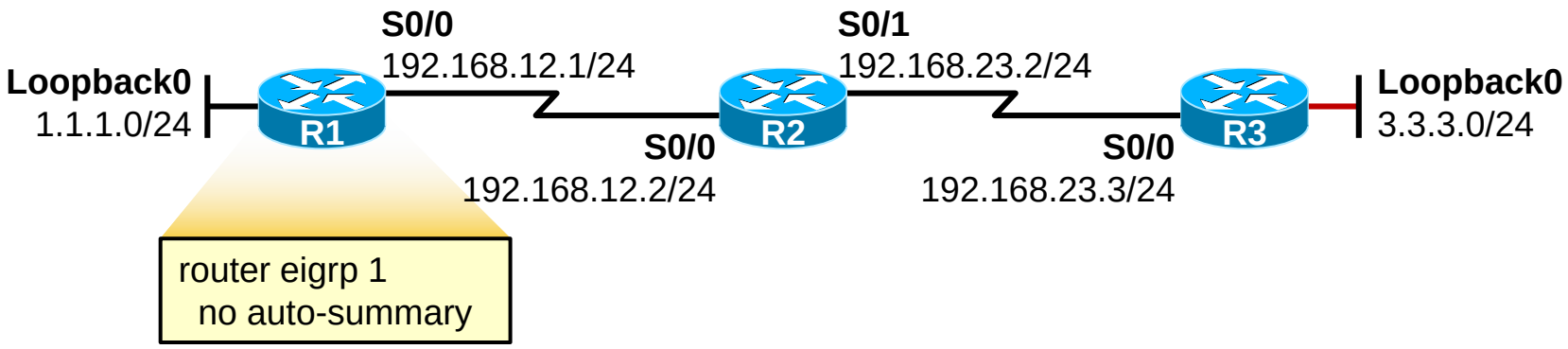
C 192.168.12.0/24 is directly connected, Serial0/0

D 1.0.0.0/8 [90/2297856] via 192.168.12.1, 00:00:58, Serial0/0

D 3.0.0.0/8 [90/2297856] via 192.168.23.3, 00:00:39, Serial0/1

C 192.168.23.0/24 is directly connected, Serial0/1

基础配置示例（关闭自动汇总）



R2#show ip route

C 192.168.12.0/24 is directly connected, Serial0/0

1.0.0.0/24 is subnetted, 1 subnets

D 1.1.1.0 [90/2297856] via 192.168.12.1, 00:00:06, Serial0/0

D 3.0.0.0/8 [90/2297856] via 192.168.23.3, 00:00:39, Serial0/1

C 192.168.23.0/24 is directly connected, Serial0/1

查看及排错

Router#show ip eigrp neighbors	Displays the neighbors discovered by IP EIGRP
Router#show ip eigrp topology	Displays the IP EIGRP topology table
Router#show ip route eigrp	Displays current EIGRP entries in the routing table
Router#show ip protocols	Displays the parameters and current state of the active routing protocol process
Router#show ip eigrp traffic	Displays the number of IP EIGRP packets sent and received

查看及排错

Router#debug eigrp packet	Displays all types of EIGRP packets, both sent and received
Router#debug eigrp neighbor	Displays the EIGRP neighbor interaction
Router#debug ip eigrp route	Displays advertisements and changes EIGRP makes to the routing table
Router#debug ip eigrp summary	Displays a brief report of the EIGRP routing activity
Router#show ip eigrp events	Displays the different categories of EIGRP activity, including route calculations

EIGRP负载均衡

- **等价负载均衡**
  - 所谓的等代价路径指的到达同一个目的地度量值相等的路径。
  - 默认最多支持4条等价路径之间进行流量负载，最大可为16条，命令：Maximum-paths ?
- **非等价负载均衡**
  - EIGRP也能在度量值不同的多条路径之间执行流量负载。

EIGRP非等价负载均衡

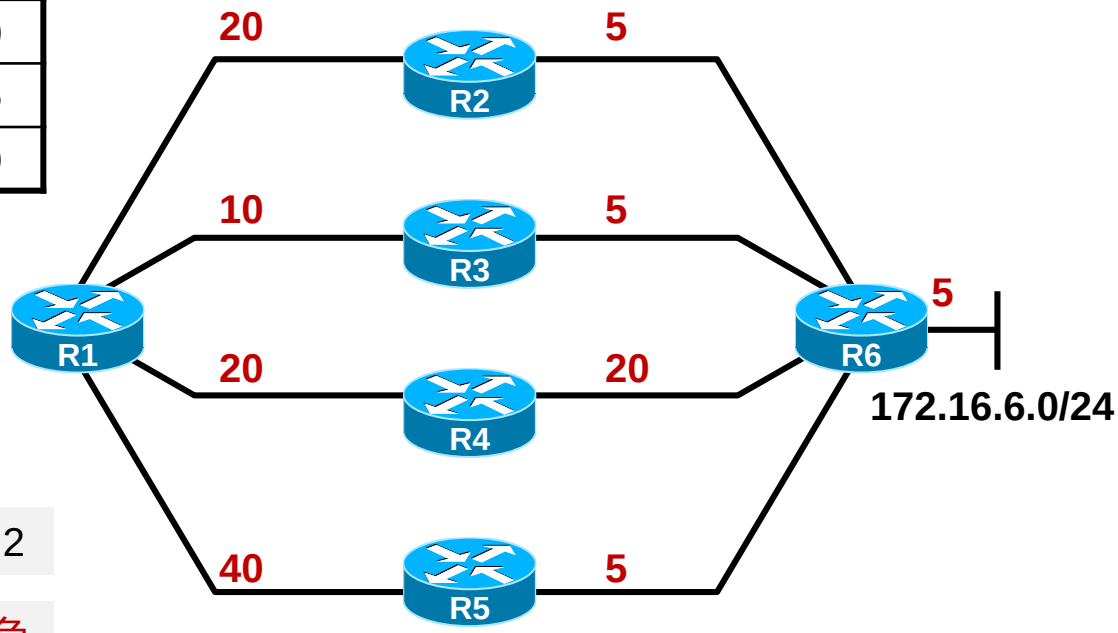
Router(config-router)# **Variance** *multiplier*

- multiplier默认值为1，范围1~128。
- EIGRP在多条路径上执行非等价负载均衡的条件：
  - 路由必须是无环的（即满足FC条件：AD<FDmin）
  - FD <= FDmin × multiplier
- 注：variance不指定最大路径，而指定一个基数（用于乘积计算）。

EIGRP非等价负载均衡

R1的拓扑数据库

Network	Neighbor	FD	AD
6.0/24	R2	30	10
	R3	20	10
	R4	45	25
	R5	50	10



Router(config-router)# Variance 2

- R1将使用R2及R3进行不等价负载均衡；流量比例为：2/5 : 3/5

红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You

红茶三杯
Vinsoney

学习 沉淀 成长 分享

OSPF

红茶三杯（朱SIR）微博：http://t.sina.com/vinsoney

Latest update: 2012-06-01

Content

OSPF协议基础

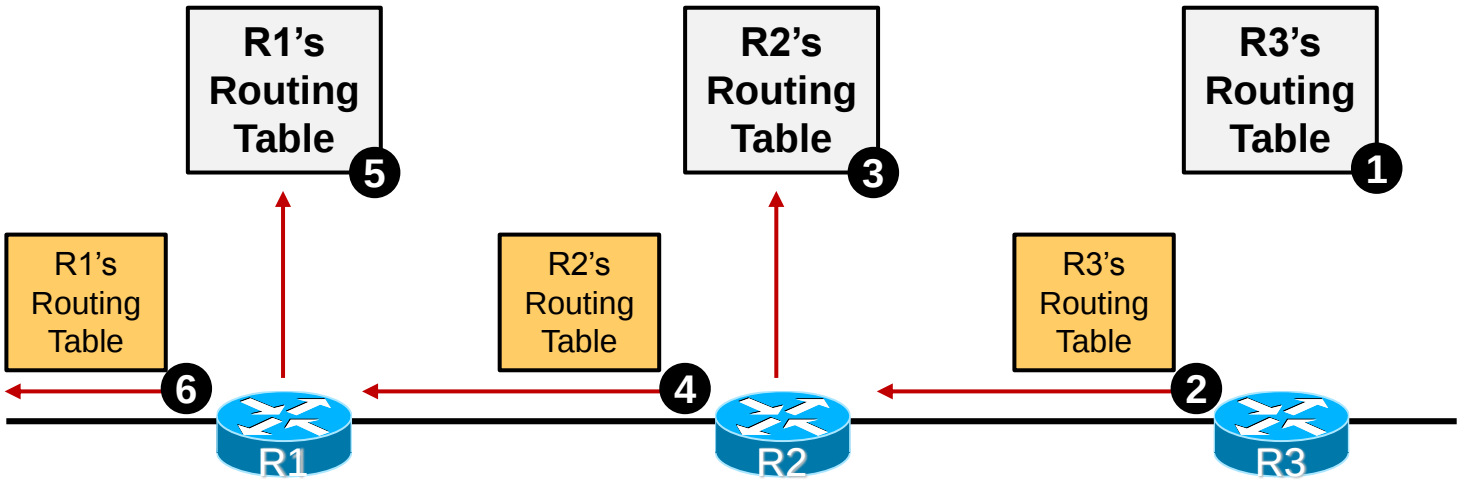
OSPF的配置及验证

红茶三杯
Vinsoney

OSPF协议基础

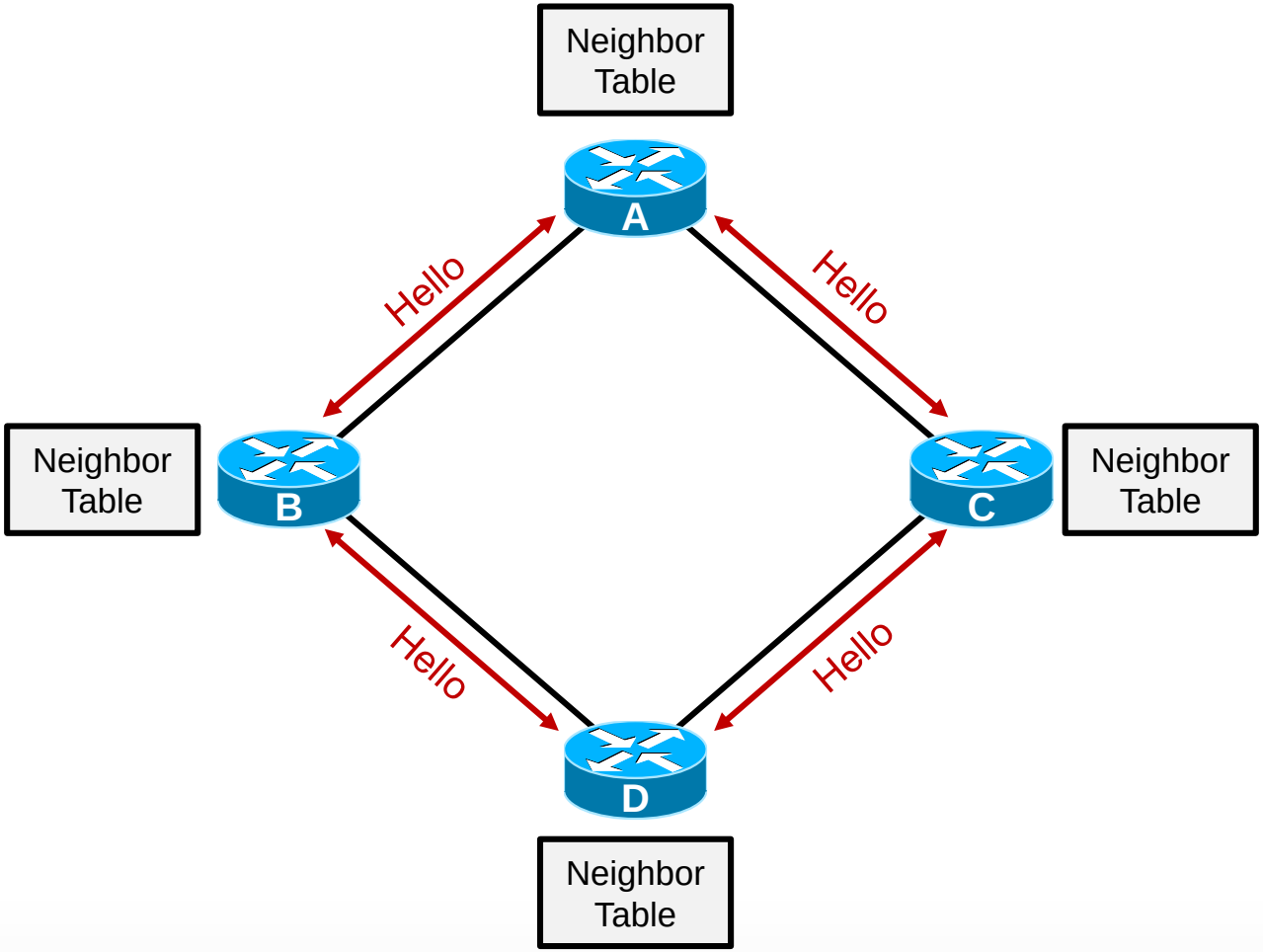
- 链路状态路由协议特点
- OSPF概述
- OSPF metric
- RouterID
- 报文类型
- 邻居关系建立过程
- DR、BDR的概念
- 多路访问网络中的LSA泛洪
- OSPF网络类型
- OSPF area的概念

距离矢量路由协议 回顾

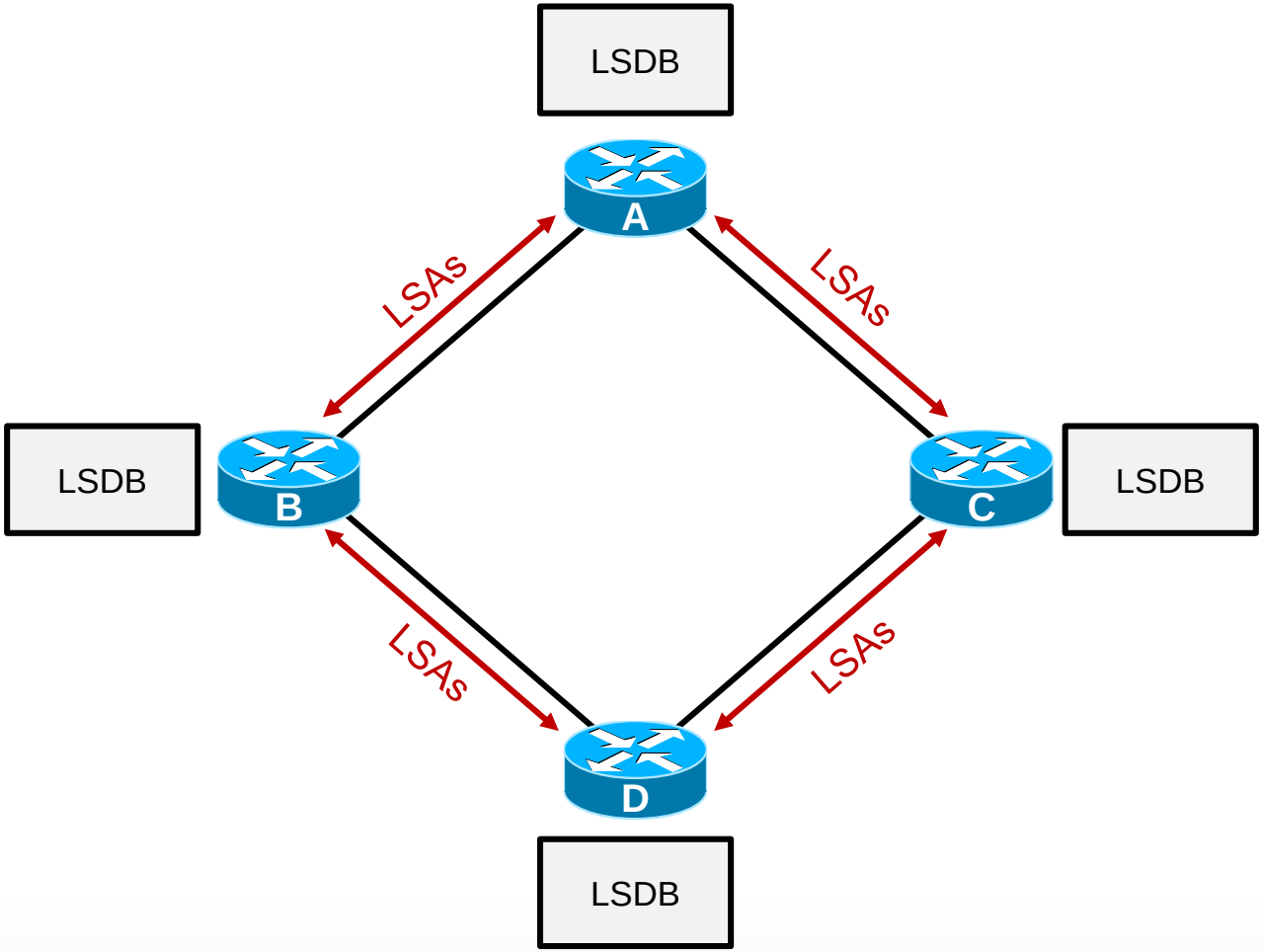


- 运行距离矢量路由协议的路由器会周期性的泛洪自己的路由表，也就是说协议更新消息中包含的就是路由信息。
- 路由器无法了解网络的拓扑结构，只是通过路由更新及简单的机制来学习路由。这种方式称为依照传闻的更新。

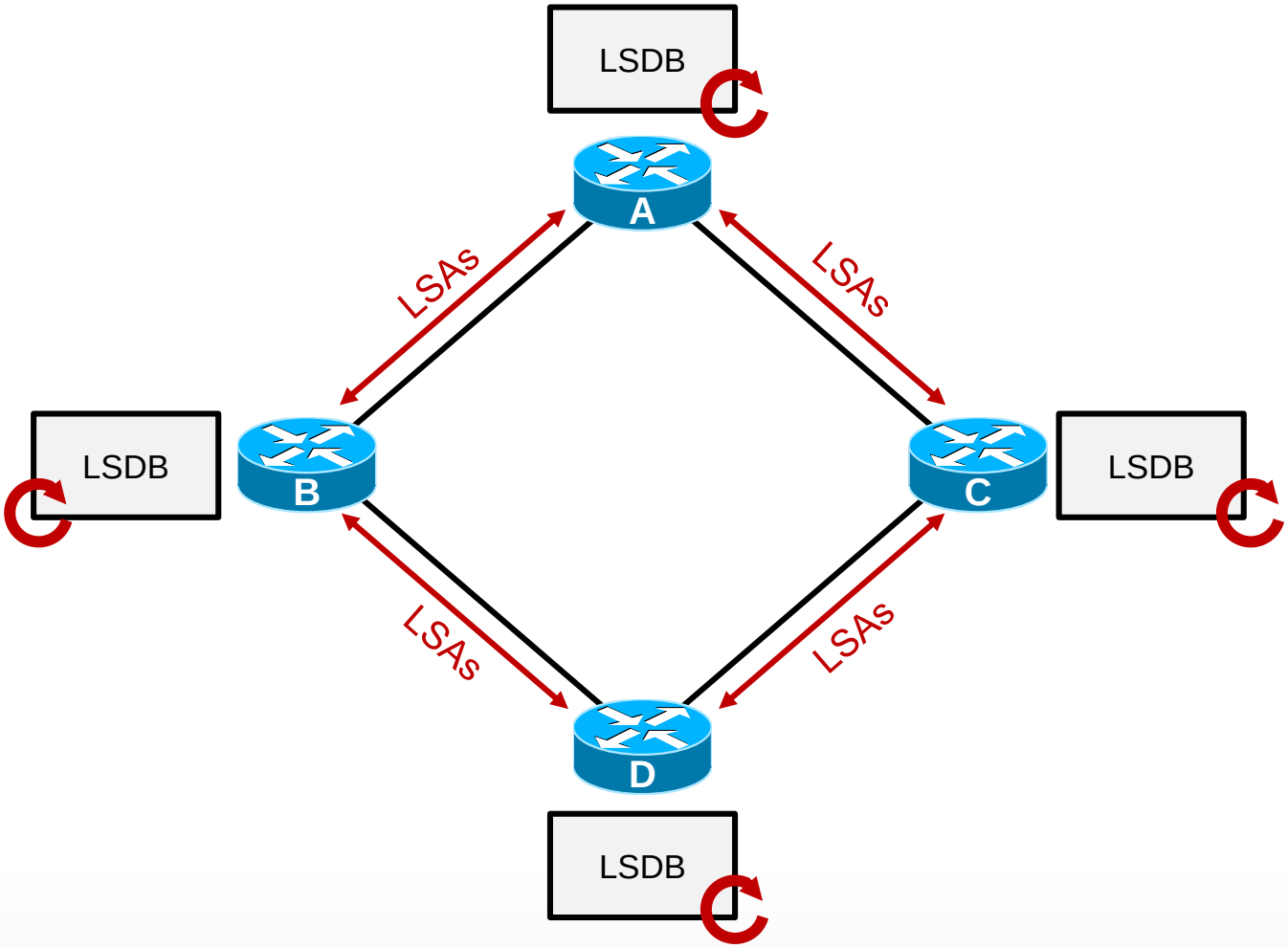
链路状态路由协议 – 发现邻居



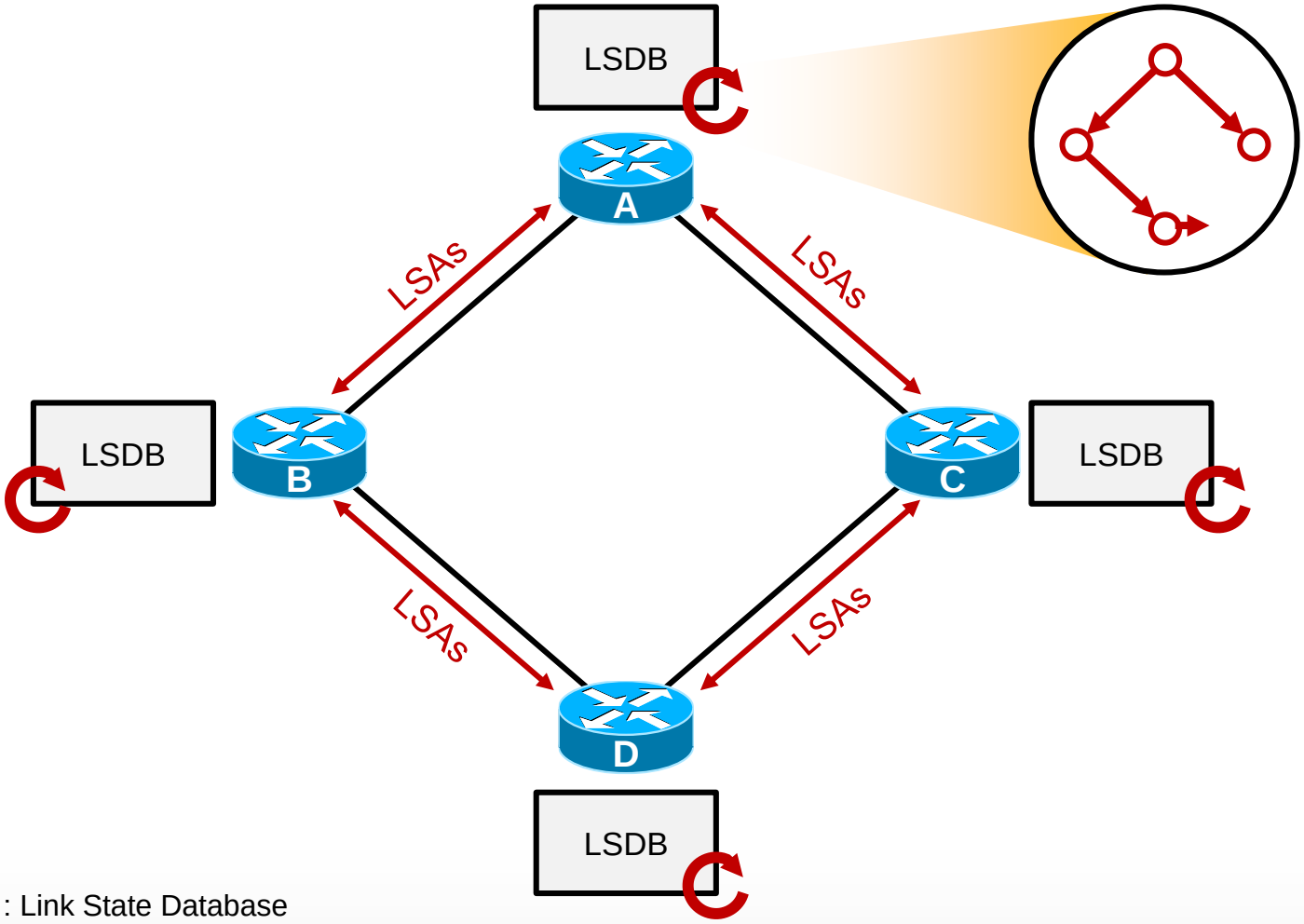
链路状态路由协议 – 泛洪LSAs



链路状态路由协议 - SPF

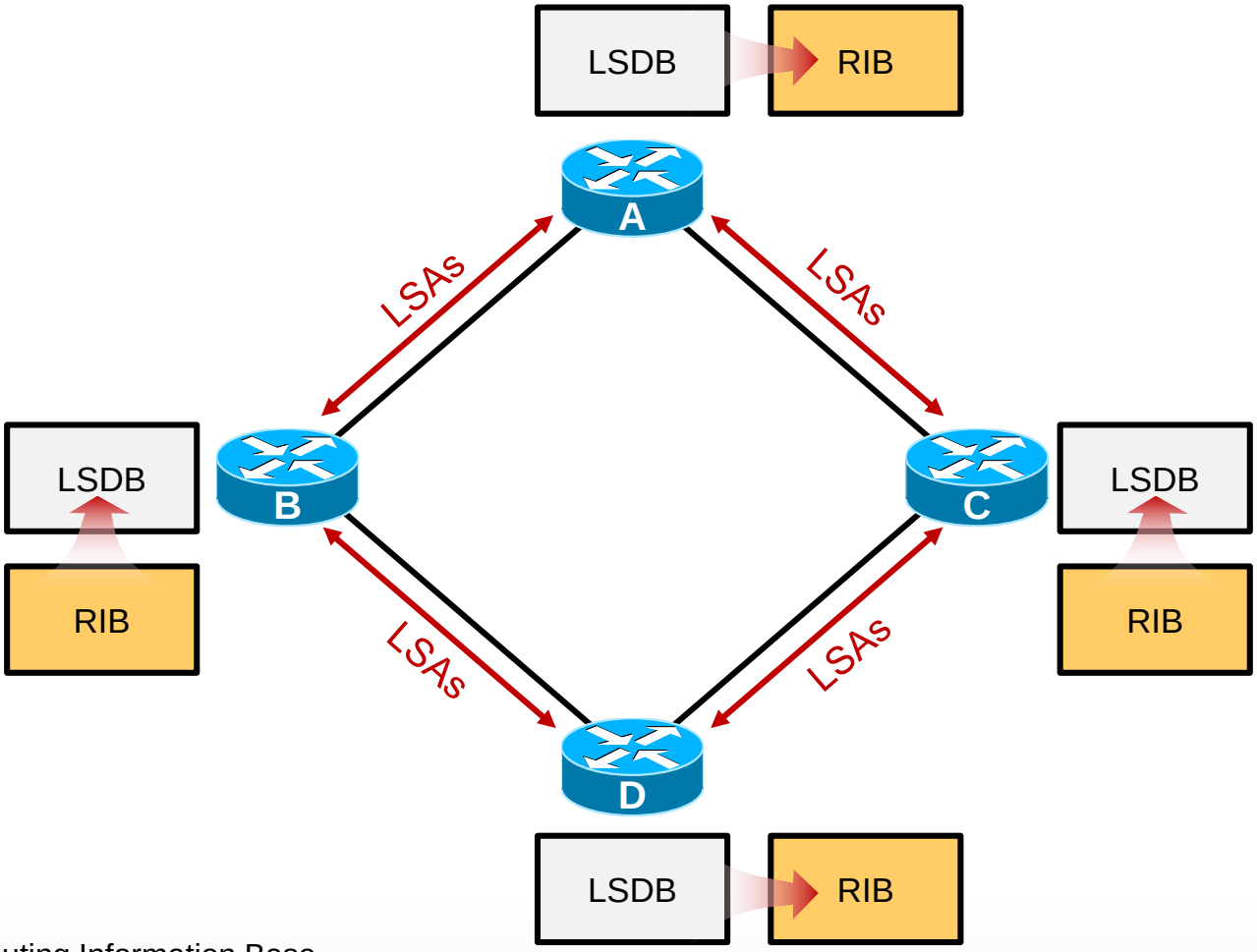


链路状态路由协议 - SPF



LSDB : Link State Database

链路状态路由协议 – 生成路由



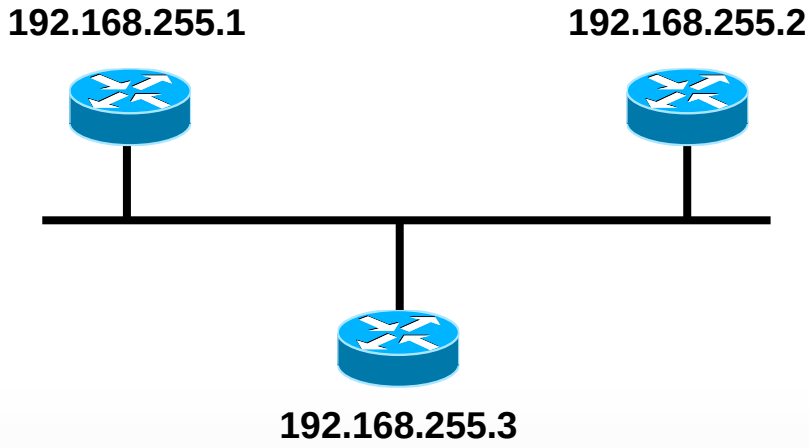
RIB : Routing Information Base

OSPF简介

- OSPF（Open Shortest Path First，开放最短路径优先）是典型的链路状态路由协议，是目前业内使用最广泛的IGP之一；
- 路由器之间交互的是链路状态信息，而不是直接交互路由；
- 每台OSPF路由器都知晓网络拓扑结构，采用SPF算法计算达到目的地的最短路径；
- 支持VLSM，支持手工路由汇总；
- 多区域的设计使得OSPF能够支持更大规模的网络。

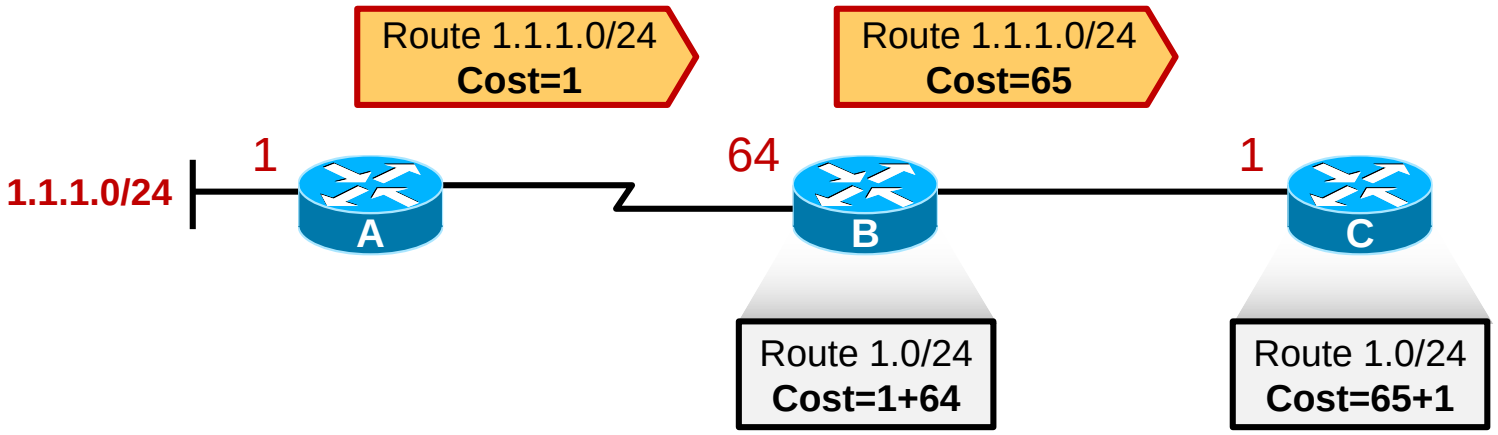
Router-ID

- Router Identifier，路由器标示符，用于在一个OSPF域中唯一地标识一台路由器，每台运行OSPF的路由器具备Router-ID；
- OSPF Router-ID的设定可以通过手工配置的方式，或使用自动获取的方式。自动选取的机制是：若路由器存在loopback接口，则选最大的loopback接口IP地址，若无则选活跃的物理接口中IP地址最大的作为RouterID；
- Router-ID值遵循稳定第一的原则。



OSPF metric

- OSPF使用Cost（开销）作为路由的度量值。
- 在每一个运行OSPF的接口上，都维护着一个接口Cost，接口Cost=100M/接口带宽，其中100M为OSPF的参考带宽值
- 一条路由的Cost由该路由从起源到本路由器沿途所有入站接口的Cost值累加。



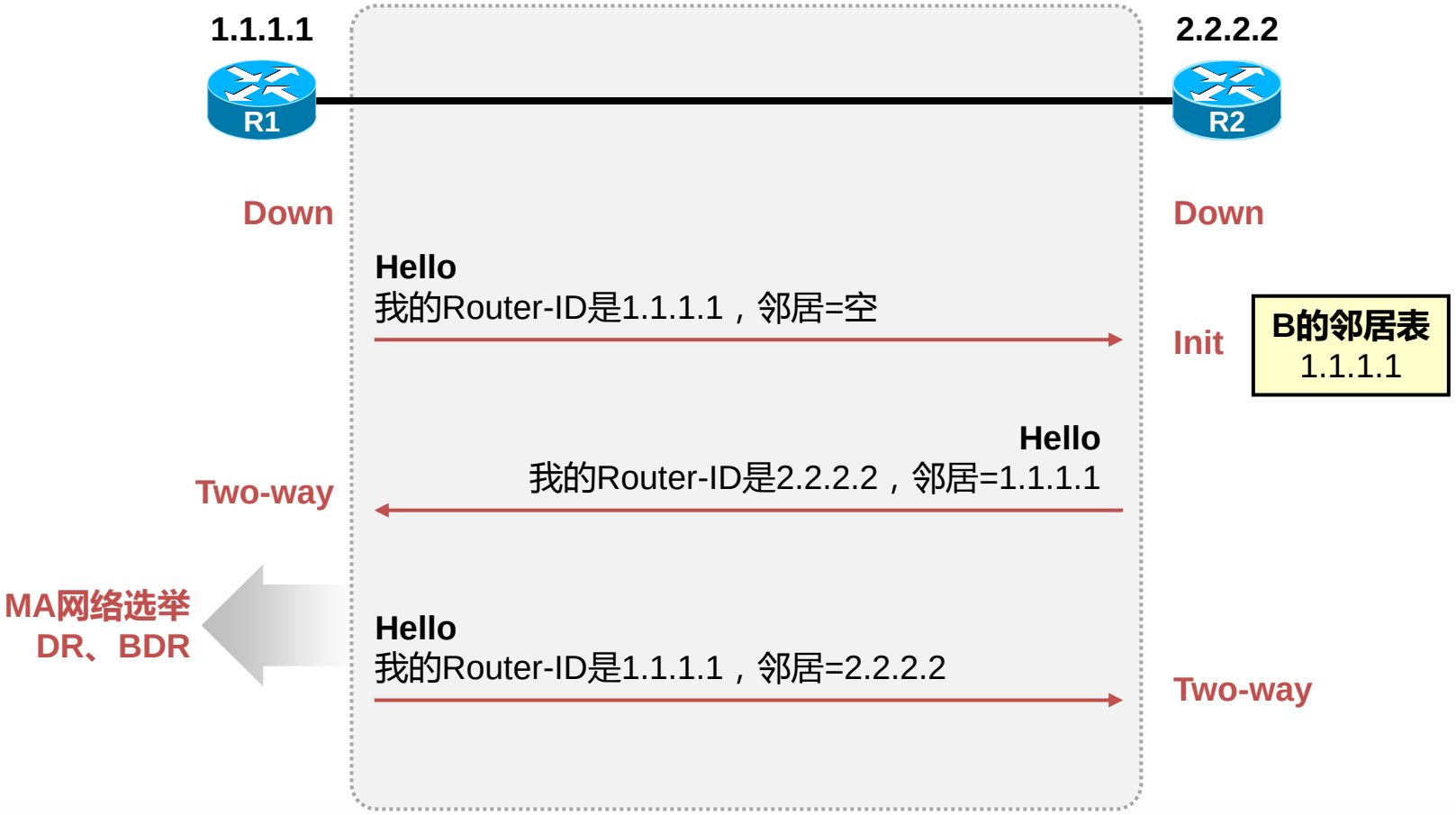
OSPF Packets

Hello	发现直连链路上的OSPF邻居、维护邻居关系。
DD Database Description	链路状态数据库描述报文，该报文有两种类型，一种是空的DD，用于协商Master/Slave，另一种则包含LSA的头部信息，用于描述LSDB的摘要。
LSR Link State Request	链路状态请求报文，用于向OSPF邻居请求链路状态信息。
LSU Link State Update	链路状态更新报文，在该报文中就包含完整的链路状态信息。
LSAck Link State Ack	用于确保OSPF报文的可靠传输。

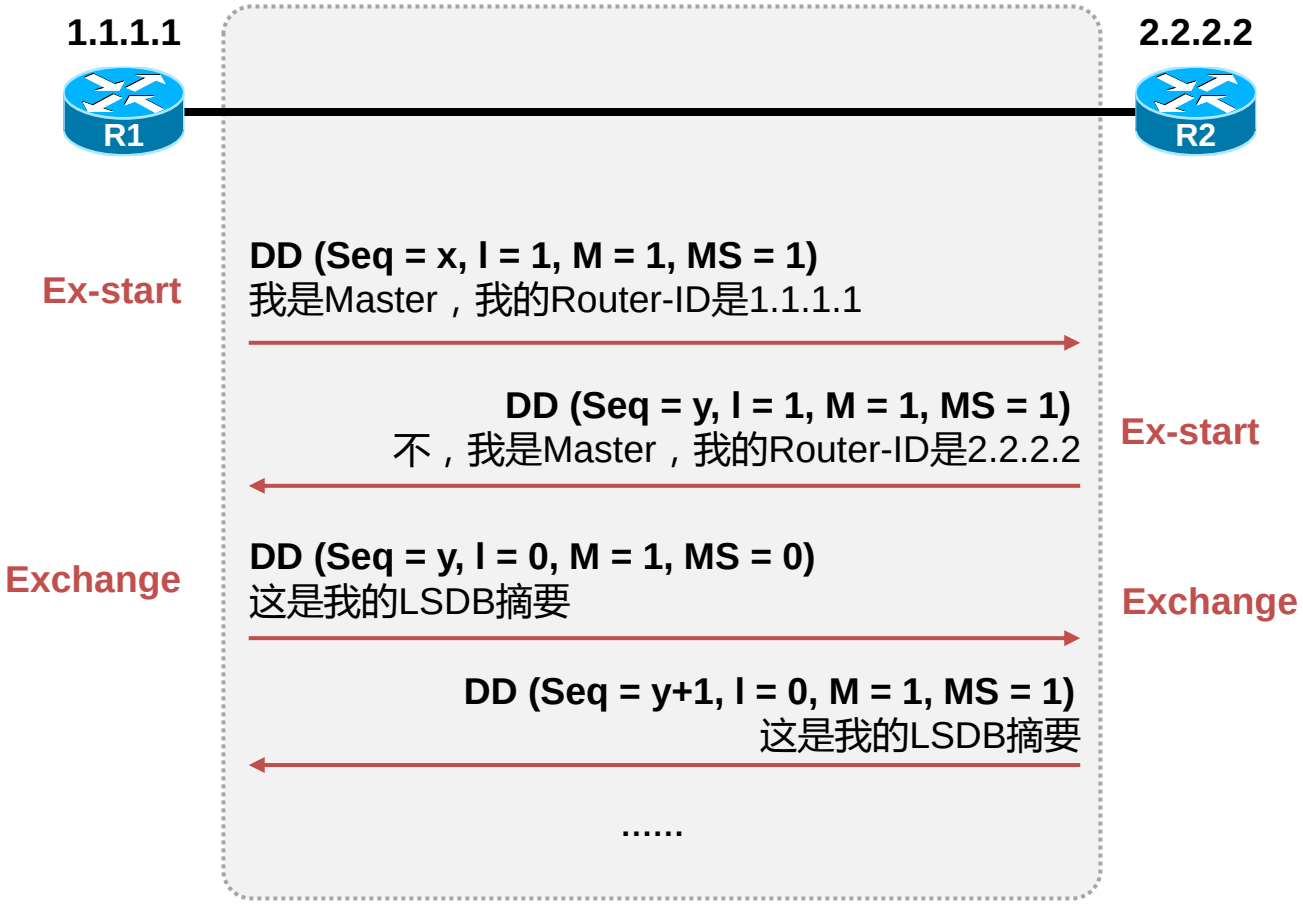
OSPF的三张表

- **邻居表（Neighbor Table）：**
  - 两台路由器的OSPF要协同工作，最基本的要求是两者需形成圈毗邻的邻接关系，邻居表存储了OSPF路由器邻居的状态以及关于该邻居的其他数据。
- **拓扑数据库（Link-state Database）：**
  - OSPF用LSA（Link State Advertisement 链路状态通告）来描述网络拓扑信息，LSDB中存储着路由器产生或者收到的LSA。
- **OSPF路由表（OSPF Routing Table）：**
  - 基于LSDB进行SPF算法运算，计算得出的路由被加载到路由表中。

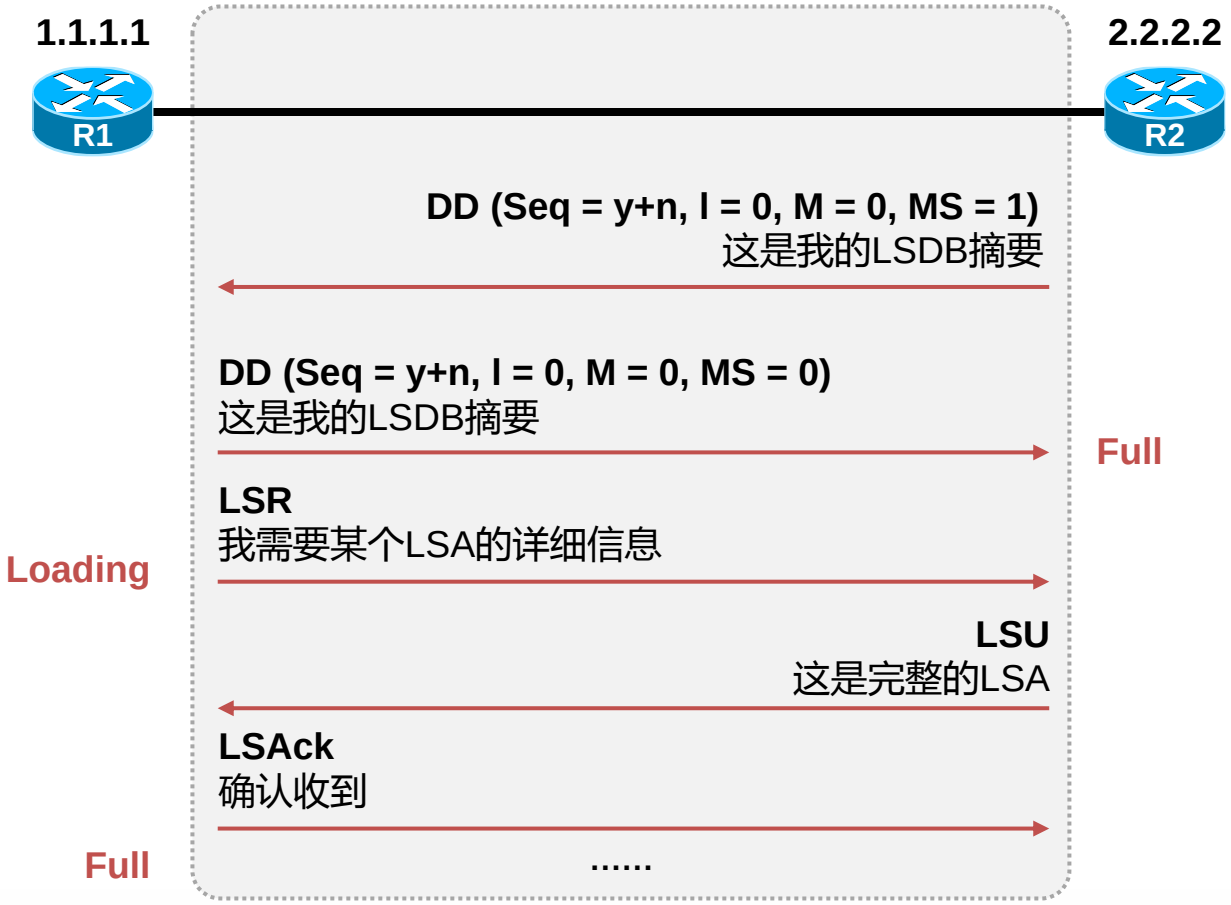
OSPF邻居关系的建立



OSPF邻居关系的建立



OSPF邻居关系的建立



OSPF邻居表

Router# show ip ospf neighbor

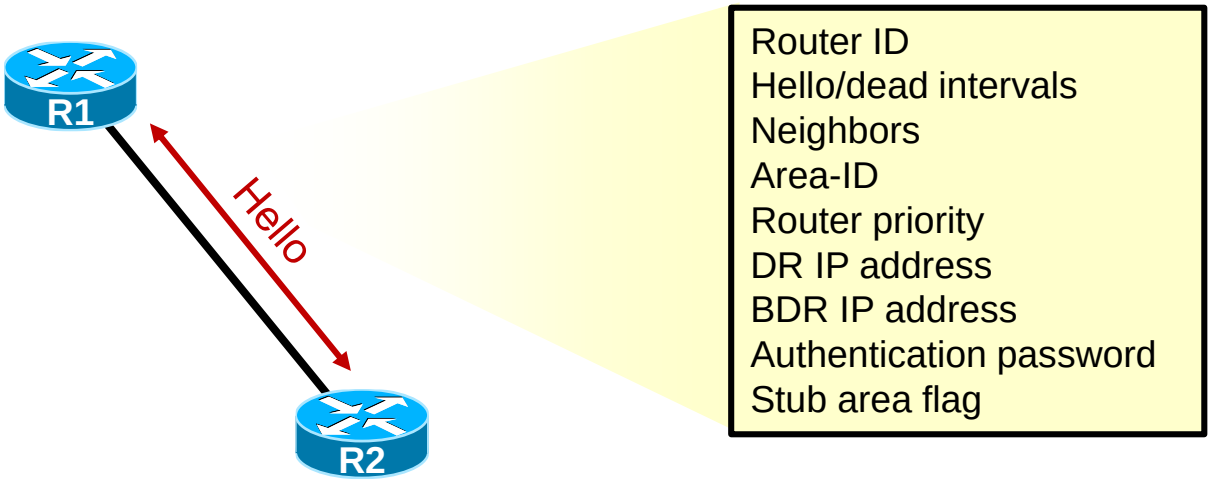
Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.0.13	1	2WAY/DROTHER	00:00:31	192.168.0.13	Ethernet0
192.168.0.14	1	FULL/BDR	00:00:38	192.168.0.14	Ethernet0
192.168.0.11	1	2WAY/DROTHER	00:00:36	192.168.0.11	Ethernet0
192.168.0.12	1	FULL/DR	00:00:38	192.168.0.12	Ethernet0

OSPF over Ethernet - Multiaccess Network

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.0.11	1	FULL/ -	00:00:39	10.1.1.2	Serial1

OSPF over HDLC - Point-to-Point Network

Hello Packet

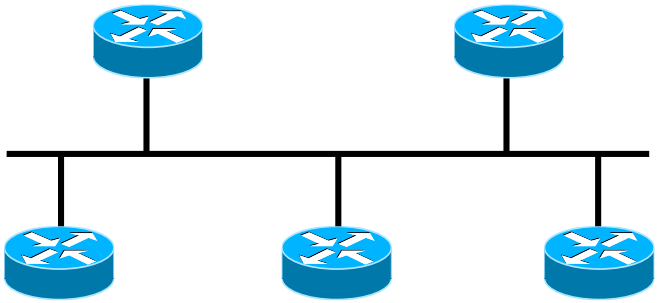


- OSPF使用Hello报文来发现直连链路上的其他OSPF路由器，Hello报文发向组播地址224.0.0.5（All-OSPF-Routers）
- 两台OSPF路由器（的接口）需具备匹配的参数才能够建立起OSPF邻居关系

OSPF Network-Type 网络类型

- OSPF支持多种网络类型：Broadcast、P2P、NBMA、P2MP。
- 网络类型的概念是一个接口级别的概念，一个OSPF接口的网络类型受该接口的数据链路层封装影响，不用的网络类型，OSPF的操作有所不同。

