

报文 Message / Packet 泛指在网络上传输的信息单元，有时“报文”偏向应用层的信息。

数据报 Datagram 无连接传输的独立数据单元，例如 UDP 传输的单个单元就是数据报。

帧 Frame 数据链路层的信息单元，例如以太网帧。

分组 Packet 网络层的信息单元，例如 IP 数据包。

信元 Cell ATM 网络中固定长度的传输单元。

信号 Signal 物理层的电磁或光信号，用于实际传输。

⚠️ 注意：

有些术语在不同层可能会混用，比如 “packet” 可以指网络层的包，也可以泛指报文。数据报（datagram）强调 无连接、独立，而 packet 更中性。

# OSI模型

应用层application

表示层presentation

会话层session

传输层transport – 端口号

网络层network – IP地址（“电话号”）

数据链路层data link – MAC地址（“身份证”）

物理层physical – 无线，光纤

## 物理层

– 模数转换，光数转换

早期 – 没有交换机（switch，数据链路层设备），用集线器（hub，物理层设备）

缺点：半双工；

泛洪机制，每个接口都转发，数据不安全；

数据冲突，两人同时发数据会变成冲突碎片

– 载波侦听多路访问CSMA/CD（Carrier Sense发之前侦听 Multiple Access多点接入 with Collision Detection碰撞检测）

## 数据链路层

### MAC地址

Medium Access Control，烧录在网卡的ROM（储存）里，48bit（24bit厂商+24bit） - 6个十六进制数位

ipconfig -all

### 交换机

#### ARP协议

Address Resolution Protocol，通过IP地址解析MAC地址，地址表保存时间约300秒。发送过程：

源发送ARP请求：源MAC地址+目的MAC地址设为12个F（发送给所有人）+自己IP地址+询问目的MAC地址

交换机记录地址表：记录源MAC地址+发送端口

泛洪发送（全F）

ARP应答：源MAC地址+目的MAC地址+自己IP地址+回复自己MAC地址

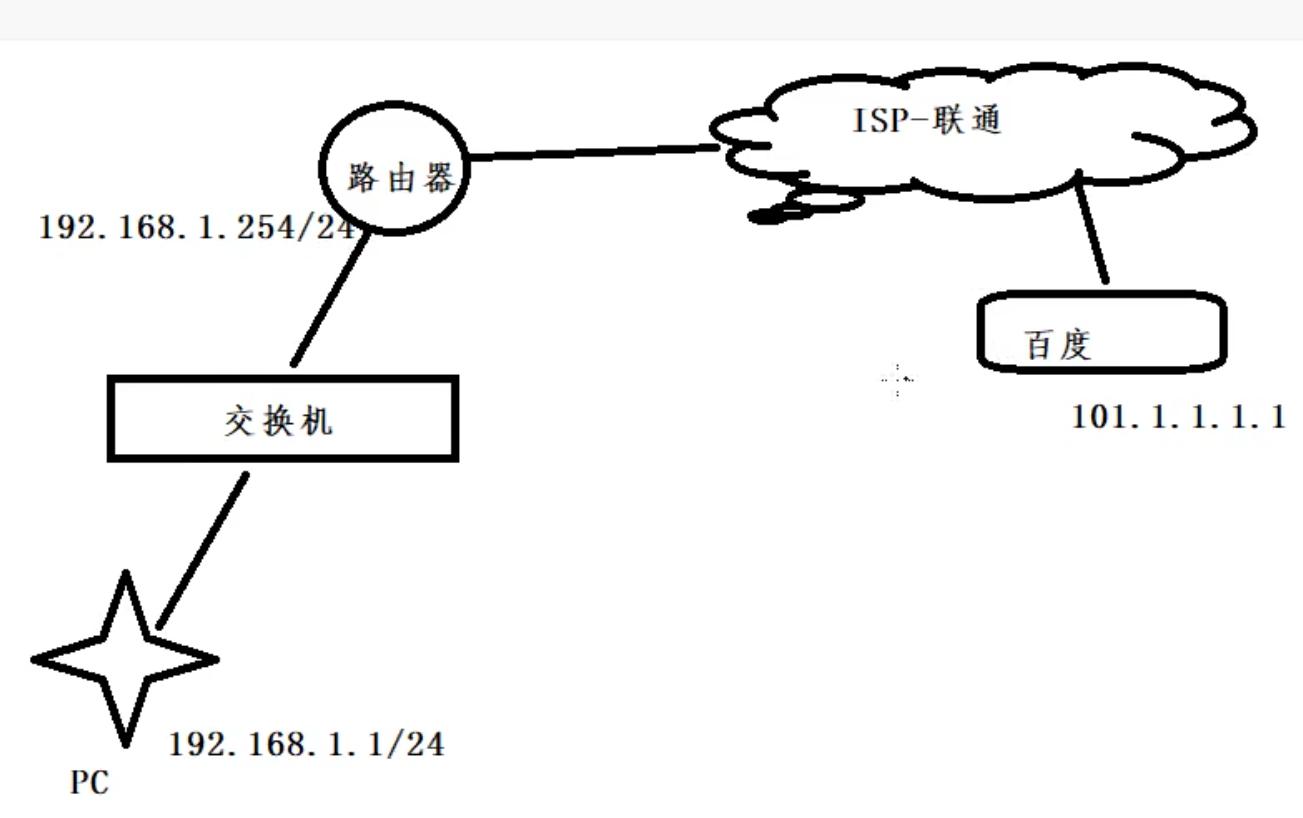
交换机记录地址表：记录目的MAC地址+发送端口

交换机转发ARP应答：源和目的都知道了彼此的MAC地址，交换机记录了MAC地址表

Eg. PC访问不同网段的目的地，把数据包转发给网关，网关再进行转发。需要知道网关的MAC地址，发送ARP请求，网关回复ARP应答。

网关（gateway） – 跨网段转发数据。

（PC的网关是路由器，路由器的网关是联通的路由器）



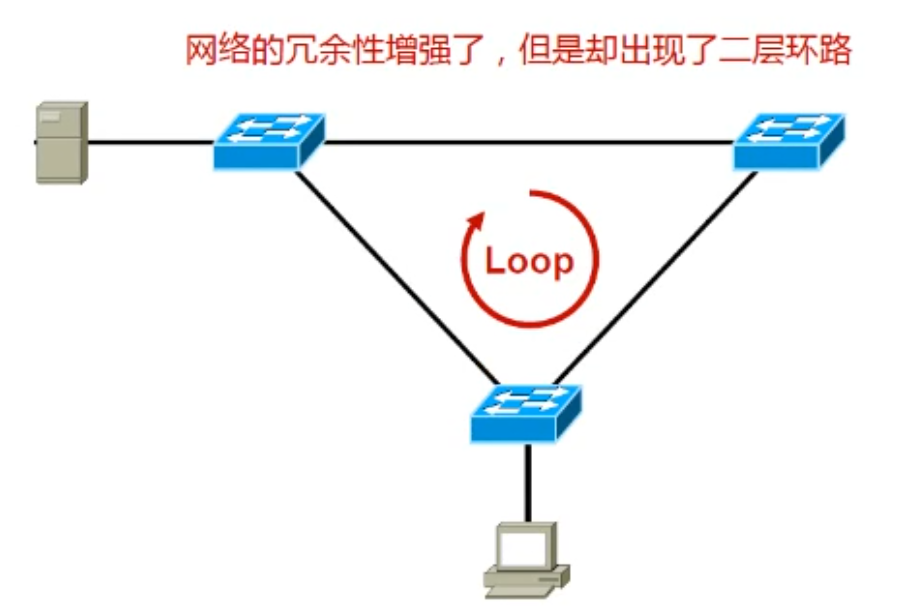
#### STP协议

Spanning Tree Protocol，生成树协议

避免二层环路

二层环路

为了避免单点故障，可以引入一台新的交换机，就会造成二层环路



STP作用

消除环路，临时堵塞一个端口

链路备份，当活动链路发生故障时，激活备用链路，恢复网络联通性

协议

选举一个根桥Root Bridge，bridge ID（桥优先级（默认都为32768）越小越优先 – 桥mac地址越小越优先）

在非根桥交换机上选举一个根端口RP（Root Port，cost值越小越优先 – 上位发送者的 – 端口Port ID），接收根桥发送过来的BPDU，Bridge Protocol Data Unit网桥协议单元