OSPF Network-Type 网络类型

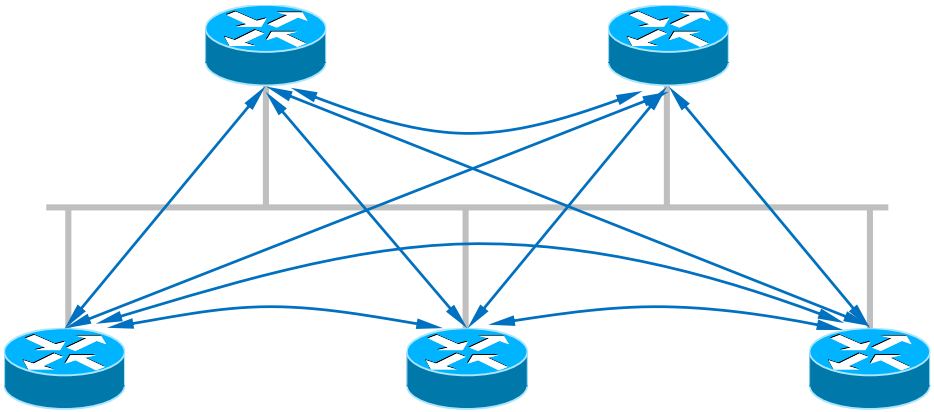


Broadcast Multi-Access
广播型多路访问

Point-to-Point
点对点

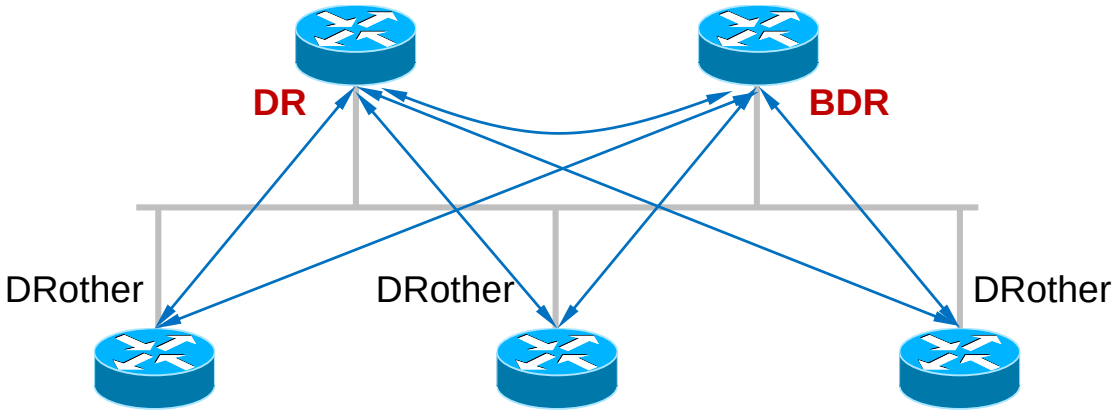
NBMA
非广播型多路访问

DR、BDR



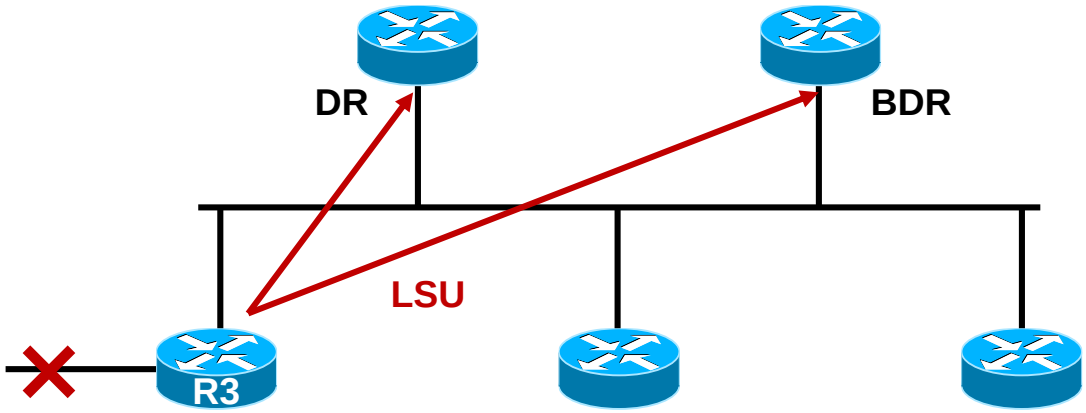
- MA（Multi-Access）多路访问网络有两种类型：广播型多路访问网络（BMA）及非广播型多路访问网络（NBMA）。以太网是一种典型的广播型多路访问网络（见上图）。
- 在MA网络中每台OSPF路由器需与其他的所有路由器建立OSPF邻居关系，这就导致网络中存在过多的OSPF邻接关系。
- 当拓扑出现变更，网络中的LSA泛洪可能会造成带宽的浪费和设备资源的损耗。

DR、BDR



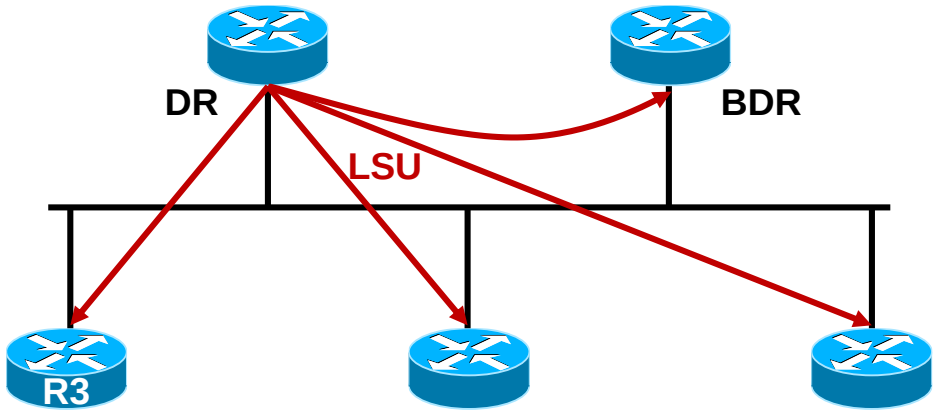
- 为减少MA网络中的OSPF泛洪，OSPF会在每一个MA网络中选举一个指定路由器 DR（Designated Router）和一个备用指定路由器BDR（Backup Designated Router）。
- MA网络中的路由器都只与DR、BDR建立OSPF邻接关系，DRother之间不会建立全毗邻的OSPF邻接关系，只是停滞在2way状态。
- BDR 会监控 DR 的状态，并在当前 DR 发生故障时接替其角色。
- 选举规则：OSPF DR优先级最高的接口成为该MA的DR，如果优先级相等（默认为1），则具有最高的OSPF Router-ID的路由器（的接口）被选举成DR，并且DR具有非抢占性。

MA网络中LSA的泛洪 -1



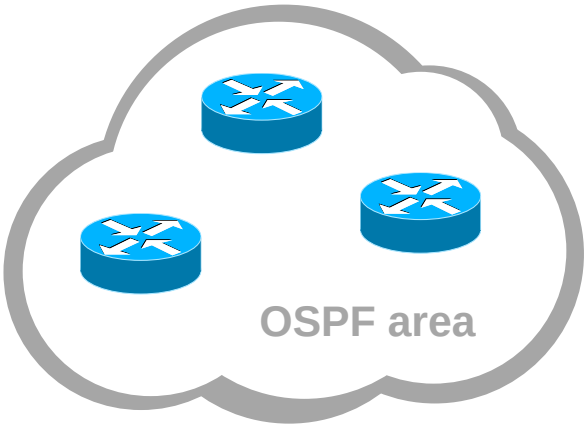
- 路由器R3感知到拓扑变更，向组播地址**224.0.0.6**发送LSU
- DR、BDR监听224.0.0.6这一组播地址

MA网络中LSA的泛洪 -2



- DR向组播地址**224.0.0.5**发送更新以便通知其它路由器
- 所有的OSPF路由器监听224.0.0.5这一组播地址，便能收到DR泛洪的LSU
- 路由器收到包含变化后的LSA的LSU后，更新自己的LSDB，对更新的链路状态数据库执行SPF算法，必要时更新路由表。

OSPF Single Area



- 同一个area内的路由器需同步LSDB，随着网络规模越来越大，路由器数量越来越多，每台路由器维护的LSDB就非常庞大；
- 当网络拓扑变更时LSA泛洪严重；区域内部的动荡会引起全网路由器的SPF计算；
- LSDB太庞大，路由器的资源消耗过多，设备性能下降，影响数据转发；
- 每台路由器都需要维护的路由表越来越大，单区域内路由无法汇总。

OSPF Multiple Areas

- OSPF多区域的设计减小了LSA洪泛的范围，有效地把拓扑变化的影响控制在区域内，达到网络优化的目的；
- 在区域边界可以做路由汇总，减小了路由表规模；
- 充分利用OSPF特殊区域的特性，进一步减少LSA泛洪，从而优化路由；
- 多区域提高了网络的扩展性，有利于组建大规模的网络 。

红茶三杯
Vinsoney

OSPF的配置及验证

基础配置

- 创建OSPF进程并进入OSPF进程配置模式

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

  - Process-ID为OSPF进程号，进程号只具有本地意义

- 在特定接口上激活OSPF

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

基础配置

- 查看OSPF邻居表

```
Router# show ip ospf neighbor
```

- 查看OSPF LSDB

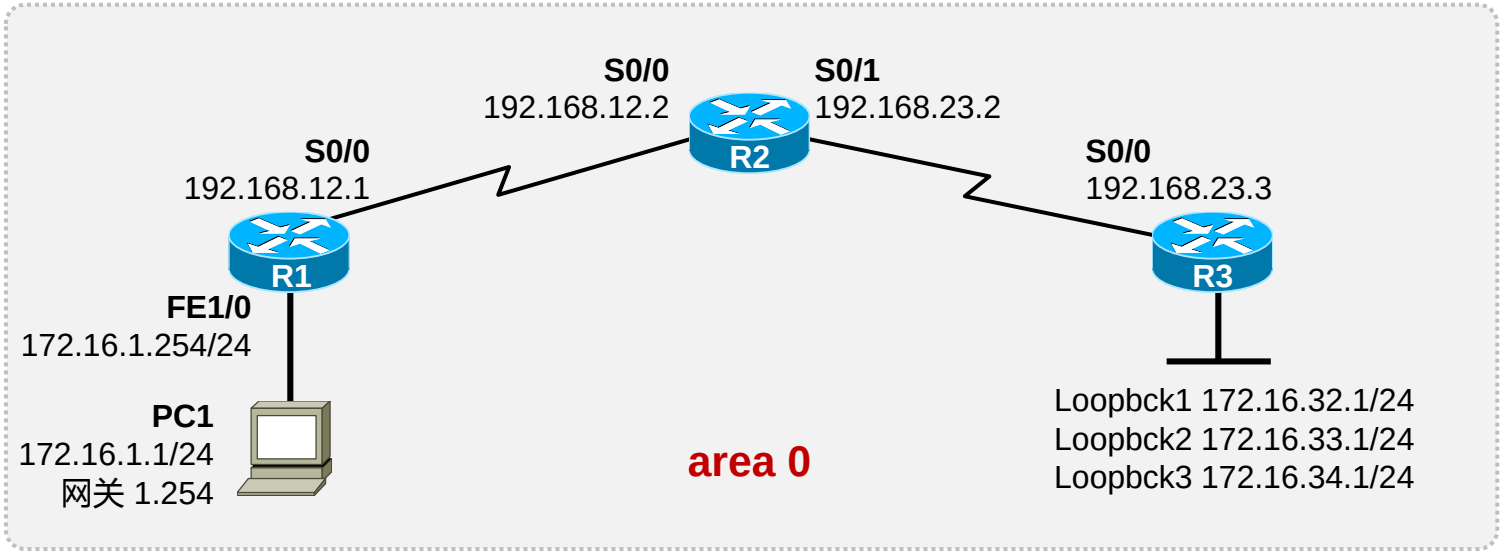
```
Router# show ip ospf database
```

Wildcard-Mask

- Wildcard-Mask 通配符掩码为32bit的、使用点分十进制格式表示的掩码
- 与IP地址搭配，用于指示该IP地址中哪些比特需要严格匹配，哪些比特无所谓

Network Mask	Widcard Mask
为1的bit表示IP地址中的网络位	为1的bit表示该bit无所谓（无需匹配）
为0的bit表示IP地址中的主机位	为0的bit表示该bit需严格匹配

配置示例1：单区域OSPF



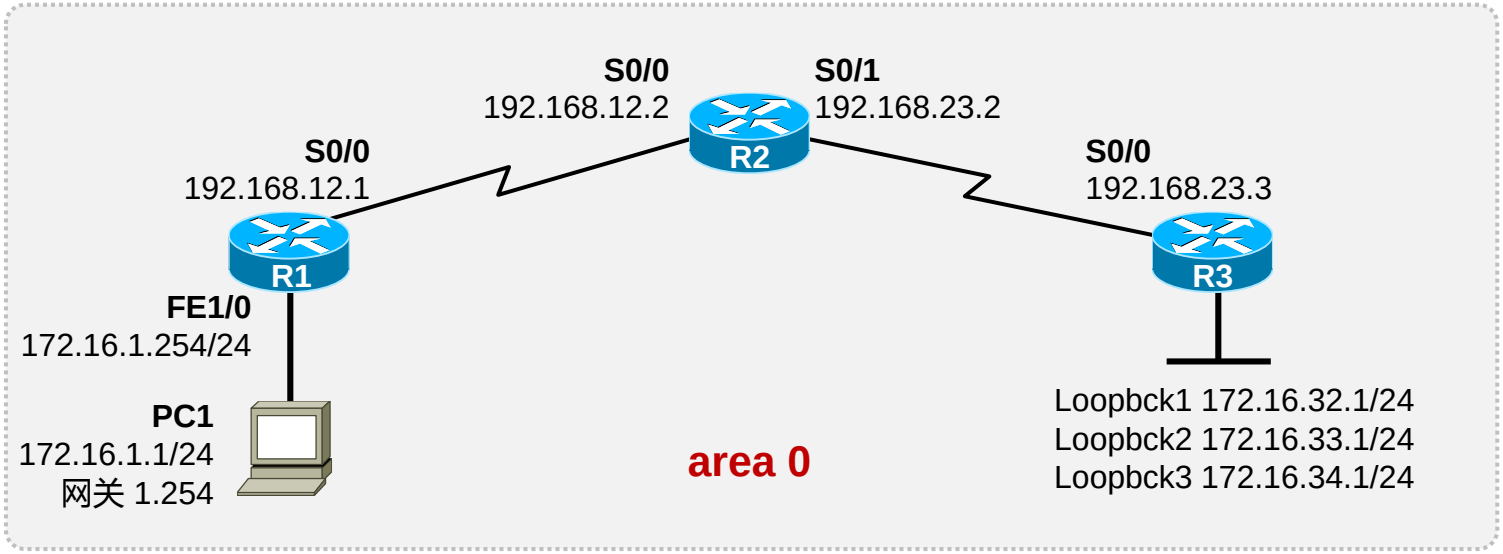
R1

```
router ospf 1
  router-id 1.1.1.1
  network 192.168.12.0 0.0.0.255 area 0
  network 172.16.1.0 0.0.0.255 area 0
```

R2

```
router ospf 1
  router-id 2.2.2.2
  network 192.168.12.0 0.0.0.255 area 0
  network 192.168.23.0 0.0.0.255 area 0
```

配置示例1：单区域OSPF (cont.)



R3

```
router ospf 1
  router-id 3.3.3.3
  network 192.168.23.0 0.0.0.255 area 0
  network 172.16.32.0 0.0.0.255 area 0
  network 172.16.33.0 0.0.0.255 area 0
  network 172.16.34.0 0.0.0.255 area 0
```

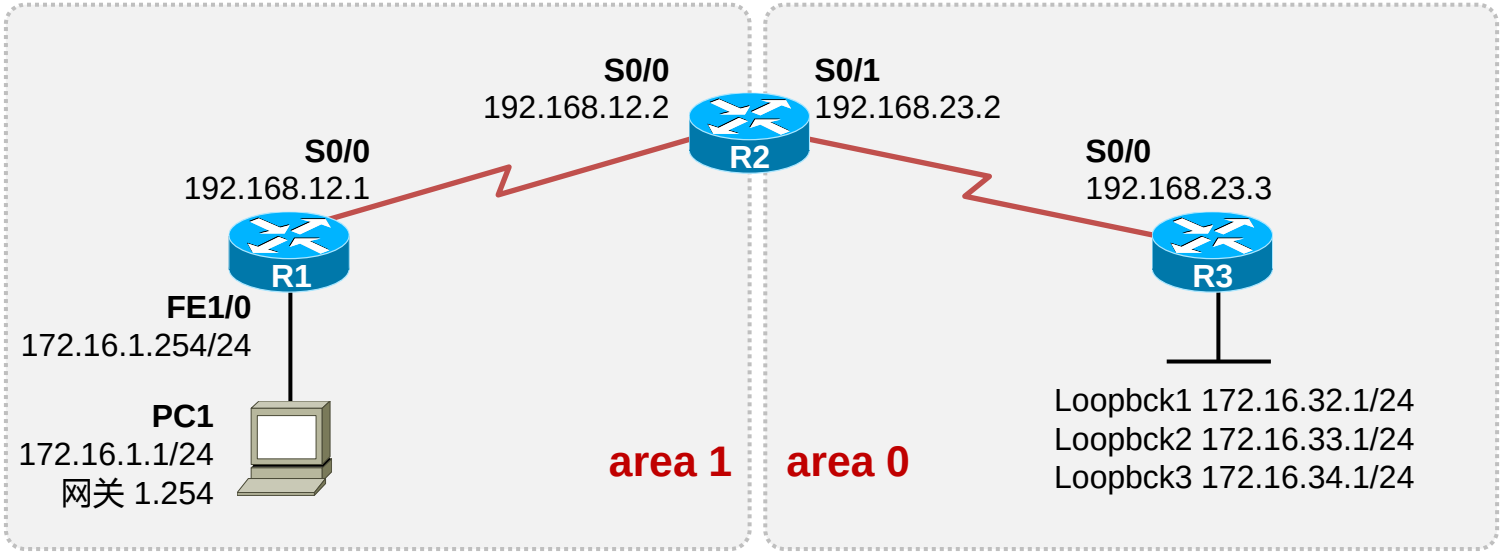
PC

```
no ip routing

Interface fastethernet 0/0
  ip address 172.16.1.1 255.255.255.0

ip default-gateway 172.16.1.254
```

配置示例2：多区域OSPF



R1

```
router ospf 1
  router-id 1.1.1.1
  network 192.168.12.0 0.0.0.255 area 1
  network 172.16.1.0 0.0.0.255 area 1
```

R2

```
router ospf 1
  router-id 2.2.2.2
  network 192.168.12.0 0.0.0.255 area 1
  network 192.168.23.0 0.0.0.255 area 0
```

红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You

红茶三杯
Vinsoney

学习 沉淀 成长 分享

二层交换基础

红茶三杯 http://weibo.com/vinsoney

Latest update: 2012-08-01

Content

红茶三杯
Vinsoney

二层交换基础

- 园区网中的二层交换
- 二层交换机的主要功能
- MAC地址的概念
- 交换机的寻址

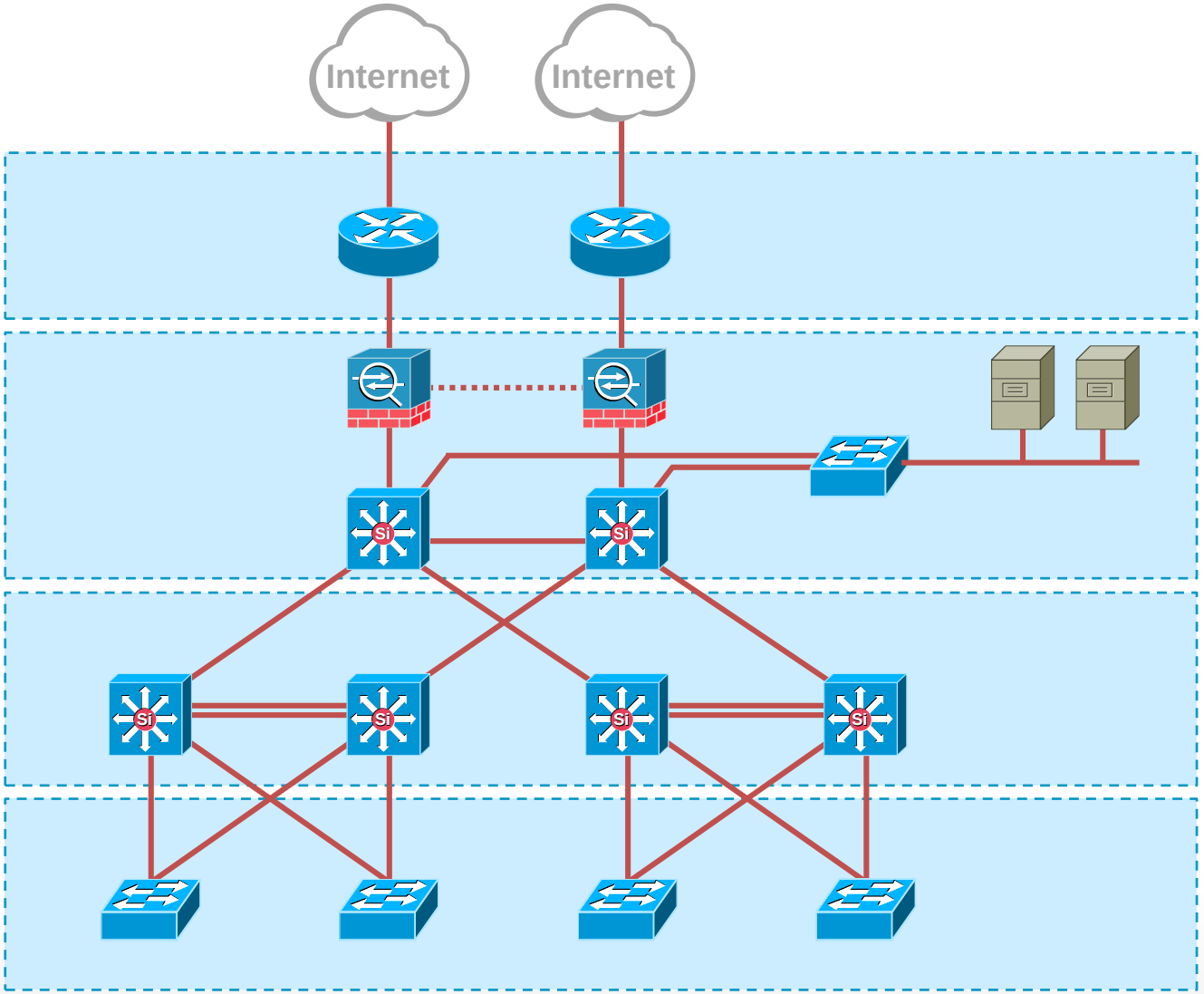
园区网

出口层（OR）
广域网接入
出口策略
带宽控制

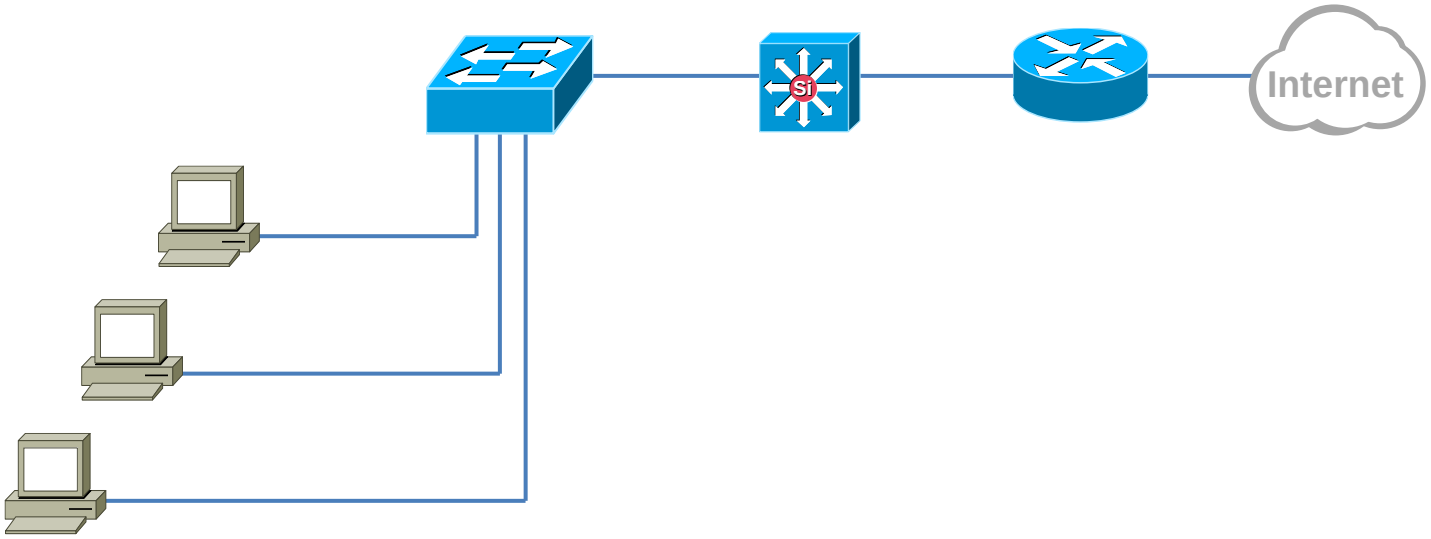
核心层（CO）
高速转发
服务器接入
路由选择

汇聚层（GS）
流量汇聚
链路冗余
设备冗余
路由选择

接入层（AS）
用户接入
接入安全
访问控制

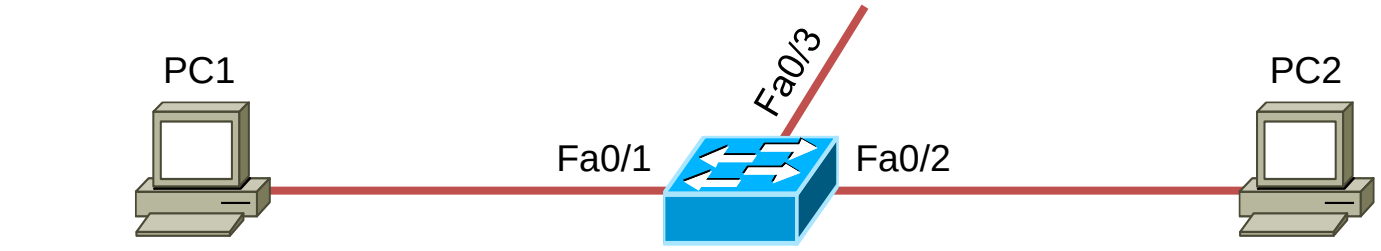


二层交换机的主要功能



- 终端设备的接入；
- 以太网数据帧的交换，根据目的MAC地址转发数据帧；
- 学习MAC地址，并维护MAC地址表；
- 防止二层环路。

MAC地址

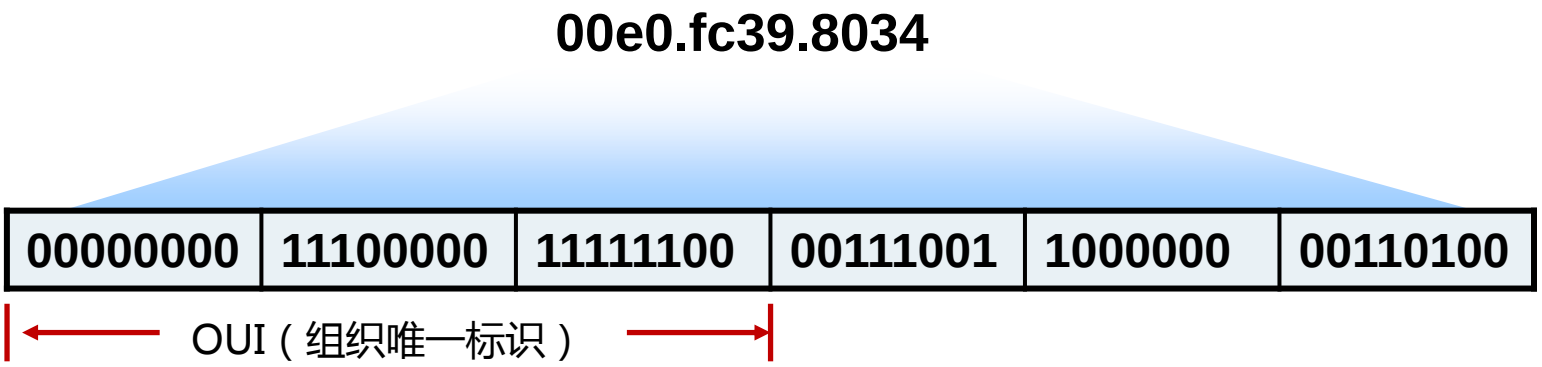


源MAC	0050-5600-0001
目MAC	0050-5600-0002
源IP	192.168.1.1
目IP	192.168.1.2

交换机查看数据帧的二层头部；在自己的MAC地址表中查找目的MAC；随后将数据帧从特定的端口转发出去。

源MAC	0050-5600-0001
目MAC	0050-5600-0002
源IP	192.168.1.1
目IP	192.168.1.2

MAC地址



- MAC地址有48位，通常被表示为点分十六进制数；
- MAC地址全球唯一，由 IEEE对OUI进行管理和分配；
- 每个地址由两部分组成，分别是供应商代码和序列号。其中前24位二进制代表该供应商代码。剩下的24位由厂商自己分配。

MAC地址表

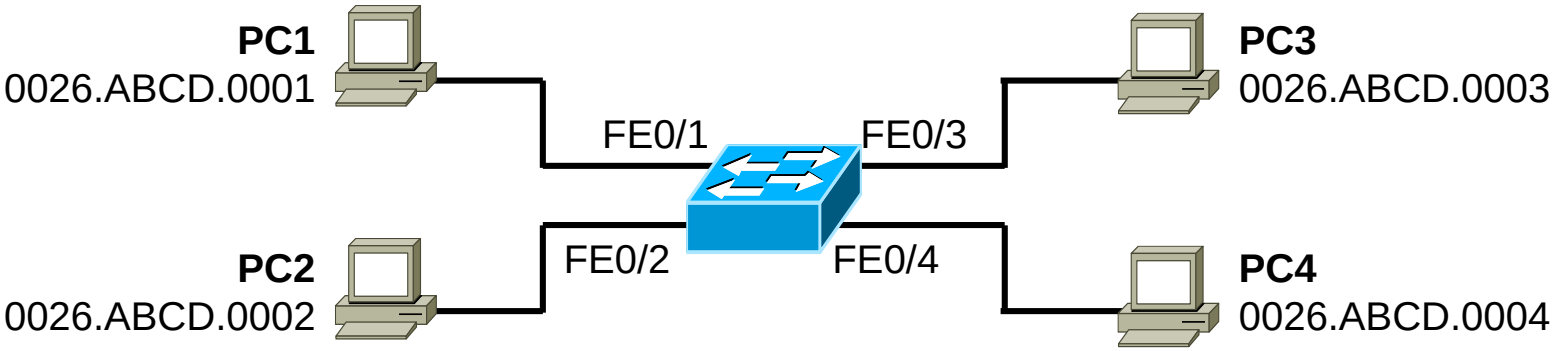
switch#show mac-address-table

Mac Address Table

Vlan	Mac Address	Type	Ports
1	0002.8502.def0	DYNAMIC	Gi0/1
1	0015.f915.8e80	DYNAMIC	Gi0/1
1	0030.b637.8e10	DYNAMIC	Gi0/1
10	0027.450b.c00a	STATIC	Gi0/2
20	00d0.bbe4.da59	DYNAMIC	Gi0/5

Catalyst交换机默认情况下动态MAC表项的老化时间为300s

二层交换机的寻址及数据交换



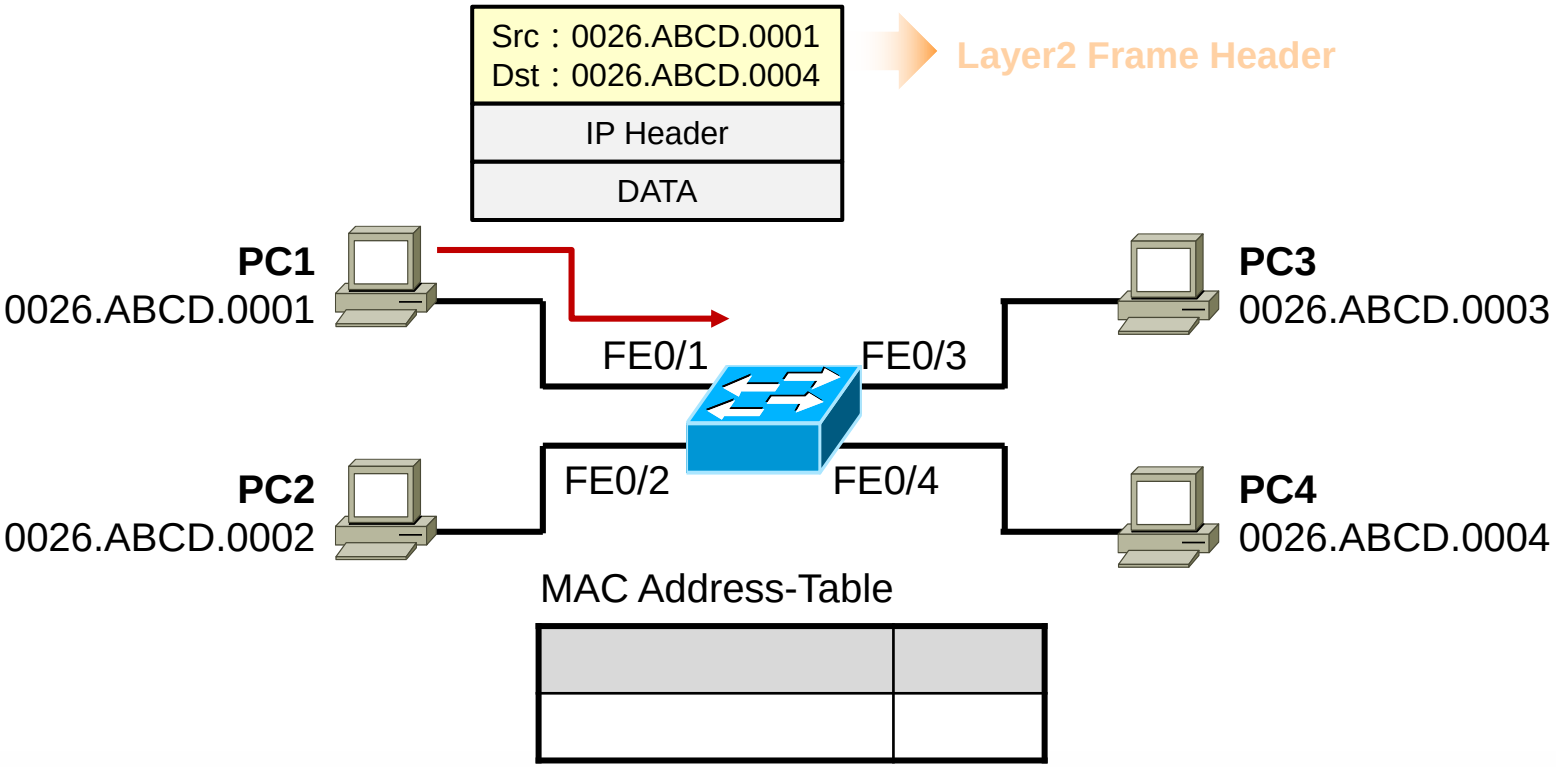
MAC Address-Table

MAC Address	Port

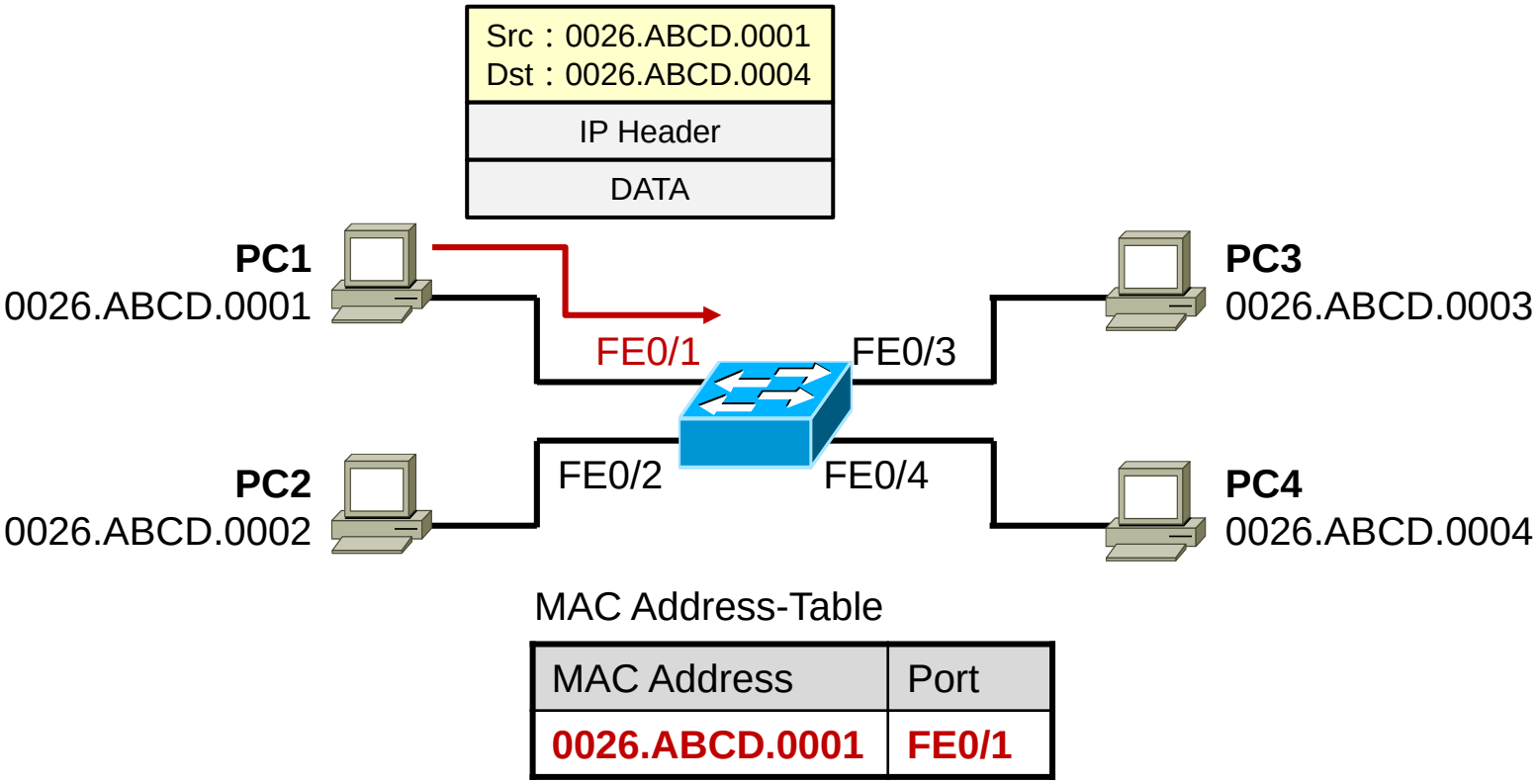
① 初始情况下交换机的MAC地址表是空的。

二层交换机的寻址及数据交换

② PC1发送一个数据帧给PC4，
暂且假设PC1已经知道PC4的MAC地址。



二层交换机的寻址及数据交换

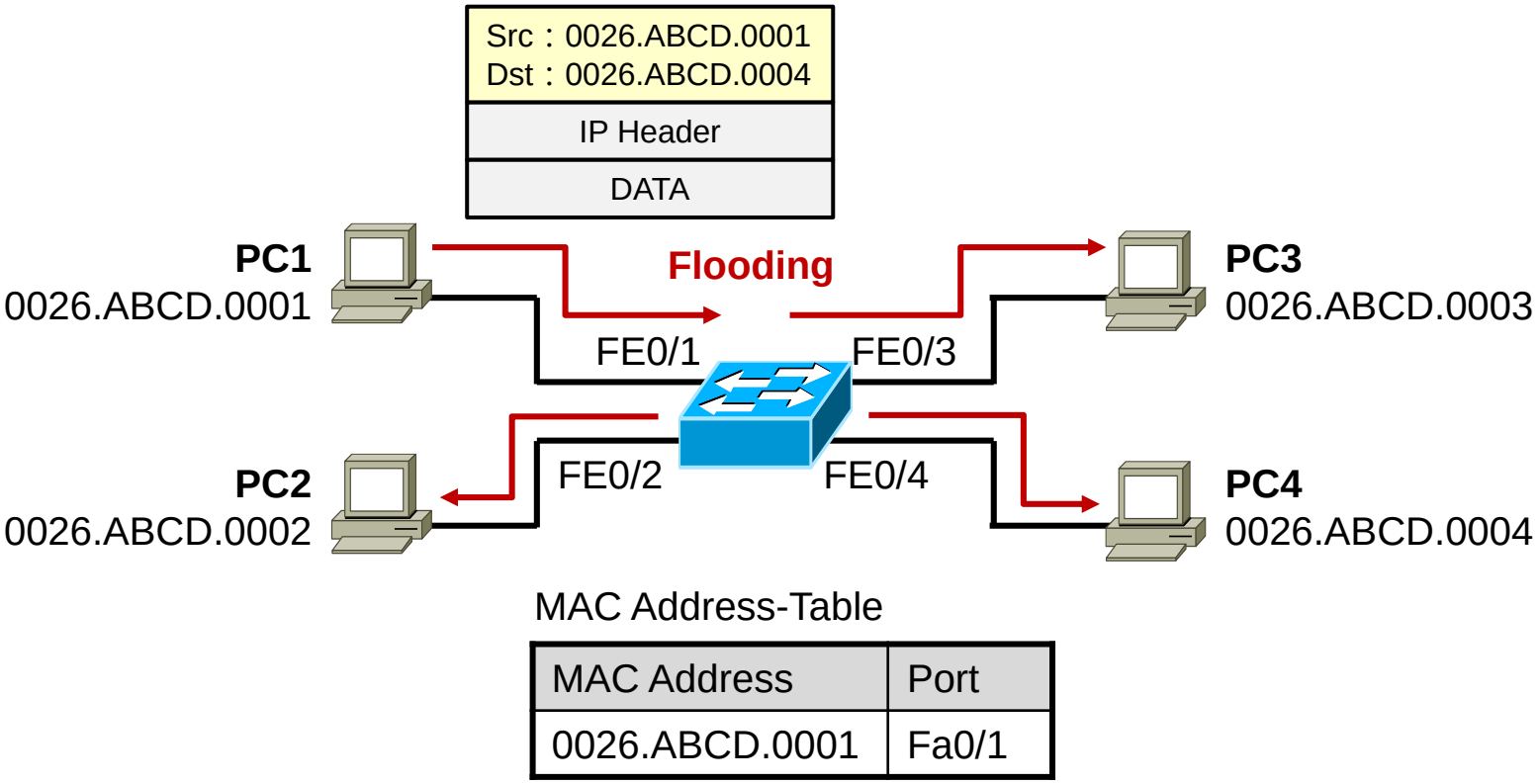


MAC Address-Table

MAC Address	Port
0026.ABCD.0001	**FE0/1**

③ 交换机在收到数据帧后，将数据帧的源MAC地址学习到MAC地址表中，并与接收该帧的接口FE0/1口关联。

二层交换机的寻址及数据交换

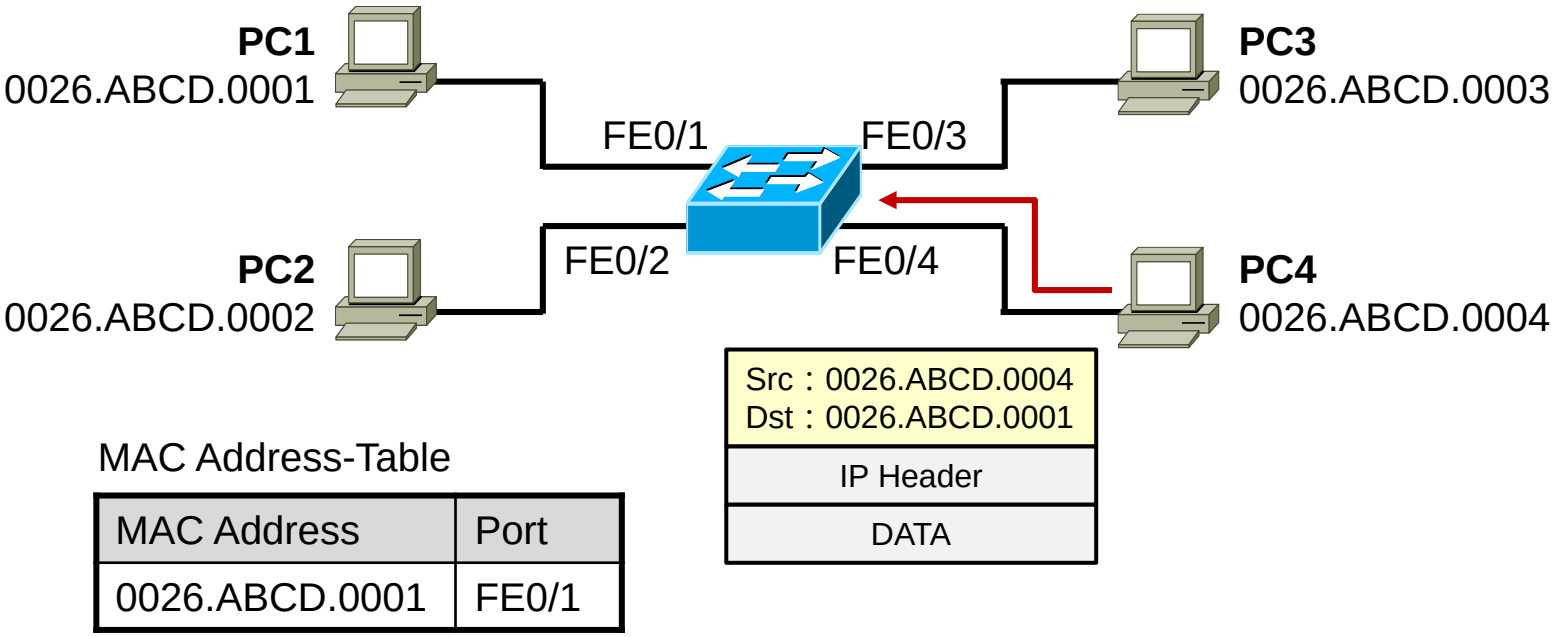


MAC Address-Table

MAC Address	Port
0026.ABCD.0001	Fa0/1

④ 交换机在MAC地址表中查询数据帧的目的MAC地址，发现没有匹配的表项，因此将数据帧从除了其入站接口之外的所有接口泛洪出去。

二层交换机的寻址及数据交换

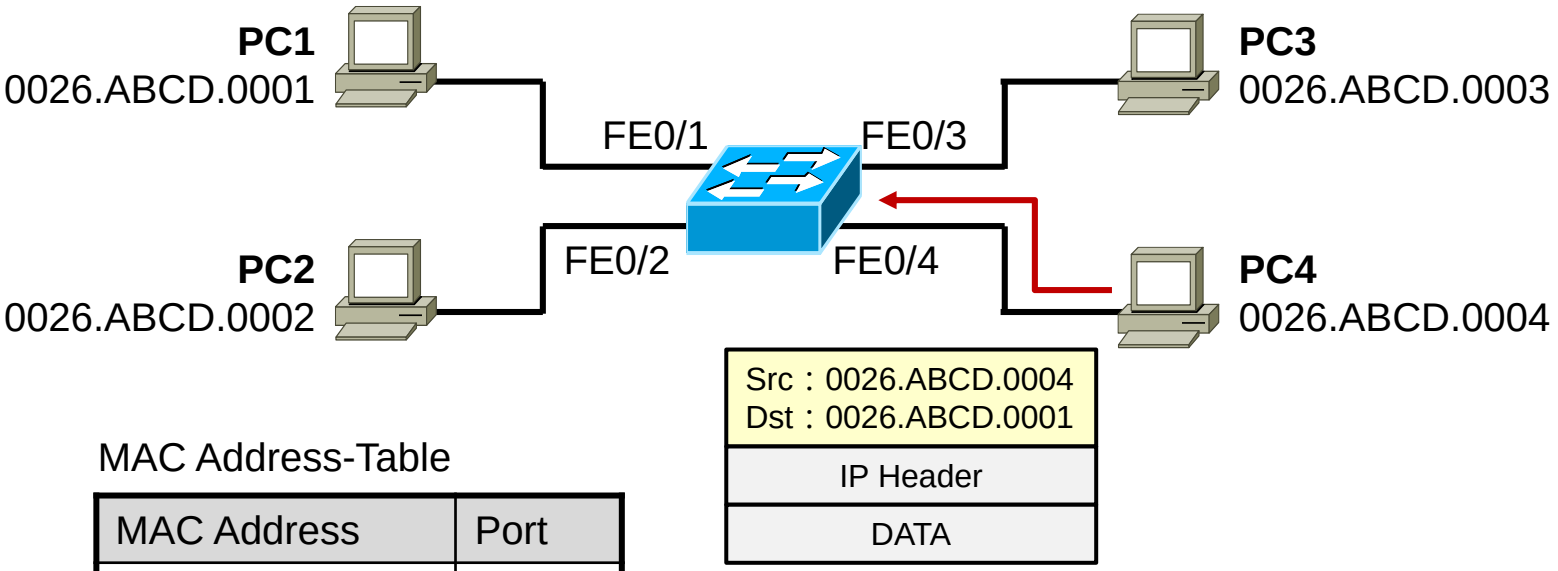


MAC Address-Table

MAC Address	Port
0026.ABCD.0001	FE0/1

⑤ PC2及PC3收到数据帧后将其丢弃，因为这些数据帧并非发送给自己；PC4则收下数据帧。现在PC4要回复数据给PC1

二层交换机的寻址及数据交换

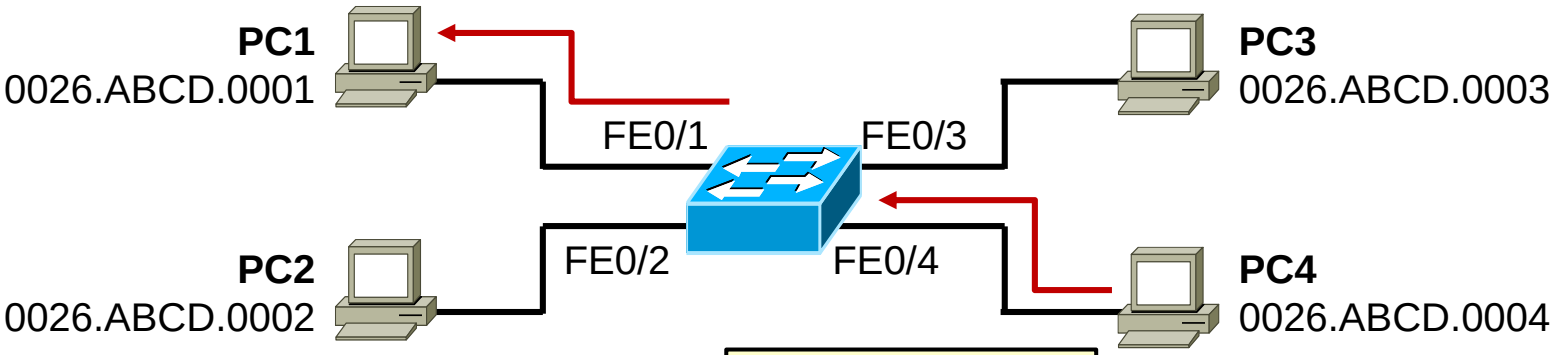


MAC Address-Table

MAC Address	Port
0026.ABCD.0001	FE0/1
0026.ABCD.0004	**FE0/4**

⑥ 交换机收到了数据帧，将帧头中的源MAC地址学习到MAC表中，并与接口F0/4关联。

二层交换机的寻址及数据交换



MAC Address-Table

MAC Address	Port
0026.ABCD.0001	**FE0/1**
0026.ABCD.0004	FE0/4

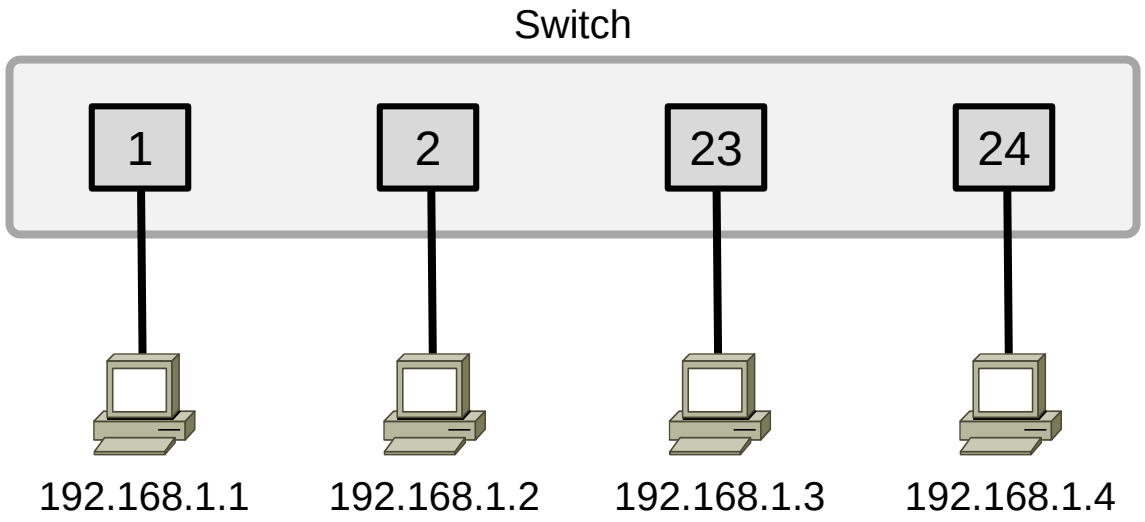
⑦ 随后交换机在MAC表中查找数据帧的目的MAC地址，发现有一个匹配的表项，出接口是Fa0/1，于是将数据帧转发到Fa0/1口