## 网络层

### IP地址

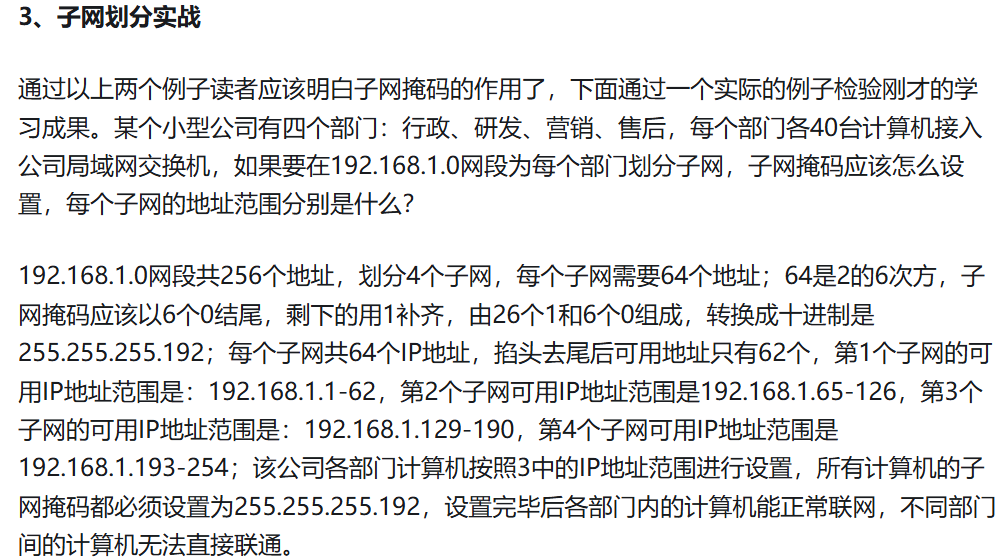
32bit - 点分十进制，每8位转换成十进制

192.168.1. 1

网络位 主机位

网段：192.168.1.0/**24** 前24个bit是网络位，后8个bit代表256个IP地址

子网掩码子网掩码（Subnet Mask）– 分割网络位



特殊IP地址：第一个IP地址表示网段 eg. 192.168.1.0

最后一个IP地址表示广播 eg. 192.168.1.255

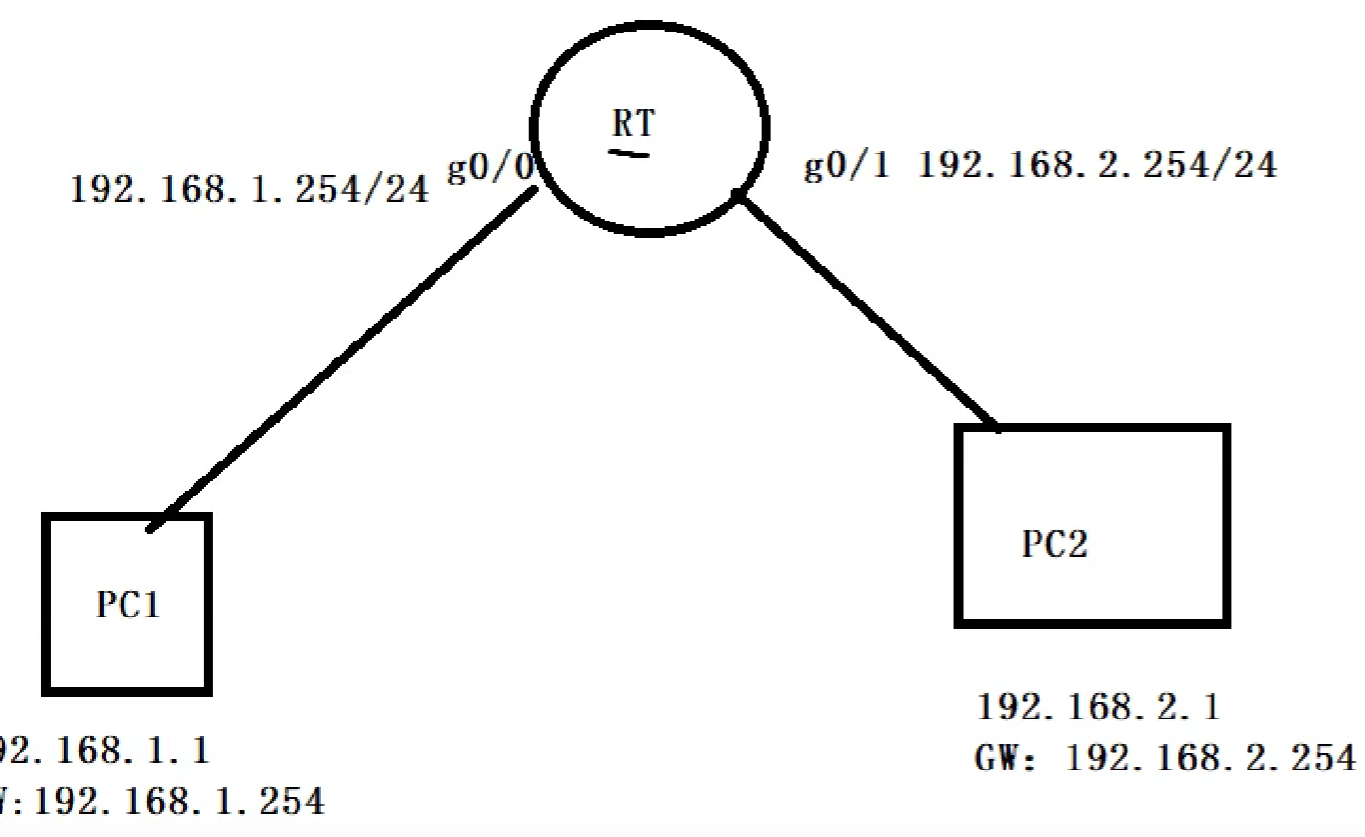
通常会预留第一个或最后一个当作网关的IP地址 eg. 192.168.1.1/254

### 路由器

交换机基于MAC地址-MAC地址表转发，路由器基于IP地址-路由表转发。

路由分为三种：直连（配置IP地址时自动生成），静态路由，动态路由（手动分配）

PC1想要和PC2通信，转发过程：

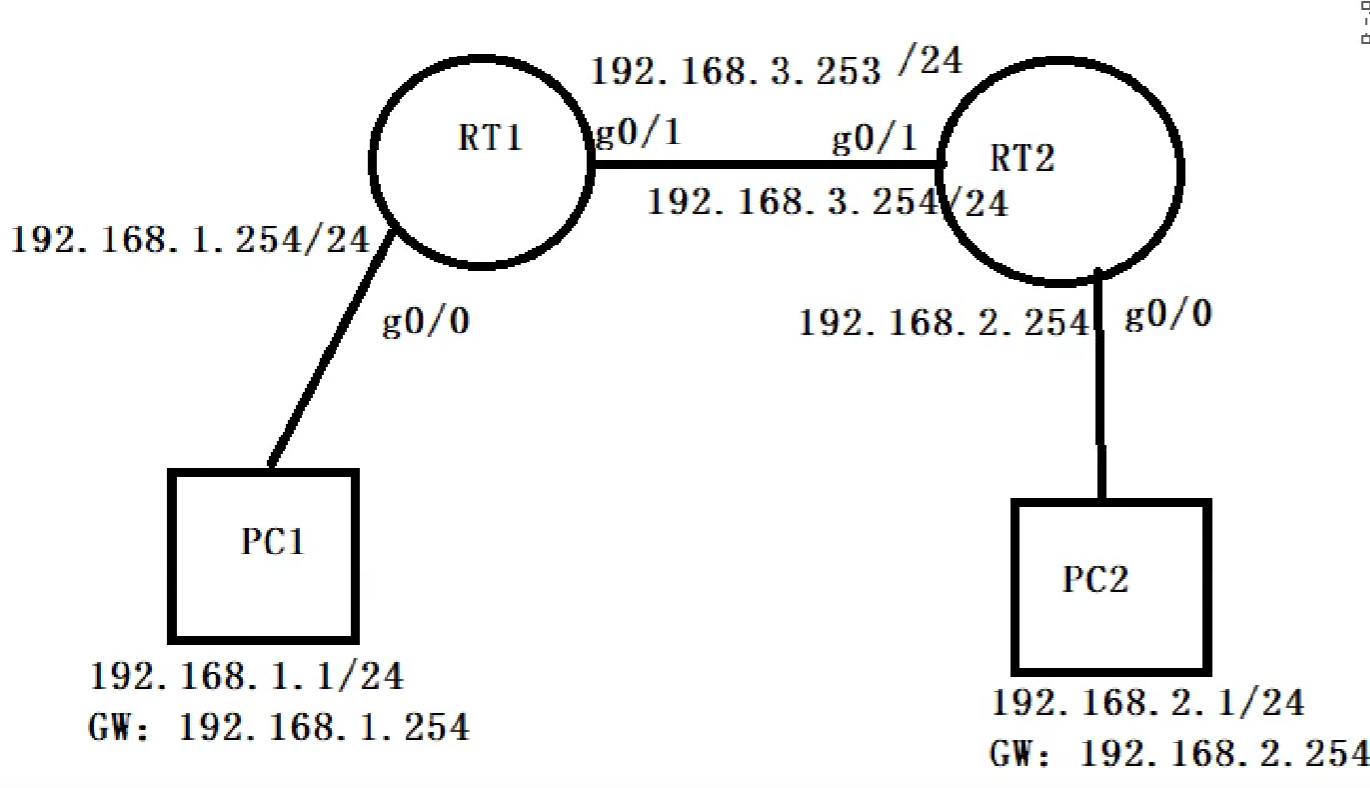


路由器给接口配置IP地址时会生成直连路由：g0/0 192.168.1.0/24（PC1网段）; g0/1 192.168.2.0/24（PC2网段）

发送数据包给路由器：PC1IP地址+PC2IP地址+PC1接口+RT 接口

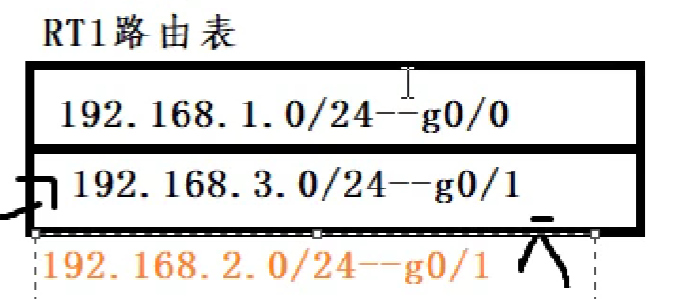
路由器查询目的IP地址并查找网段，转发至对应网段，发送数据包改为：PC1IP地址+PC2IP地址+RT 接口+PC2接口

Eg.