红茶三杯
Vinsoney

VLAN及Trunk

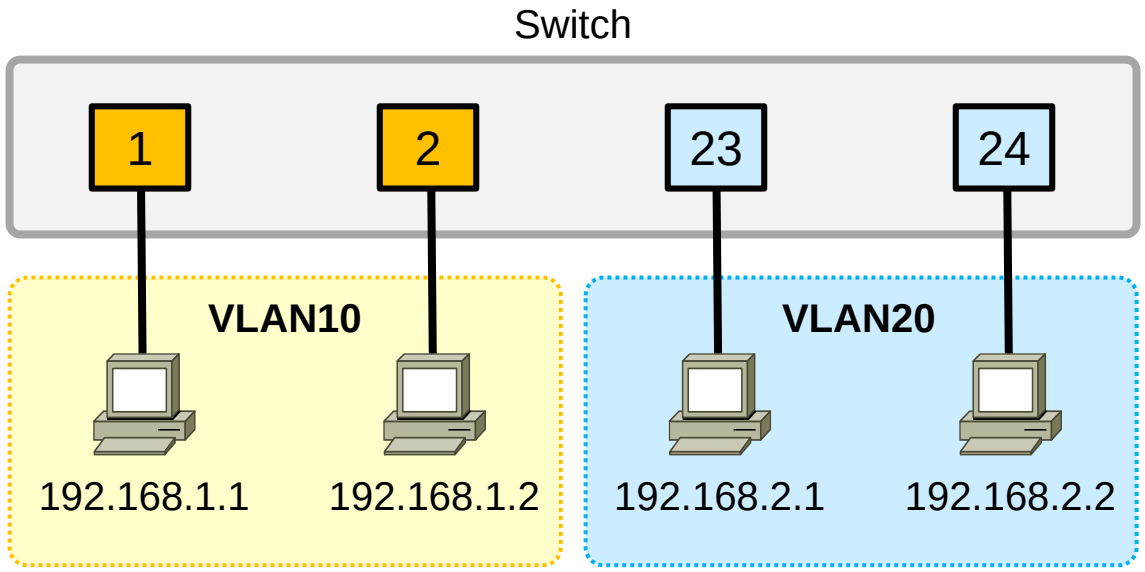
- VLAN带来什么
- VLAN的概念
- Trunk的概念

为什么需要VLAN



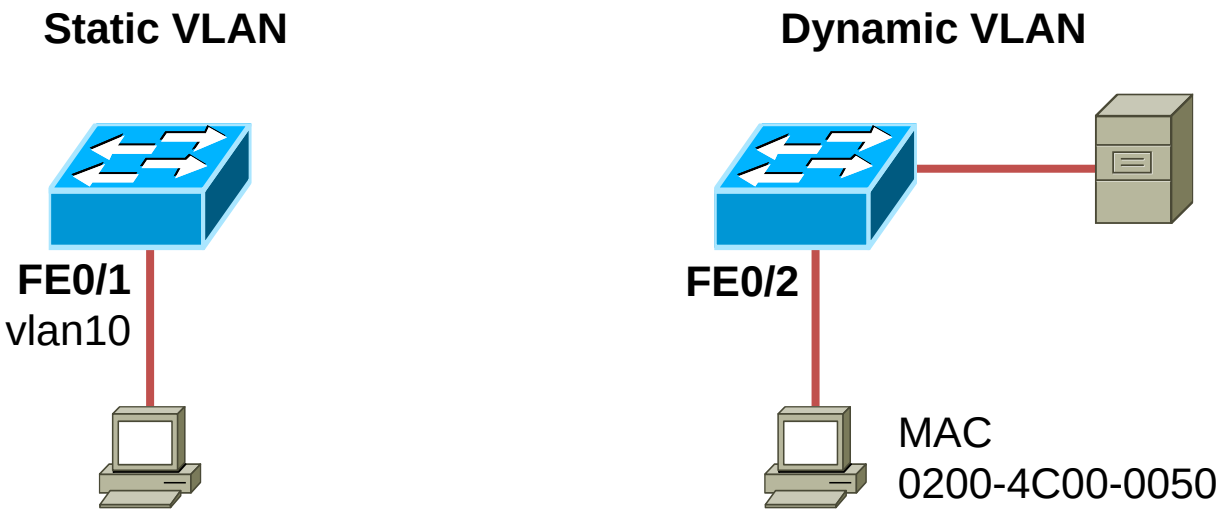
- 交换机的所有接口属于一个广播域，往往也是一个逻辑子网；
- 用户无法根据业务需要灵活的在交换机上进行广播域的隔离；
- 随着网络规模越来越大、数量越来越多，广播风暴将给网络带来重大问题。

为什么需要VLAN



- VLAN（Virtual LAN）技术提供了一种灵活的解决方案；
- 将交换机的接口根据业务需要添加到不同的VLAN中，从而实现二层隔离。

VLAN的成员模式



- 静态 VLAN - 以手工的方式将接口加入特定的VLAN；
- 动态 VLAN - 根据接入到交换机的客户端的MAC地址等信息，动态地将交换机的接口添加到特定的VLAN。

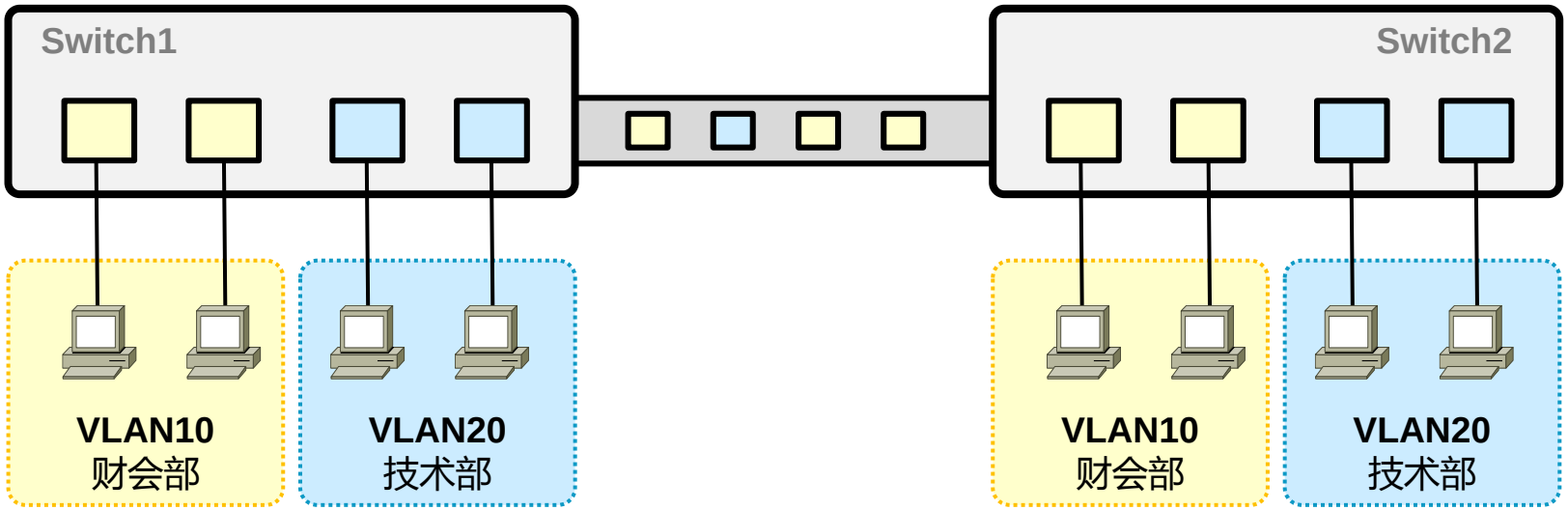
VLAN知识点小结

- 一个VLAN中所有设备处于同一广播域内，不同的VLAN为不同的广播域，一个VLAN一般是一个IP网段，不同的VLAN规划到不同的IP网段；
- 不同的VLAN之间二层隔离，广播不能跨越VLAN传播，因此不同VLAN之间的设备无法进行二层通信，需通过三层设备实现互通；
- VLAN中成员关系多基于交换机的接口进行静态地分配，划分VLAN就是将交换机的接口添加到特定VLAN；
- VLAN工作于OSI参考模型的第二层，是二层交换机的一个非常根本的工作机制。

Access接口

- Access是交换机二层接口的一种类型，通常用于连接终端（例如PC或服务器）或路由器；
- Access接口只能加入一个VLAN，默认交换机上的二层接口都加入VLAN1。

Trunk接口



- 当一条链路需要承载多个VLAN的流量时，需使用trunk技术；
- Trunk链路两端的交换机需采用相同的干道协议（Dot1q或ISL）；
- Trunk技术使得VLAN能够跨交换机，Trunk链路两端的接口需指定为Trunk类型。

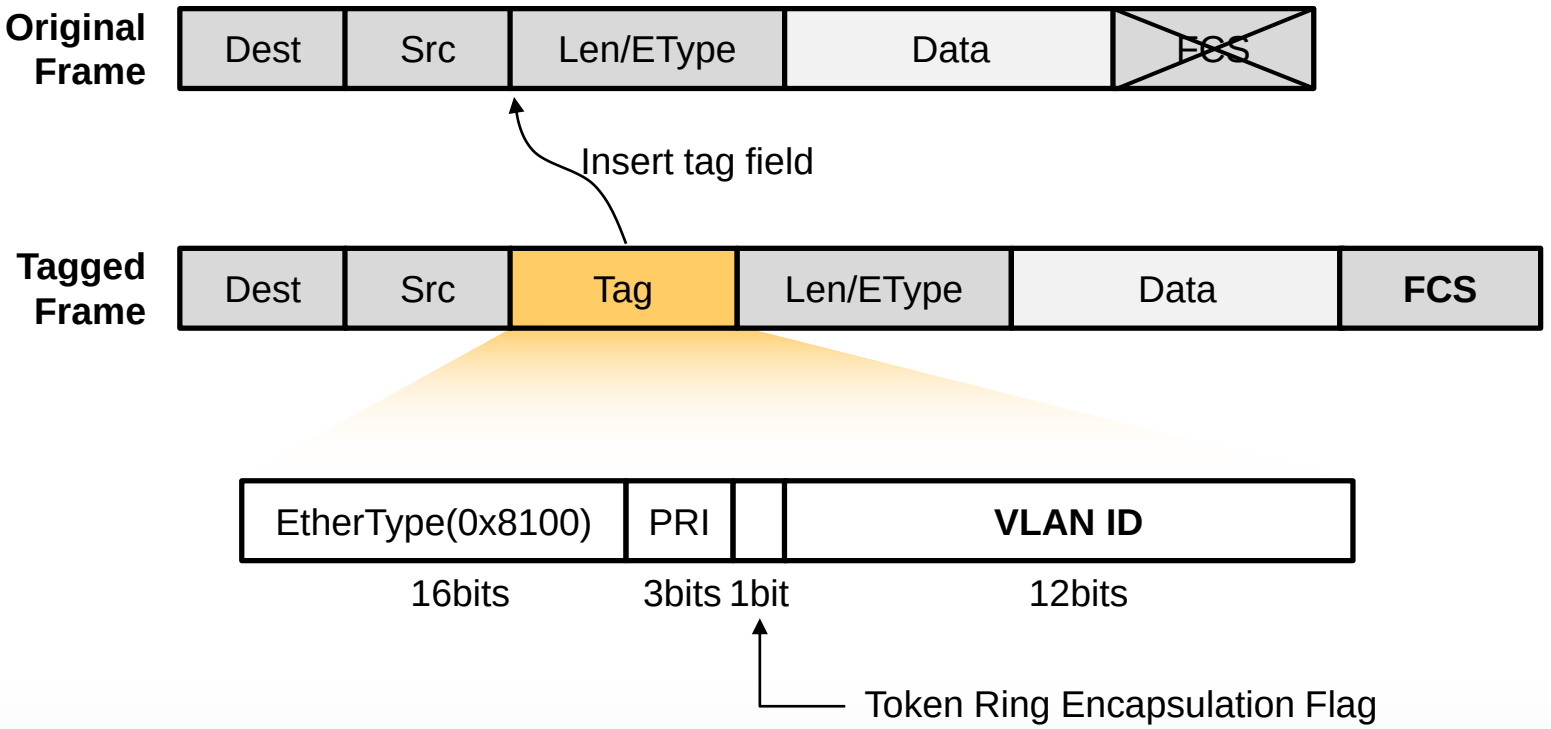
Trunk协议类型：ISL

- CISCO私有封装协议，通过硬件（ASIC）实现
- 在交换机或路由器与交换机之间，在交换机与具有ISL网卡的服务器之间可以实现

DA	TYPE	User	SA	LEN	AAAA03	HSA	VLAN	BPDU	INDEX	RES
40bit	4	4	48	16	24	24	15	1	16	16

Trunk协议类型：802.1q

- 802.1q是一种公有标准，也称为Dot1q



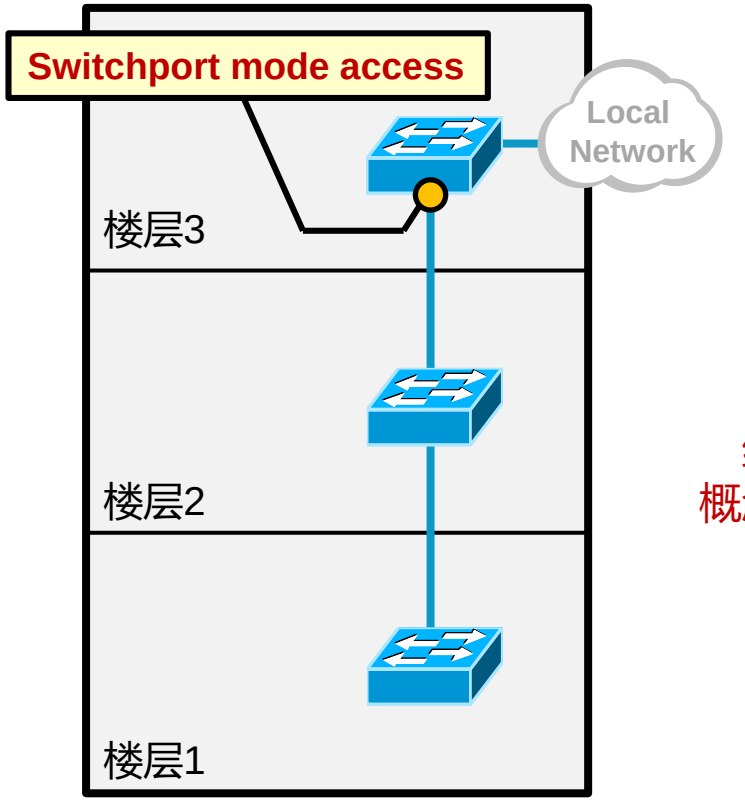
Trunk协议类型：802.1q

- 公有标准，在数据帧头的源MAC字段后插入一个802.1q的头部；
- 默认情况，在802.1Q Trunk上对所有的VLAN打Tag，除了Native VLAN；
- Native VLAN，也称为本征VLAN，是在trunk上无需打标签的VLAN，默认为vlan1，可手工修改，Trunk链路两端所配置的Native VLAN ID必须一致；
- Tag标记字段详细信息：
  - Tag 标记字段包含一个2 bytes EtherType（以太类型）字段、一个3bits的PRI字段、1bit的CFI字段、12bits的VLAN ID字段。

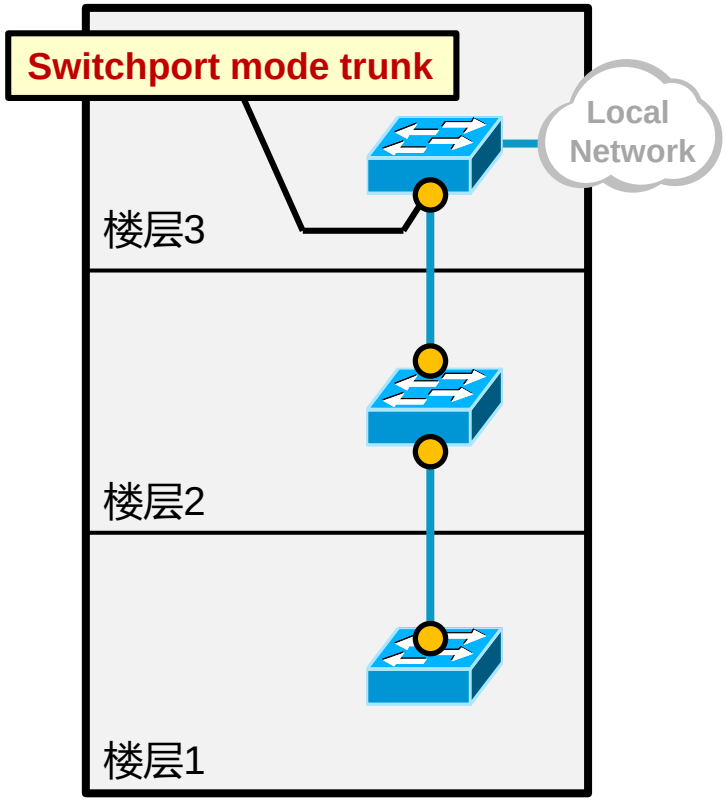
VLAN的范围

VLAN ID	范围	用途	是否通过VTP传播
0和4095	保留	用户不能使用	不适用
1	常规范围	默认VLAN，不可删除	是
2-1000	常规范围	用户能够创建、使用和删除	是
1001	常规范围	用户不能创建、使用和删除	是
1002-1005	保留	FDDI和令牌环	不适用
1006-1009	保留		不适用
1010-1024	保留		不适用
1025-4094	保留	有限使用	否

Case2 园区网中的楼层交换机



级联的
概念及问题



红茶三杯
Vinsoney

二层交换的基本配置

VLAN的基本配置

创建VLAN

```
Switch(config)# vlan 2
Switch(config-vlan)# name TechDept
```

配置Access模式的接口用于连接终端设备，并且将接口加入特定VLAN

```
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access  vlan 2
```

VLAN的基本配置

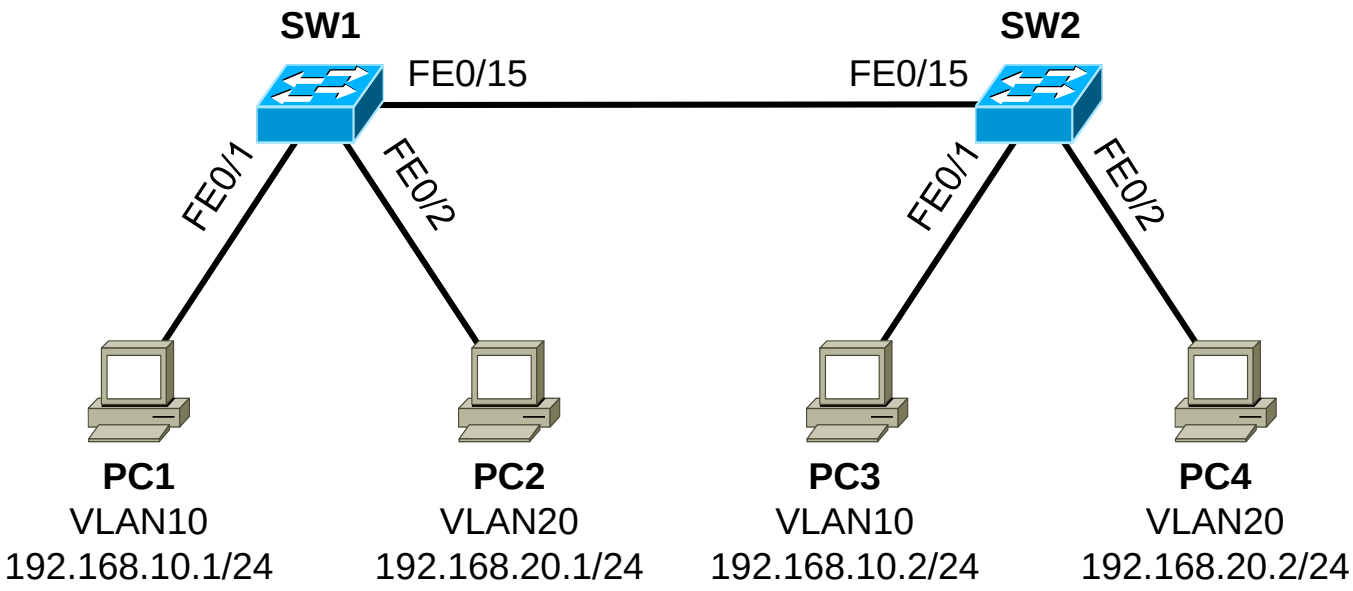
配置Trunk封装方式

```
Switch(config)# interface fa0/15
Switch(config-if)# switchport trunk encapsulation {isl | dot1q | negotiate}
```

开启端口trunk模式

```
Switch(config-if)# switchport mode {dynamic {auto | desirable} | trunk}
```

二层交换实验



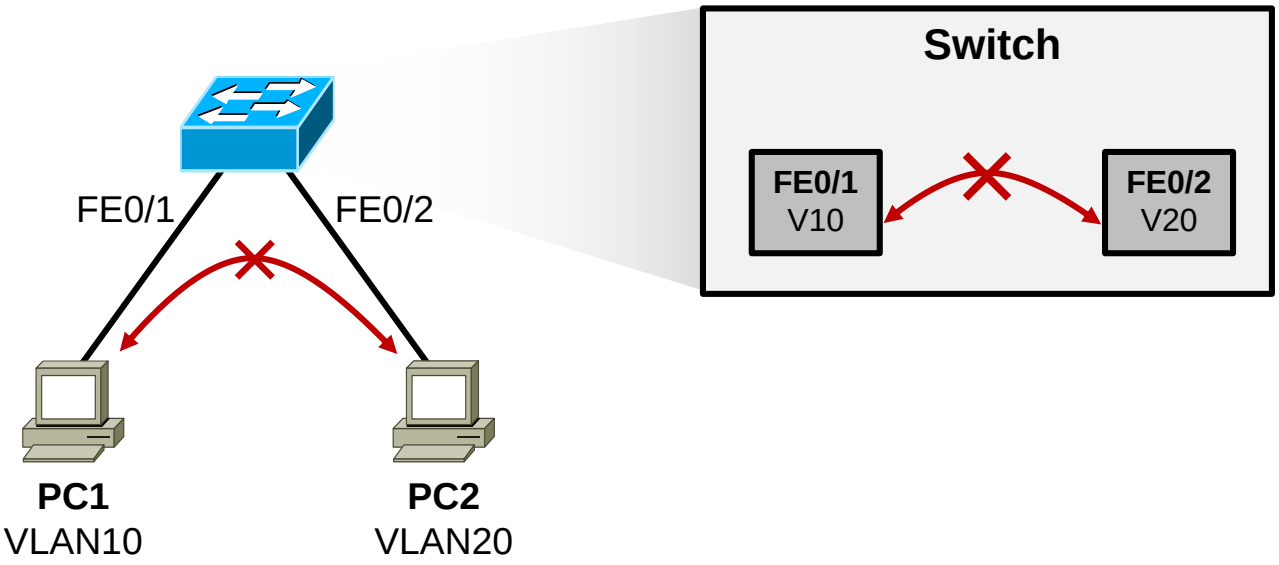
- PC1、PC2、PC3、PC4的IP地址及所属VLAN如图所示；
- 按照图示要求完成实验，使得相同VLAN内的节点，例如PC1与PC3能够互访；PC2与PC4能够互访。

红茶三杯
Vinsoney

实现VLAN间的互访

VLAN之间二层隔离

- 每个VLAN都是一个独立的广播域，不同的VLAN之间二层就已经隔离，因此属于不通VLAN的节点之间是无法直接互访的。

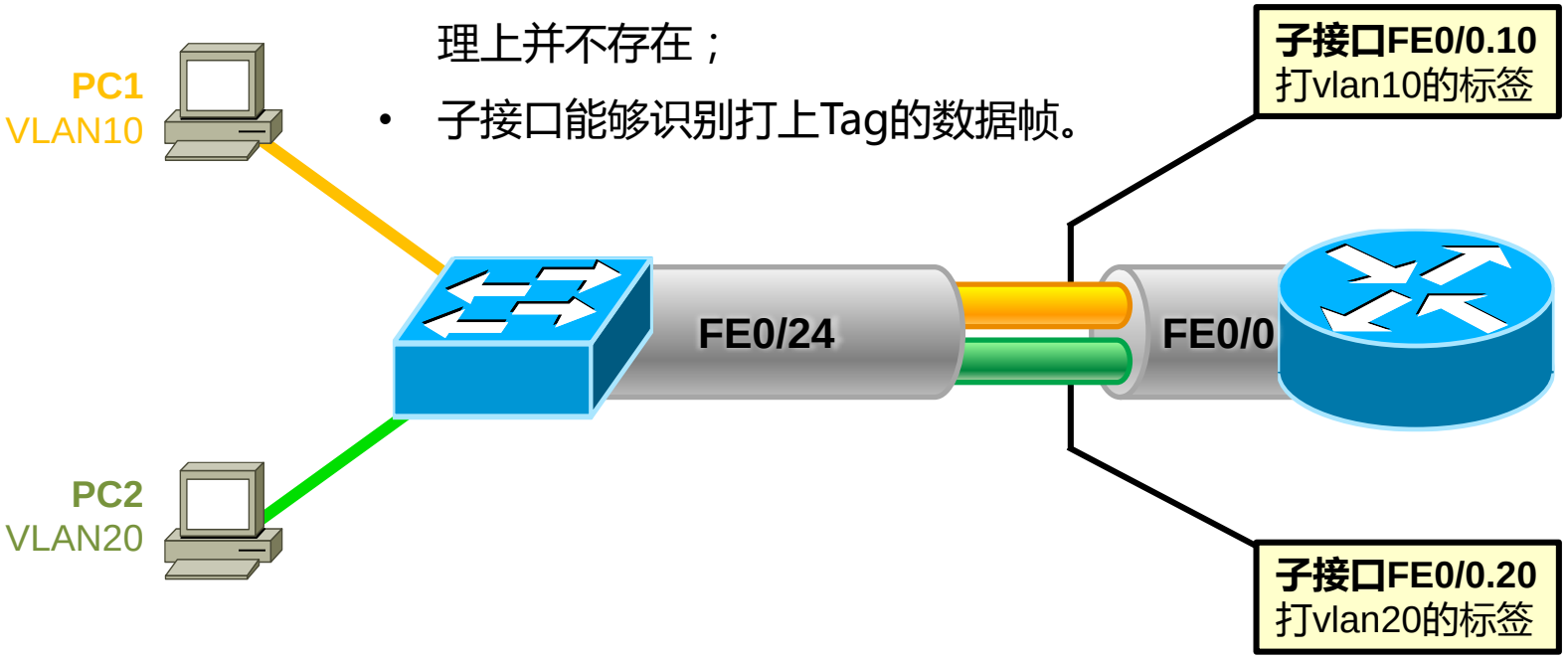


使用路由器物理接口实现VLAN间互访

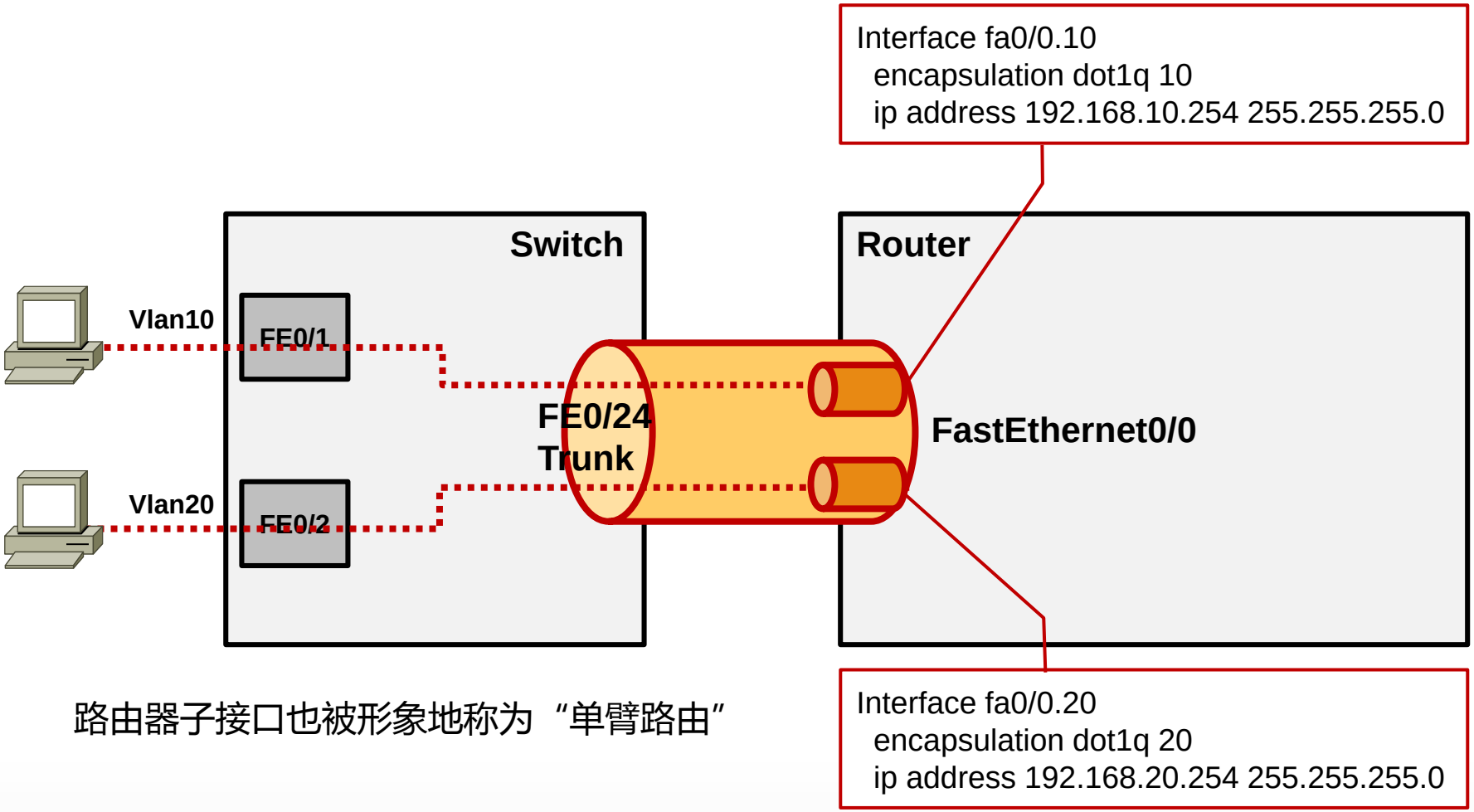
- 路由器能够实现不同广播域之间的数据路由；
- 每一个VLAN都需要有一个物理接口进行对接；
- 路由器端口资源有限，这种方案扩展性不高。

使用路由器子接口实现VLAN间互访

- 在路由器上基于物理接口来创建子接口，通过子接口与VLAN对接，子接口是逻辑接口，物理上并不存在；
- 子接口能够识别打上Tag的数据帧。

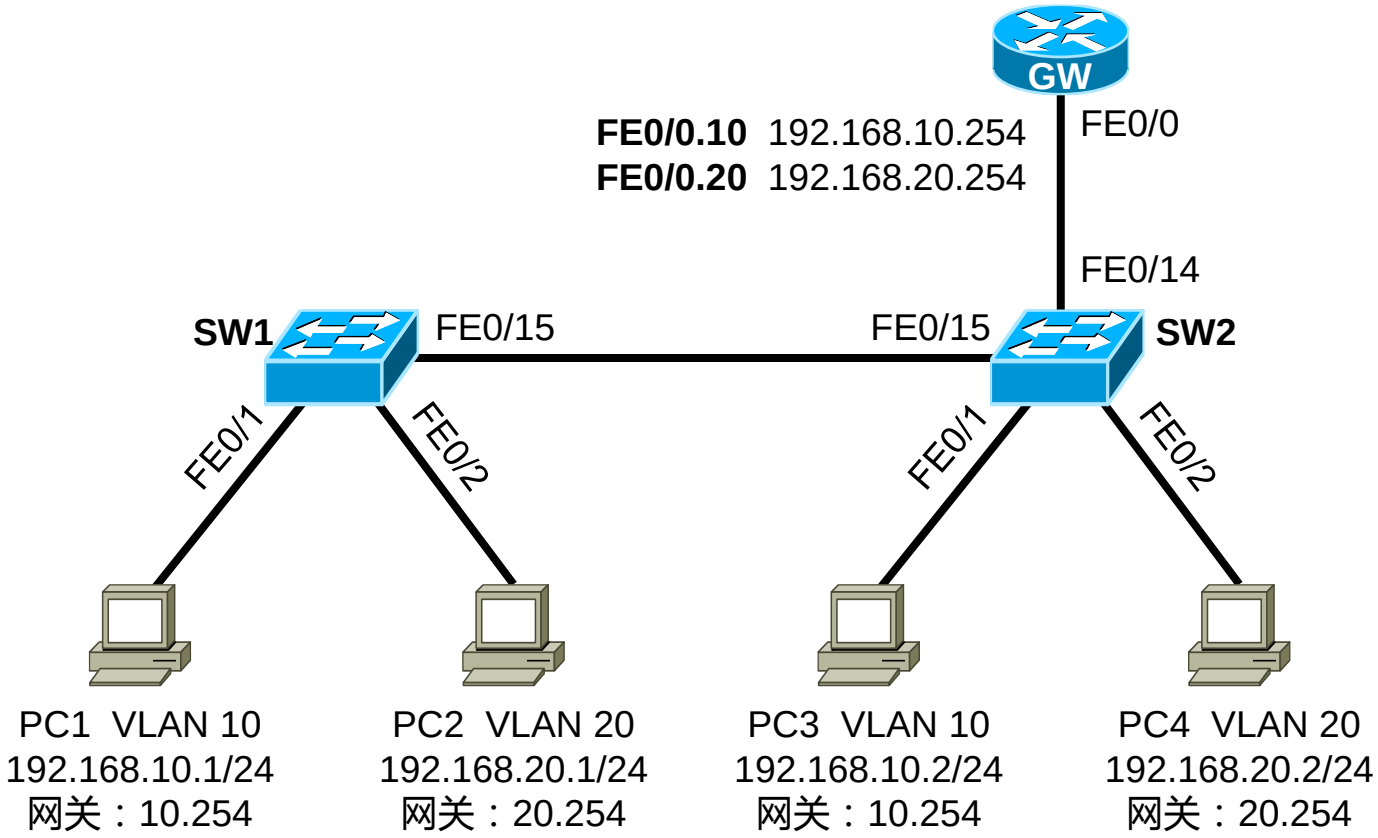


使用路由器子接口实现VLAN间互访

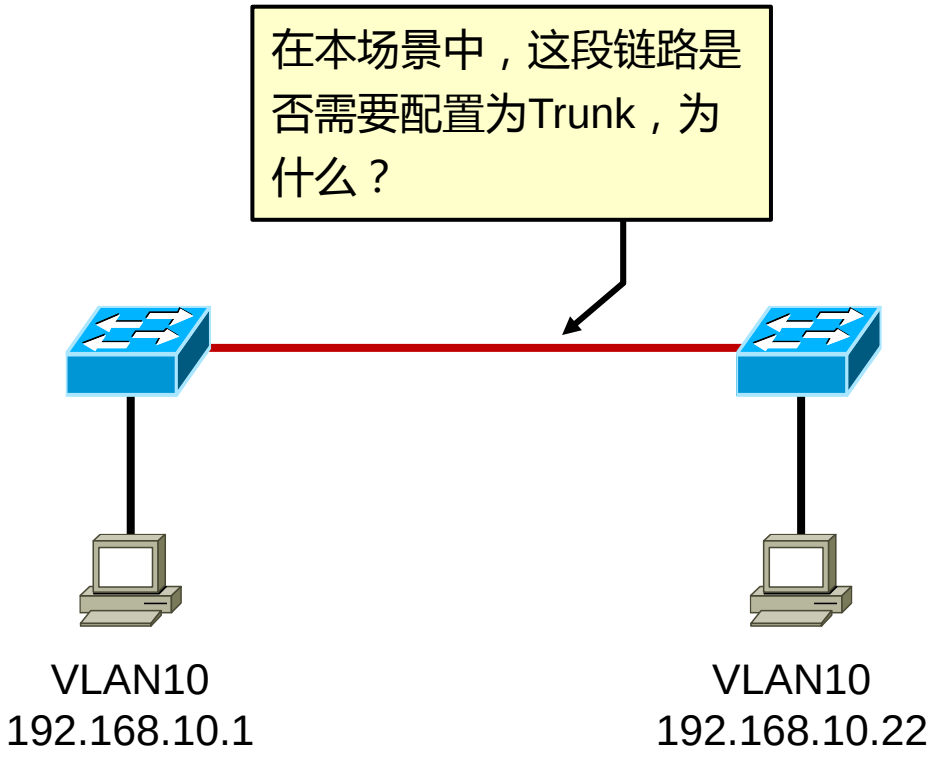


路由器子接口也被形象地称为“单臂路由”

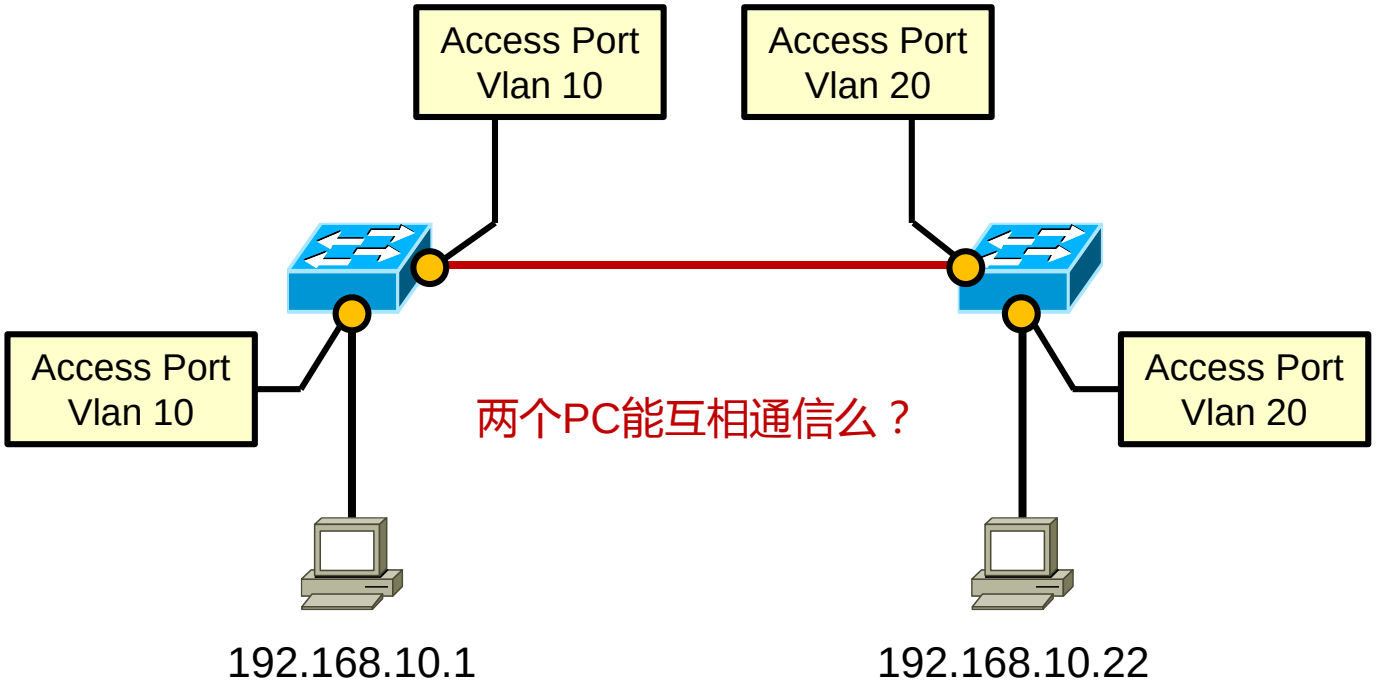
单臂路由实验



Q&A

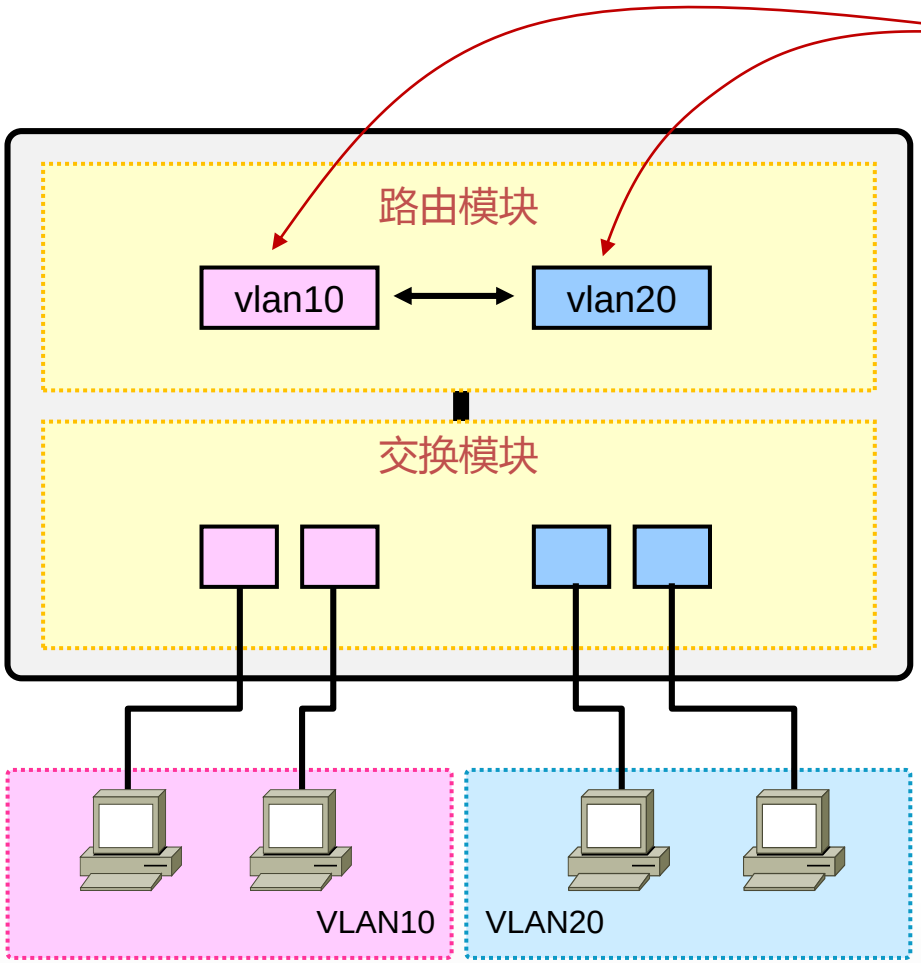

在本场景中，这段链路是否需要配置为Trunk，为什么？
VLAN10
192.168.10.1
VLAN10
192.168.10.22

Q&A

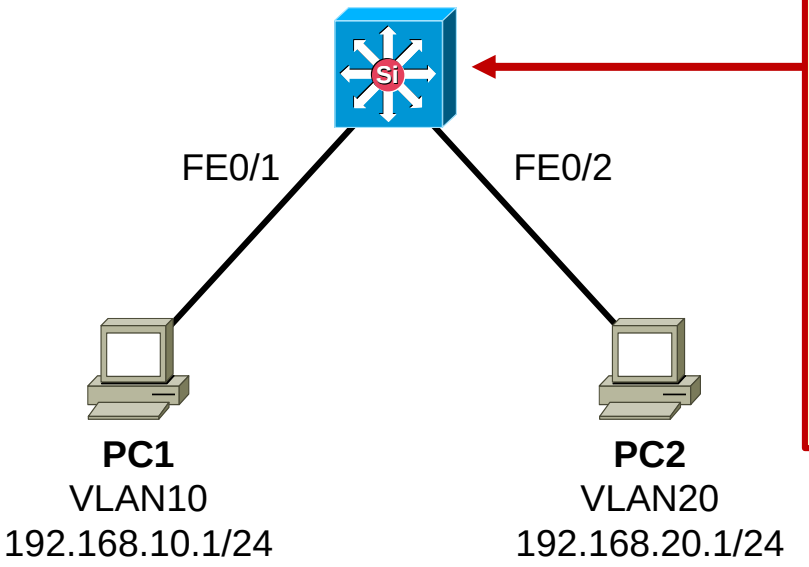

Access Port
Vlan 10
Access Port
Vlan 20
Access Port
Vlan 10
两个PC能互相通信么？
Access Port
Vlan 20
192.168.10.1
192.168.10.22

Switch Virtual Interfaces（SVI）

交换式虚拟接口（SVI）
VLAN接口（三层接口）
interface vlan 10或20



使用SVI实现VLAN间互访




```
vlan 10 20
!
interface fastethernet 0/1
    switchport mode access
    switchport access vlan 10
interface fastethernet 0/2
    switchport mode access
    switchport access vlan 20
!
Ip routing
Interface vlan 10
    ip address 192.168.10.254 255.255.255.0
Interface vlan 20
    ip address 192.168.20.254 255.255.255.0
```

红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You

红茶三杯
Vinsoney

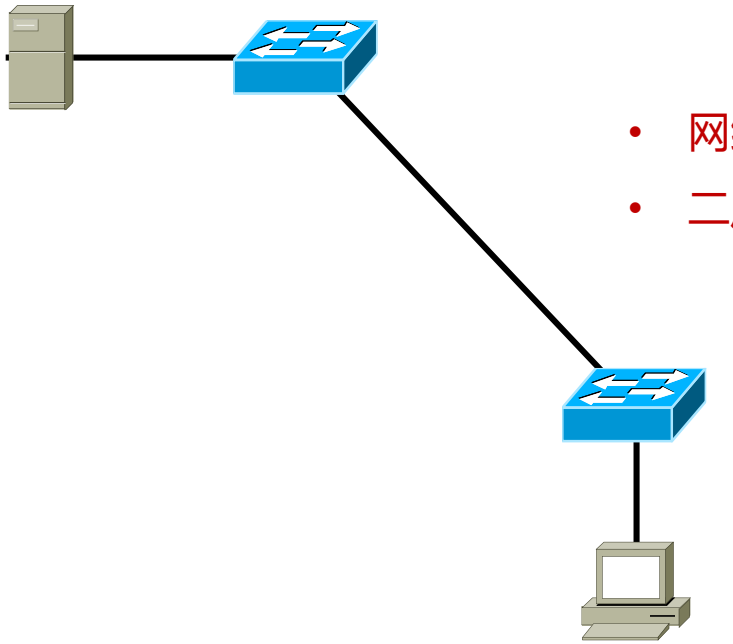
学习 沉淀 成长 分享

STP生成树协议

红茶三杯 http://weibo.com/vinsoney

Latest update: 2012-08-01

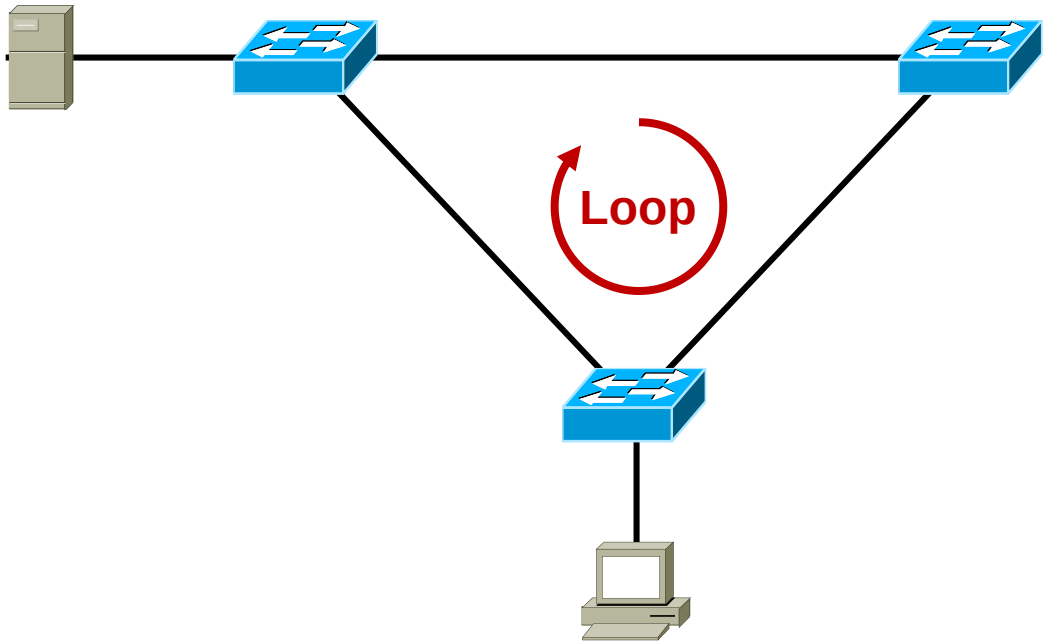
技术背景



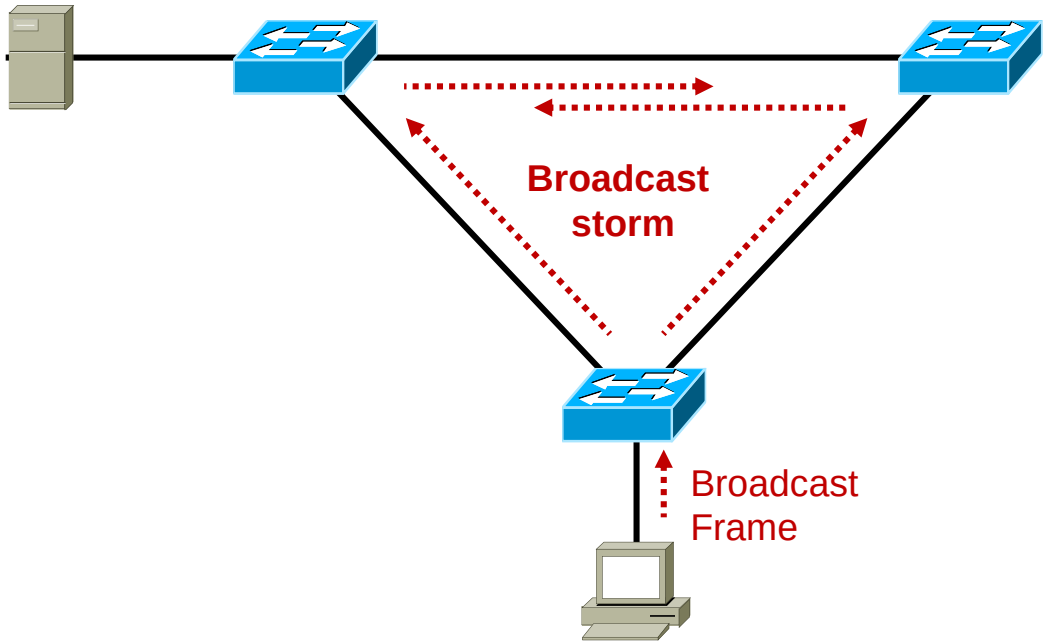
- 网络存在单点 / 单线路故障
- 二层链路没有冗余

二层环路

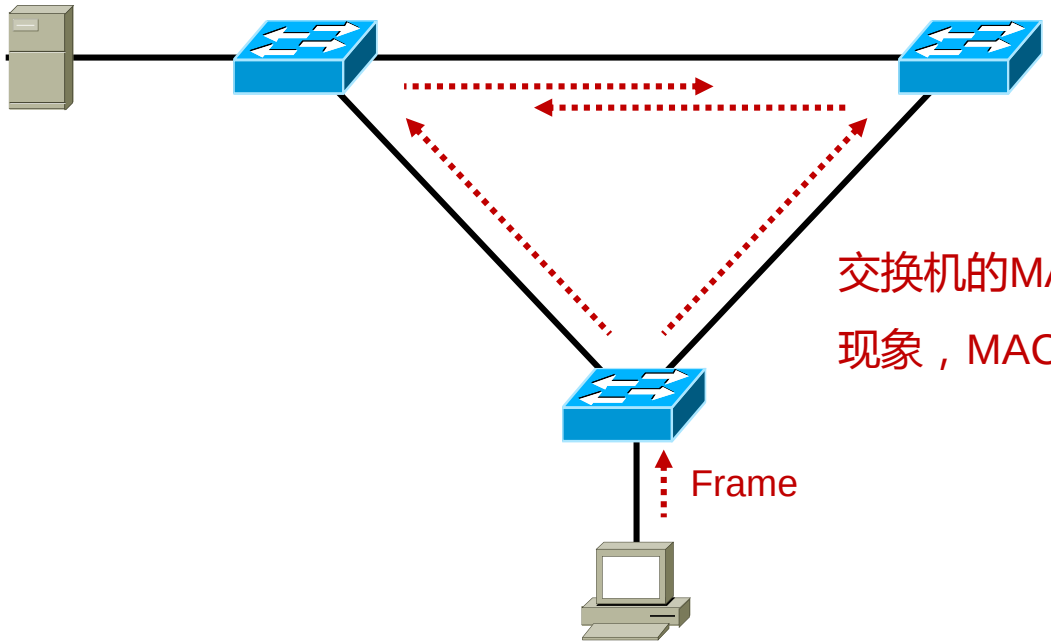
网络的冗余性增强了，但是却出现了二层环路



环路带来的问题：广播风暴



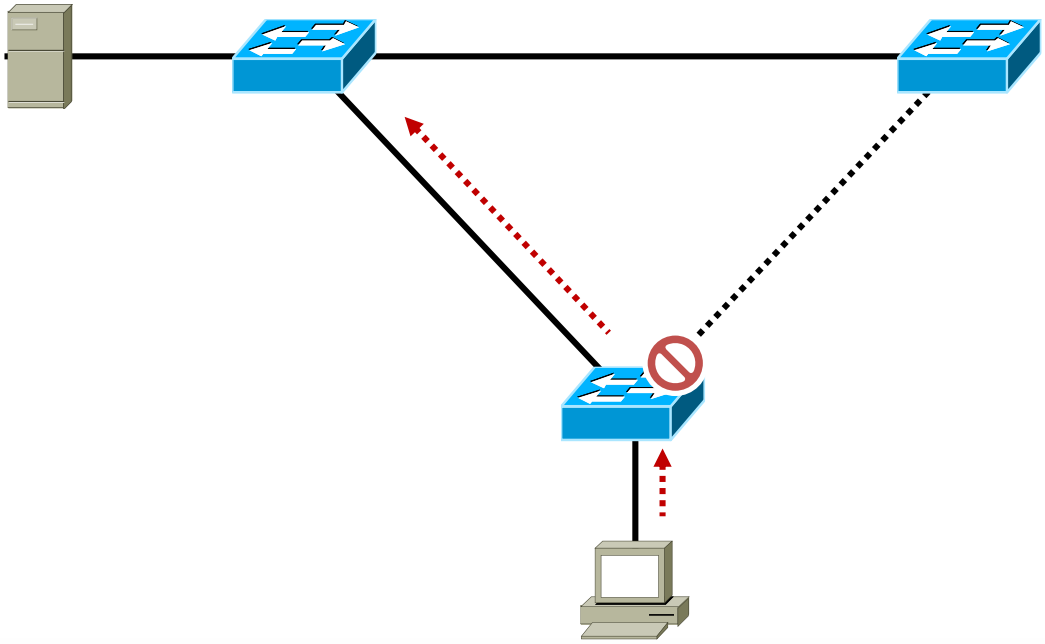
环路带来的问题：MAC表紊乱



交换机的MAC表出现MAC漂移现象，MAC地址表紊乱

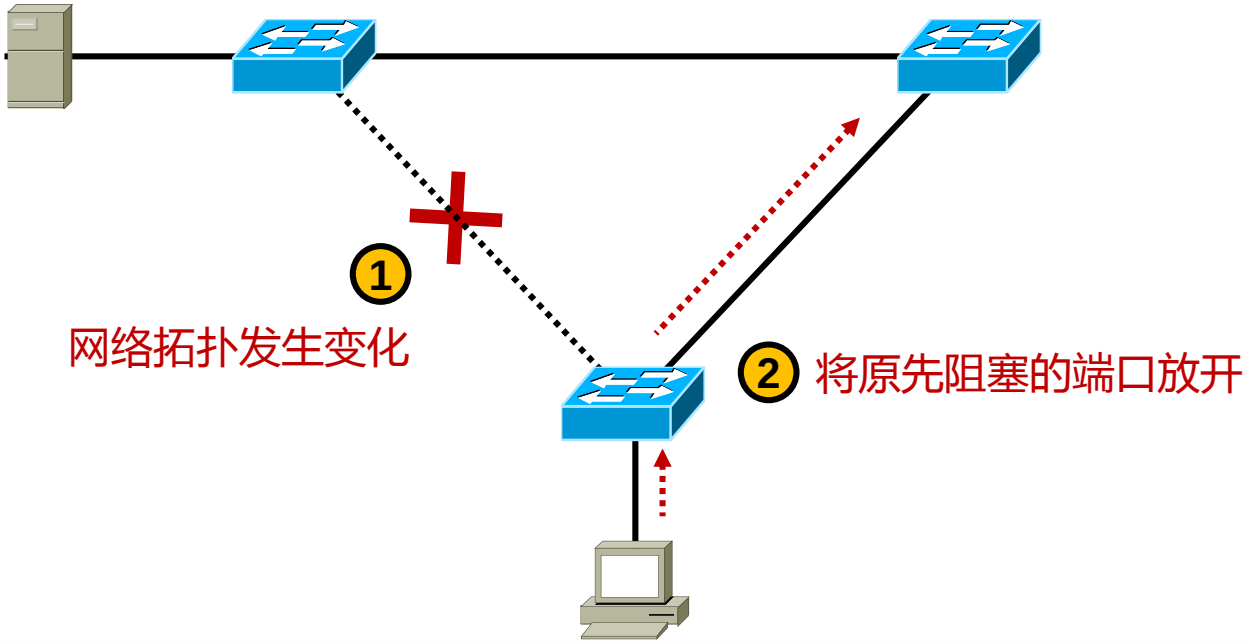
STP生成树协议

在网络中部署生成树后，交换机之间会进行协议报文的交互并进行计算，最终将网络中的某个接口进行阻塞（Block），从而打破环路。



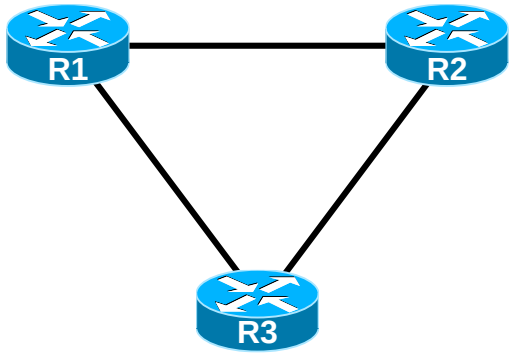
STP生成树协议

生成树能够感知网络拓扑的变化，并进行重新计算，以便保证网络的冗余性。



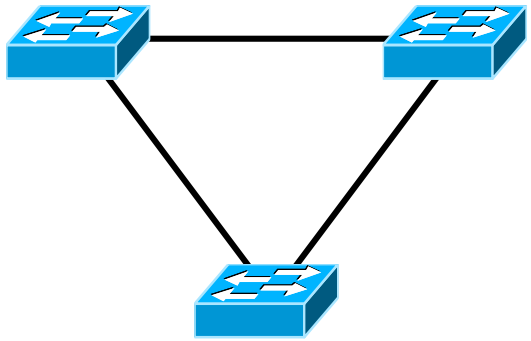
Q&A 二层及三层环路

Layer3 Loop



- 通常是由于路由环路导致网络中出现三层环路；
- 动态路由协议有一定的防环能力；
- IP数据报文头部中的TTL值亦可用于防止报文被无止尽地转发。

Layer2 Loop



- 通常是由于网络有二层冗余的需求或人为的误接线缆导致；
- 需借助特定的协议或机制防环；
- 二层数据帧头部中并没有任何信息可用于防止数据帧被无止尽地转发。

STP的概念

- Spanning-Tree Protocol简称STP，生成树协议，被广泛部署在二层交换网络中，用于防止网络出现二层环路，同时增加网络的冗余性。
- 交换机之间通过生成树协议数据的交互来完成所需信息的搜集，在此基础上交换机进行相应的计算，最终将交换机的某个（或某些）接口阻塞从而打破环路。
- 生成树有多个标准，传统的生成树是802.1D标准。
- Cisco基于IEEE802.1D开发了 增强的私有生成树协议PVST+。

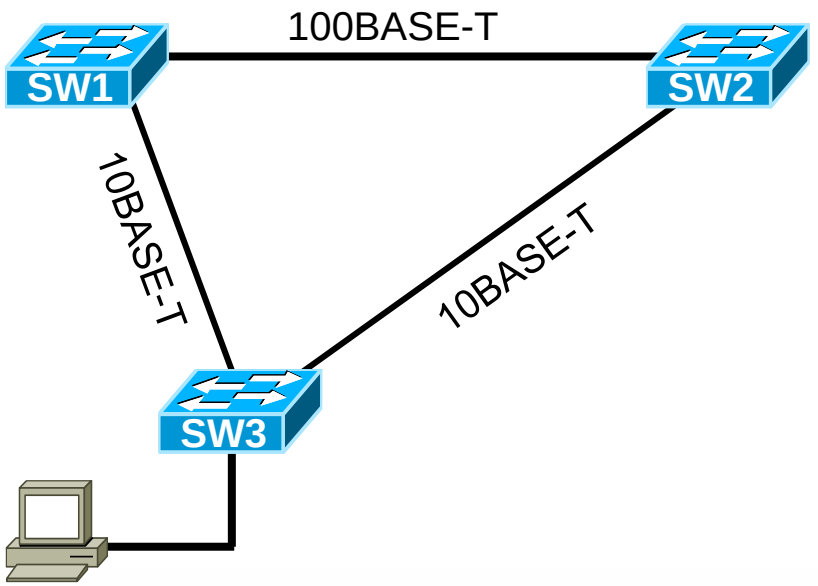
STP的计算

1 每个交换网络选举一个根桥RB
2 每个非根桥上选举一个根端口RP
3 每个段选举一个指定端口DP
4 阻塞非指定端口NDP

[RB] Root Bridge

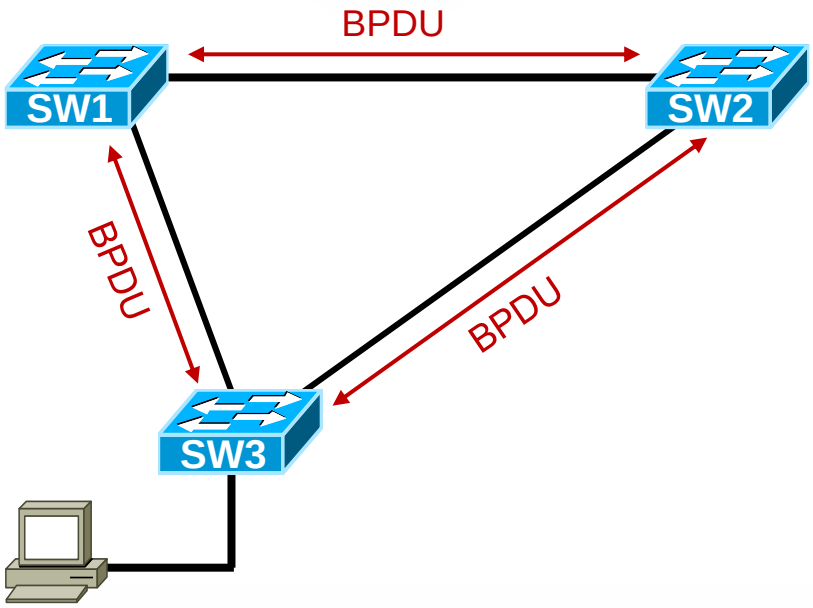
[RP] Root Port

[DP] Designated port



计算的依据

BPDU Bridge Protocol Data Unit
网桥协议数据单元



BPDU

字节	字段	描述
2	协议	代表上层协议（BPDU），该值总为0
1	版本	（802.1D的总为0）
1	TYPE	“配置BPDU”为0、“TCN BPDU”为80
1	标志	LSB最低有效位表示TC标志；MSB最高有效位表示TCA标志
8	根桥ID	根网桥的桥ID
4	路径开销	到达根桥的STP cost
8	网桥ID	BPDU发送桥的ID
2	端口ID	BPDU发送网桥的端口ID（优先级+端口号）
2	消息寿命 Message age	从根网桥发出BPDU之后的秒数，每经过一个网桥都减1，所以它本质上是到达根桥的跳数。
2	最大寿命 Max age	当一段时间未收到任何BPDU，生存期到达MAX age时，网桥认为该端口连接的链路发生故障。默认20S
2	HELLO时间	根网桥连续发送的BPDU之间的时间间隔。默认2S
2	转发延迟	在监听和学习状态所停留的时间间隔。默认15S

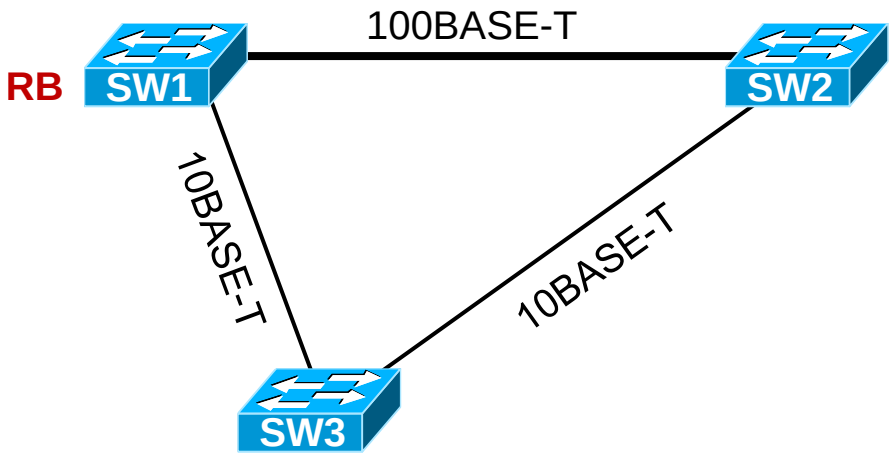
1 每个交换网络选举一个根桥RB

1 每个交换网络选举一个根桥RB
2 每个非根桥上选举一个根端口RP
3 每个段选举一个指定端口DP
4 阻塞非指定端口NDP

[RB] Root Bridge

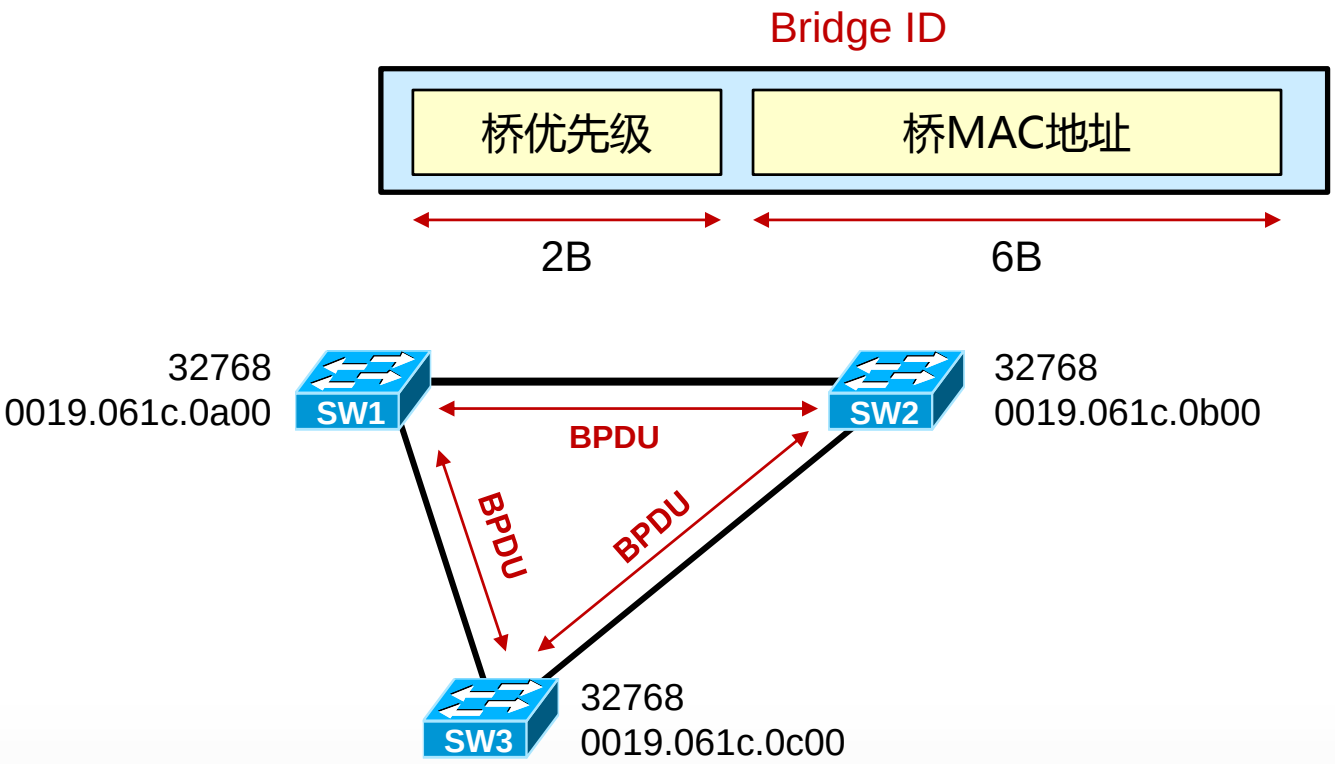
[RP] Root Port

[DP] Designated port



Bridge ID

- Bridge Identifier，交换机的STP标识符；
- 拥有最小BID的交换机成为根桥。



2 每个非根桥上选举一个根端口RP

1 每个交换网络选举一个根桥RB
2 每个非根桥上选举一个根端口RP
3 每个段选举一个指定端口DP
4 阻塞非指定端口NDP

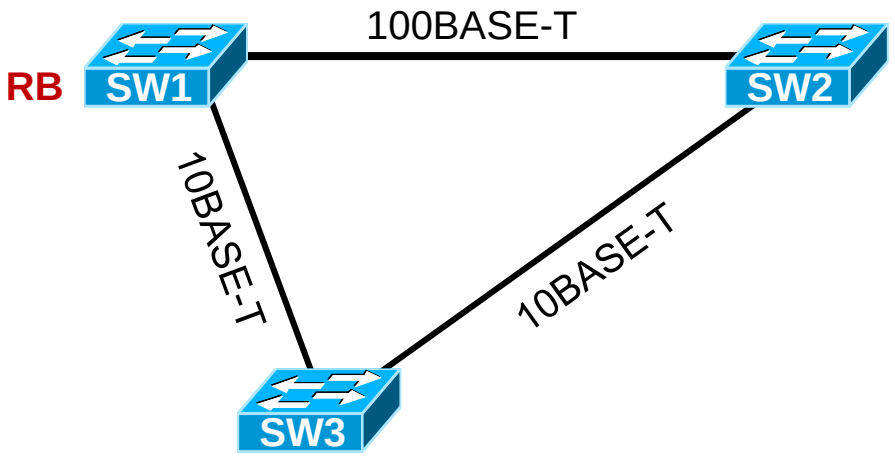
比较顺序（均比小）：

1、根桥ID

2、到根桥的路径开销

3、网桥ID

4、端口ID



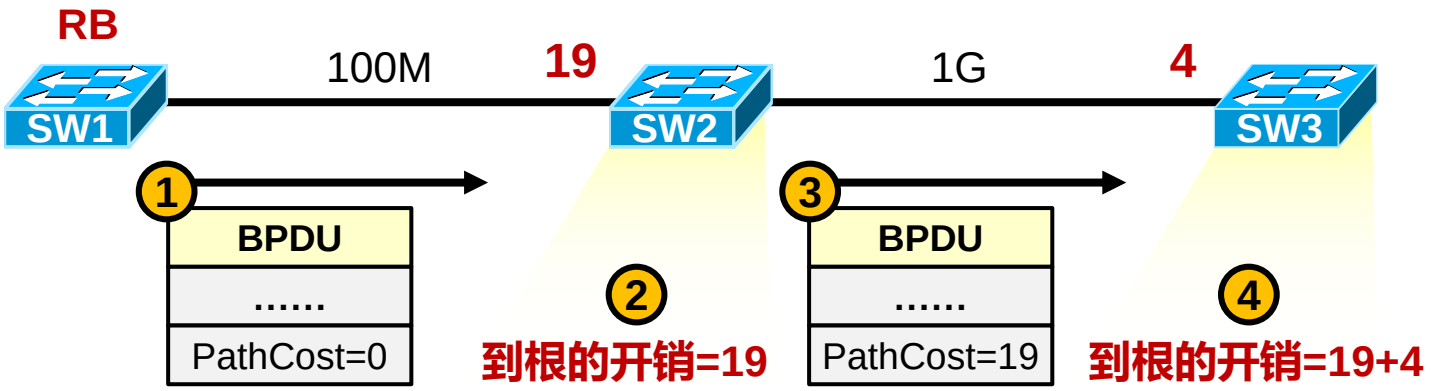
STP接口Cost与接口带宽的对应关系

Link Speed	Cost (New IEEE Specification)	Cost (Old IEEE Specification)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

路径开销是接口cost累加，而接口cost是基于接口带宽的

STP Path Cost

- 非根桥某个接口到RB的路径开销等于该接口的Cost加上这个接口收到的BPDU中包含的Path Cost值。



Port ID

- Port Identifier，接口标识符，共有2个字节。
- Port ID （2字节）= 接口优先级（1字节）+接口编号（1字节）。
- 缺省情况下接口优先级为128，范围是0-255。

2 每个非根桥上选举一个根端口RP

1 每个交换网络选举一个根桥RB
2 每个非根桥上选举一个根端口RP
3 每个段选举一个指定端口DP
4 阻塞非指定端口NDP

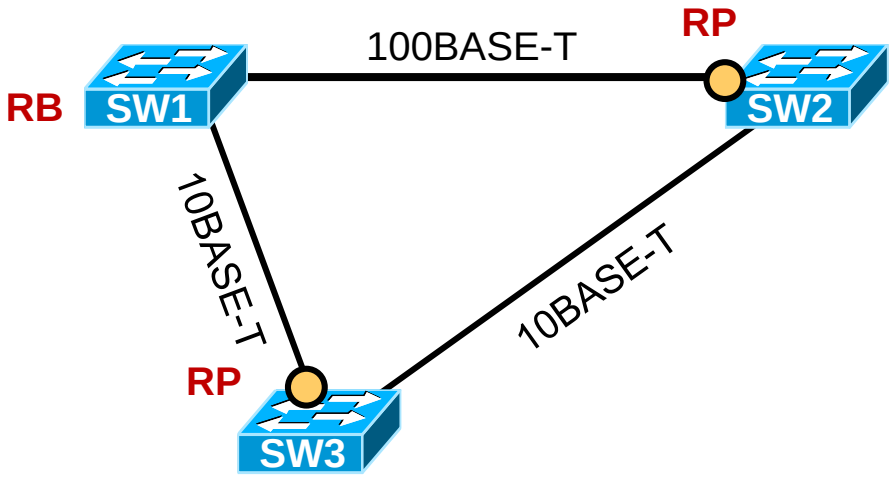
比较顺序（均比小）：

1、根桥ID

2、到根桥的路径开销

3、网桥ID

4、端口ID



3 每个段选举一个指定端口DP

1 每个交换网络选举一个根桥RB
2 每个非根桥上选举一个根端口RP
3 每个段选举一个指定端口DP
4 阻塞非指定端口NDP

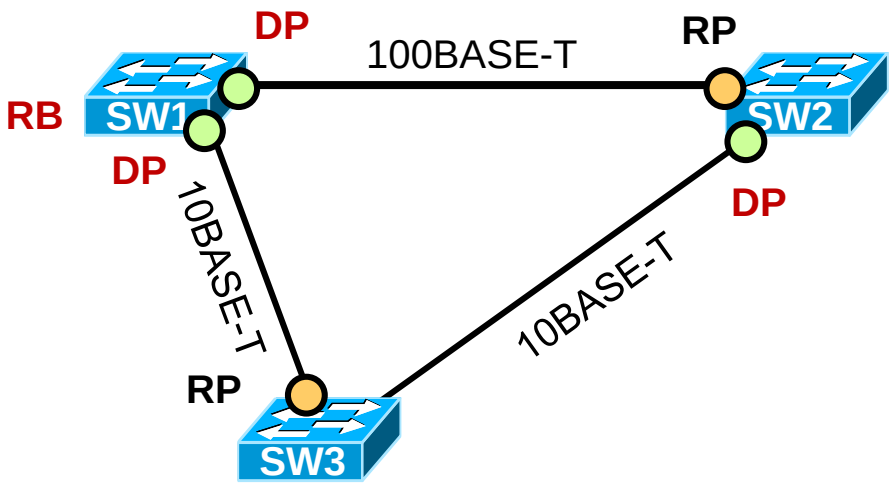
比较顺序（均比小）：

1、根桥ID

2、到根桥的路径开销

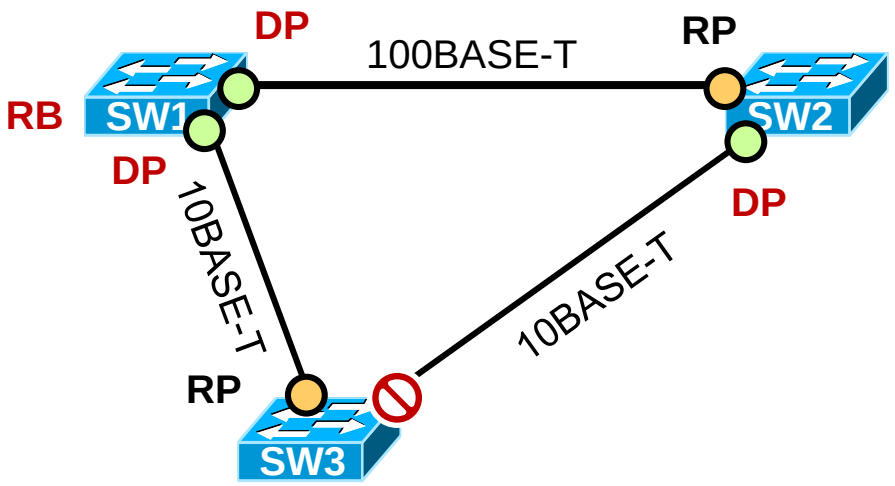
3、网桥ID

4、端口ID



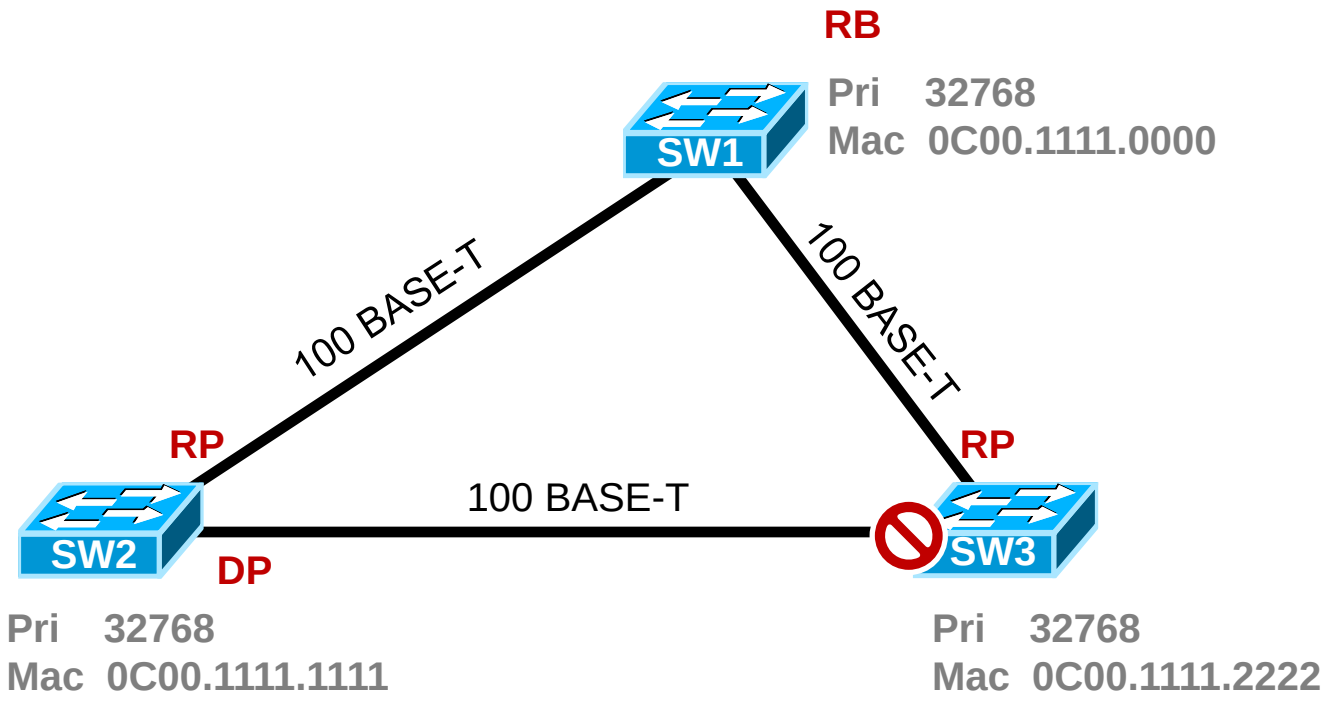
3 每个段选举一个指定端口DP

1 每个交换网络选举一个根桥RB
2 每个非根桥上选举一个根端口RP
3 每个段选举一个指定端口DP
4 阻塞非指定端口NDP



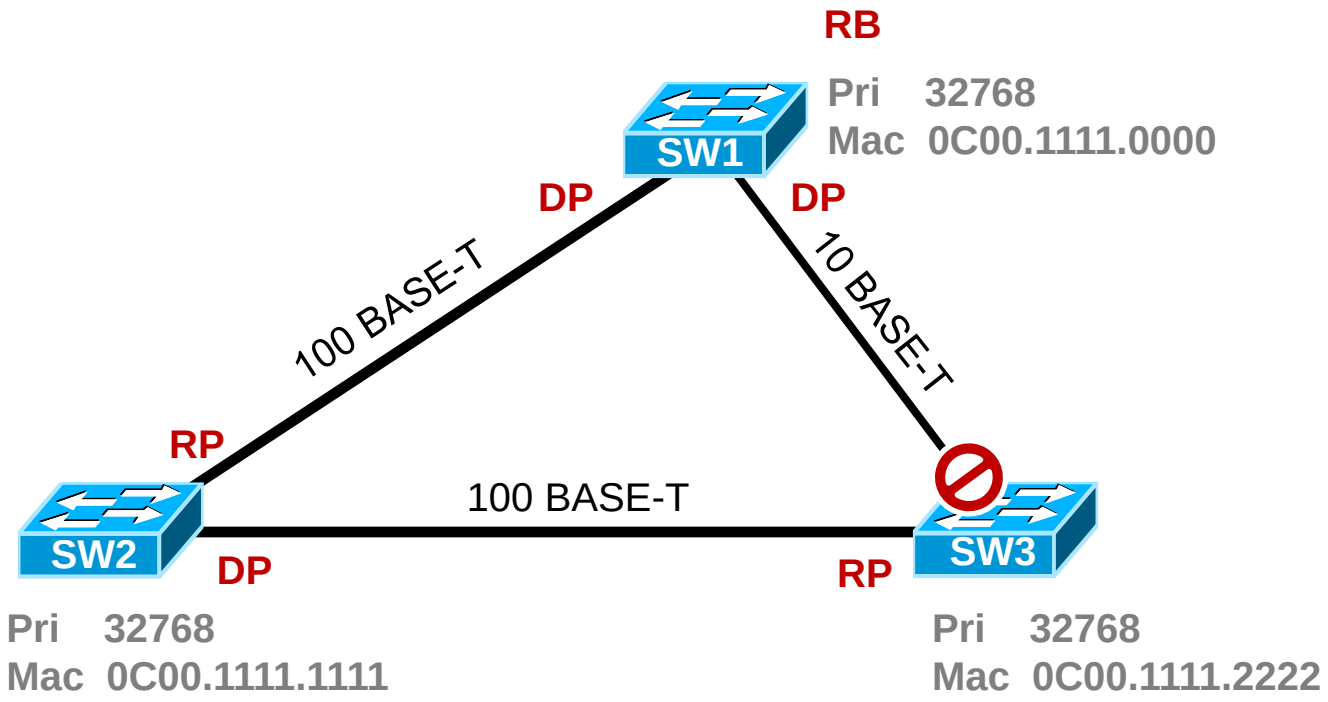
STP案例

- CASE1



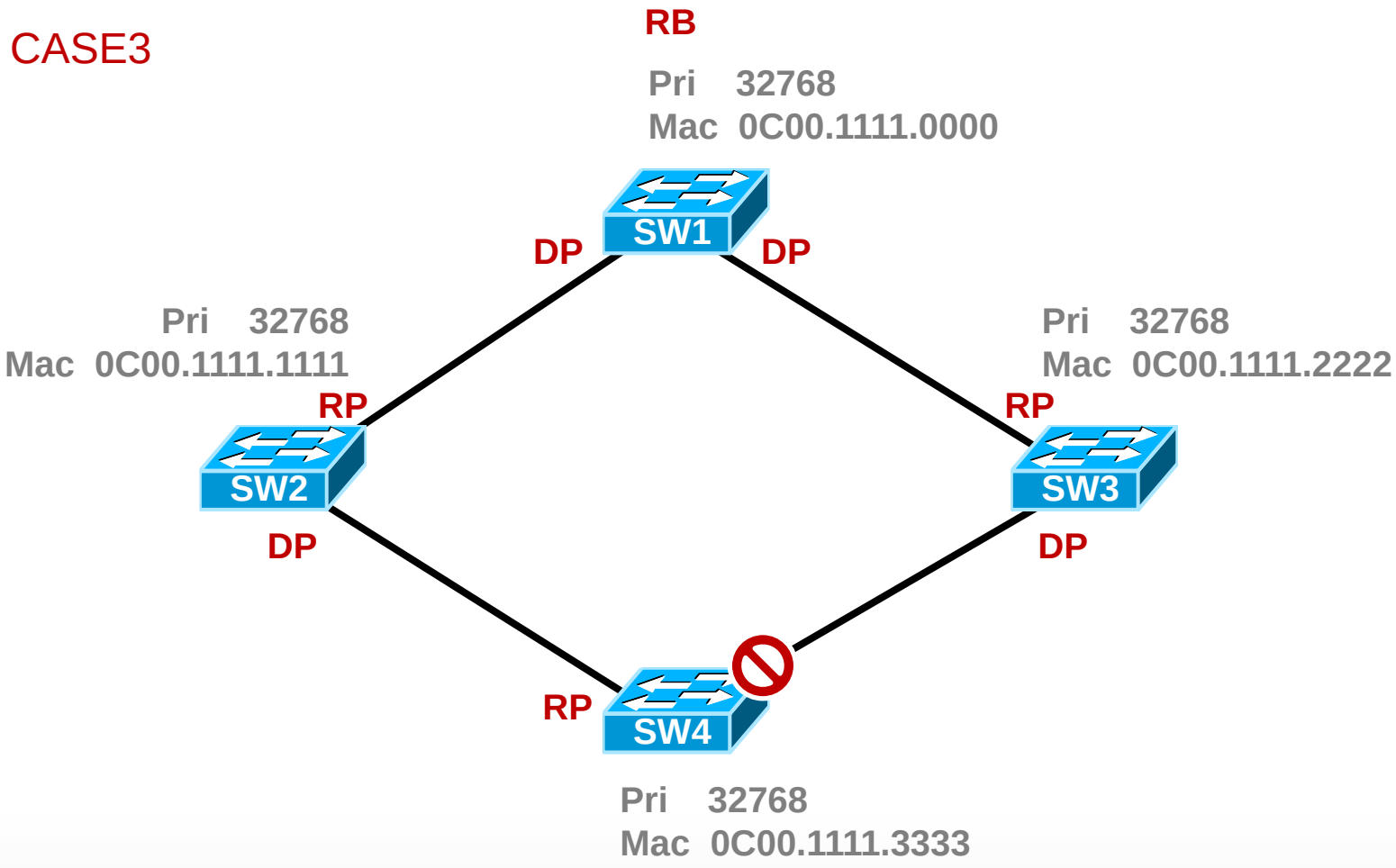
STP案例

- CASE2



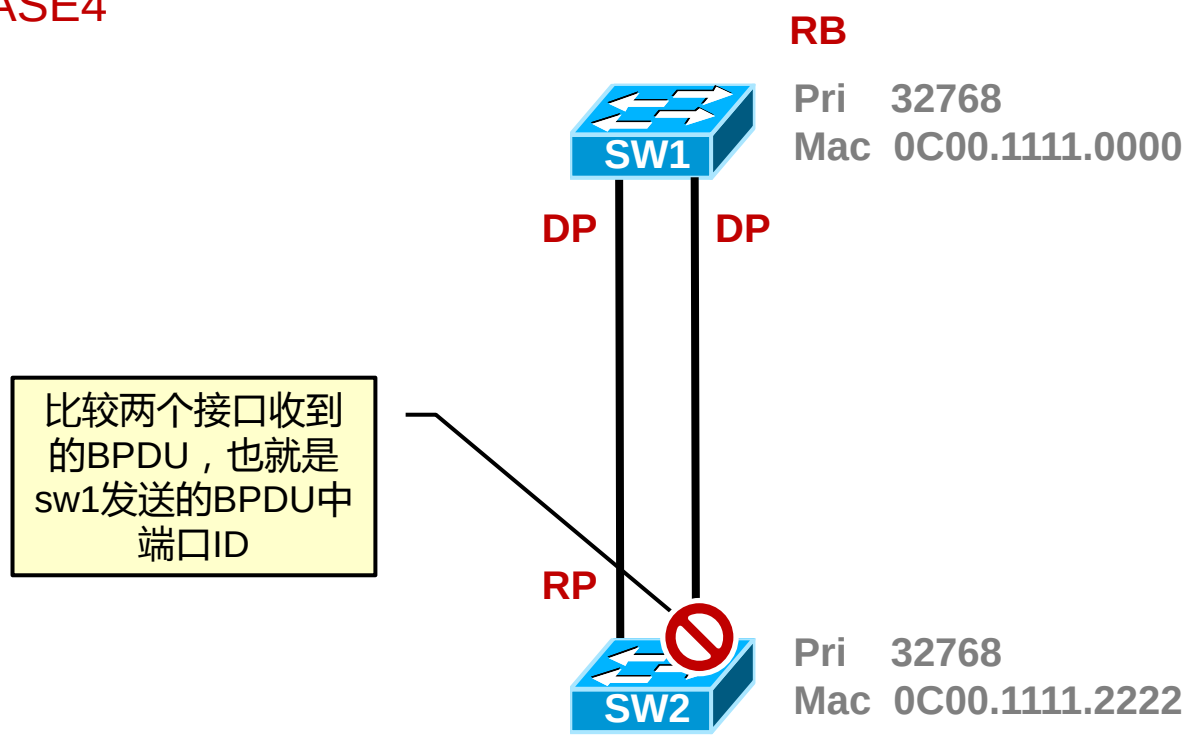
STP案例

- CASE3



STP案例

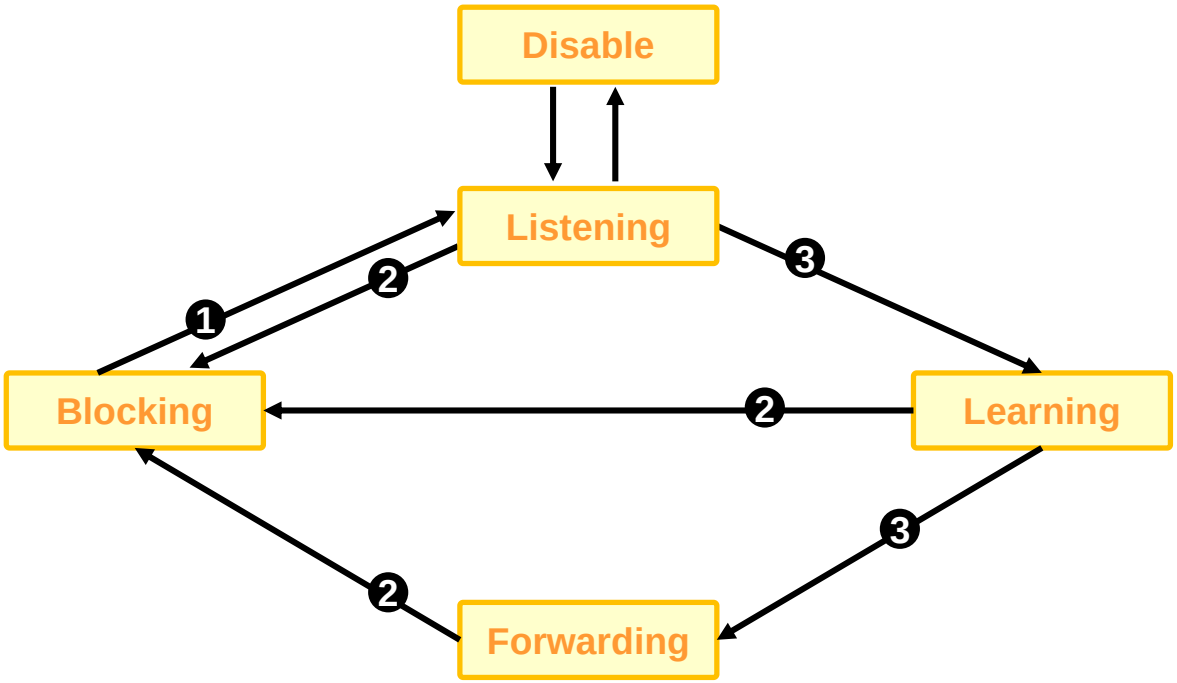
- CASE4



STP的端口状态

Disable	不收发任何报文
Blocking	不接收也不转发帧，接收但不发送BPDU，不学习MAC地址
Listening	不接收也不转发帧，接收并且发送BPDU，不学习MAC地址
Learning	不接收也不转发帧，接收并且发送BPDU，学习MAC地址
Forwarding	接收并转发帧，接收并且发送BPDU，学习MAC地址

STP的端口状态



❶ 端口被选举为DP或RP

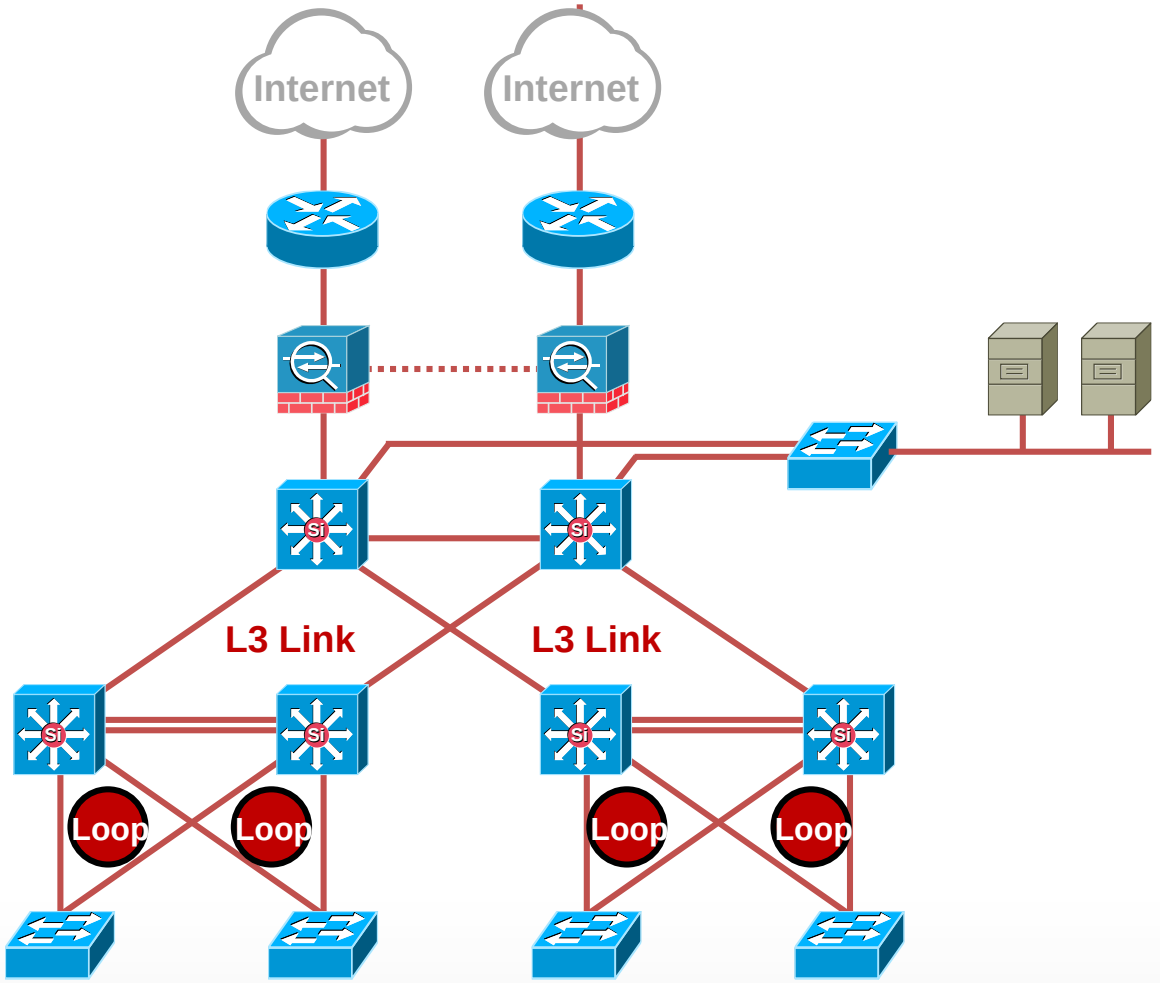
❷ 端口被选举为NDP

❸ 经过Forward Delay间隔，默认15s

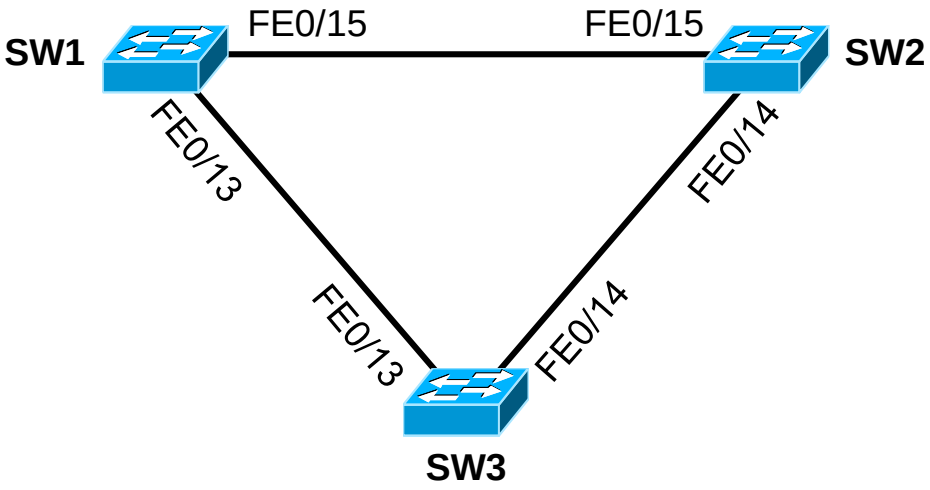
STP的端口状态

- In the blocking state, ports can only receive BPDUs. It may take up to 20 seconds to change from this state；
- In listening state, switches determine if there are any other paths to the root bridge. the forward delay and lasts for 15 seconds. In the listening state, user data is not being forwarded and MAC addresses are not being learned；
- In learning state user data is not forwarded, but MAC addresses are learned from any traffic that is seen. The learning state lasts for 15 seconds and is also called the forward delay；
- In forwarding state user data is forwarded and MAC addresses continue to be learned. BPDUs are still processed；