PC1 PC2不能通信，因为RT1不能识别192.168.2.0/24网段。需要使用静态/动态路由，让RT1 RT2互相交换路由表中的路由。

#### 静态路由

需要管理员手动编写路由表 

设置静态路由：目标网段+目标掩码+下一跳地址/出接口

Eg. 192.168.1.0 255.255.255.0 e0/1

P.S. 默认路由，是静态路由，是电脑的网关

IPv4 路由表 （route print）

============================================================

活动路由：

网络目标（目的IP）网络掩码 网关（下一跳地址） 接口 跃点数

0.0.0.0 0.0.0.0 172.20.10.1 172.20.10.6 45

0.0.0.0可以匹配任意不知道的网段

实验：静态路由的配置

环回口Loopback Interface，路由器后面的主机，虚拟，可以配置IP地址

#### 动态路由

路由器之间能主动告诉对方自己路由表

##### IGP（RIP, EIGRP, OSPF）

内部网关路由协议Interior Gateway Protocol，在自制系统内部运行（eg. 联通内部）

- 距离矢量路由协议，传递实际的路由信息（网段+掩码）：

**1. RIP**（Routing Information Protocol，路由信息协议），

**2. EIGRP**（Enhanced Interior Gateway Routing Protocol，增强型内部网关路由协议），AD90；

特点

有链路状态路由协议的特征（有邻居的概念）

收敛快，能根据网络拓扑变化迅速切换

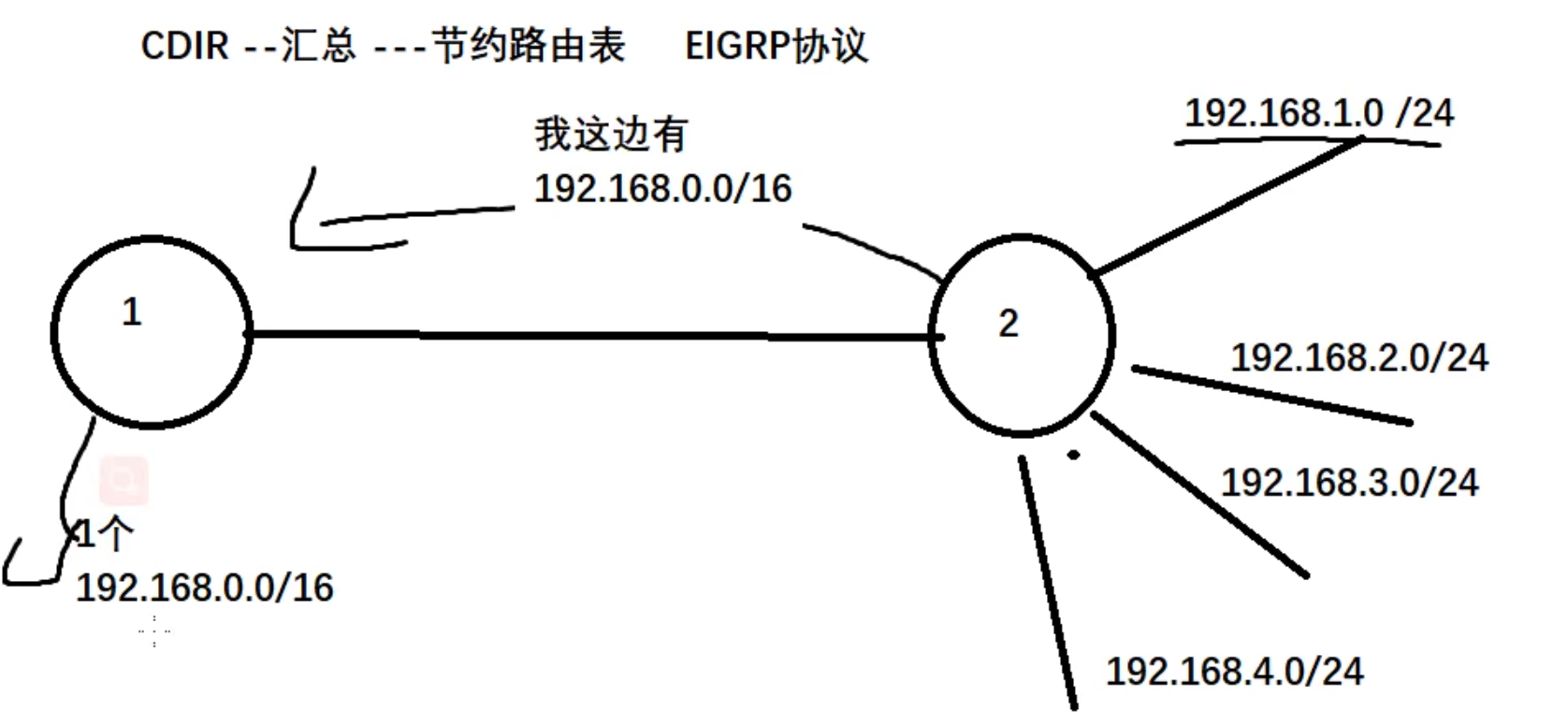
触发更新，增量更新，没有周期更新

唯一支持不等价负载均衡（两条路都走）的路由协议

无类路由协议，传递路由时可以携带子网掩码（RIP v1是有类路由协议，遵从默认子网掩码，不能携带，RIP v2无类）

支持VLSM（子网划分，Variable Length Subnet Masking） - 因为携带子网掩码

支持CIDR（汇总，节约路由表，Classless Inter-Domain Routing），多个连续网段可以合并成一条路由，比如192.168.0.0/24 和 192.168.1.0/24 可以聚合成 192.168.0.0/23。



配置EIGRP

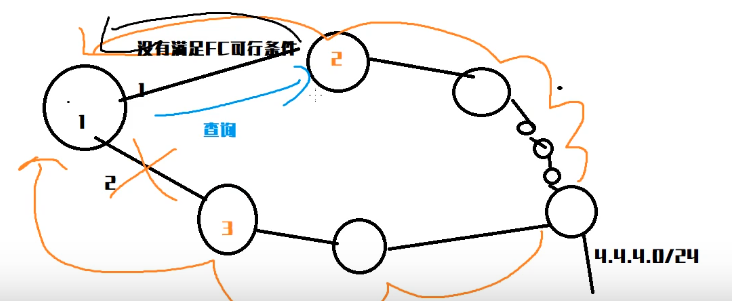
* 开启，配置自治系统编号（可以设置为优先级管理距离90）
* 宣告直连网段 network 192.168.1.0 0.0.0.255（反掩码（通配符掩码）wild card bits）