生成树在工程中的运用



基础实验



红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You

红茶三杯
Vinsoney

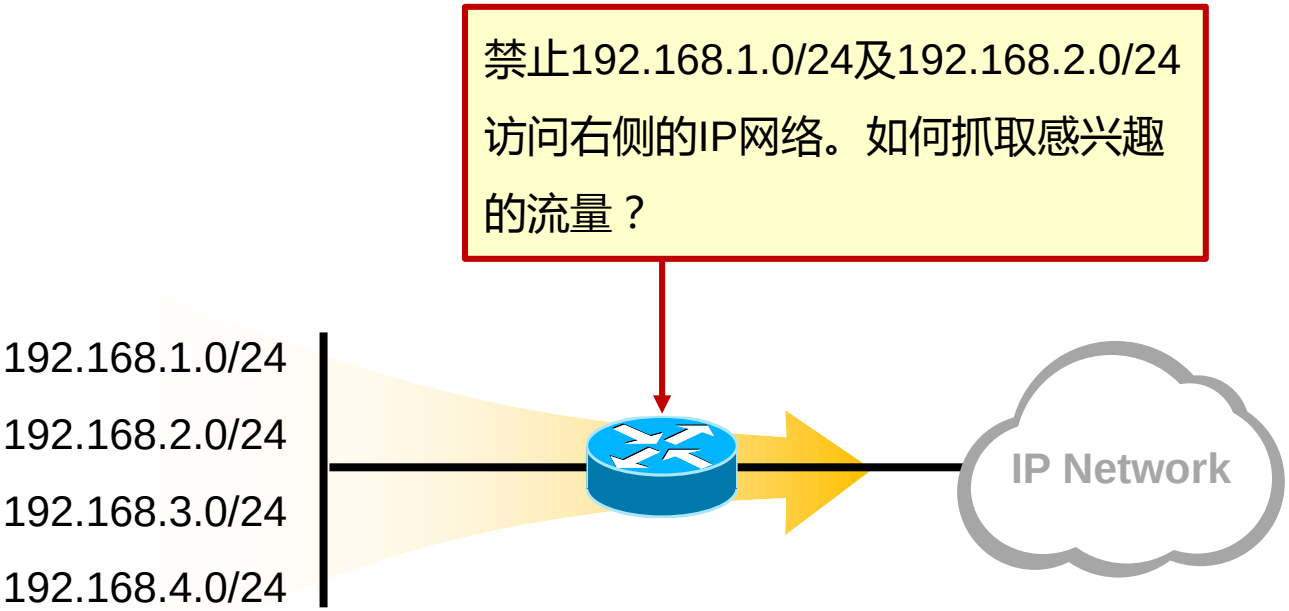
学习 沉淀 成长 分享

ACL访问控制列表

红茶三杯 http://weibo.com/vinsoney

Latest update: 2012-08-01

技术背景

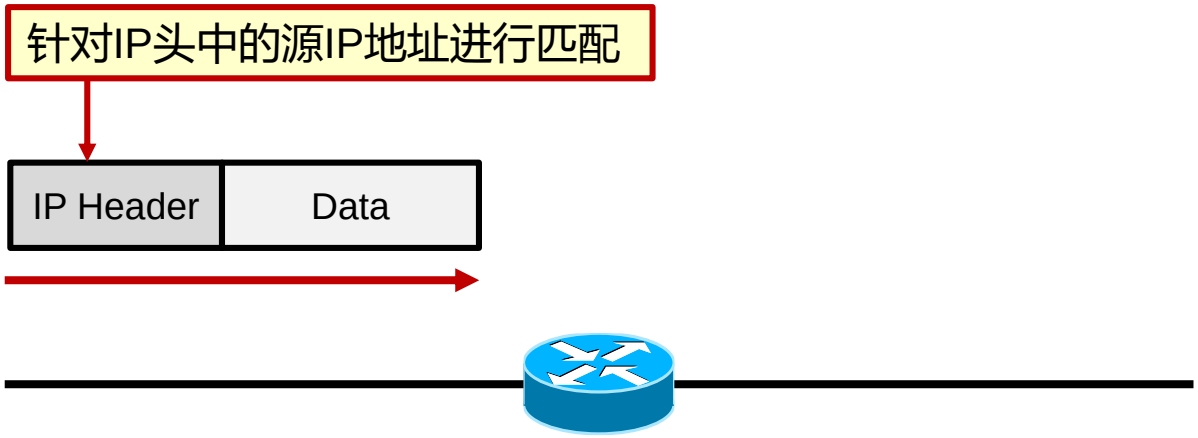

禁止192.168.1.0/24及192.168.2.0/24访问右侧的IP网络。如何抓取感兴趣的流量？
192.168.1.0/24
192.168.2.0/24
192.168.3.0/24
192.168.4.0/24
IP Network

ACL

- Access Control List ，简称ACL，访问控制列表，是一个非常重要的基础性工具，是一系列有序的条目，每个条目包含“条件”以及“动作”两元素。
- 能够通过匹配IP报文中的相关字段对感兴趣数据包进行抓取。
- 除了能够抓取数据包，还能够用于抓取特定路由，以便执行路由策略。
- ACL在报文过滤、路由策略、NAT、VPN、QoS等都有广泛的应用。

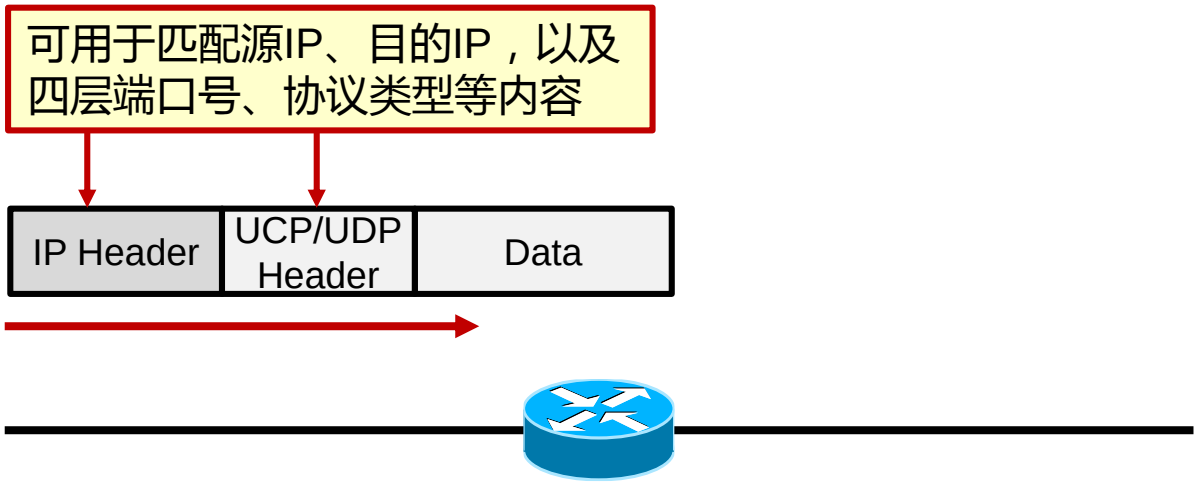
ACL的类型

- 标准访问控制列表
  - 只能匹配报头中的源IP地址；
  - 只能针对整个协议采取动作，而无法针对特定的协议类型。

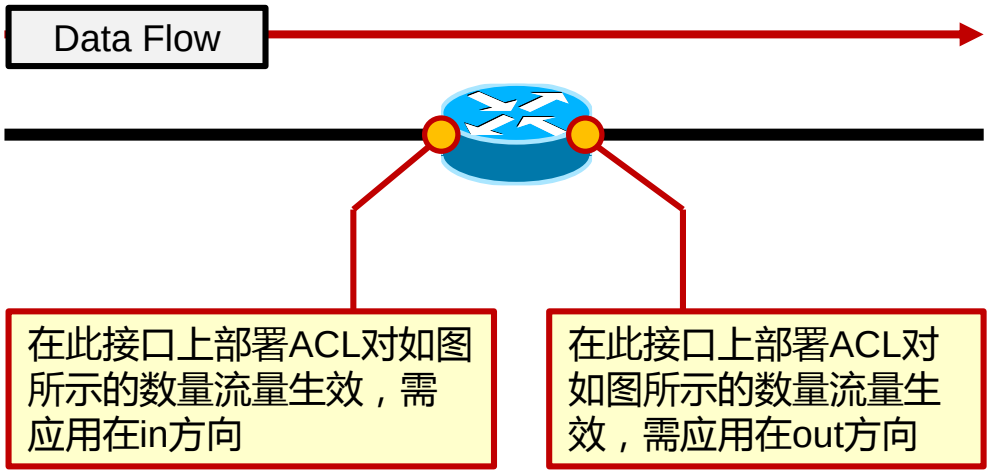


ACL的类型

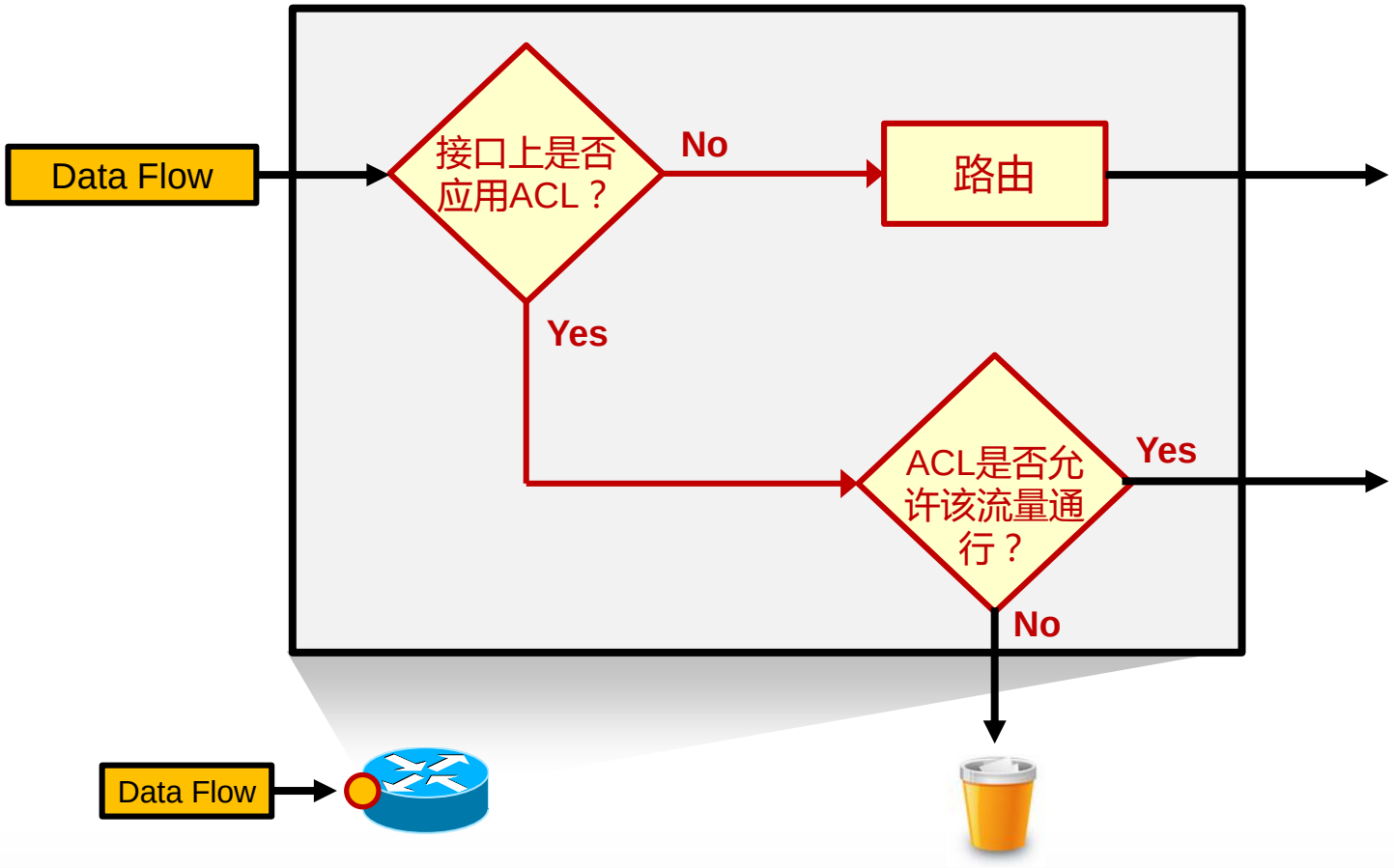
- 扩展访问控制列表
  - 能匹配报文中的源、目的IP地址，以及四层端口号等信息；
  - 可以针对具体的协议类型进行匹配，例如抓取TCP、UDP或者ICMP流量。



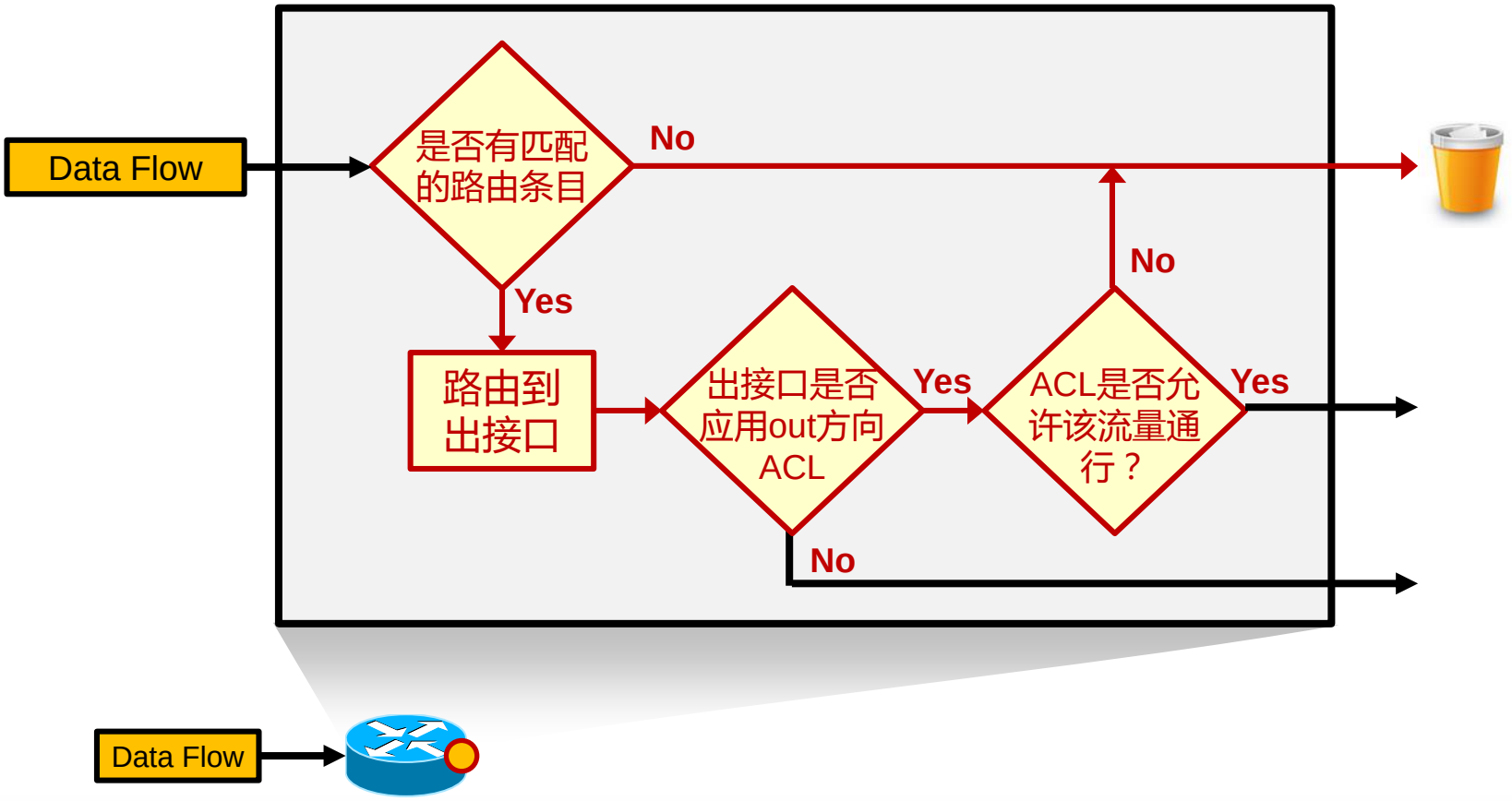
In / Out


Data Flow
在此接口上部署ACL对如图所示的数量流量生效，需应用在in方向
在此接口上部署ACL对如图所示的数量流量生效，需应用在out方向

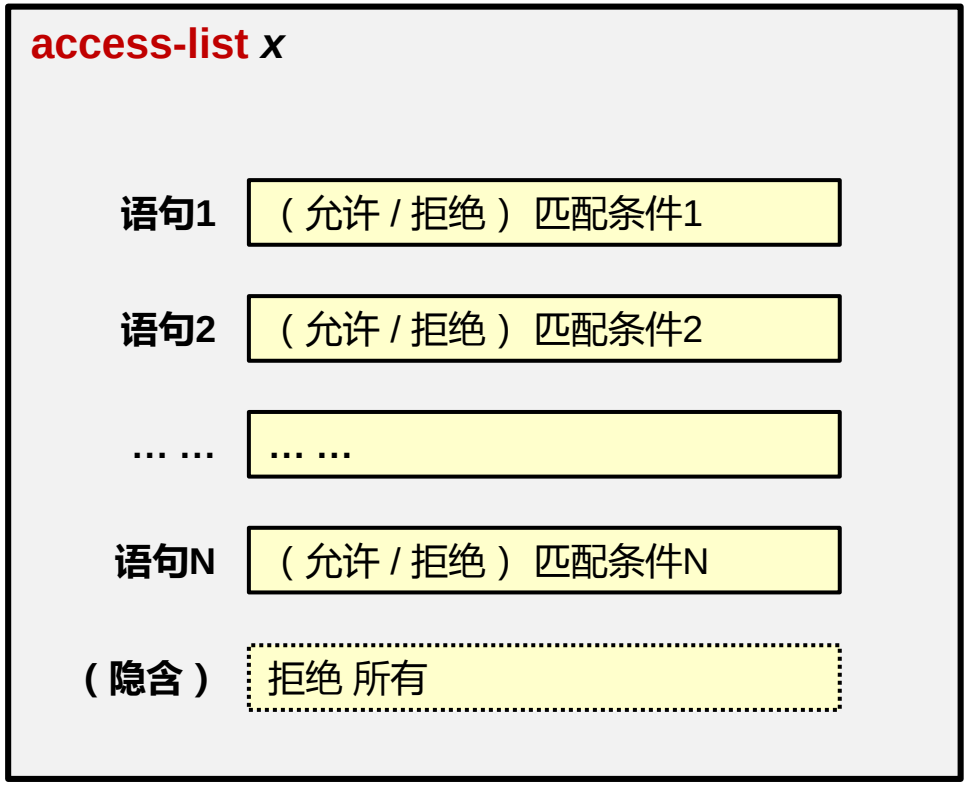
In方向的ACL


Data Flow
接口上是否应用ACL？
No
路由
Yes
ACL是否允许该流量通行？
Yes
No
Data Flow

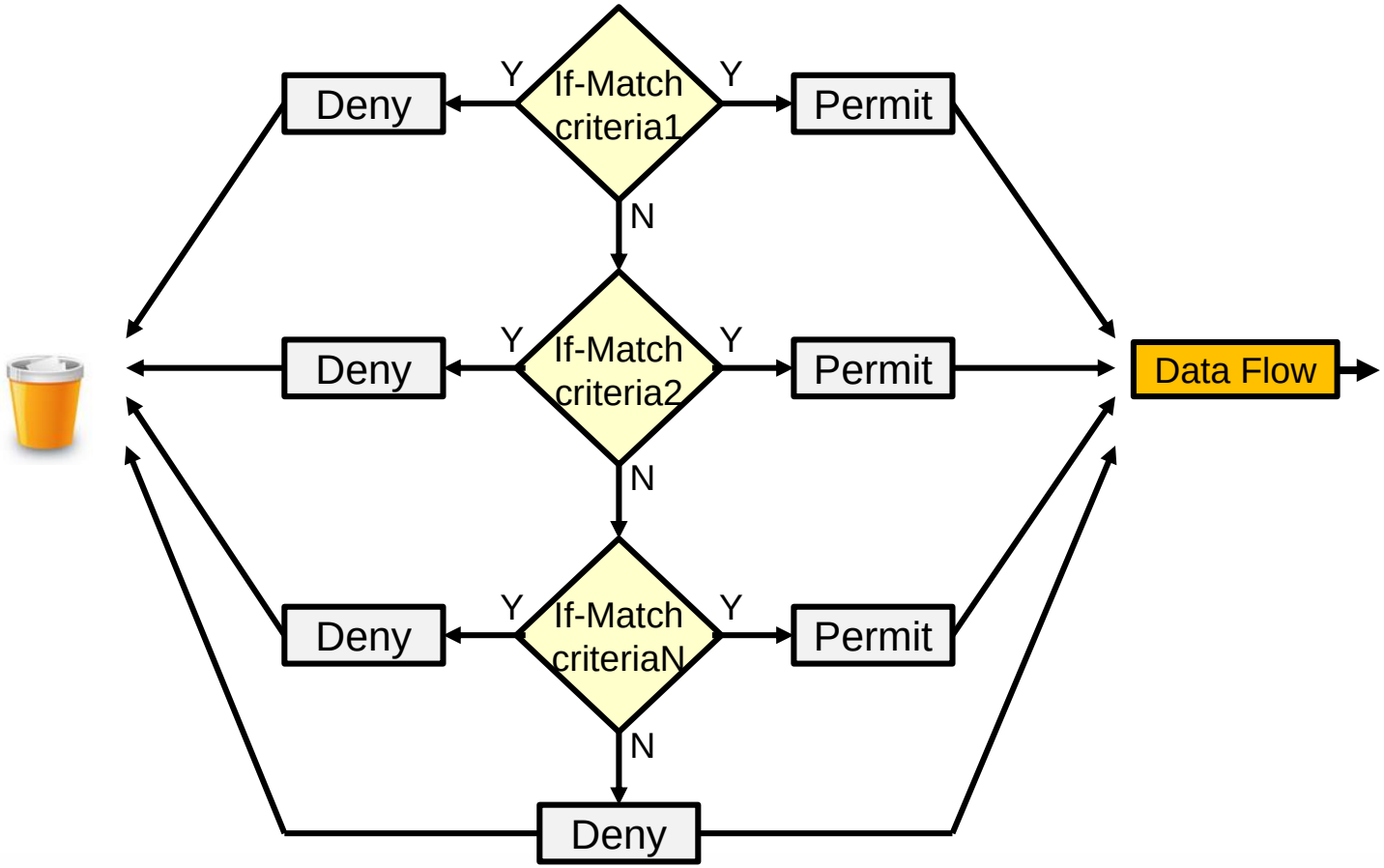
Out方向的ACL



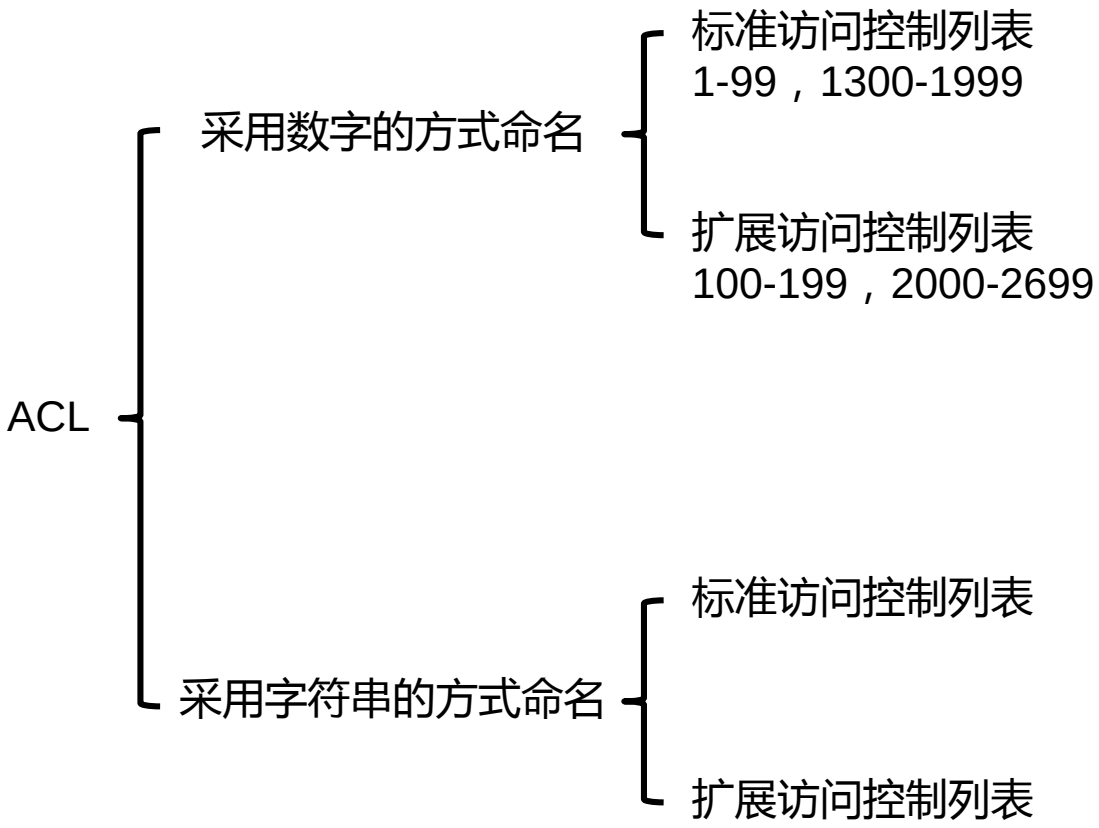
Access-list



ACL的匹配顺序



ACL的命名


ACL
采用数字的方式命名
标准访问控制列表
1-99，1300-1999
扩展访问控制列表
100-199，2000-2699
采用字符串的方式命名
标准访问控制列表
扩展访问控制列表

标准ACL的配置（采用数字的方式命令）

- **创建标准ACL**

  Router(config)# **access-list** *acl-number* {**permit|deny**} *source* [*wildcard mask*]

  - 标准ACL的编号值范围1-99,1300-1999
  - 通配符掩码未写，则默认为 0.0.0.0
  - “**no access-list** *acl-num*” 将会删除整个ACL列表

- **将创建好的ACL应用在接口上**

  Router(config-if)# **ip access-group** *acl-num* { **in | out** }

  - 当使用ACL进行报文过滤时，ACL被应用在接口特定的接口，同时关联要部署的方向（In/Out）

Wildcard Mask 通配符掩码

- Wildcard Mask，通配符掩码，常被称为反掩码，长度为32bits，和IPv4地址搭配，同于确定被匹配的IP中哪些位可以忽略，哪些位必须一致。
- 通配符掩码中，值为1的bit表示该位忽略，值为0的bit表示该位需严格匹配。

192.168.1.1
192.168.1.2
192.168.1.3
192.168.1.4
……

被匹配对象

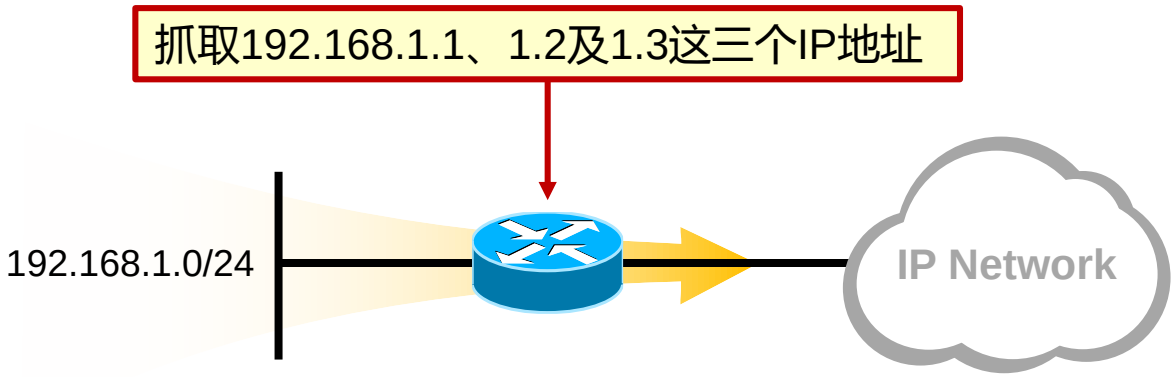
192.168.1.0 0.0.0.255

192	168	1.	0
11000000	10101000	00000001	00000000
0	0	0	255
00000000	00000000	00000000	11111111

IP Address

Wildcard Mask

Wildcard Mask 通配符掩码



IP Address	192	168	1.	0
	11000000	10101000	00000001	00000000
Wildcard Mask	0	0	0	3
	00000000	00000000	00000000	00000011

通配符掩码的特殊值

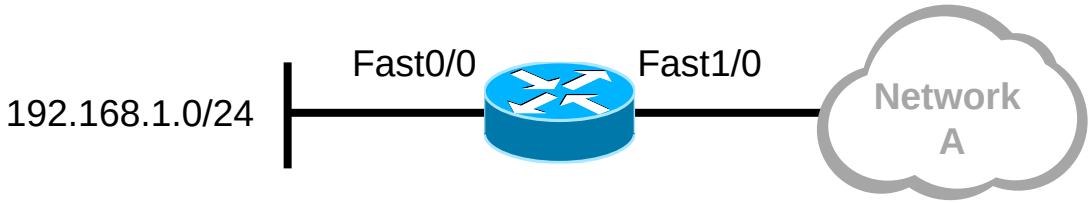
192	168	1.	1
11000000	10101000	00000001	00000000
0	0	0	0
00000000	00000000	00000000	00000000

= host 192.168.1.1

0	0	0	0
00000000	00000000	00000000	00000000
255	255	255	255
11111111	11111111	11111111	11111111

= any

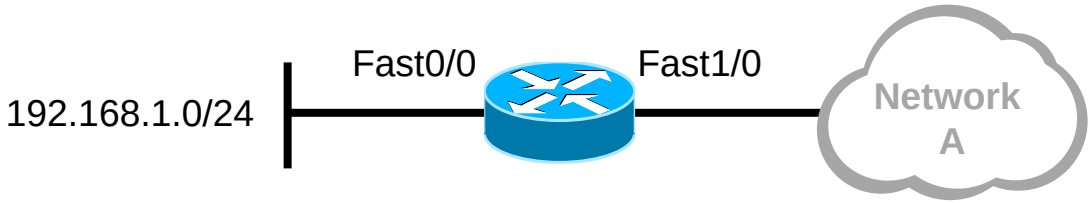
标准ACL配置示例 1



只禁止左侧子网中的192.168.1.1访问A网络，其他流量放行

```
router(config)# access-list 1 deny 192.168.1.1 0.0.0.0
或者access-list 1 deny 192.168.1.1 或 access-list 1 deny host 192.168.1.1
router(config)# access-list 1 permit 0.0.0.0 255.255.255.255
或者access-list 1 permit any
!
router(config)# interface fast0/0
router(config-if)# ip access-group 1 in
```

标准ACL配置示例 2



只禁止左侧子网中的192.168.1.1-192.168.1.30访问A网络，其他流量放行

```
router(config)# access-list 1 deny 192.168.1.0 0.0.0.31
router(config)# access-list 1 permit any
router(config)# interface fast0/0
router(config-if)# ip access-group 1 in
```

扩展ACL的配置（采用数字的方式命令）

- **创建扩展ACL**

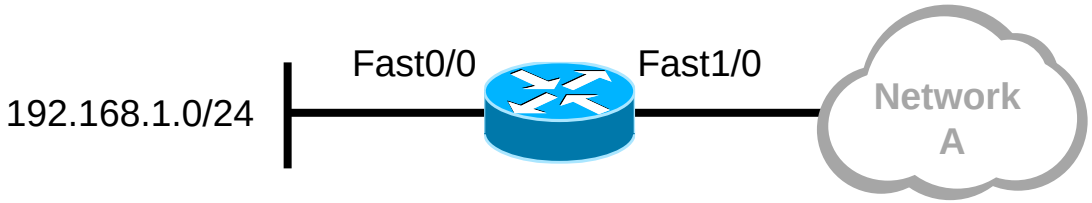
  Router(config)# **access-list** *acl-num* **{permit | deny} protocol** *source src-wildcard* **[operator port]** *destination dst-wildcard* **[***operator port***] [established] [log]**

  - 扩展ACL的编号值范围100-199，2000-2699
  - 可以匹配源目的IP地址、四层端口号、协议类型等元素

- **将创建好的ACL应用在接口上**

  Router(config-if)# **ip access-group** *acl-num* { **in | out** }

扩展ACL配置示例 1

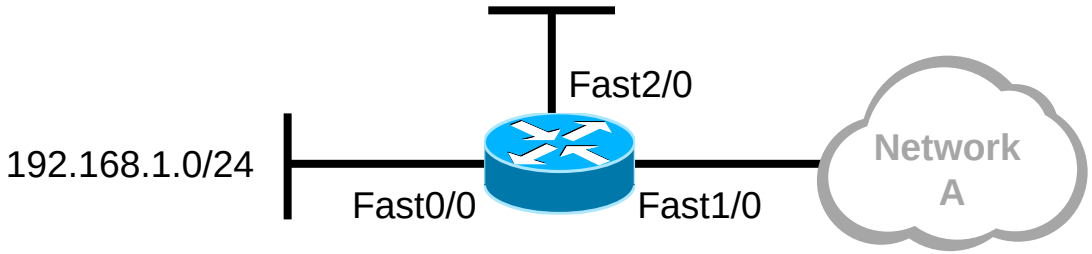


只禁止A网段中的192.168.1.1-192.168.1.30 访问A网络的服务器192.168.2.200

其他流量放行

```
router(config)# access-list 100 deny ip 192.168.1.0 0.0.0.31 host 192.168.2.200
router(config)# access-list 100 permit any
router(config)# interface fast0/0
router(config-if)# ip access-group 1 in
```

扩展ACL配置示例 2



只禁止所有用户访问A网络的服务器的Telnet服务，其他流量放行

```
router(config)# access-list 100 deny tcp any host 192.168.2.200 eq 23
router(config)# access-list 100 permit ip any any
router(config)# interface fast1/0
router(config-if)# ip access-group 1 out
```

配置命令的ACL

- **创建一个使用字符来命名的ACL**

Router(config)# **ip access-list {standard | extended}** *name*
Router(config {std-|ext-}nacl)# [*sequence-number*] {**permit | deny**} {ip access list test conditions}

  - 可以在命令的前面使用序号来创建每条语句，如果不手工输入序号，则默认从10开始，并以10为步长累加
  - 使用no加上特定的序号即刻删除该条语句

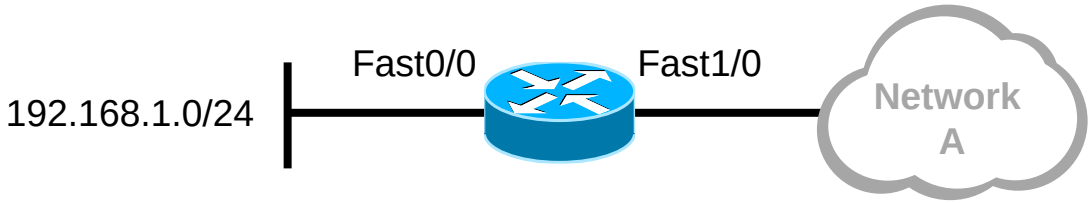
- **将创建好的ACL应用在接口上**

Router(config-if)# **ip access-group** *acl-num* { **in | out** }

阶段性总结

- 每个接口、每个方向、针对一种特定协议，只能应用1 个ACL。
- 提前组织好ACL语句的顺序，将匹配几率最高条目的放在ACL的最顶部，这可以提升网络设备的工作效率。
- 无法从ACL中删除某一条语句，只能将ACL整个删除然后重新编写，除非使用命名访问列表。
- ACL在所有语句的末尾隐含了一条拒绝所有的语句（deny any），因此ACL里至少要有1条permit语句。
- 创建了ACL 后要把它应用起来（例如应用在接口上用于过滤数据），否则该ACL并不生效。
- ACL 用于过滤经过设备的数据包，它并不会过滤设备自己产生的数据包。

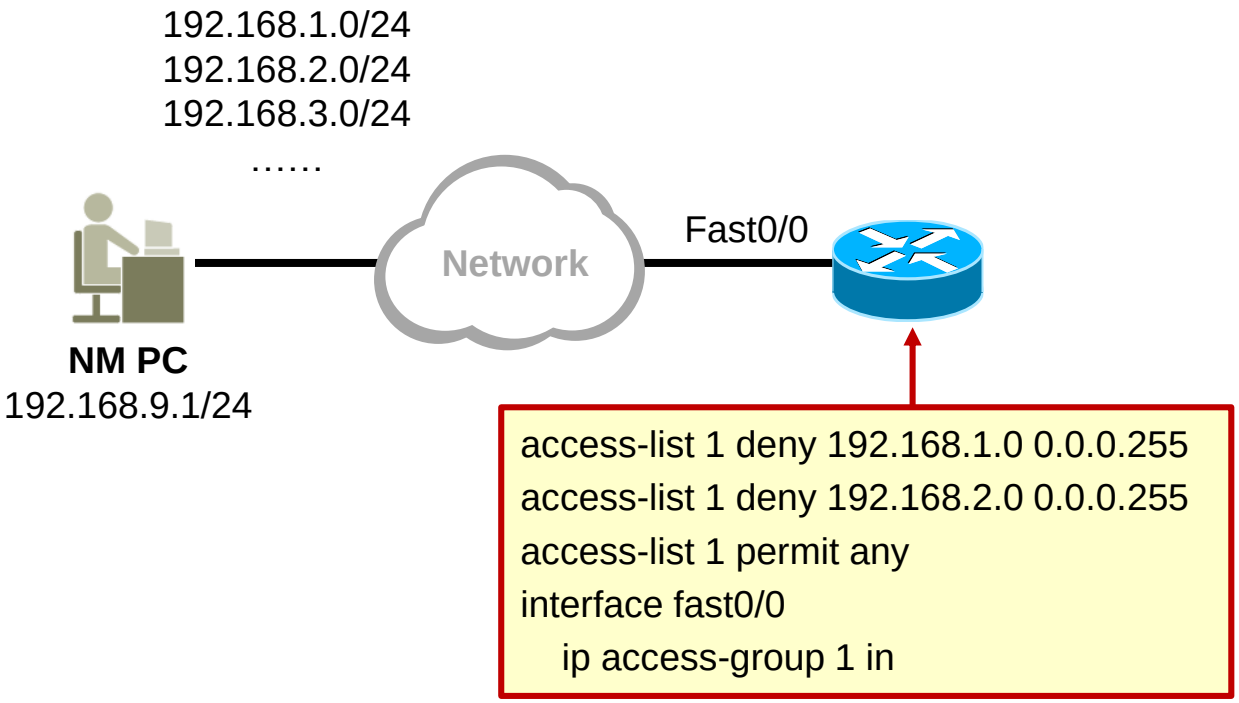
Case1




```
router(config)# access-list 1 deny 192.168.1.0 0.0.0.255
router(config)# access-list 1 permit host 192.168.1.1
router(config)# interface fast0/0
router(config-if)# ip access-group 1 in
```

192.168.1.1 能否访问到A网段？

Case2



- 当前路由器上部署了ACL应用在fast0/0口，ACL如上图所示，禁止192.168.1.0/24及192.168.2.0/24这两个网段的流量进入路由器的fast0/0
- 现在需求变更，要放开192.168.2.0/24这个网段的流量
- 工程师通过电脑远程登录到路由器，他……

红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You

红茶三杯
Vinsoney

学习 沉淀 成长 分享

NAT网络地址转换

红茶三杯 http://weibo.com/vinsoney

Latest update: 2012-08-01

Content

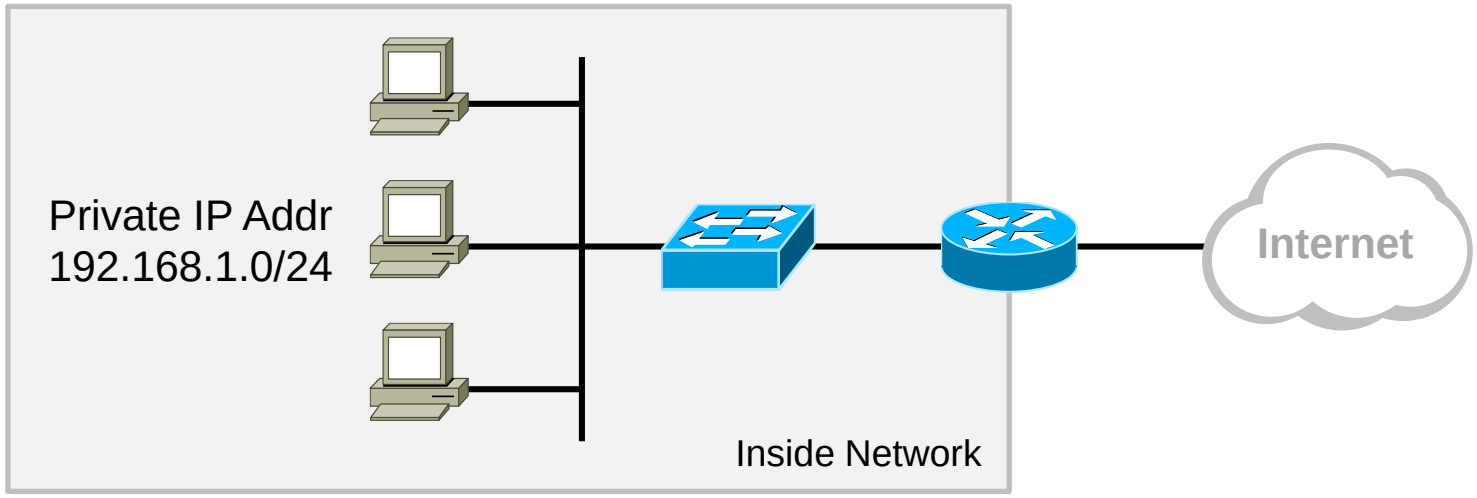
NAT概述

工作机制详解

配置及实现

NAT概述

NAT技术背景



- 私有IP地址的定义极大程度的缓解了IPv4地址紧缺的问题。
- 私有IP地址可以在本地局域网、私有网络内部随意使用，但是这些地址在公网上是不可被路由的，因此私有IP地址无法直接访问公网。
- NAT网络地址转换技术能够将数据包中的IP地址进行转换。

私有IPv4地址空间

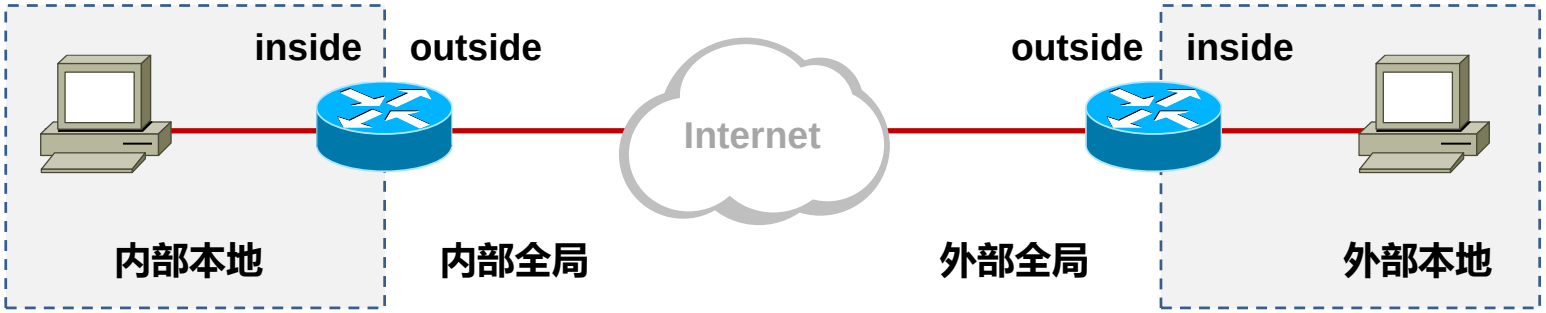
- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

NAT优缺点

优点	缺点
节省IP地址空间	增加转发延迟
解决IP地址重叠问题	丧失端到端的寻址能力
增加网络的连入Internet的弹性	某些应用不支持NAT
网络变更的时候减少IP重编址带来的麻烦	需要一定的内存空间支持动态存储NAT表项
对外隐藏内部地址，增加网络安全性	需要耗费一定CPU资源进行NAT操作 需耗费一定的内存资源存储NAT表项

NAT术语

术语	解释
内部本地	转换之前内部源地址的名字
外部本地	转换之前目标主机的名字
内部全局	转换之后内部主机的名字
外部全局	转换之后外部目标主机的名字



红茶三杯
Vinsoney

NAT工作机制详解

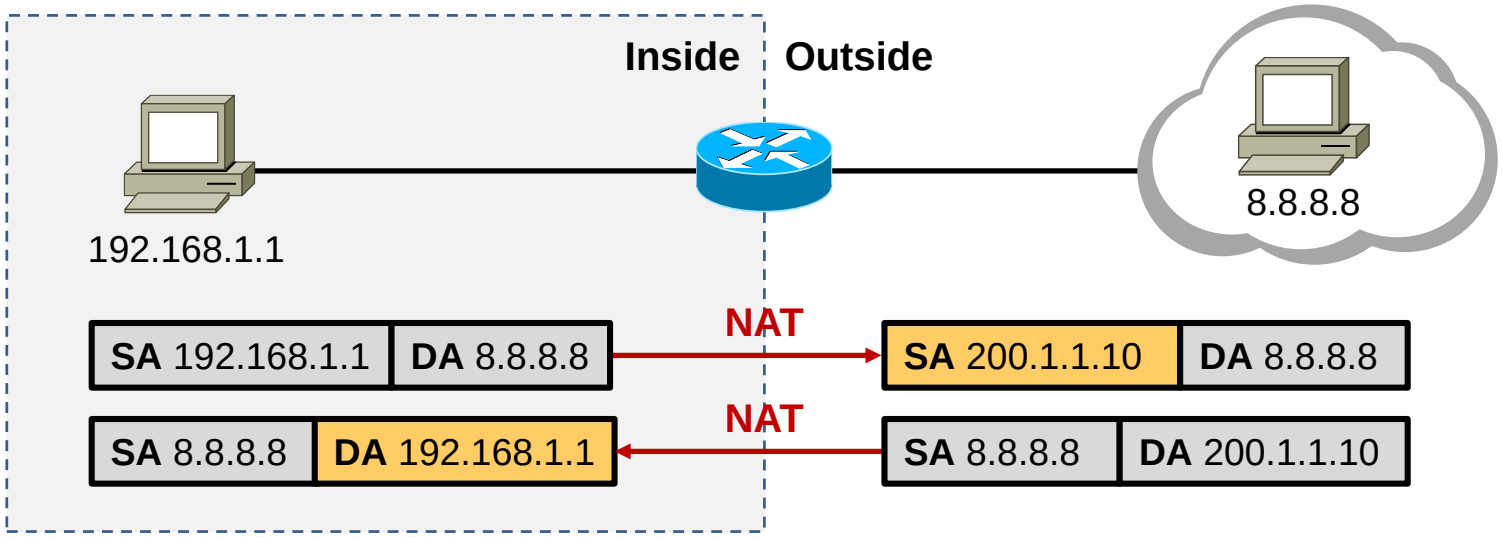
- 静态NAT
- 基于地址池的源地址转换
- PAT端口地址转换

Static NAT

- Static NAT，静态NAT，用于将内部本地地址（私有IP）与内部全局地址（公有IP）进行一对一的映射。缺点是需要每一个内部IP地址需独占一个宝贵的公网IP地址。即，如果某个合法IP地址已经被NAT静态地址转换定义，即使该地址当前没有被使用，也不能被用作其它的地址转换。而且这种方式是静态手工创建的NAT映射，可扩展性不高
- 这种方法主要用在内网中存在需要对公网提供服务的服务器的场景，类似的例子有WEB服务器、邮件服务器、FTP服务器等。
- Static NAT支持IP对IP的映射，以及端口对端口的映射。