邻居建立

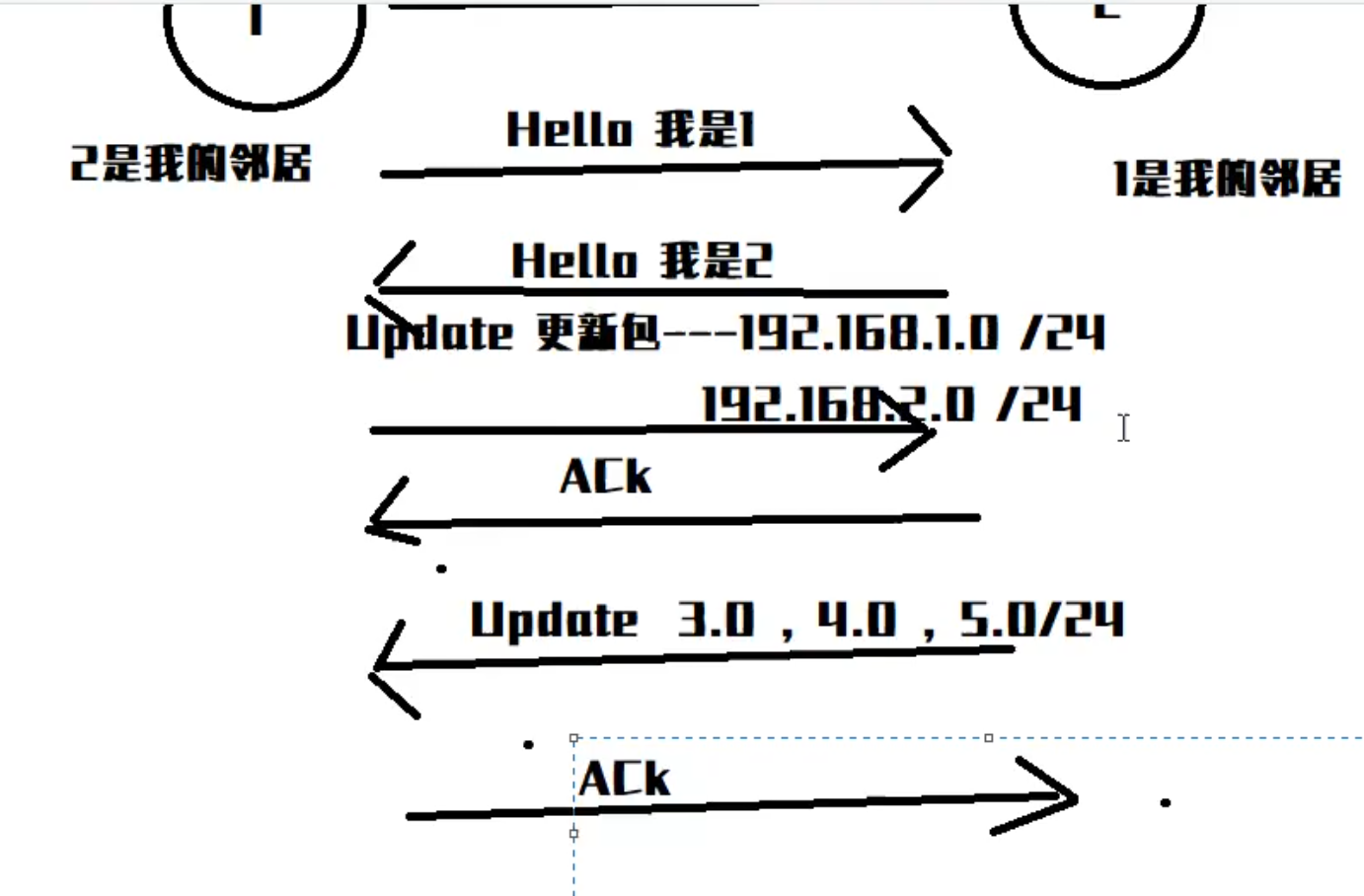
* 5s发送一次hello包
* 15s超时，邻居关系断开，从此设备收到的所有路由全部作废
* Hello包目的地址224.0.0.10，组播地址，只有运行EIGRP协议的路由器才会接受

五种数据包

* Hello – 建立维护邻居
* Update – 邻居建立之后，发送路由更新，一般组播地址
* Query – 查询，当某条路由丢失时向邻居查询关于这条路由的信息

2回复reply

* Reply – 回复
* Ack – 确认信息，确认update、query、reply，hello和ack本身不需要确认



三张表

* 路由表 – 基础路由
* 邻居表 – 列出所有的邻居
* 拓扑表 – 能到达目的网络、满足FC（Feasible Condition）可行条件的路由都会加入这个表，提取后继路由（最优路线）到路由表，有可行后继路由（如果最优路由断了，backup plan）

DUAL（Diffusing Update Algorithm）弥散更新算法

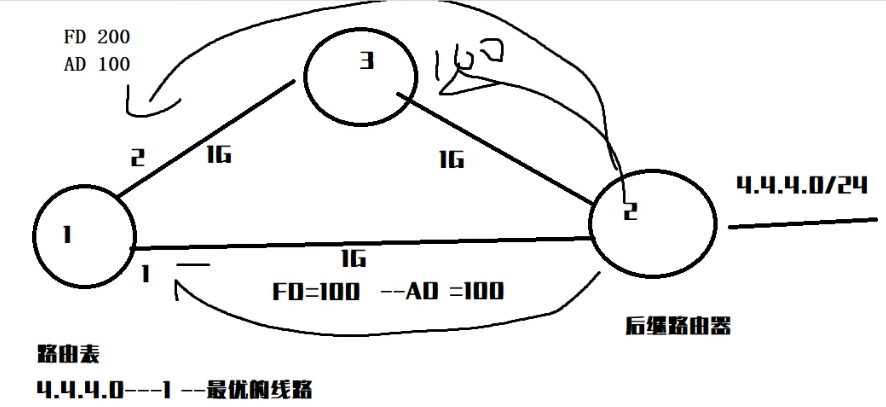
当主路径失效且没有可行后继路由Feasible Successor时：

* 当前路由进入Active状态；
* 向所有邻居发送 Query；
* 邻居收到后，如果有更好的路径则回复Reply，否则继续扩散查询；
* 直到所有邻居都回复后，路由回到 Passive 状态；
* 根据回复选择新的Successor和Feasible Successor。