Static NAT

SA : Source IP Address
DA : Destination IP Address

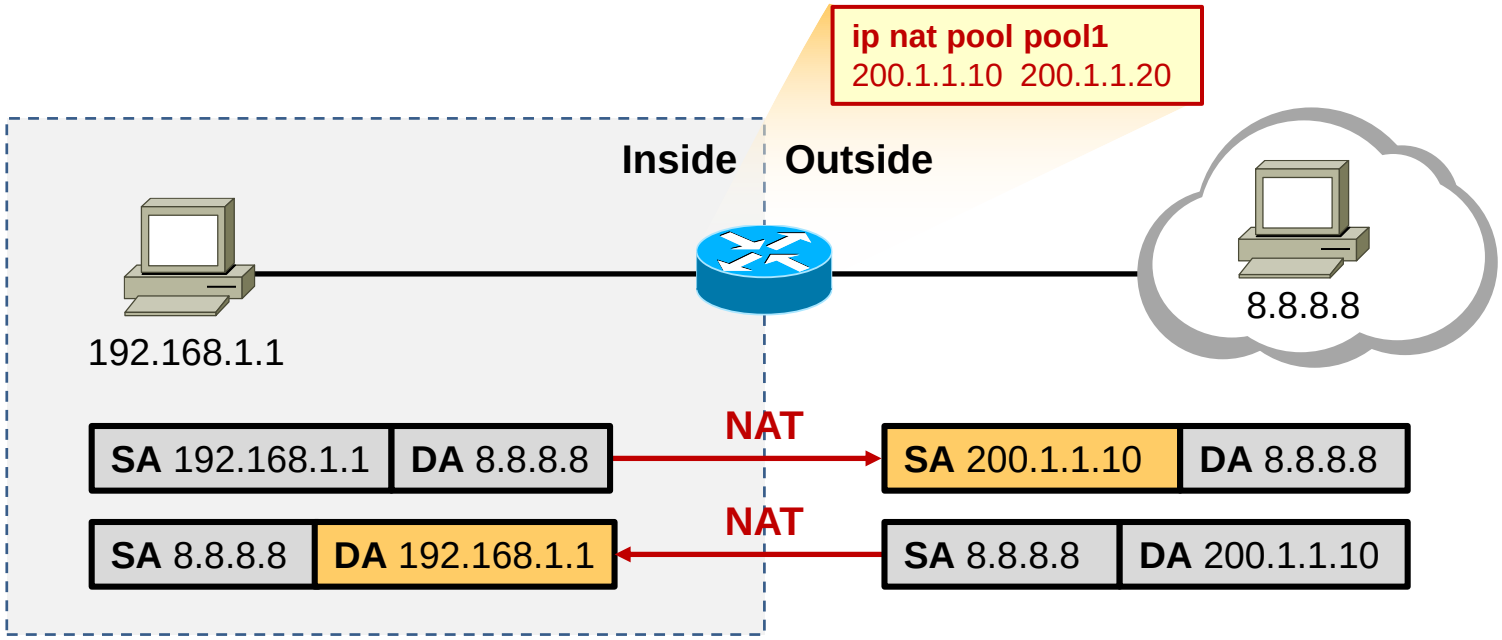


	Inside Local address	Inside Global Address
Static	192.168.1.1	200.1.1.10

基于地址池的源地址转换（一对一）

- 基于地址池的源地址转换（一对一）是一种动态NAT，其实也是一对一的映射关系。将公网地址放置在一个地址池中，在需要对外出数据包的源地址进行转换时，从地址池中取出一个公网地址供该私有地址专用，并形成NAT映射表项。
- 当已占用一个公网地址的用户在一定时间内没有数据传输时，该公网地址资源被收回到地址池中，供其他用户使用。
- 这种方式的NAT不会对数据报头部中的端口地址进行转换。

基于地址池的源地址转换（一对一）

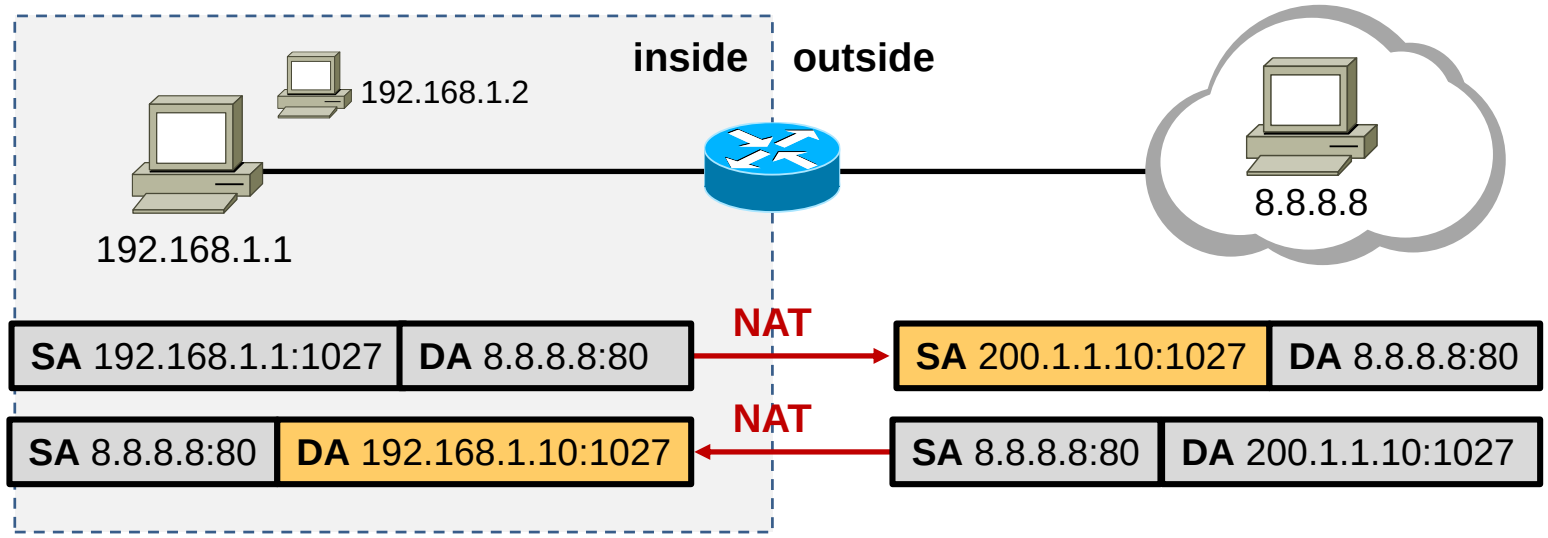


	Inside Local address	Inside Global Address
Dynamic	192.168.1.1	200.1.1.10

PAT

- 也称为端口地址转换（Port Address Translation，PAT），也即对数据包的源地址和端口均进行转换，通过这种转换，可以使多个内部本地地址同时共享同一个公网地址，通过IP+端口的方式来识别不通的源，也就是多对一的映射。
- 对于只申请到少量IP地址甚至只有一个合法IP地址却经常有很多用户同时要求上网的情况，这种转换方式非常有用。这种地址转换方式真正意义上缓解了IPv4地址紧缺的问题。在各种网络中被广泛采用。

PAT



	Inside Local address	Inside Global Address
Dynamic	192.168.1.1:1027	200.1.1.10:1027
Dynamic	192.168.1.2:1025	200.1.1.10:1025

红茶三杯
Vinsoney

NAT的配置及实现

配置静态NAT转换

- 创建NAT静态映射条目

```
Router(config)# ip nat inside source static local-ip global-ip
```

- 指定内部接口

```
Router(config-if)# ip nat inside
```

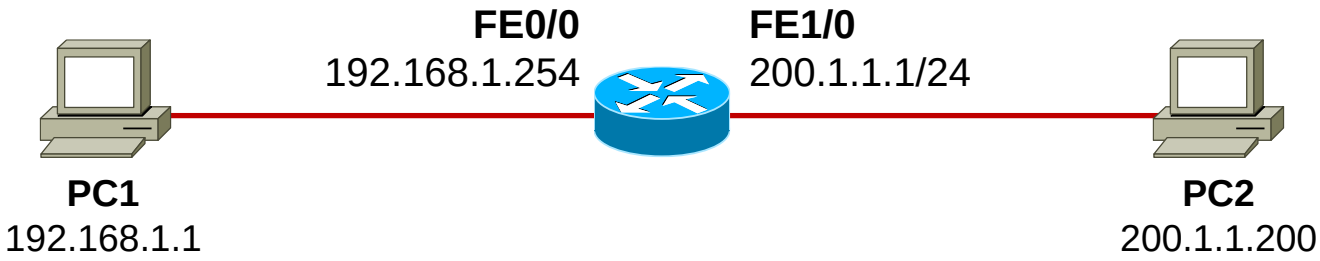
- 指定外部接口

```
Router(config-if)# ip nat outside
```

- 查看nat映射

```
Router# show ip nat translations
```

配置静态NAT转换（IP一对一映射）

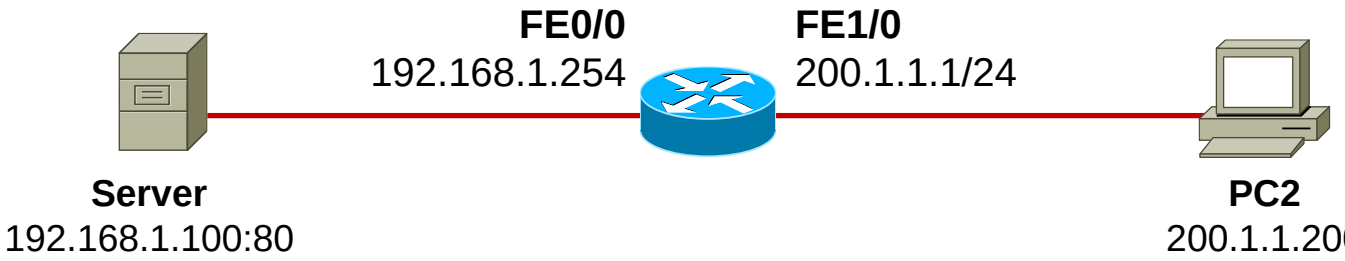



```
ip nat inside source static 192.168.1.1 200.1.1.10

interface FastEthernet 0/0
  ip nat inside
interface FastEthernet 1/0
  ip nat outside
```

```
Router# show ip nat translations
Pro  Inside global   Inside local    Outside local   Outside global
---  200.1.1.10      192.168.1.1     ---             ---
```

配置静态NAT转换（静态端口映射）




```
ip nat inside source static tcp 192.168.1.100 80  200.1.1.100 8080

interface FastEthernet 0/0
  ip nat inside
interface FastEthernet 1/0
  ip nat outside
```

```
Router# show ip nat translations
Pro   Inside global          Inside local        Outside local   Outside global
tcp   200.1.1.100:8080   192.168.1.100:80    ---                 ---
```

配置基于地址池方式的NAT（一对一）

- 创建NAT地址池

  Router(config)# **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}

- 创建ACL 用于匹配允许NAT的内网地址

  Router(config-if)# **access-list** *acl-num* **permit** *source* [*source-wildcard*]

- 将ACL与NAT地址池进行关联

  Router(config-if)# **ip nat inside source list** *acl-num* **pool** *name*

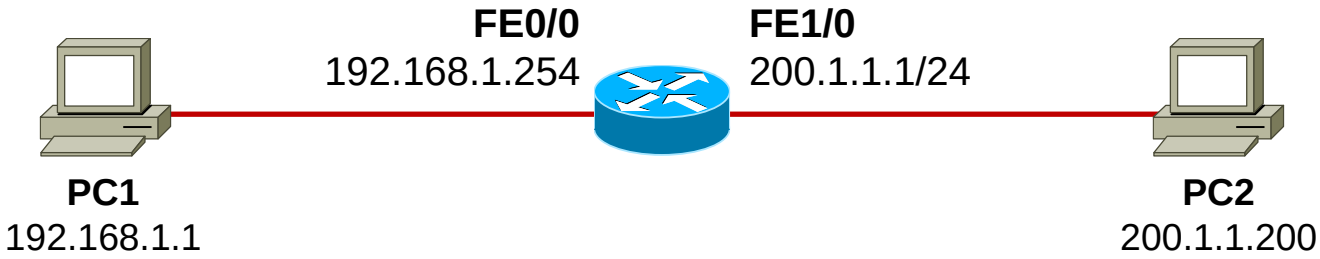
- 指定内部接口

  Router(config-if)# **ip nat inside**

- 指定外部接口

  Router(config-if)# **ip nat outside**

配置基于地址池方式的NAT（一对一）

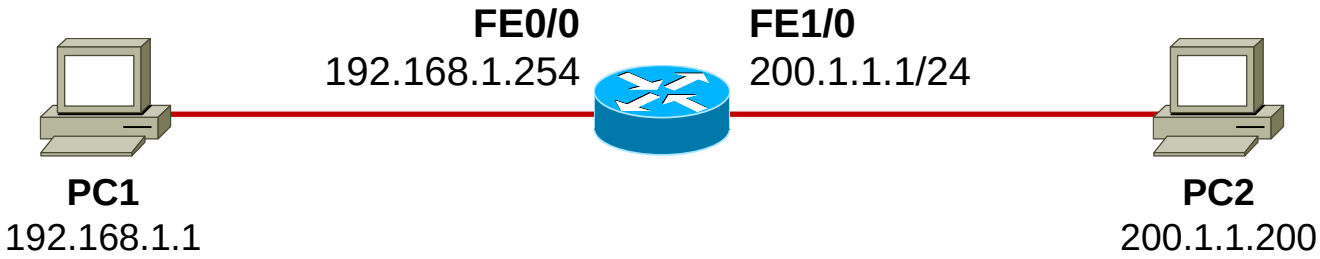



```
ip nat pool natpool 200.1.1.10 200.1.1.20 netmask 255.255.255.0

access-list 1 permit 192.168.1.0 0.0.0.255

ip nat inside source list 1 pool natpool
interface FastEthernet 0/0
  ip nat inside
interface FastEthernet 1/0
  ip nat outside
```

配置基于地址池方式的NAT（多对一）

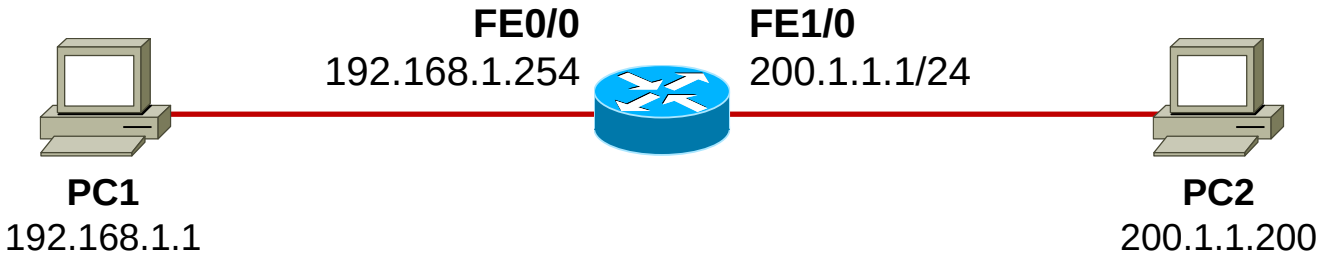



```
ip nat pool natpool 200.1.1.10 200.1.1.20 netmask 255.255.255.0

access-list 1 permit 192.168.1.0 0.0.0.255

ip nat inside source list 1 pool natpool overload
interface FastEthernet 0/0
  ip nat inside
interface FastEthernet 1/0
  ip nat outside
```

配置接口Overload




```
access-list 1 permit 192.168.1.0 0.0.0.255

ip nat inside source list 1 interface fastethernet1/0 overload

Interface FastEthernet 0/0
  ip nat inside
interface FastEthernet 1/0
  ip nat outside
```

NAT维护

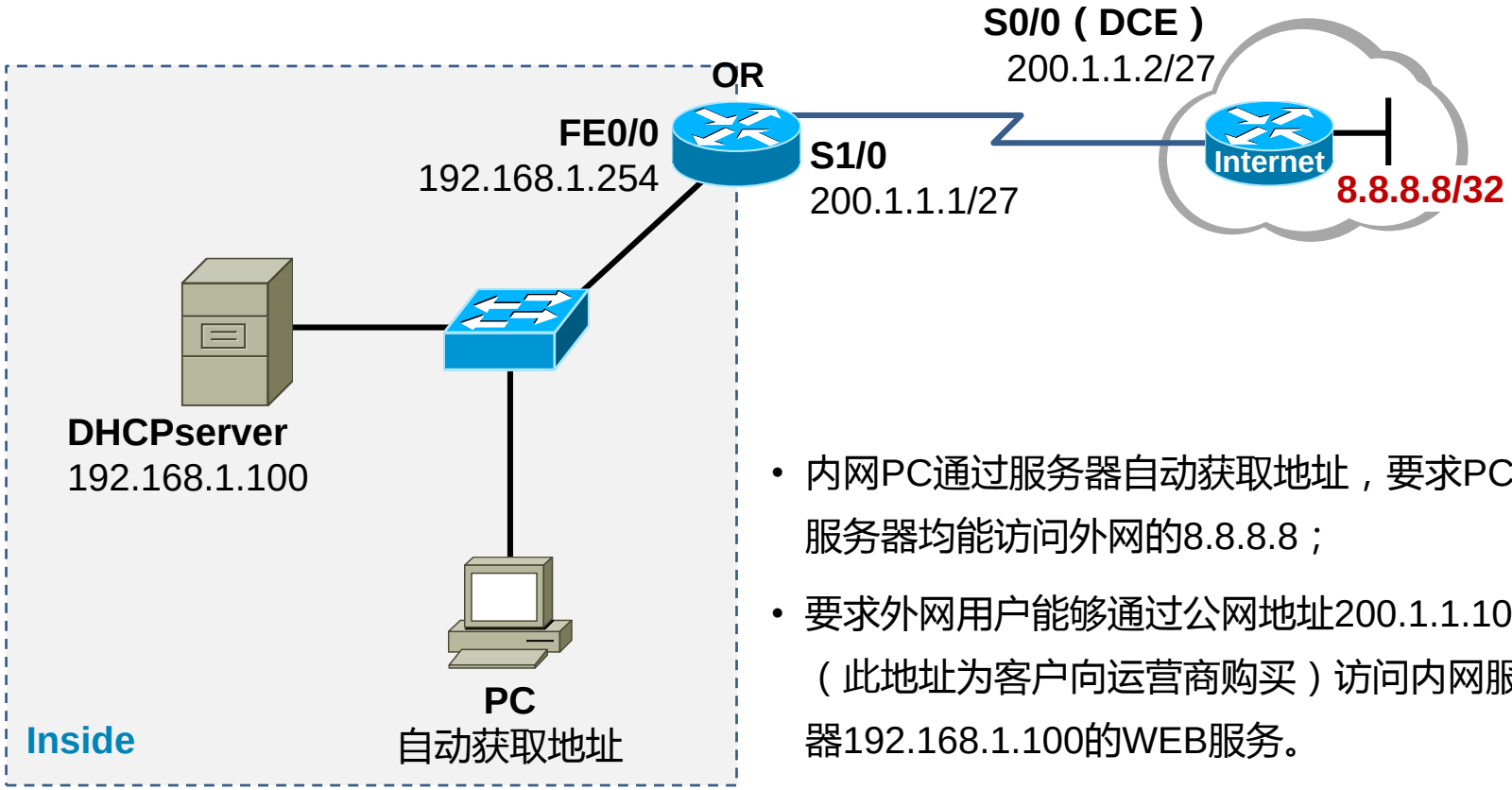
- 清楚所有动态NAT表项

```
Router# clear ip nat translation *
```

- 清楚特定的NAT表项

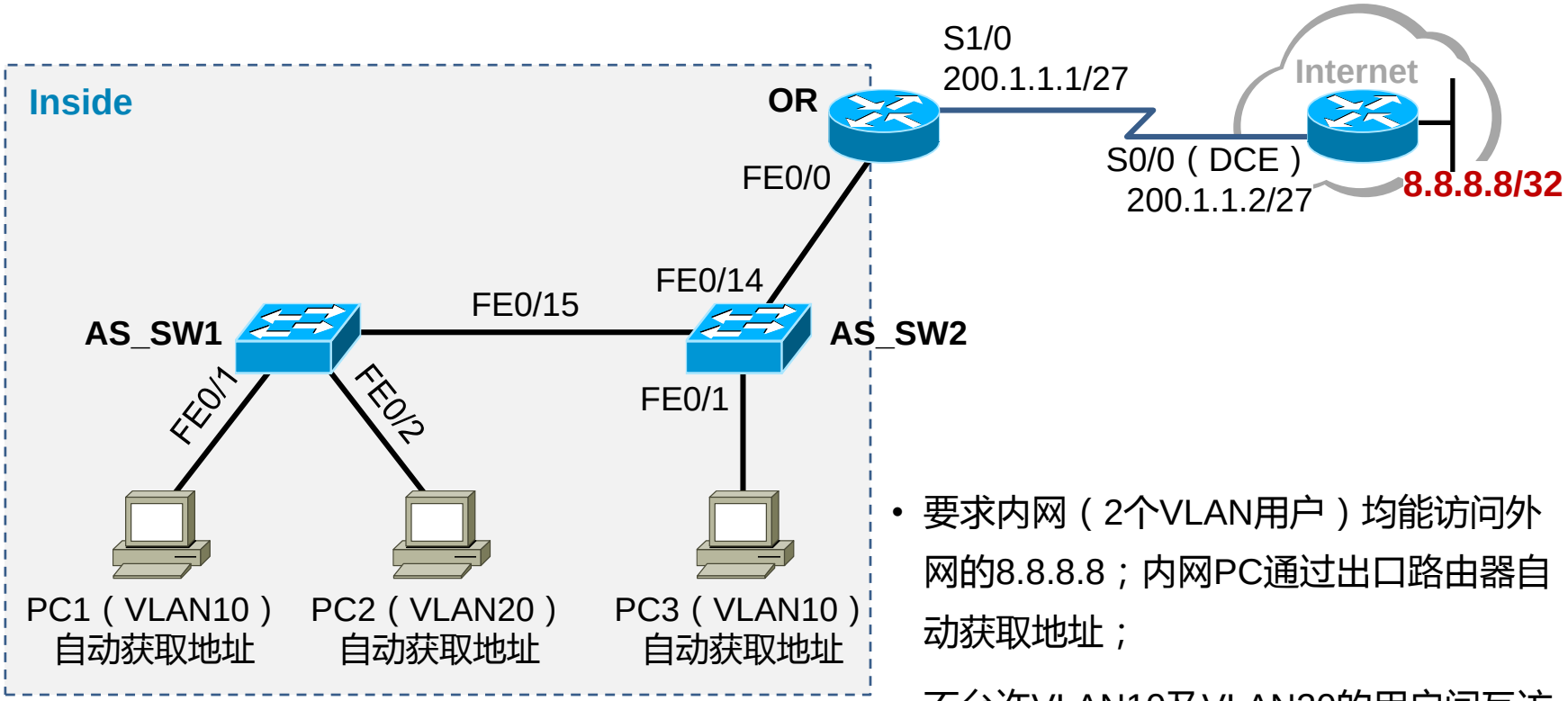
```
Router# clear ip nat translation ?
```

NAT综合小实验1



- 内网PC通过服务器自动获取地址，要求PC及服务器均能访问外网的8.8.8.8；
- 要求外网用户能够通过公网地址200.1.1.10（此地址为客户向运营商购买）访问内网服务器192.168.1.100的WEB服务。

NAT综合小实验2



- 要求内网（2个VLAN用户）均能访问外网的8.8.8.8；内网PC通过出口路由器自动获取地址；
- 不允许VLAN10及VLAN20的用户间互访。

红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You

红茶三杯
Vinsoney

学习 沉淀 成长 分享

WAN , PPP and FrameRelay

红茶三杯 微博：http://t.sina.com/vinsoney

Latest update: 2012-06-01

Content

广域网概述

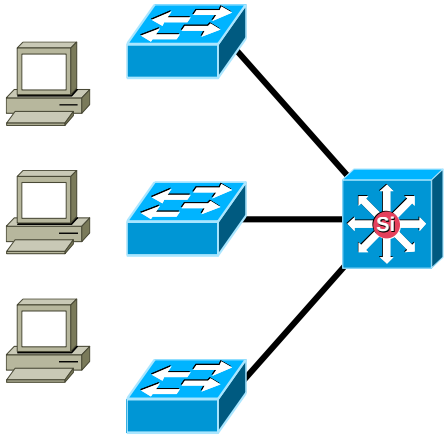
PPP

FrameRelay

广域网概述

- 什么是广域网
- 广域网链路类型
- 常见的广域网封装

Local Area Network

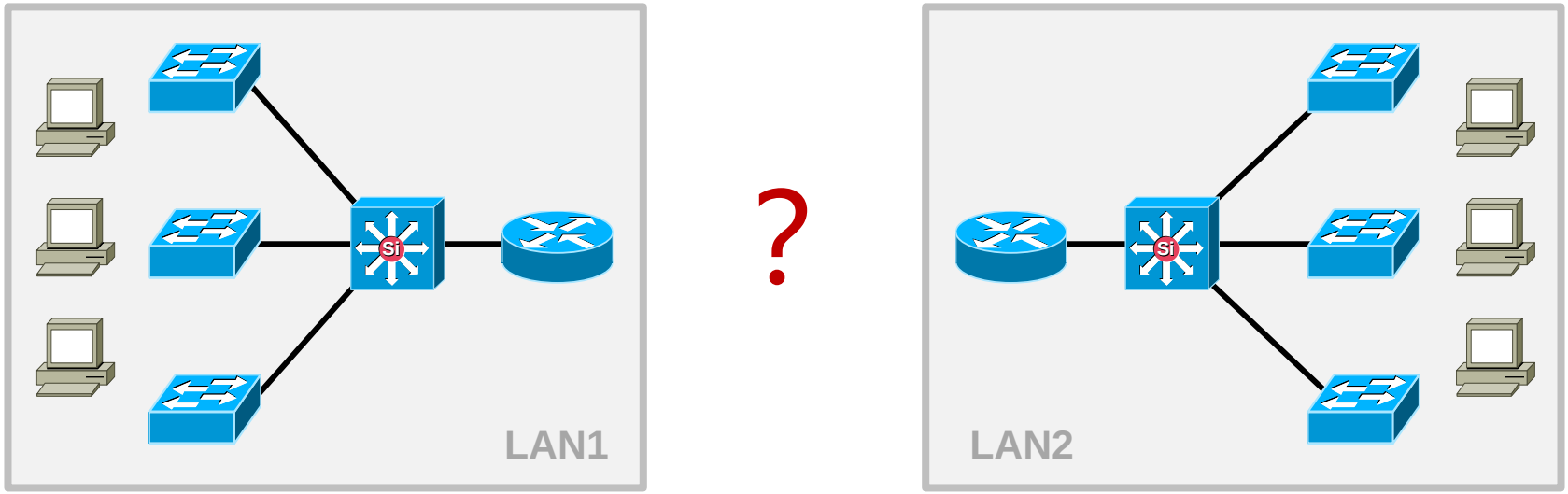


局域网（Local Area Network，LAN）

- 在一个局部的地理范围内（如一个学校、公司或园区），一般是方圆几千米以内所搭建的一张数据通信网络

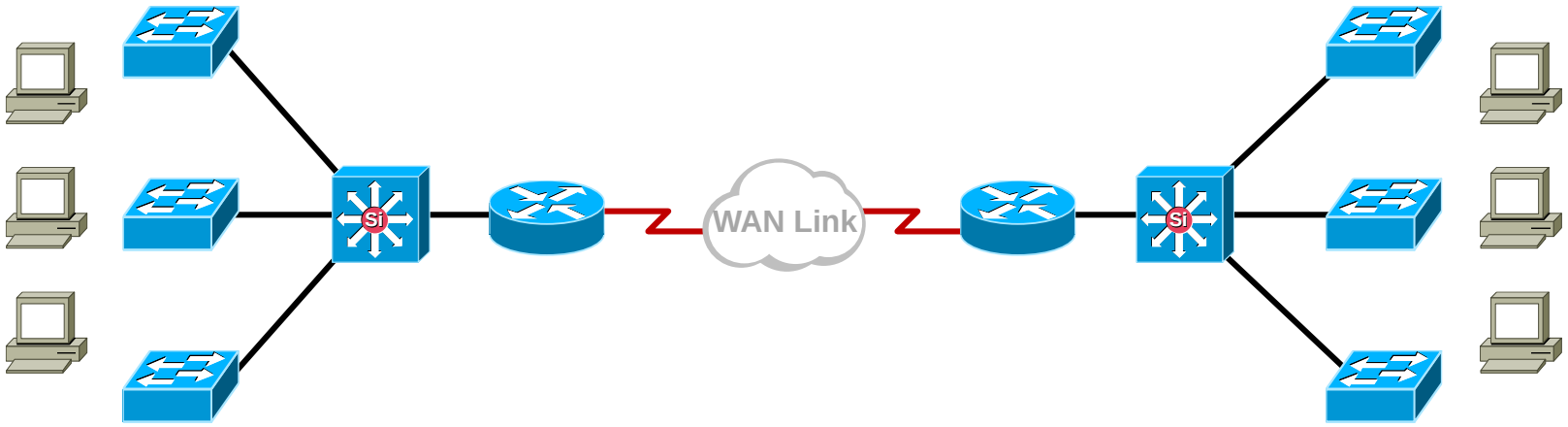
Local Area Network

分布在两地（距离较长）的LAN如何能够实现互通？



WAN Link

广域网线路用于将处于两个不同地理位置的网络连接起来



什么是广域网链路

- 用于连接LAN的、跨地理位置的数据通信链路。

  例如同属一个公司的不同分支机构（处于不同的地址位置）之间的互联链路。
- WAN链路一般需要向运营商购买
- WAN链路的地理跨越范围比LAN更广
- 链路类型多种多样，客户根据自己的需要进行选择

广域网接入方式

- 专线
- 电路交换
- 分组交换
- VPN
- 无线

广域网接入方式

- **专线**
  - 如DDN、POS、E1、以太网专线等
  - 点到点的专有连接（安全、高传输质量）
  - 支持多种物理介质与物理接口标准
  - 稳定可靠，配置与维护简单
  - 适合长时间的业务流量需求；价格相对较高

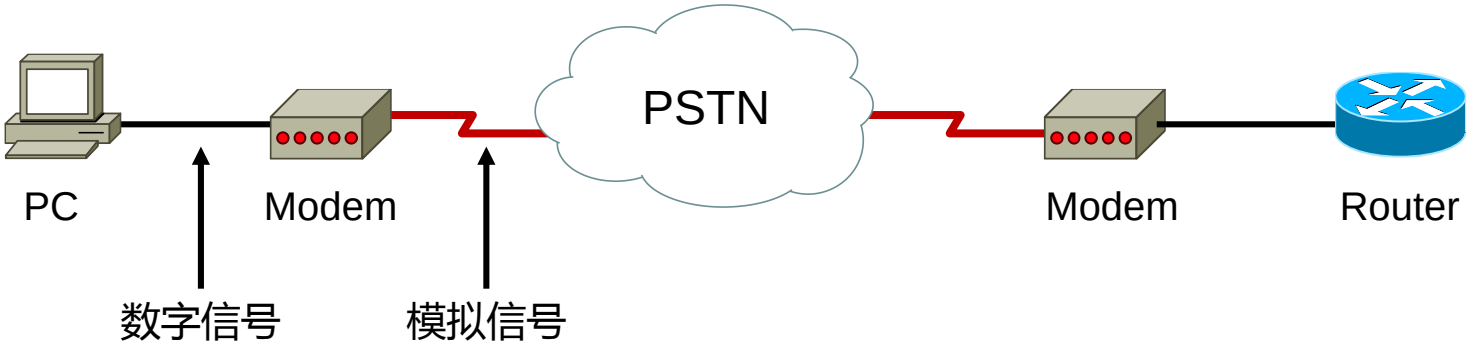
Line type	Bit Rate Capacity
56	56 kbps
64	64 kbps
T1	1.544 Mbps
E1	2.048 Mbps
J1	2.048 Mbps
E3	34.064 Mbps
T3	44.736 Mbps
OC-1	51.84 Mbps
OC-3	155.54 Mbps
OC-9	466.56 Mbps
OC-12	622.08 Mbps
OC-18	933.12 Mbps
OC-24	1244.16 Mbps
OC-36	1866.24 Mbps
OC-48	2488.32 Mbps
OC-96	4976.64 Mbps
OC-192	9953.28 Mbps
OC-768	39813.12 Mbps

广域网接入方式

- **电路交换**
  - 定义：由SP为企业远程网络节点间通信提供的临时数据传输通道，其操作特性类似电话拨号技术
  - 常见的如ISDN，PSTN
  - 逻辑连接持久有效，按需拨号
  - 传输介质主要为电话线，也可以为光纤
  - 带宽主要为56Kbps，64Kbps，128Kbps，2Mbps
  - 稳定性较差，配置与维护较复杂

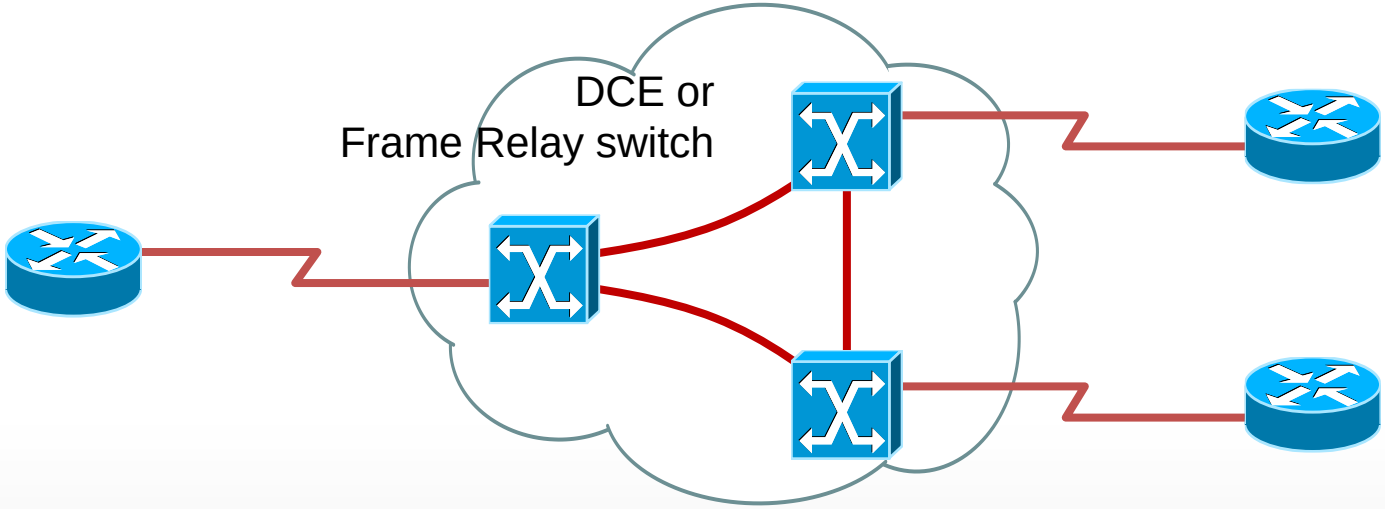
广域网接入方式

- **电路交换**
  - PSTN模拟拨号
    - 利用传统承载语音模拟信号的电话线来承载数字信号业务的拨号技术
    - 数/模信号转换
    - 带宽小，信号质量取决于电话介质信号质量

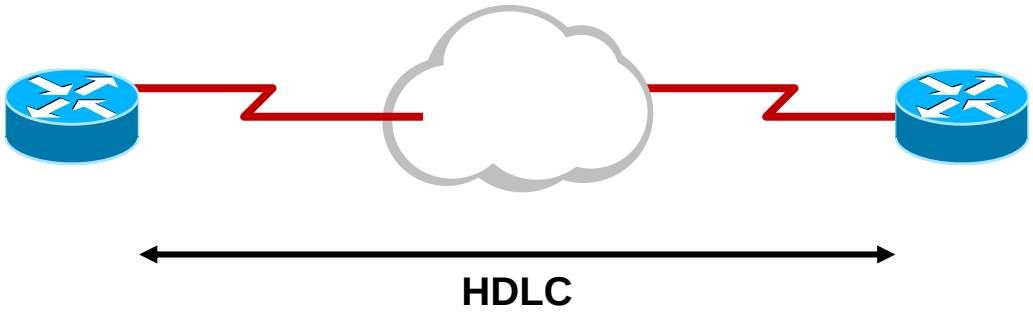


广域网接入方式

- **分组交换（包交换）**
  - 分组交换设备根据数据帧的二层地址来进行路径的选择
  - **PVC 永久虚电路**　在交换开始时就已经建立了路由
  - **SVC 交换虚电路**　根据需要建立
  - 常见业务如x.25、FrameRelay

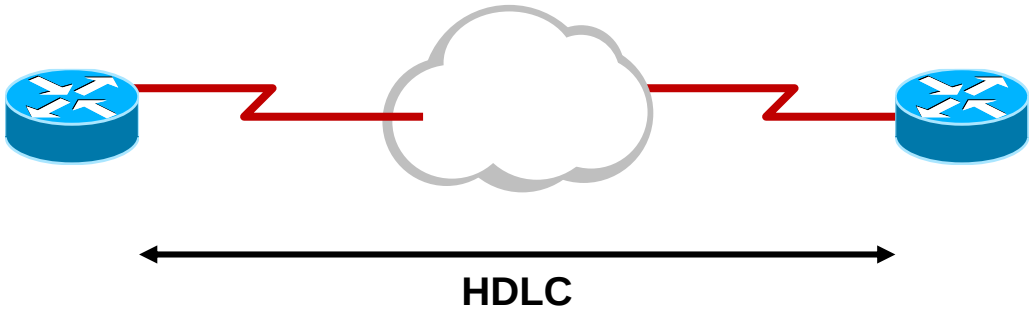


HDLC



- 专用线路在数据链路层一般采用HDLC或PPP的封装
- 专用线路是一条永久的点对点线路
- HDLC（High-level Data link Control）高级数据链路控制协议是一种在同步链路上传输数据的二层协议
- HDLC由SDLC协议发展而来
- 每个厂家的HDLC可能有所不同，因此不通厂家之间的HDLC未必能够兼容

HDLC



传统ISO HDLC只支持单协议环境

HDLC

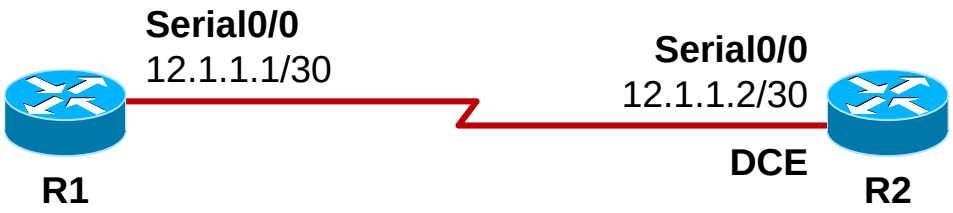
Flag	Address	Control	Data	FCS	Flag

CISCO HDLC支持多协议类似IP头的协议号字段

Cisco HDLC

Flag	Address	Control	Proprietary	Data	FCS	Flag

配置HDLC封装



R1

```
interface serial 0/0
  encapsulation hdlc
  ip address 12.1.1.1 255.255.255.252
  no shutdown
```

R2

```
interface serial 0/0
  encapsulation hdlc
  ip address 12.1.1.2 255.255.255.252
  clock rate 64000
  no shutdown
```

- CISCO IOS路由器的Serial接口缺省就是HDLC的封装
- 该HDLC实际上是CISCO私有的HDLC

红茶三杯
Vinsoney

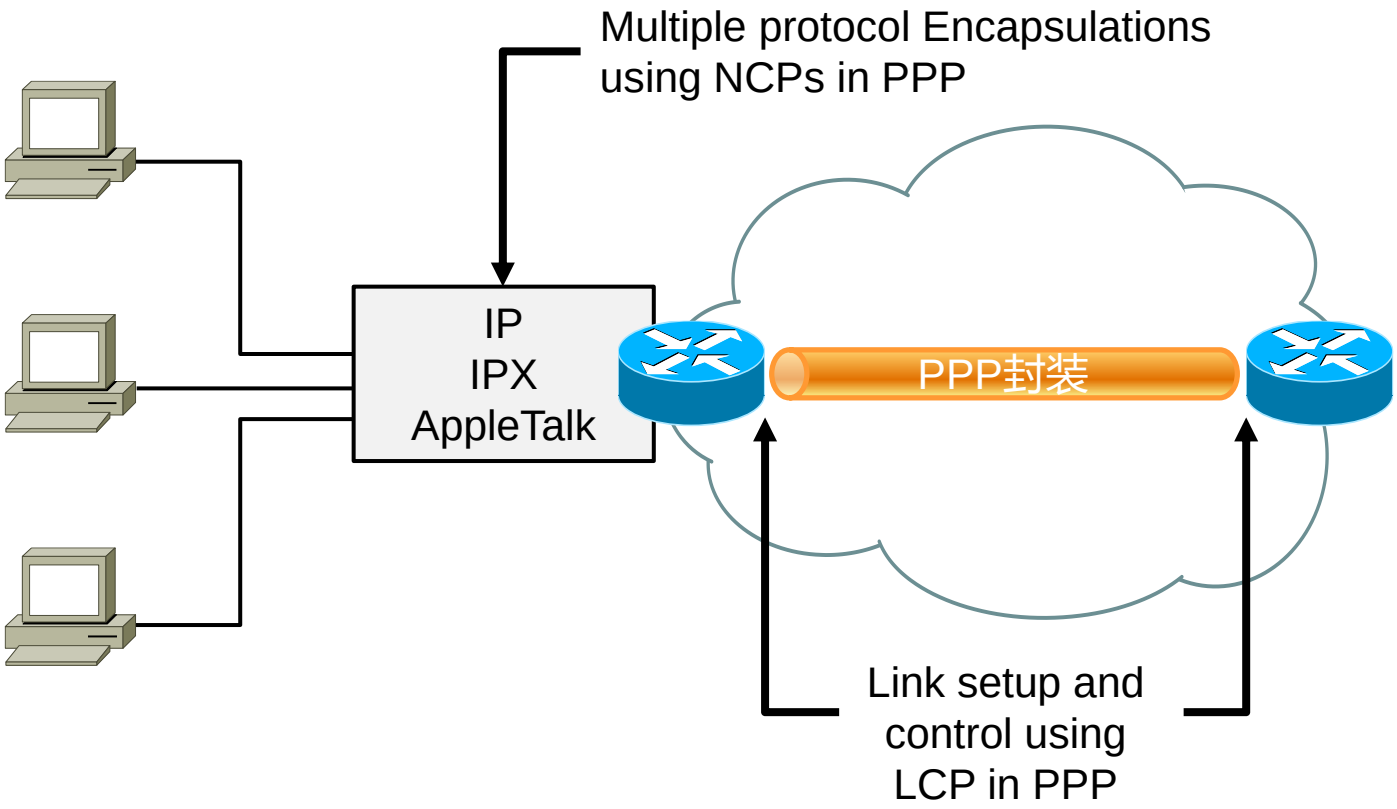
PPP

- PPP简介
- PPP的组件
- PAP及CHAP认证
- PPP配置

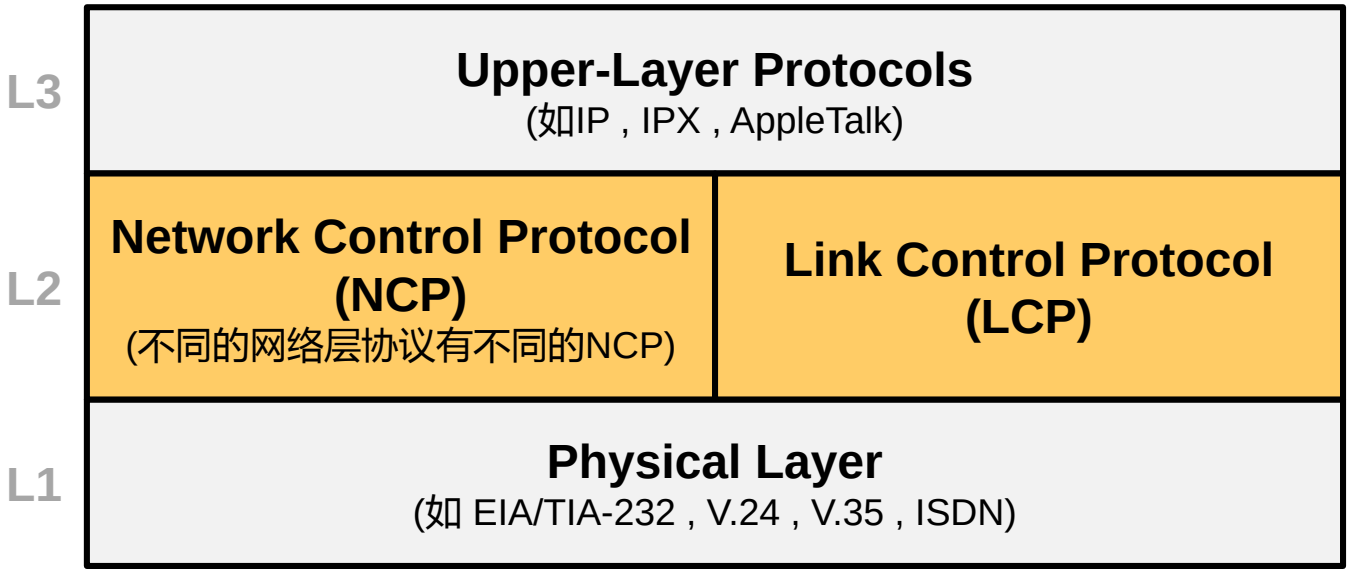
PPP简介

- **Point to Point Protocol，简称PPP**
  - 能够控制数据链路的建立；
  - 能够对IP地址进行分配和使用；
  - 支持多种网络层协议；
  - 能够配置和测试数据链路；
  - 能够进行错误检测；
  - 提供身份验证；
  - 有协商选项，能够对网络层的地址和数据压缩等进行协商。

PPP简介


Multiple protocol Encapsulations
using NCPs in PPP
IP
IPX
AppleTalk
PPP封装
Link setup and
control using
LCP in PPP

PPP的层次结构


L3
Upper-Layer Protocols
(如IP , IPX , AppleTalk)
L2
Network Control Protocol (NCP)
(不同的网络层协议有不同的NCP)
Link Control Protocol (LCP)
L1
Physical Layer
(如 EIA/TIA-232 , V.24 , V.35 , ISDN)

PPP的组件

- 链路控制协议LCP（Link Control Protocol）

  LCP负责创建，维护（Keepalive）或终止一条数据链路

  LCP还负责相关参数的协商，例如是否验证及使用的验证协议等

- 网络控制协议NCP（Network Control Protocol）

  NCP是一个协议族，负责解决物理连接上运行什么网络协议，以及解决上层网络协议发生的问题。

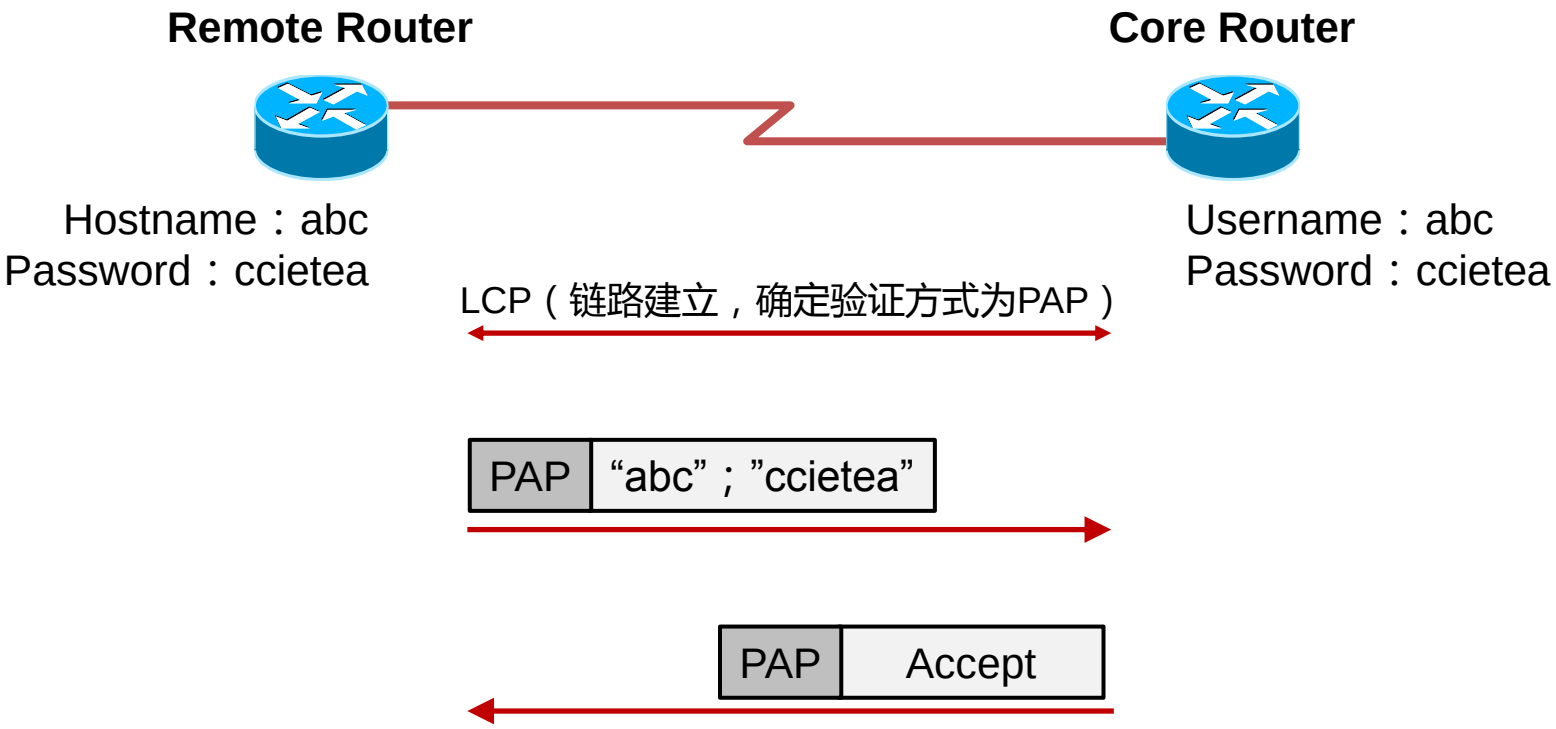
- 认证协议

  最常用的包括口令验证协议PAP（Password Authentication Protocol）和挑战握手验证协议CHAP（Challenge-Handshake Authentication Protocol）。

PPP会话的建立

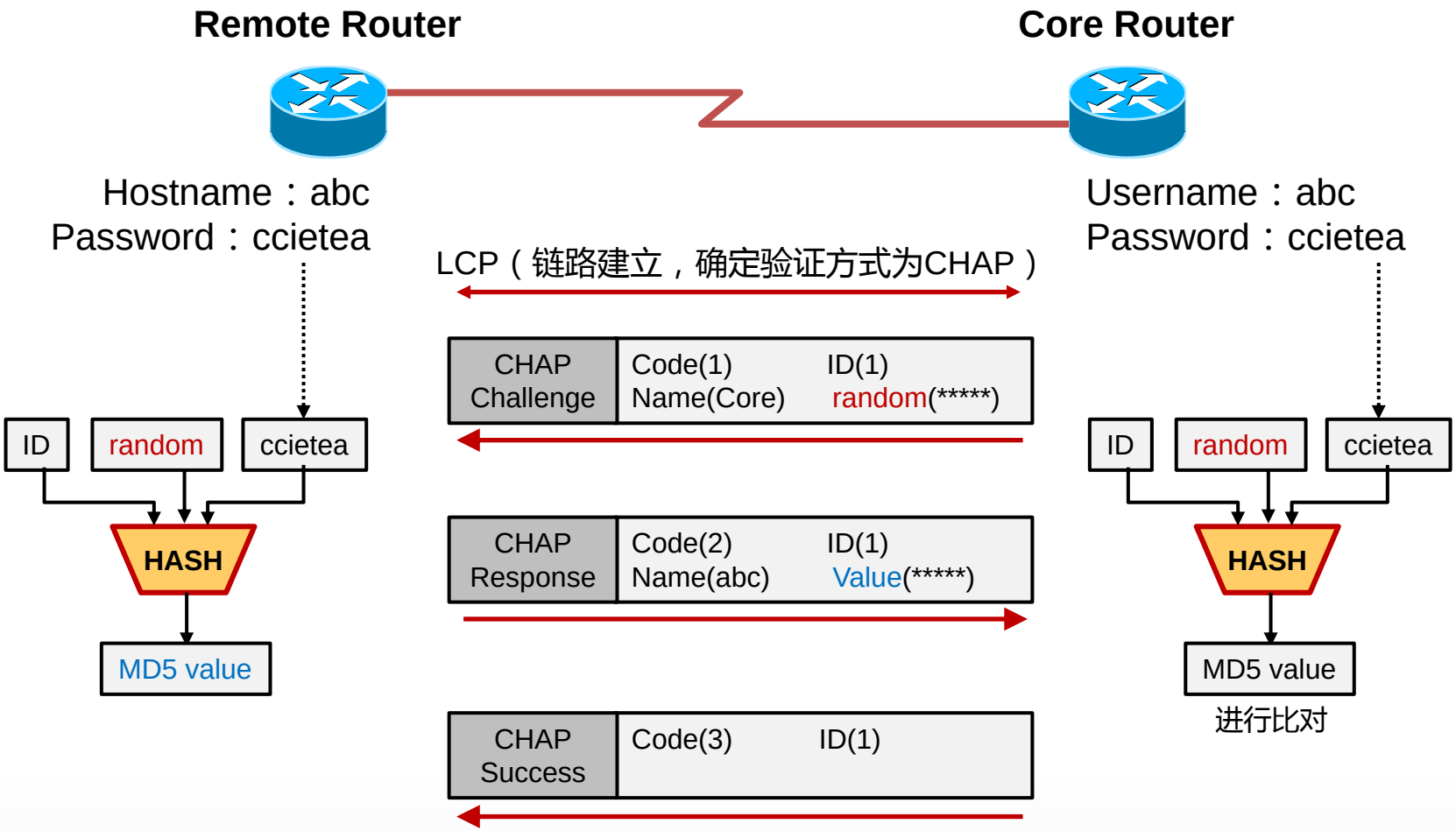
1. 链路的建立和配置协商
   - 通信双方发送LCP 帧来配置和检测数据链路。
   - 在任何网络层数据包传递之前，通信双方需通过LCP建立并且协商相关参数，这个阶段完成的标志是双方都收到对方发送来的LCP配置ACK消息。
   - LDP帧中包含一个option字段，通过该字段通信双方可以进行一系列的协商如：MTU、特定PPP字段的压缩、验证协议等。
2. 链路质量检测，认证阶段（可选）
   - 判断链路的质量是否能携带网络层信息。
   - 如果使用身份验证的话，那么验证过程发生在这步。
3. 网络层协议的配置协商
   - 通信的发起方发送NCP frame，用以选择和配置网络层协议。配置完毕后，通信双方可以发送各自的网络层协议数据分组。

PAP认证



- 2次握手
- 密码以明文的形式直接发送

CHAP认证



配置PPP和PPP认证

Router(config-if)# **encapsulation** ppp

- 为接口封装PPP

Router(config)# **hostname** *name*

- （可选）指定路由器的名字

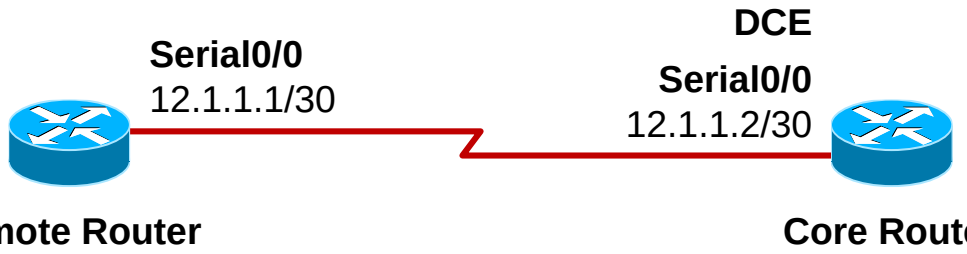
Router(config)# **username** *name* **password** *password*

- （可选）标示远端路由的用户名和密码，配置在认证服务器端

Router(config-if)# **ppp authentication** {**chap** | **chap pap** | **pap chap** | **pap**}

- （可选）启用PAP或者CHAP认证，配置在认证服务器端

示例1-ppp封装



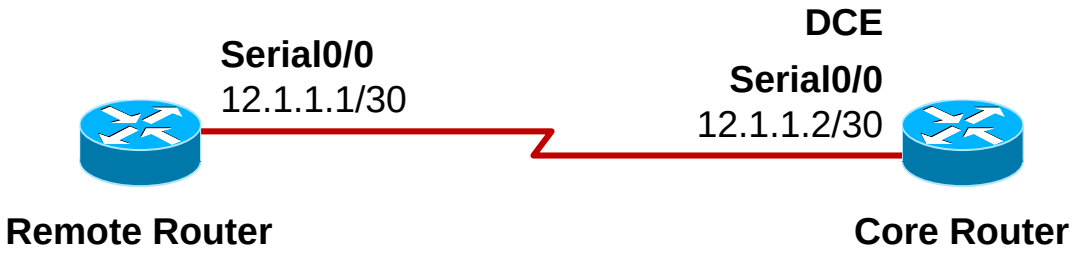
Remote Router

```
hostname remote
!
interface serial0/0
  encapsulation ppp
  ip address 12.1.1.1 255.255.255.252
```

Core Router

```
hostname Core
!
interface serial0/0
  encapsulation ppp
  clock rate 64000
  ip address 12.1.1.2 255.255.255.252
```

示例2-pap单向认证



Remote Router

```
hostname remote
interface serial0/0
  encapsulation ppp
  ip address 12.1.1.1 255.255.255.252
  ppp pap sent-username remote password ccietea
```

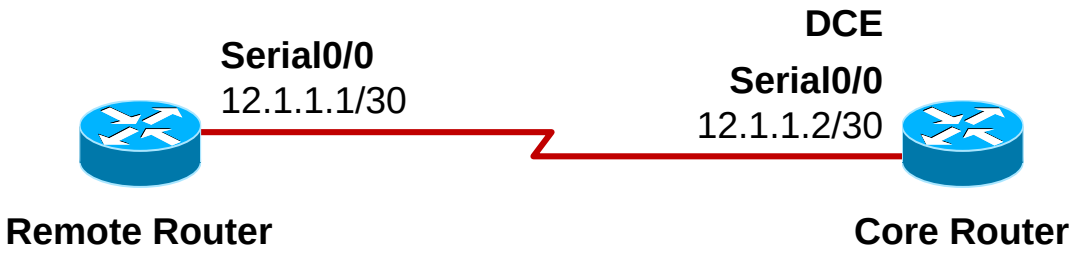
Core Router

```
hostname Core
username remote password ccietea
interface serial0/0
  encapsulation ppp
  ip address 12.1.1.2 255.255.255.252
  ppp authentication pap
```

示例2-pap单向认证 (cont.)

```
Serial0/0 is up, line protocol is up
  Hardware is M4T
  Internet address is 12.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input 00:00:53, output 00:00:01, output hang never
  Last clearing of "show interface" counters 11:09:00
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
```

示例3-chap单向认证



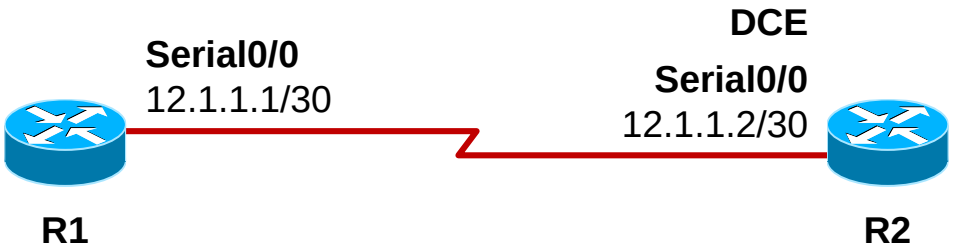
Remote Router

```
hostname remote
interface serial0/0
  encapsulation ppp
  ip address 12.1.1.1 255.255.255.252
  ppp chap hostname remote
  ppp chap password ccietea
```

Core Router

```
hostname Core
username remote password ccietea
interface serial0/0
  encapsulation ppp
  clock rate 64000
  ip address 12.1.1.2 255.255.255.252
  ppp authentication chap
```

示例4-chap双向认证



R1

```
hostname R1
username R2 password ccietea
interface serial0/0
  encapsulation ppp
  ip address 12.1.1.1 255.255.255.252
  ppp authentication chap
```

R2

```
hostname R2
username R1 password ccietea
interface serial0/0
  encapsulation ppp
  ip address 12.1.1.2 255.255.255.252
  ppp authentication chap
```

验证PPP

```
Router#show interface serial 0/0
```

```
Router#debug ppp authentication
```

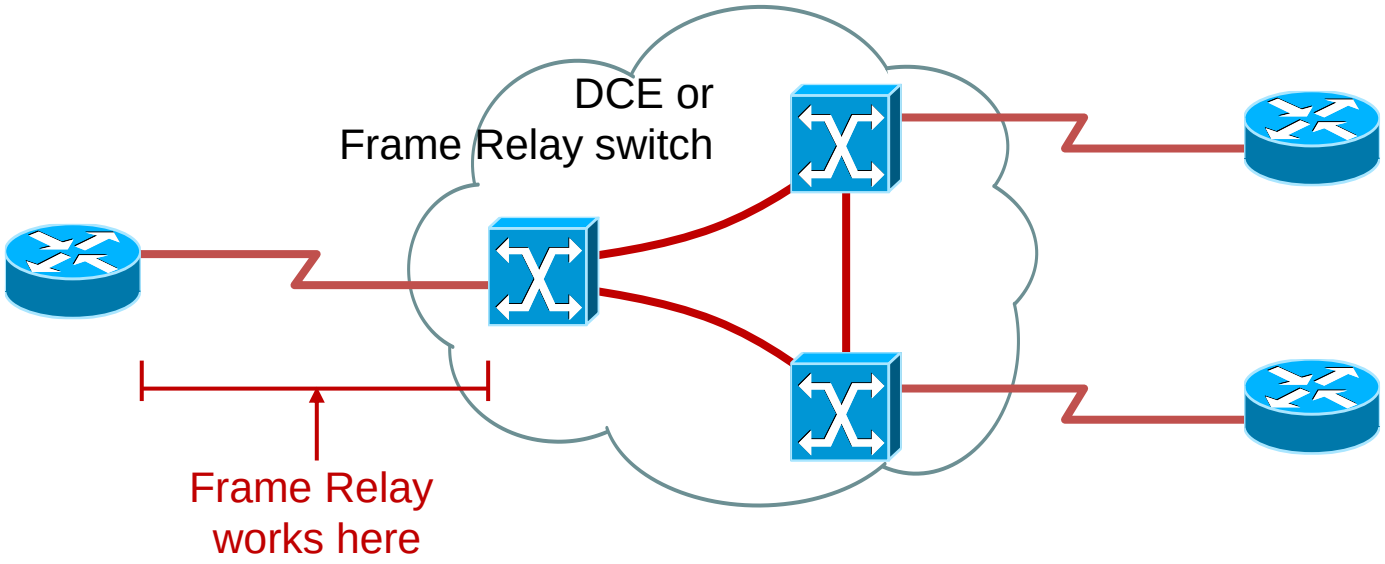
```
Router#debug ppp negotiation
```

红茶三杯
Vinsoney

Frame Relay

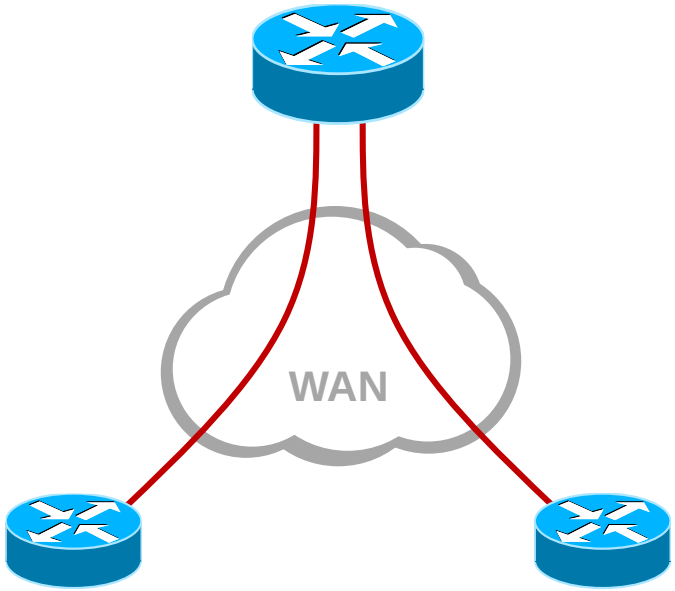
- 帧中继简介
- VC、LMI、DLCI的概念
- 帧中继映射
- Inverse-ARP的操作
- 帧中继配置

帧中继 简介

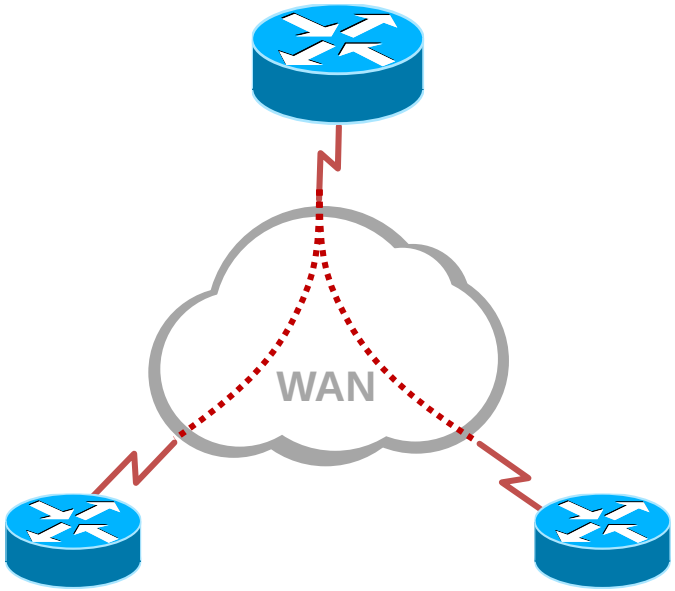


- 工作在数据链路层
- 使用虚电路进行连接
- 提供面向对象的服务

帧中继 简介



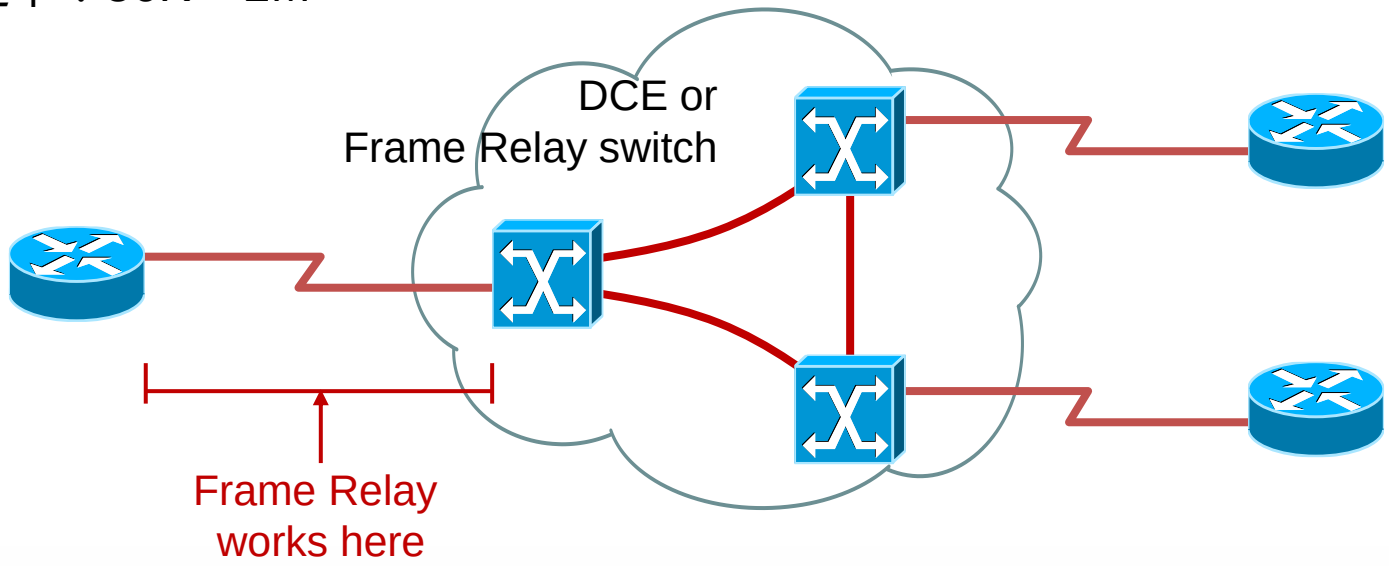
Without FR



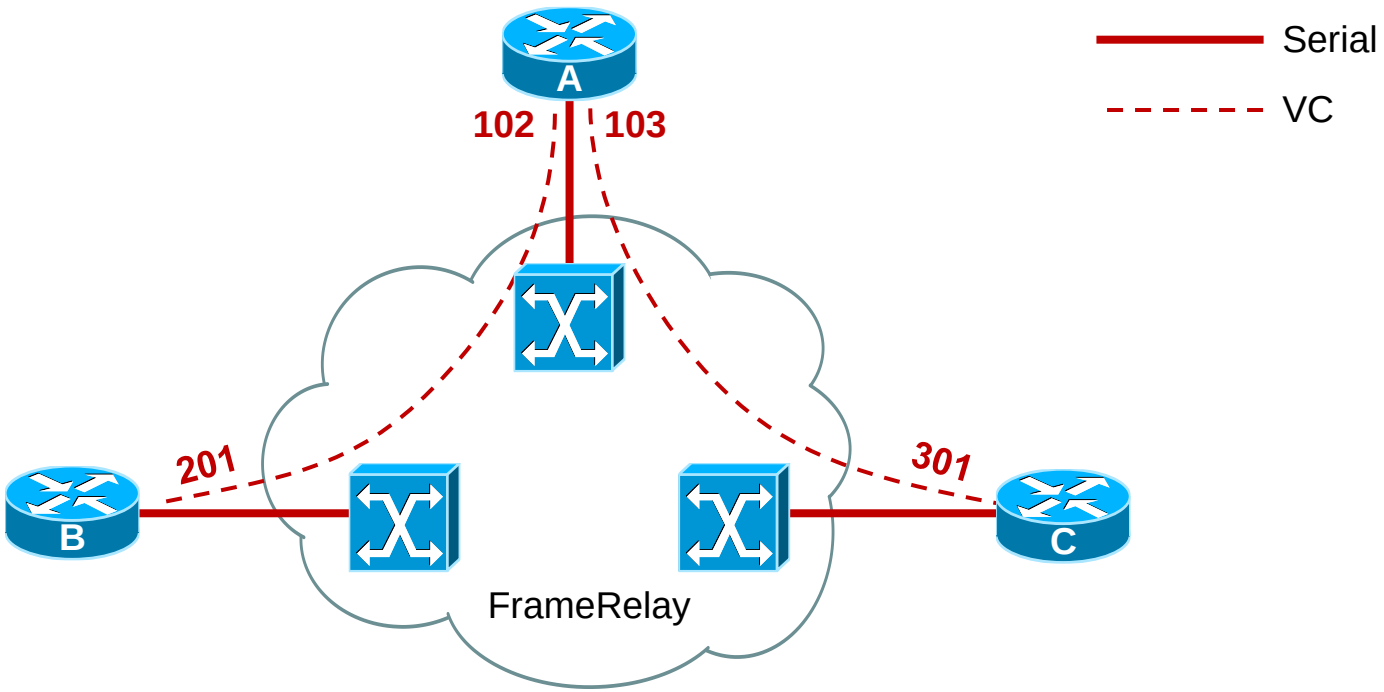
With FR

帧中继 简介

- 应用非常广泛的广域网数据链路层封装协议
- FR交换设备在用户路由器间建立虚电路，提供基于分组交换的二层通道。
- 面向连接的数据链路技术
- 速率：56K – 2M



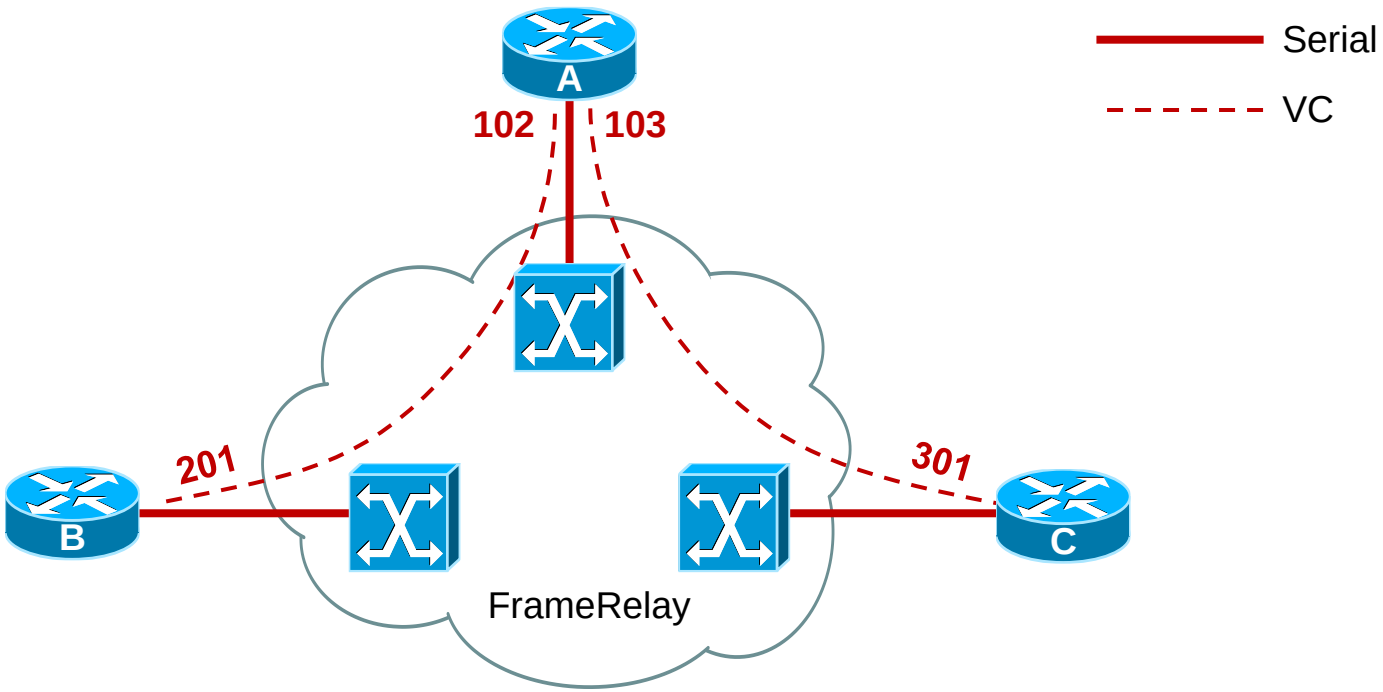
帧中继术语 VC



VC（Virtual Circuit）虚电路

- 通过帧中继网络实现的逻辑连接叫做虚电路 (VC)
- 利用虚电路，帧中继允许多个用户共享带宽，而无需使用多条专用物理线路，虚电路是以 DLCI 标识的

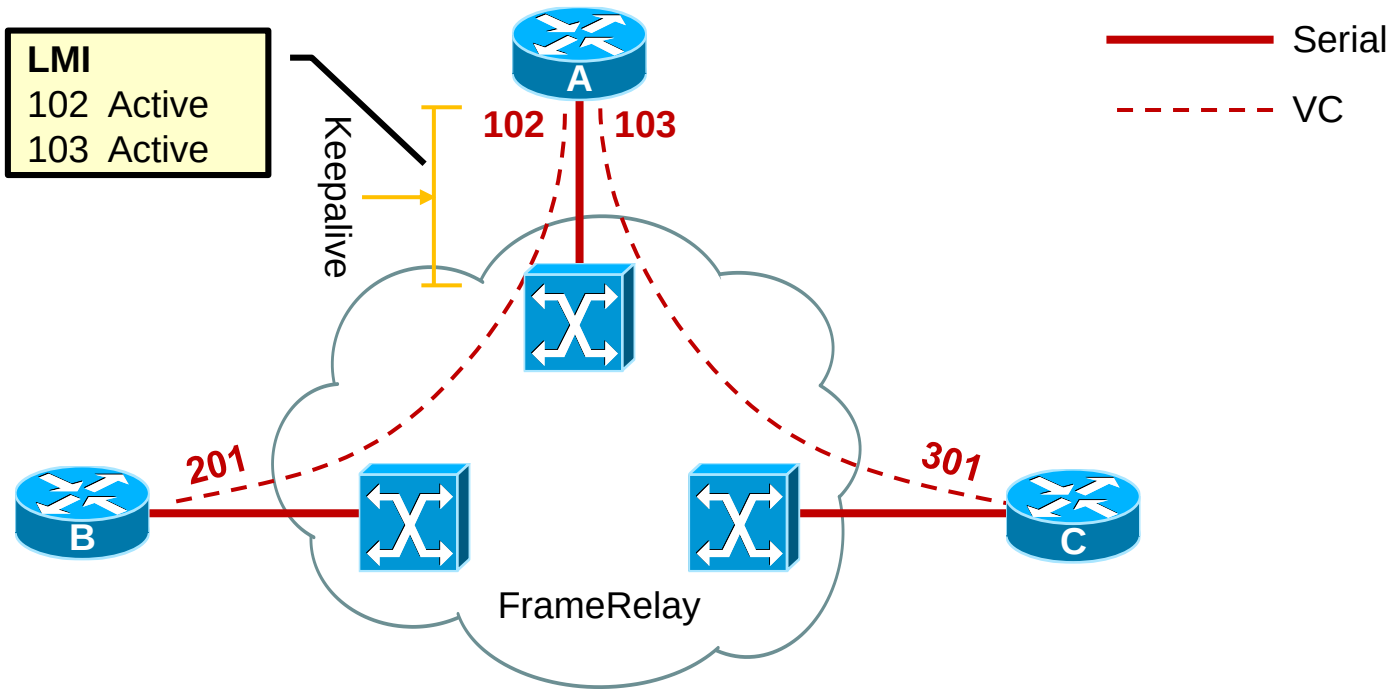
帧中继术语 DLCI



DLCI（Data Link Connection Identifier）数据链路连接标识

- 通常由帧中继服务提供商（例如电话公司）分配
- 帧中继 DLCI 仅具有本地意义
- DLCI 0 到 15 和 1008 到 1023 留作特殊用途。服务提供商分配的 DLCI 范围通常为 16 到 1007

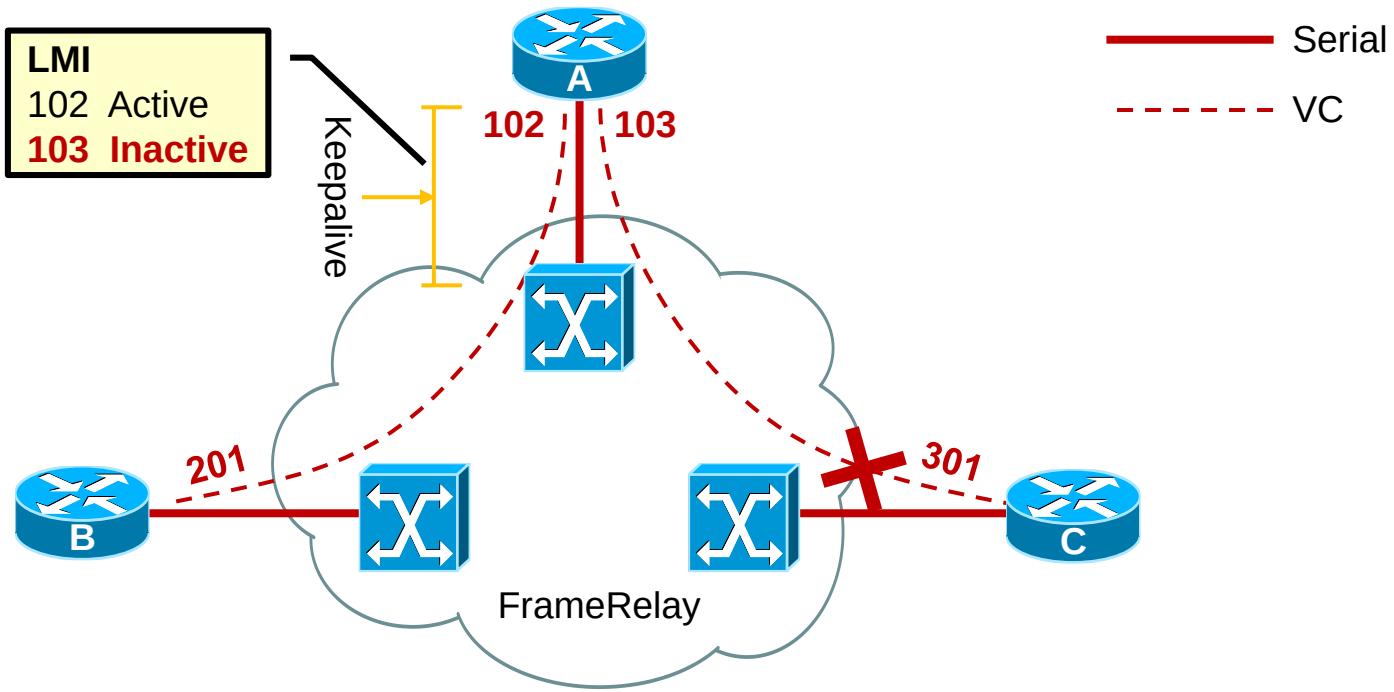
帧中继术语 LMI



LMI（Local Management Interface）本地管理接口

- 是一种信令标准，用于管理链路连接及keepalive的机制。
- 终端路由器 (DTE) 和帧中继交换机 (DCE) 之间的帧中继设备每 10 秒（或大概如此）轮询一次网络。Cisco 路由器支持以下三种 LMI： Cisco , Ansi , q933a
  在Cisco路由器上LMI类型默认是Cisco

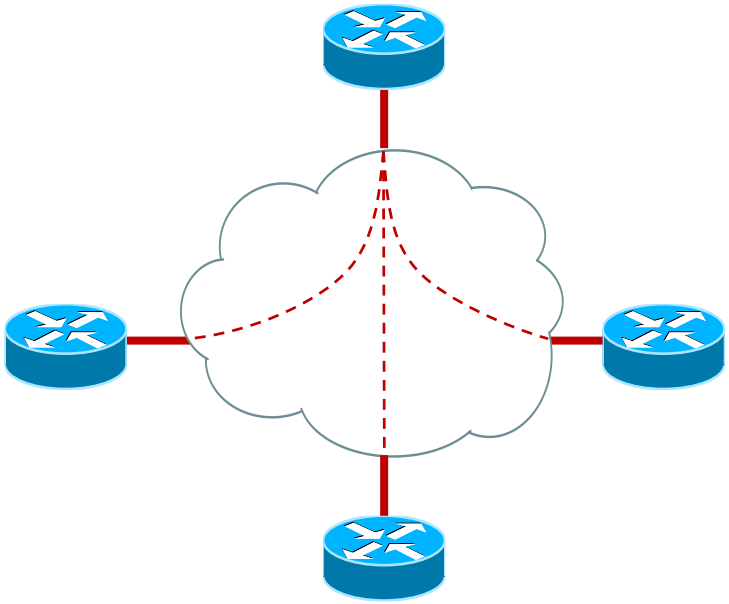
帧中继术语 LMI (cont.)



路由器从帧中继交换机的帧封装接口接受LMI信息，并将虚链路状态更新为下列3种状态之一：

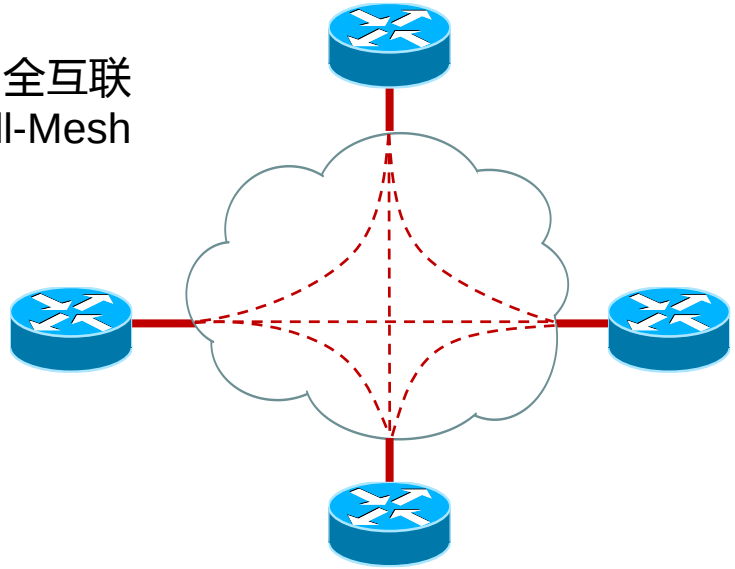
- Active state　正常状态
- Inactive state　远程路由器没有工作
- Deleted state　接口没有收到交换机的任何LMI信息，可能是映射问题或者线路问题

帧中继 拓扑

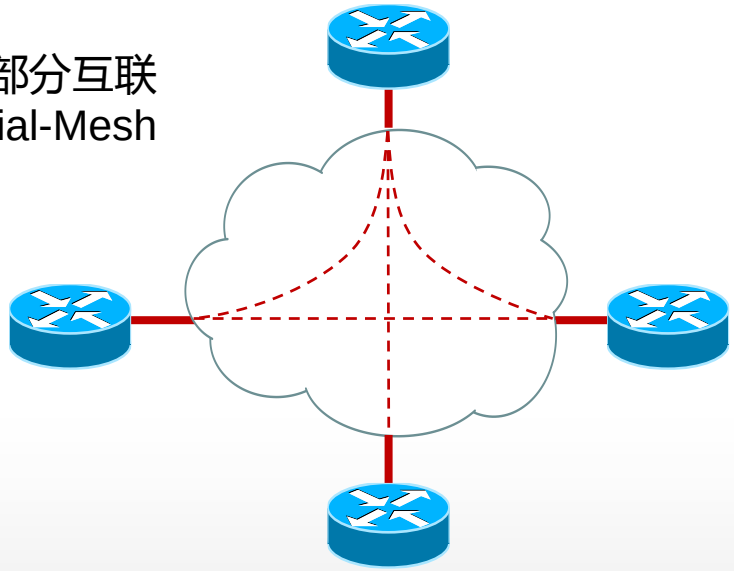


星形结构
Hub-and-spoke

全互联
Full-Mesh

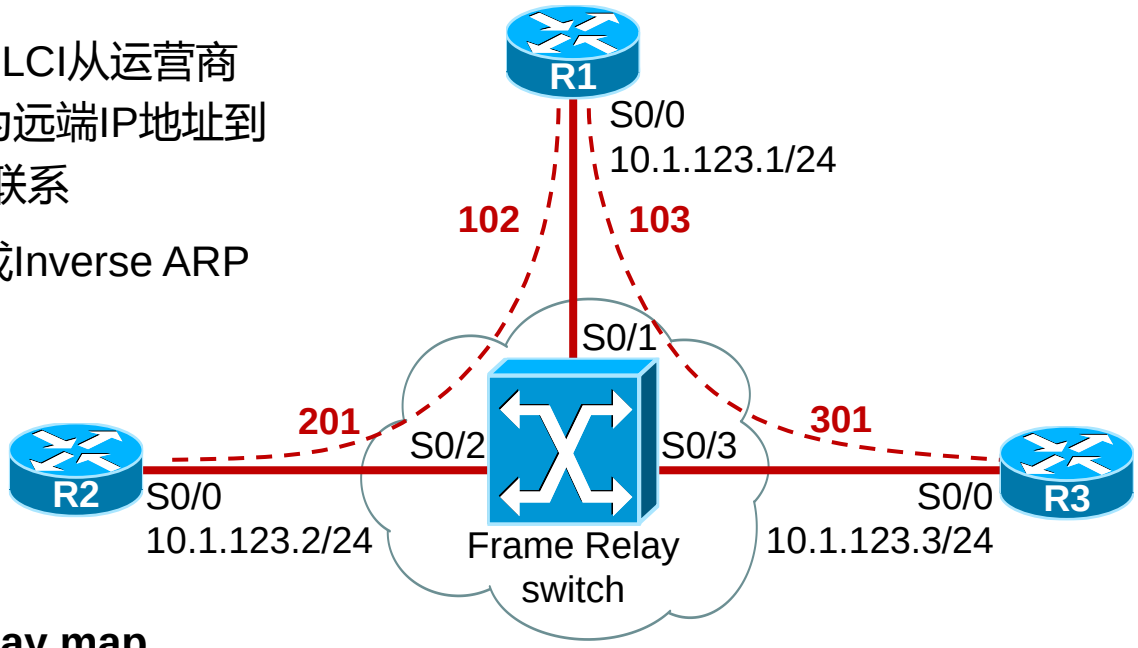


部分互联
Partial-Mesh



帧中继 地址映射

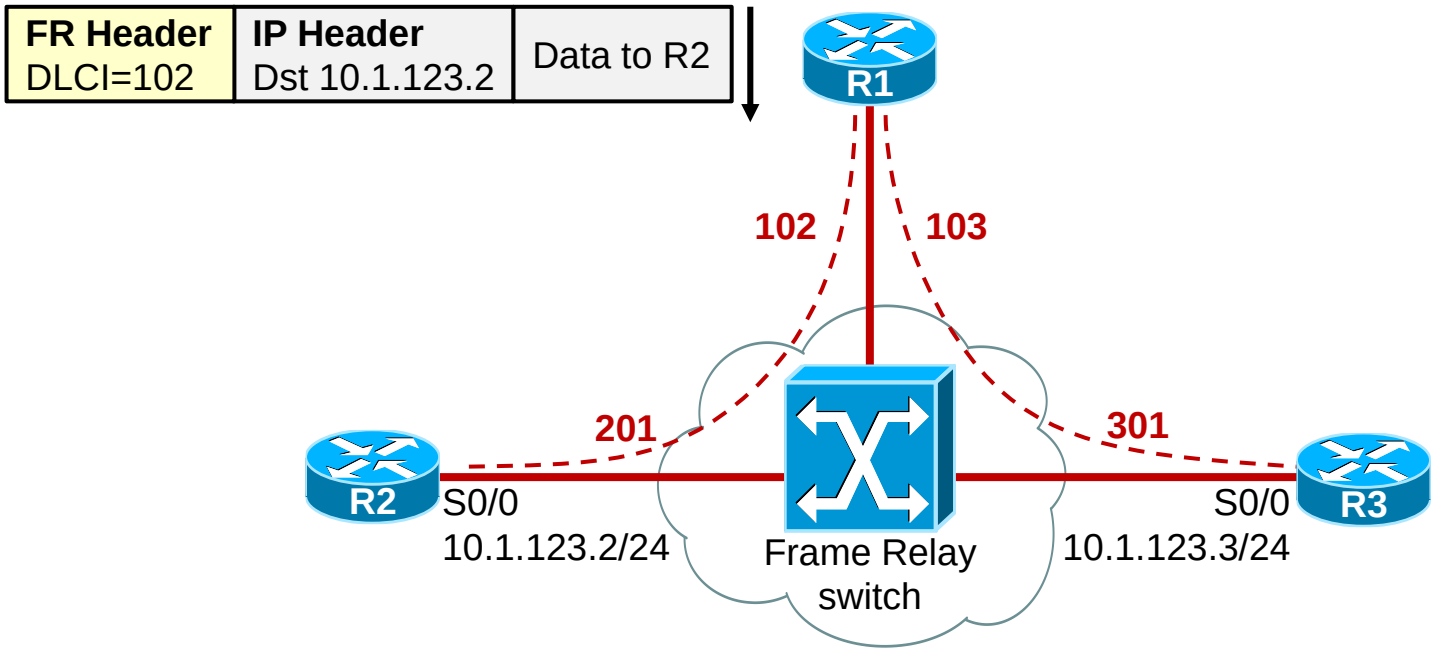
- 帧中继映射条目，DLCI从运营商处获取，映射关系为远端IP地址到**本地的DLCI**之间的联系
- 可以通过手工配置或Inverse ARP自动发现



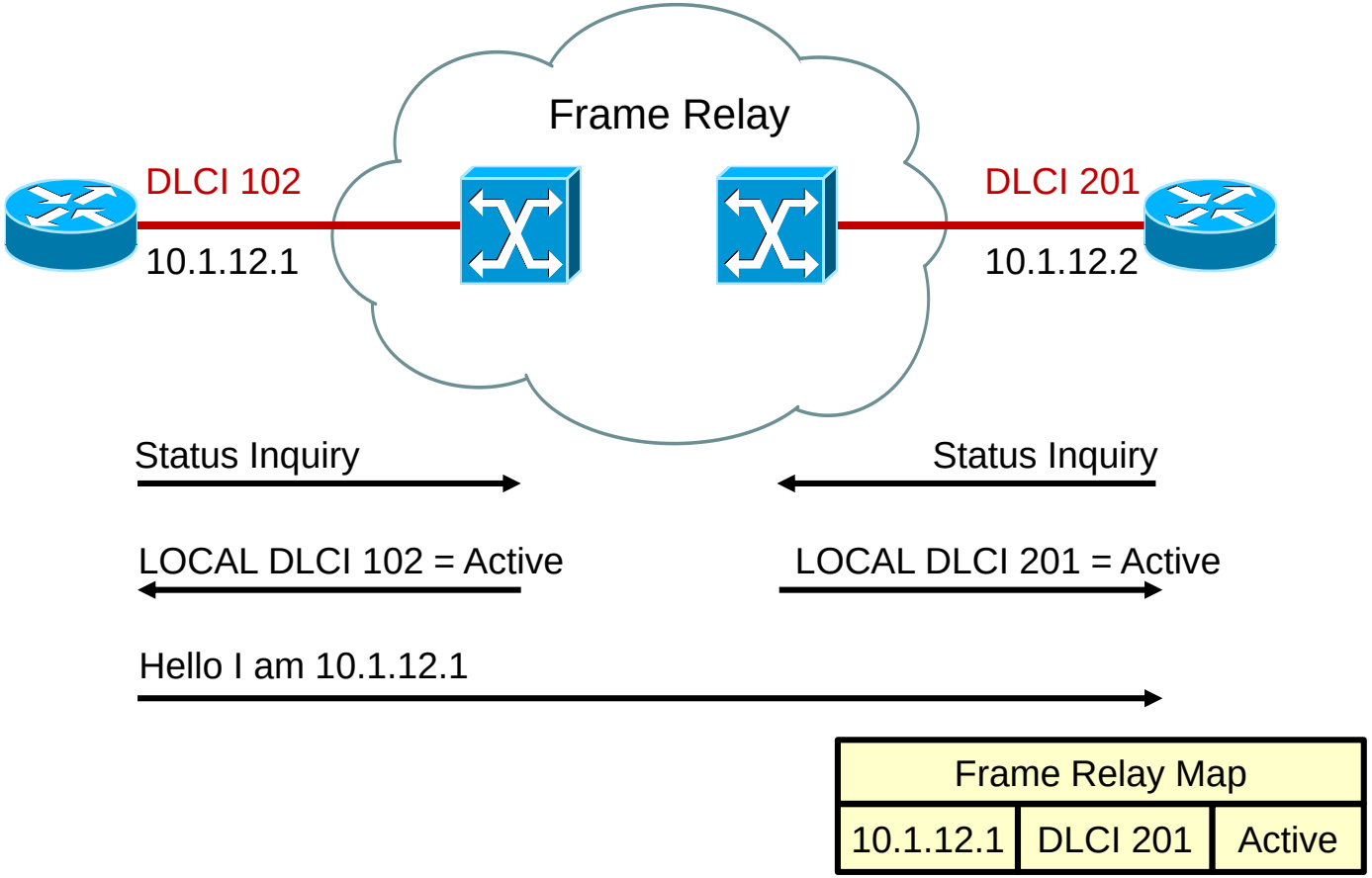
R1#show frame-relay map

```
Serial0/0 (up): ip 10.1.123.2 dlci 102(0x66,0x1860), dynamic,
              broadcast,, status defined, active
Serial0/0 (up): ip 10.1.123.3 dlci 103(0x67,0x1870), dynamic,
              broadcast,, status defined, active
```

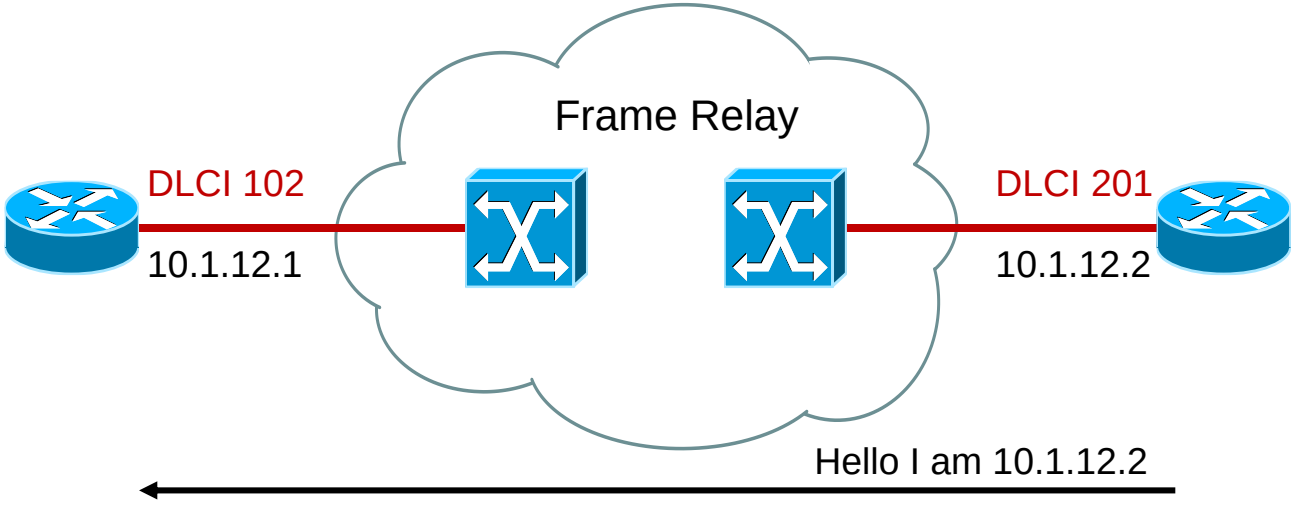
帧中继 地址映射



反向ARP和LMI的操作



反向ARP和LMI的操作 (cont.)