这种扩散式的查询与应答确保所有节点对某路由的计算同步，避免环路。

EIGRP的集中路由器角色和专业名词

* 后继路由器 – 最优路径的下一跳路由器
* FD（Feasible Distance）可行距离 – 从自己到目的网段的全程距离=度量值
* AD通告距离（Advertised Distance），也叫RD（Reported Distance） - 邻居到达目标网段的全程距离
* FC可行条件 – AD < FD，所以下图2无法加入路由表，不满足FC

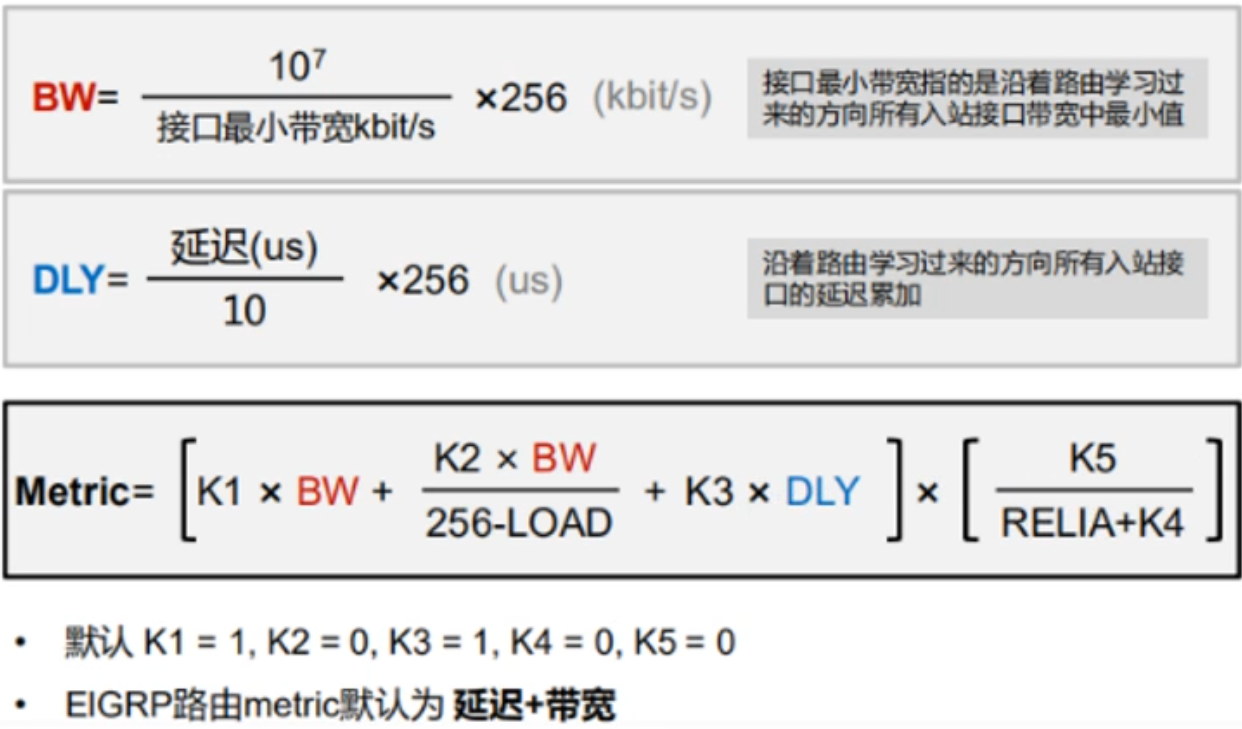


改为

* 可行后继路由器 – 备份路径的下一跳路由器

EIGRP度量值计算（管理值90）

* 根据带宽，延迟，可靠性，MTU，负载计算



* BW（根据路由上所有的接口带宽最小值计算）+DLY（根据所有延迟累加计算）

3. 基于传闻的方式传递路由信息，直接生成路由表，不需了解网络拓扑 – 可能造成路由环路 – 解决：水平分割：传递的路由不能回传

- 链路状态路由协议，传递路由信息+拓扑信息 LSA（Link-State Advertisement，邻居的信息） - 需要根据SPF（Shortest Path First，Dijkstra 算法）算法计算LSA，可以避免环路

1. **OSPF**（Open Shortest Path First）AD110

链路状态路由协议

* 链路状态 – LSA（Link-State Advertisement） - 路由信息+拓扑信息 – 基于LSA可以画出拓扑
* SPF算法（Shortest Path First，Dijkstra）计算LSA值
* OSPF – 开放式最短路径优先协议，公有

优点

* 有触发更新 – 有新增网段、链路故障才会更新
* 也有周期更新 – 30分钟更新全网LSA
* 支持VLSM（子网划分）和CIRD（汇总）
* 有邻居概念
* 有区域概念