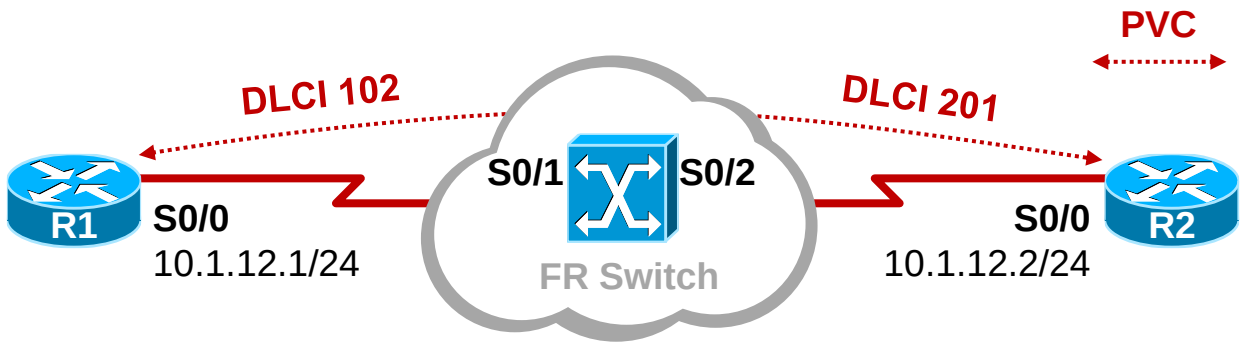


Frame Relay Map		
10.1.12.2	DLCI 102	Active

Keepalive

Keepalive

基础配置1 主接口封装帧中继（Inverse-ARP）

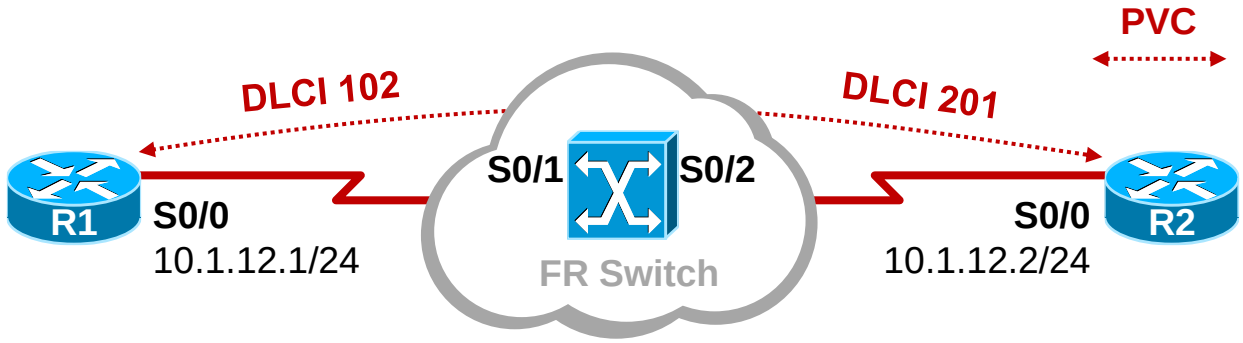


Frame Relay Switch（可用路由器模拟）的配置：

```
FRswitch(config)# frame-relay switching          !! 在模拟帧中继交换机的路由器上配置

FRswitch(config)# interface Serial0/1
FRswitch(config-if)# encapsulation frame-relay
FRswitch(config-if)# frame-relay intf-type dce
FRswitch(config-if)# clock rate 64000
FRswitch(config-if)# frame-relay route 102 interface Serial0/2 201
!! 配置PVC，上面这条命令可以形象的理解为S0/1接口的DLCI 102对应到S0/2接口的DLCI 201
FRswitch(config-if)# no shutdown
FRswitch(config-if)# exit
未完待续……
```

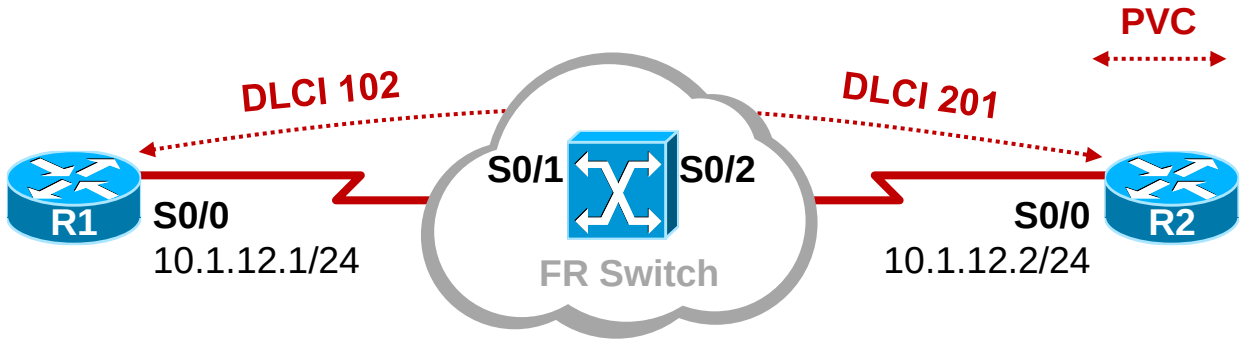
基础配置1 主接口封装帧中继（Inverse-ARP）



Frame Relay Switch（可用路由器模拟）的配置：

```
……接上一页
FRswitch(config)# interface Serial0/2
FRswitch(config-if)# encapsulation frame-relay
FRswitch(config-if)# clock rate 64000
FRswitch(config-if)# frame-relay intf-type dce
FRswitch(config-if)# frame-relay route 201 interface Serial0/1 102
FRswitch(config-if)# no shutdown
```

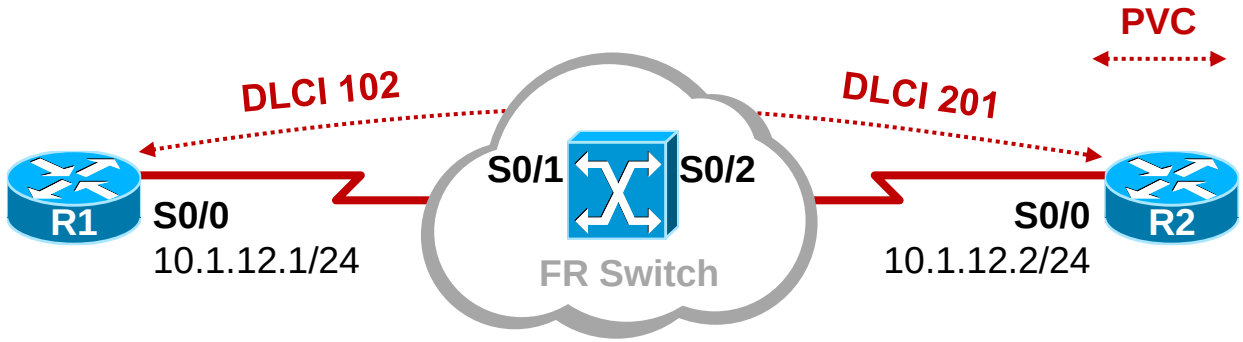
基础配置1 主接口封装帧中继（Inverse-ARP）



R1的配置如下：

```
R1(config)#interface serial 0/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#ip address 10.1.12.1 255.255.255.0
R1(config-if)#no shutdown
```

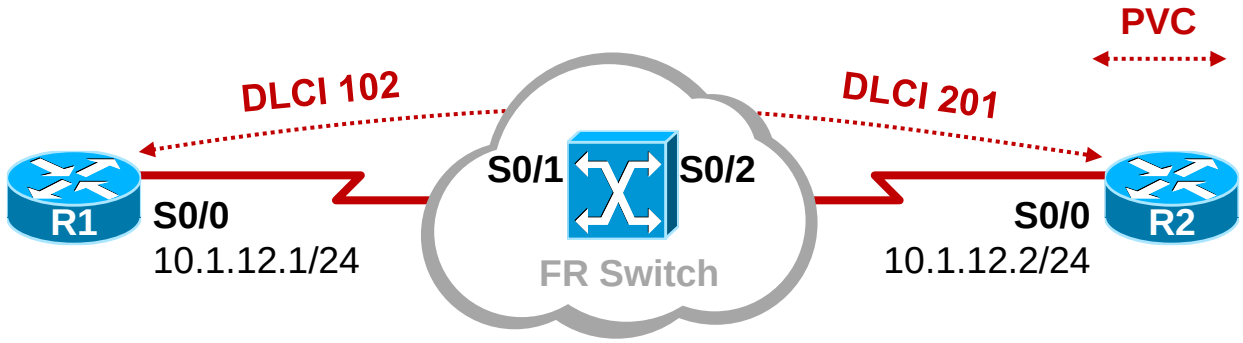
基础配置1 主接口封装帧中继（Inverse-ARP）



R2的配置如下：

```
R2(config)#interface serial 0/0
R2(config-if)#encapsulation frame-relay
R2(config-if)#ip address 10.1.12.2 255.255.255.0
R2(config-if)#no shutdown
```

基础配置1 主接口封装帧中继（Inverse-ARP）



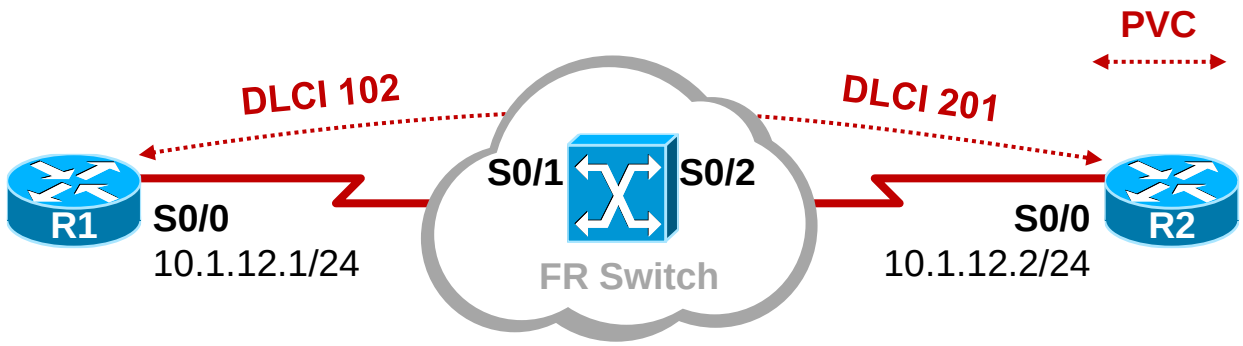
R1#show frame-relay map

```
Serial0/0 (up): ip 10.1.12.2 dlci 102(0x66,0x1860), dynamic,
              broadcast,
              CISCO, status defined, active
```

R2#show frame-relay map

```
Serial0/0 (up): ip 10.1.12.1 dlci 201(0xC9,0x3090), dynamic,
              broadcast,
              CISCO, status defined, active
```

基础配置2 主接口封装帧中继（静态映射）



R1的配置如下：

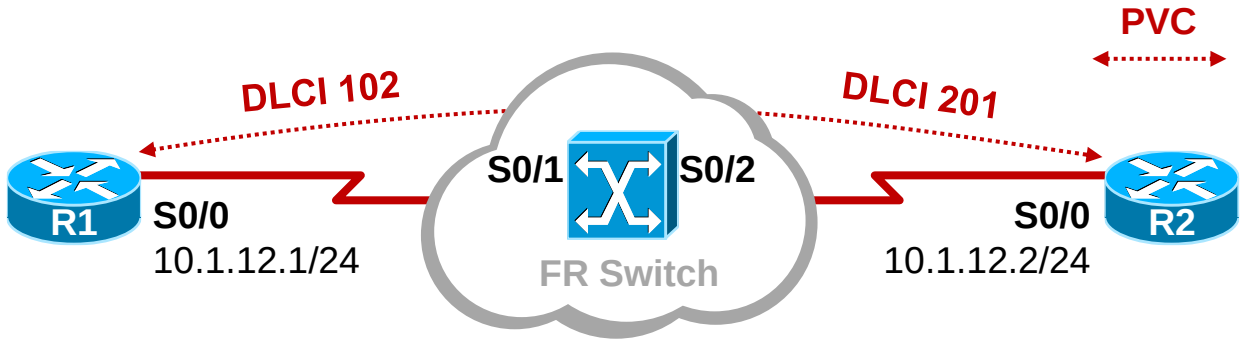
```
R1(config)#interface serial 0/0
R1(config-if)#no frame-relay inverse-arp                    !!关闭inverse-arp
R1(config-if)#frame-relay map ip 10.1.12.2 102 broadcast
R1(config-if)#ip address 10.1.12.1 255.255.255.0
```

Broadcast关键字为可选，加上此关键字，则该条PVC将具有“广播”的支持能力，所谓的帧中继环境下的广播，指的是向所有的PVC都发送一份数据的拷贝，实现类似广播的操作。

R2的配置如下：

```
R2(config)#interface serial 0/0
R2(config-if)#no frame-relay inverse-arp
R2(config-if)#frame-relay map ip 10.1.12.1 201 broadcast
R2(config-if)#ip address 10.1.12.2 255.255.255.0
```

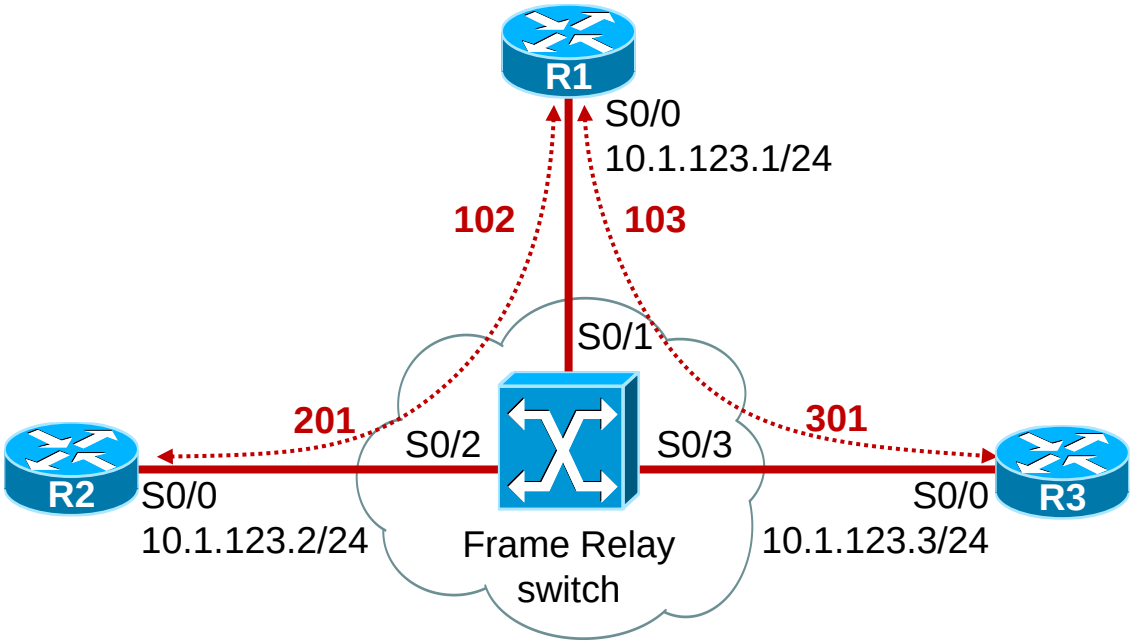
基础配置2 主接口封装帧中继（静态映射）



R1#show frame-relay map

```
Serial0/0 (up): ip 10.1.12.2 dlci 102(0x66,0x1860), static,
                broadcast,
                CISCO, status defined, active
```

基础配置3 主接口封装帧中继（Hub&Spoke）



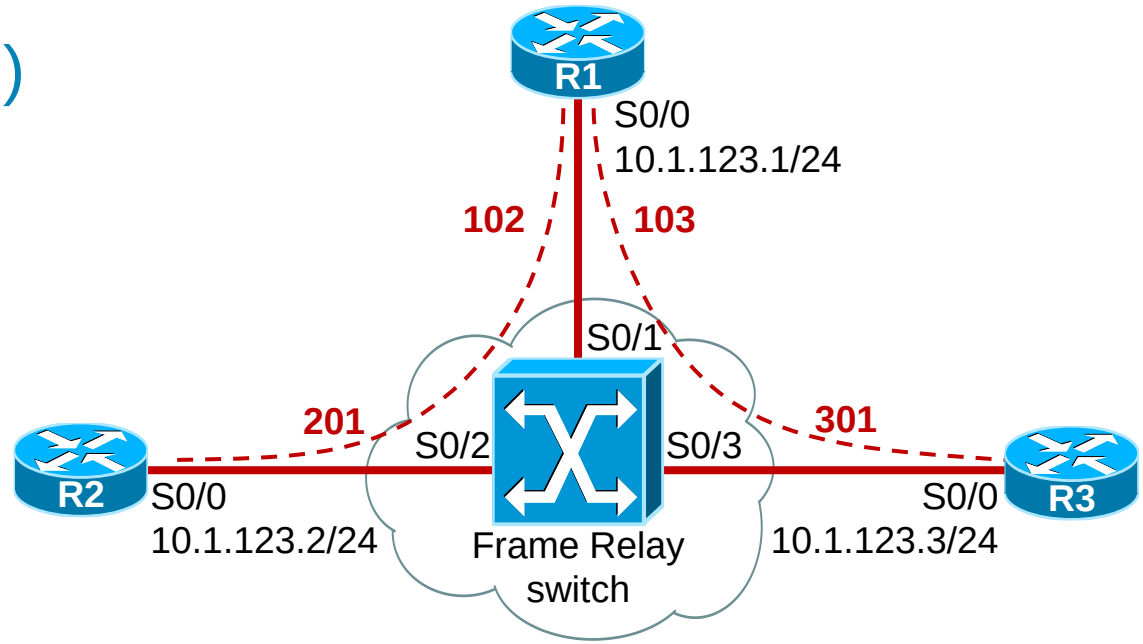
基础配置3 主接口封装帧中继（Hub&Spoke）

Frame Relay Switch（用路由器模拟）的配置：

```
frame-relay switching
interface Serial0/1
 no ip address
 encapsulation frame-relay
 clock rate 64000
 frame-relay intf-type dce
 frame-relay route 102 interface Serial0/2 201
 frame-relay route 103 interface Serial0/3 301
```

```
interface Serial0/2
 no ip address
 encapsulation frame-relay
 clock rate 64000
 frame-relay intf-type dce
 frame-relay route 201 interface Serial0/1 102
!
interface Serial0/3
 no ip address
 encapsulation frame-relay
 clock rate 64000
 frame-relay intf-type dce
 frame-relay route 301 interface Serial0/1 103
```

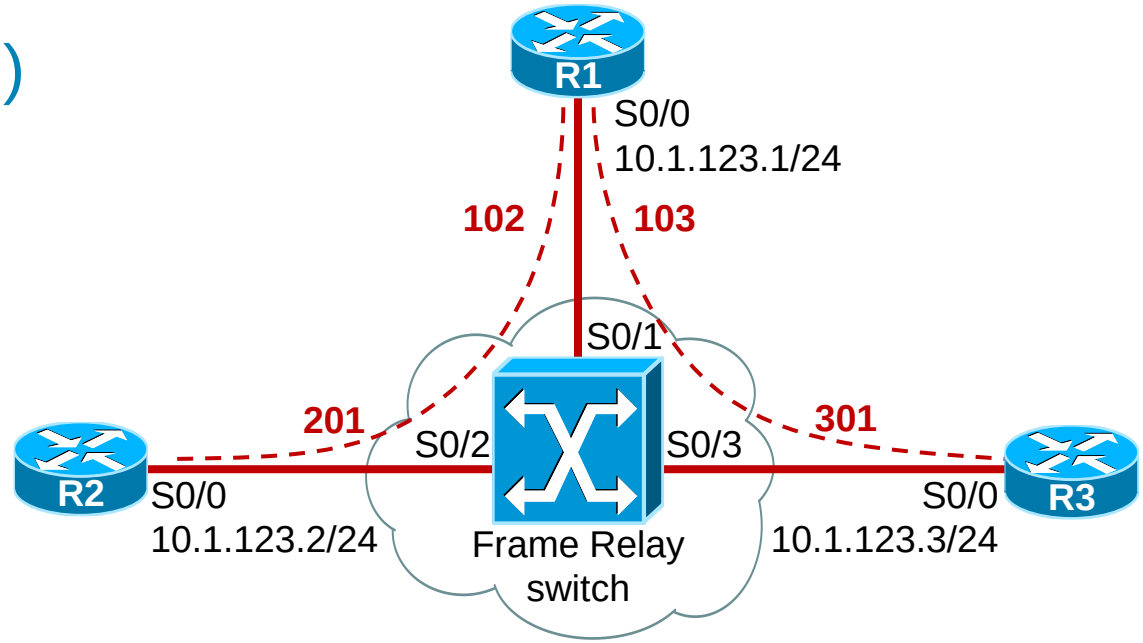
帧中继的配置 (cont.)



R1的配置：

```
interface Serial0/0
 ip address 10.1.123.1 255.255.255.0
 encapsulation frame-relay
 no frame-relay inverse-arp            // 关闭inverse-arp
 frame-relay map ip 10.1.123.2 102 broadcast    //手工配置帧中继映射
 frame-relay map ip 10.1.123.3 103 broadcast
```

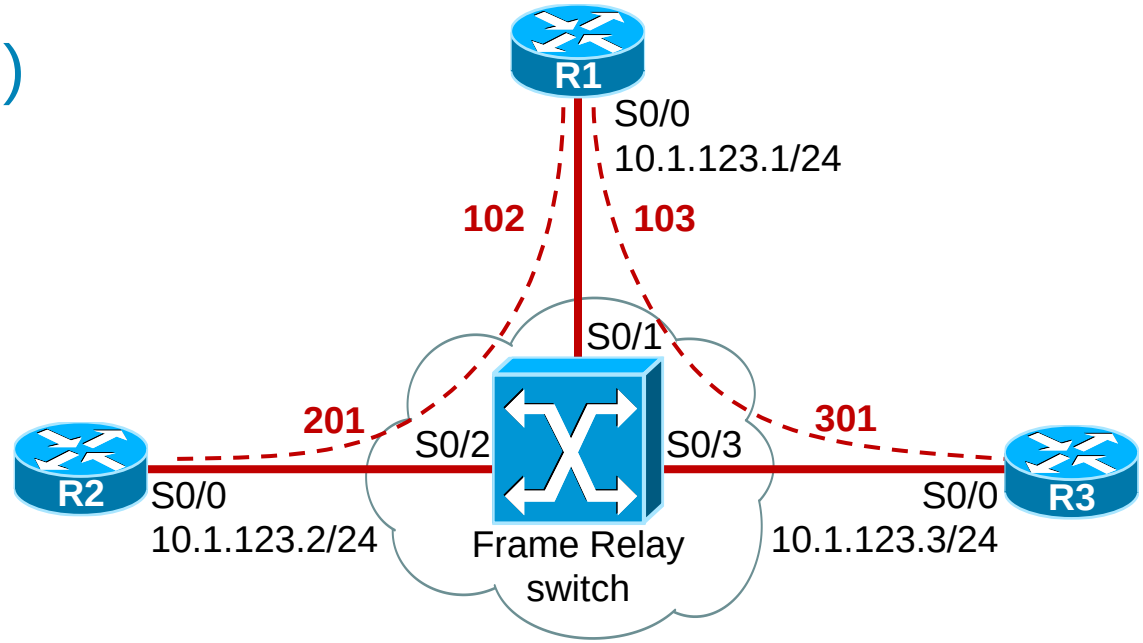
帧中继的配置 (cont.)



R2的配置：

```
interface Serial0/0
 ip address 10.1.123.2 255.255.255.0
 encapsulation frame-relay
 no frame-relay inverse-arp
 frame-relay map ip 10.1.123.1 201 broadcast
```

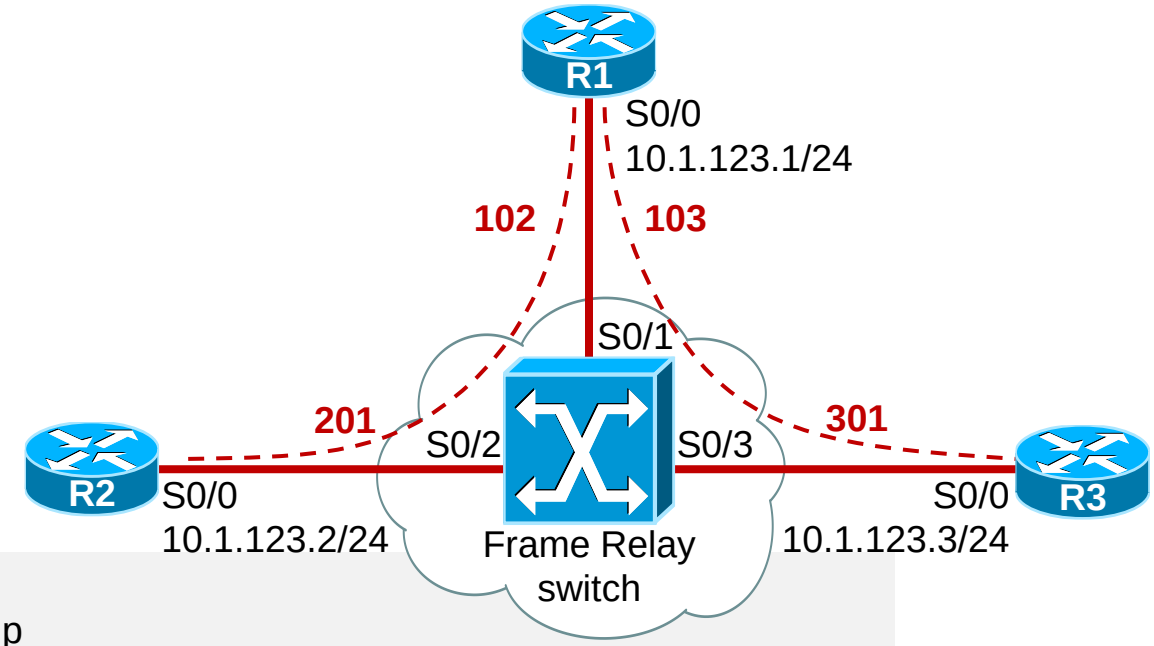
帧中继的配置 (cont.)



R3的配置：

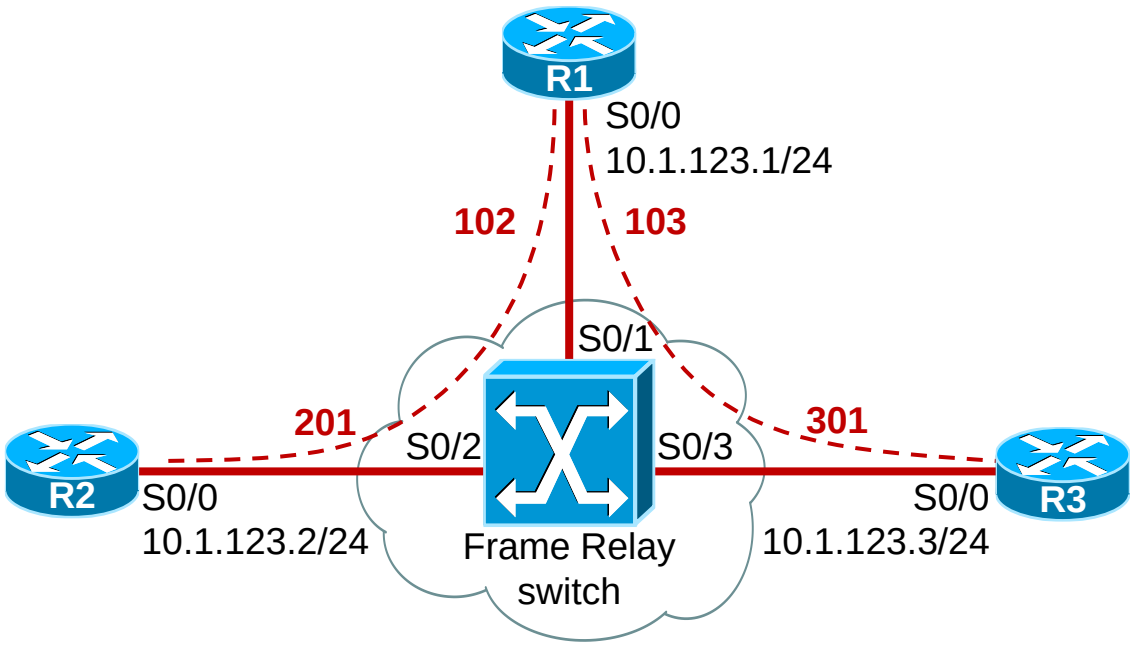
```
interface Serial0/0
 ip address 10.1.123.3 255.255.255.0
 encapsulation frame-relay
 no frame-relay inverse-arp
 frame-relay map ip 10.1.123.1 301 broadcast
```

帧中继的配置 验证



R1#show interfaces serial 0/0
Serial0/0 is up, line protocol is up
  Hardware is M4T
  Internet address is 10.1.123.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  LMI enq sent 182, LMI stat recvd 183, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 0/0, interface broadcasts 0

帧中继的配置 验证

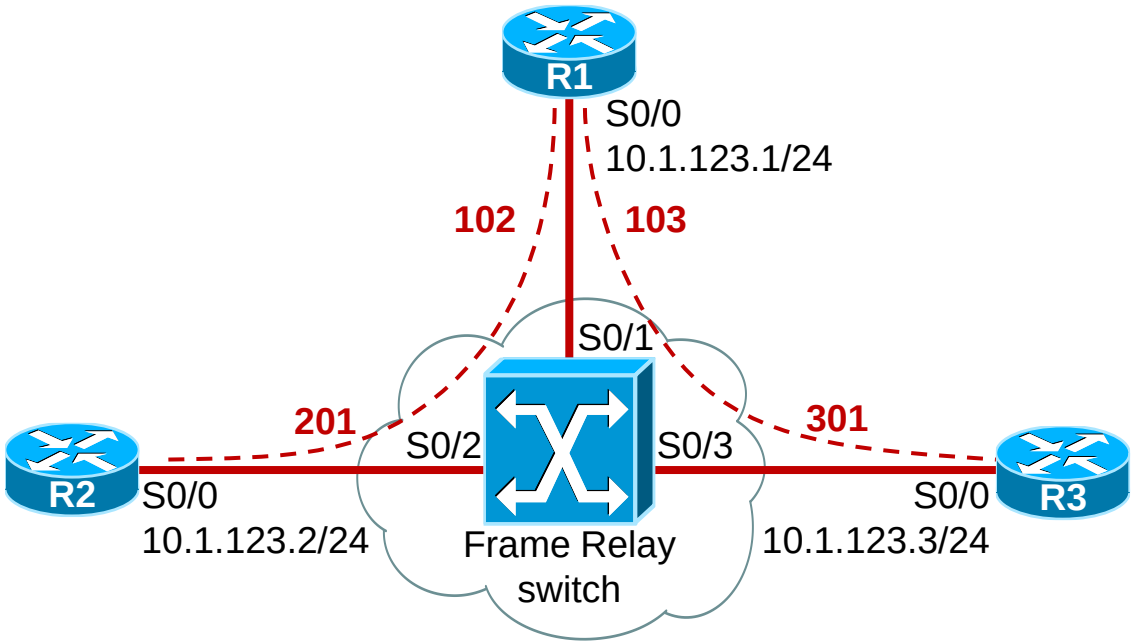


R1#show frame-relay map

Serial0/0 (up): ip 10.1.123.2 dlci 102(0x66,0x1860), static,
broadcast,
CISCO, status defined, active

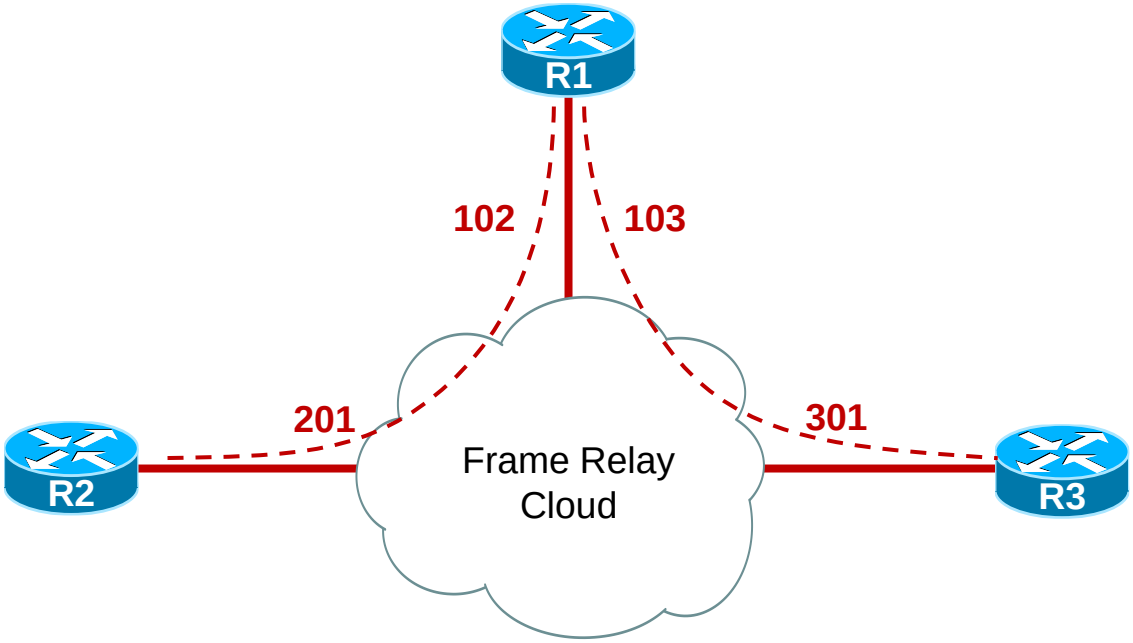
Serial0/0 (up): ip 10.1.123.3 dlci 103(0x67,0x1870), static,
broadcast,
CISCO, status defined, active

帧中继的配置 问题



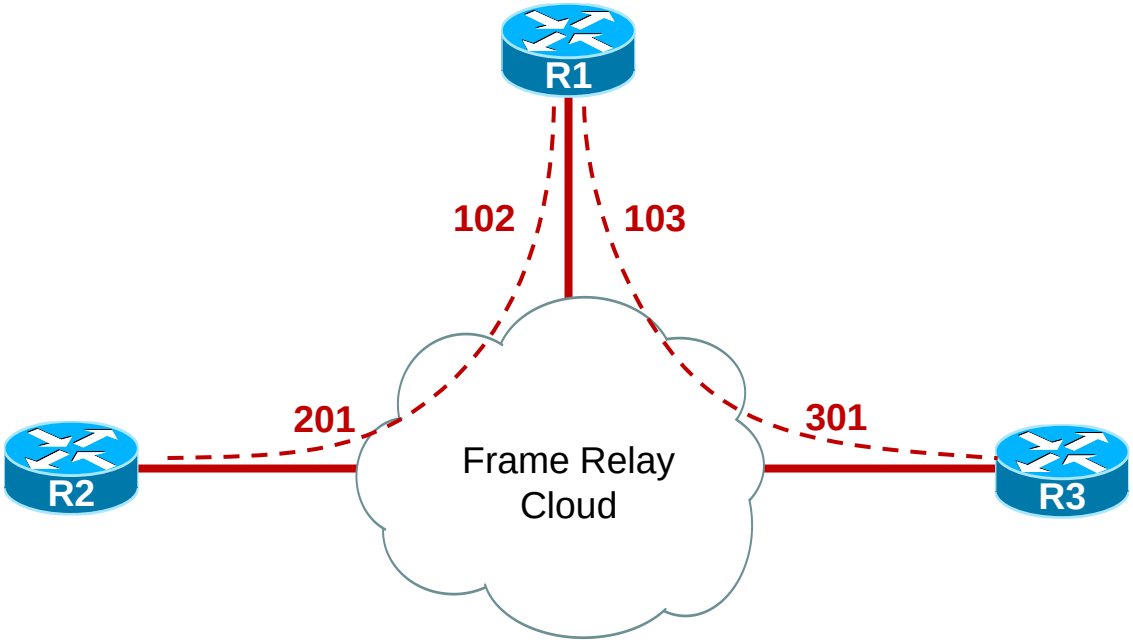
- 完成上述配置后，R1与R2之间，R1与R3之间的通信就没有问题了
- R2与R3之间如何通信呢？
- R1、R2、R3都无法ping通自己本地的接口，为何？

帧中继环境中的动态路由协议 问题1



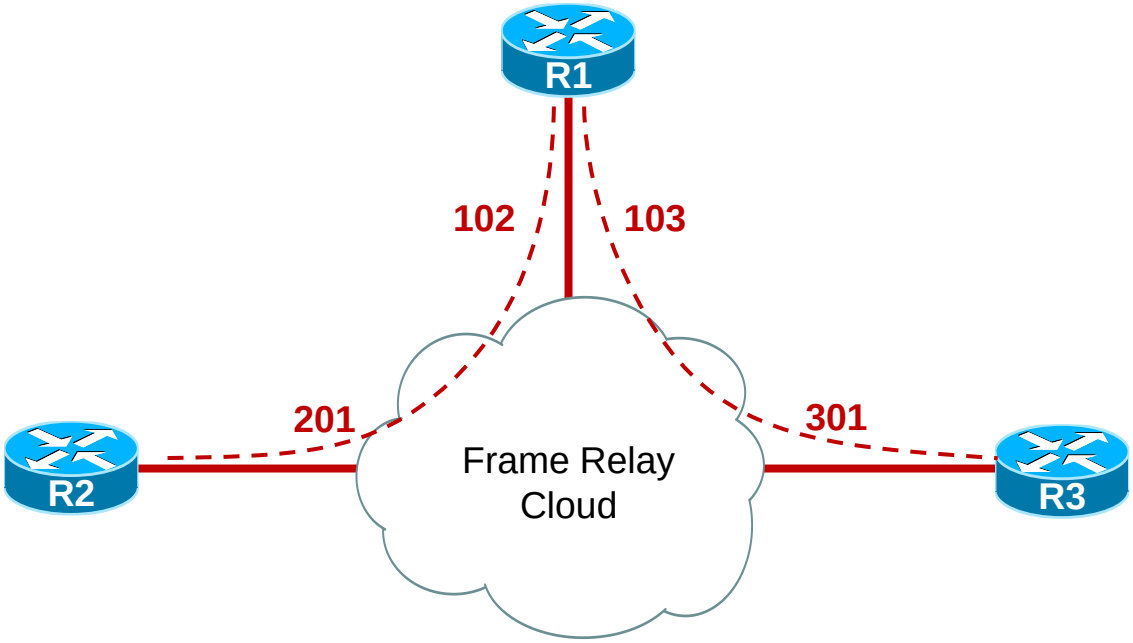
- 问题1：帧中继是典型的NBMA网络，也就是非广播多路访问网络，并不支持广播，然而包括RIP、EIGRP、OSPF等在内的路由协议都需要组播或广播的支持，那么在帧中继环境下运行上述动态路由协议，会否有问题？

帧中继环境中的动态路由协议 问题1



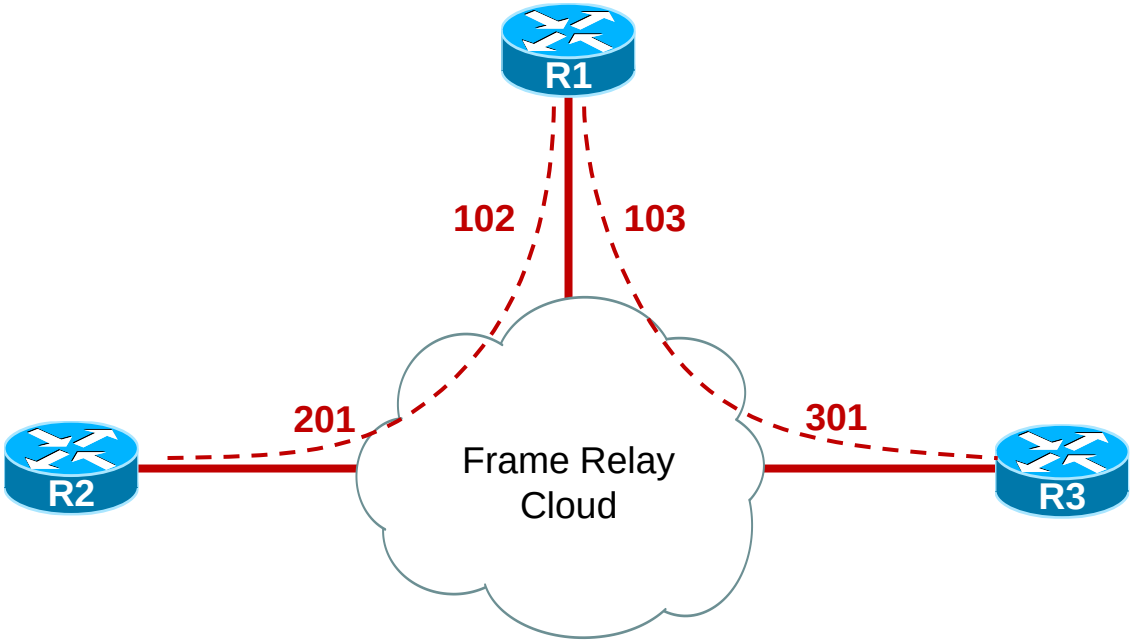
- 帧中继虽不支持广播，但是可以“模拟”广播的操作，做法即是通过向所有PVC发送一份数据的拷贝。
- 在建立PVC的时候，通过invers-arp自动建立的映射，默认就开启上述特性；如果是手工配置映射，则必须加上broadcast关键字

帧中继环境中的动态路由协议 问题1



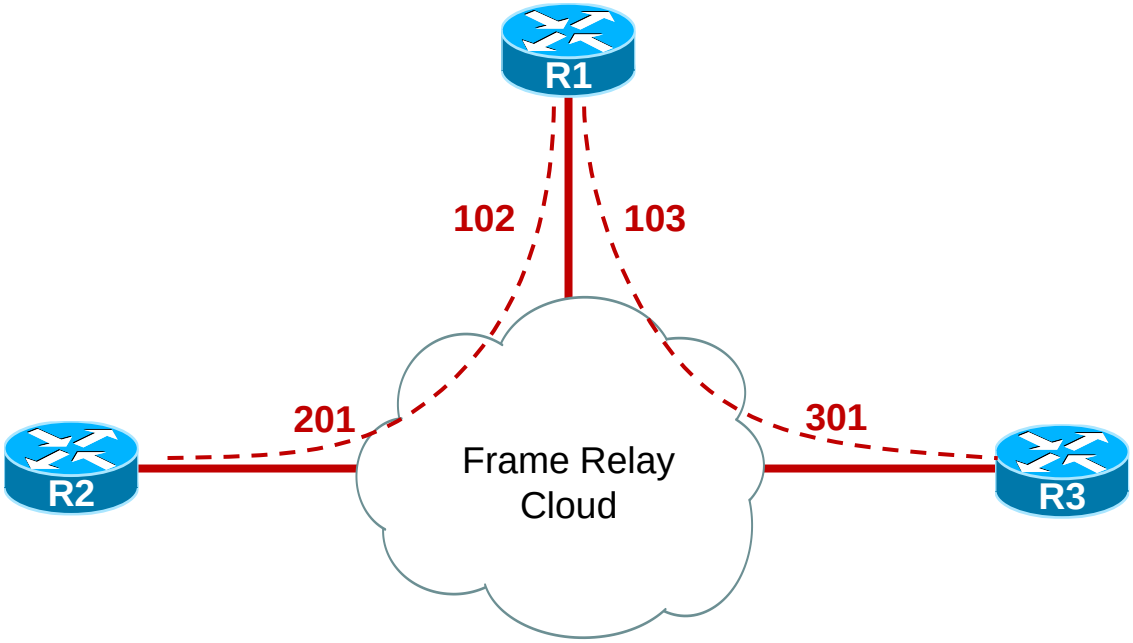
- 如果帧中继链路无法通过上述方法实现广播的支持能力，那么可以借助动态路由协议自身的特性来实现邻居建立或路由信息的交互，例如单播更新等。
- 此模块内容请见相应的专题课件

帧中继环境中的动态路由协议 问题2



- 问题2：在hub&spoke拓扑环境中（如上图），距离矢量路由协议的运作会遇到一个问题，R1使用一个接口承载两条PVC，当R1R2R3运行距离矢量路由协议时，由于存在水平分割机制，R2，R3将无法学习到对方的路由。

帧中继环境中的动态路由协议 问题2



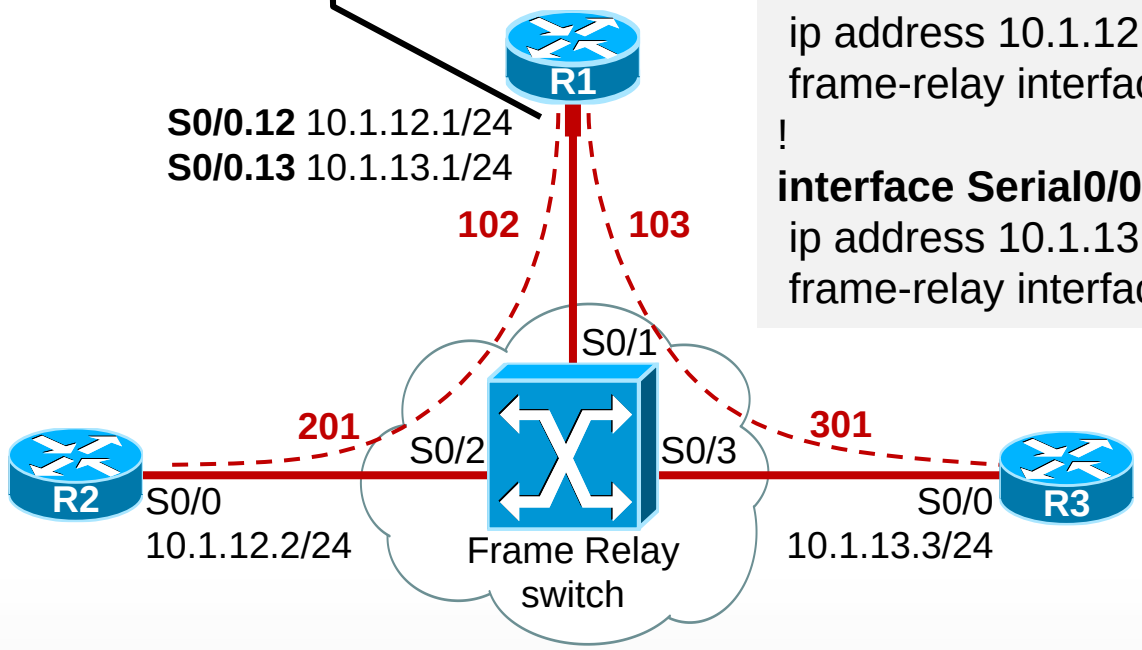
- 解决办法1：可在R1的接口上关闭水平分割
- 解决办法2：使用P2P子接口建立PVC

配置帧中继子接口

- **点到点**
  - 子端口看作是点到点的专线;
  - 每一个点到点连接的子接口要求由自己的子网;
  - 适用于星型拓扑结构;
- **点到多点**
  - 点子接口应用在 NBMA 网络，因此它们无法解决水平分割所带来的问题;
  - 由于使用的是单独的子网可以保存地址空间;
  - 适用于 Partial-Mesh 和 Full-Mesh 拓扑结构中;

配置帧中继P2P子接口

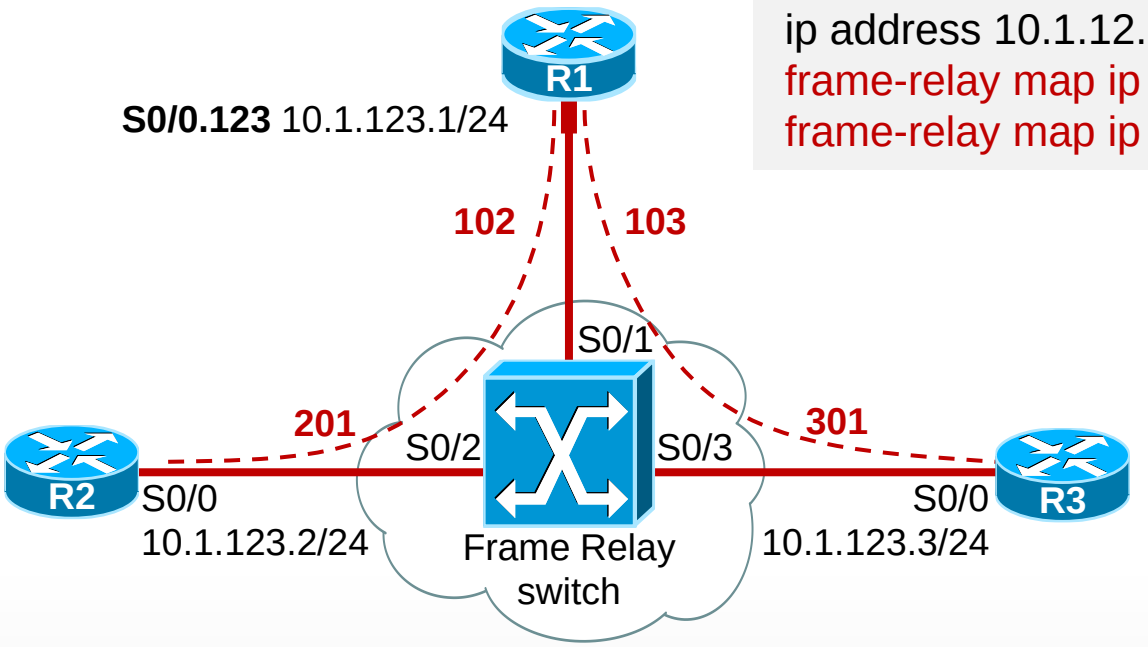
S0/0被划分成两个子接口后，分别与R2、R3建立PVC并运行动态路由协议，那么前面提到的水平分割问题就可以迎刃而解。



R1的配置如下：

```
interface Serial0/0
 no ip address
 encapsulation frame-relay
!
interface Serial0/0.12 point-to-point
 ip address 10.1.12.1 255.255.255.0
 frame-relay interface-dlci 102
!
interface Serial0/0.13 point-to-point
 ip address 10.1.13.1 255.255.255.0
 frame-relay interface-dlci 103
```

配置帧中继P2MP子接口



R1的配置如下：

```
interface Serial0/0
 no ip address
 encapsulation frame-relay
!
interface Serial0/0.123 multipoint
 ip address 10.1.12.1 255.255.255.0
 frame-relay map ip 10.1.123.2 102 broadcast
 frame-relay map ip 10.1.123.3 103 broadcast
```

其他验证及查看命令

router# show frame-relay map

- 查看帧中继的映射条目

router# show frame-relay lmi [*type number*]

- 显示LMI的统计信息

router# show frame-relay pvc [type number [dlci]]

- 显示PVC的统计信息

router# debug frame-relay lmi

router# clear frame-relay-inarp

红茶三杯
Vinsoney

学习 沉淀 成长 分享

关注@红茶三杯：weibo.com/vinsoney

Thank You