区域

* 更新LSA：把自己的所有LSA都更新给邻居，达到全网路由器LSA数据库一致 – 导致LSA数据库科过于庞大，占用内存 – 分区域
* 骨干区域：are0，只有一个，网络核心，设备性能最好
* 非骨干区域：网络边界，必须连接骨干区域，多区域可以隔离一些LSA

三张表

* 邻居表
* 路由表
* 拓扑表LSDB（Link-State Database），LSA数据库

OSPF网络类型

* **点对点**
* 点对多点，一对多
* **广播多路访问，使用以太网交换机。为了减少泛洪，使用三种路由角色：**

DR（Designated Router）

BDR（Backup Designated Router）

DROther

DR和BDR只有一个，剩下的是DROther。DROther发送LSA只有DR和BDR能收到（使用OSPF报文，目的组播IP地址224.0.0.6，只有DR和BDR侦听，所有路由器侦听224.0.0.5），DR收到后统一下发给所有DROther。DR的选举：根据**接口优先级**，越大越优先，默认都为1，手动配置；优先级一致就根据**Router ID（RID）**，越大越优先，以IP地址形式表示，可以手工配置和自动选举，默认选环回口，如果没有环回口就根据物理接口选最大的。

* 非广播多路访问，使用ATM交换机，不支持广播

度量值（Cost值）计算

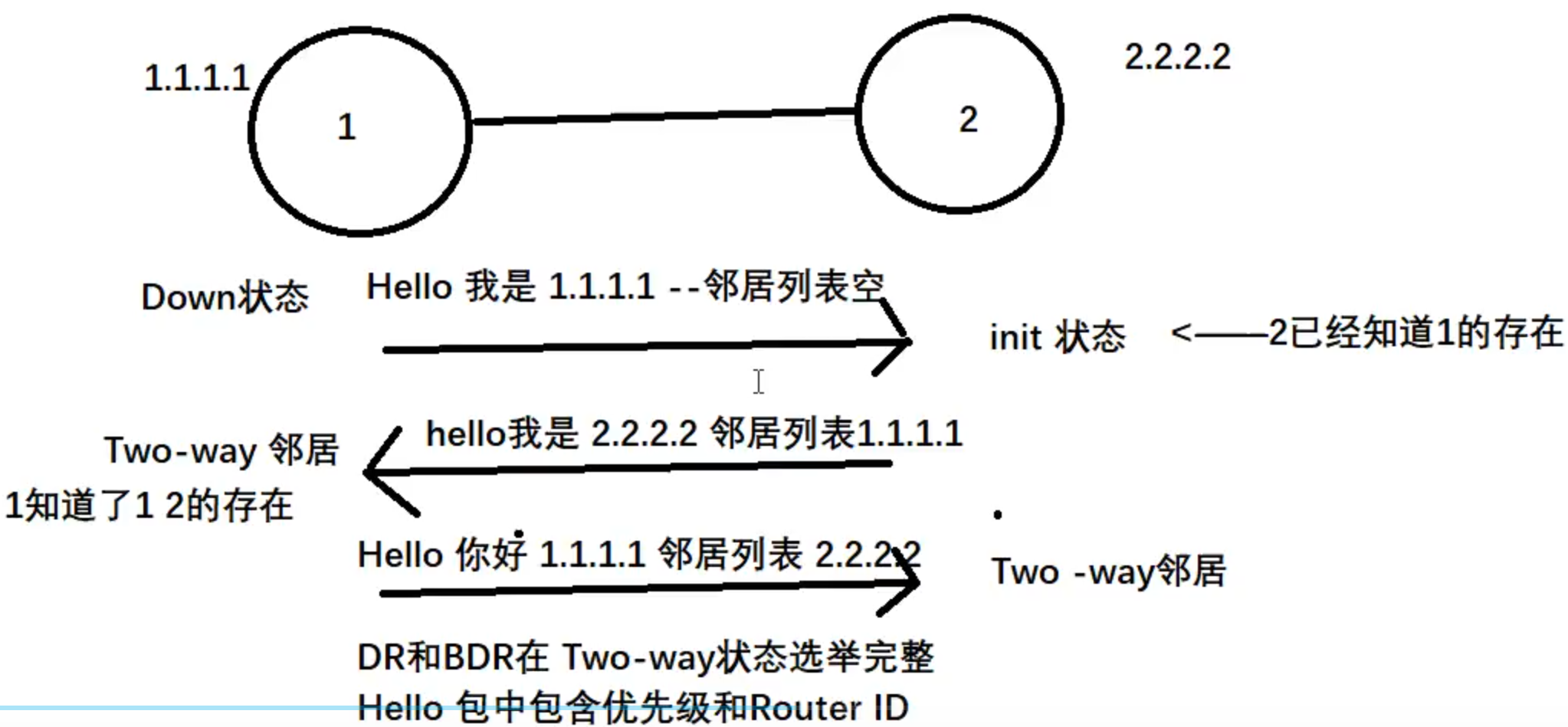
* 接口参考带宽/接口带宽，默认参考带宽为100。Eg. 物理接口100M，度量值为1。

五种数据包

* Hello – 建立邻居，维护邻居
* DBD（DD），Database Description – LSA描述信息，目录摘要
* LSR，Link-State Request – 请求LSA
* LSU，Link-State Update – LSU里面包含LSA
* LSAck – 用于确认LSU

OSPF状态机

* 邻居（Neighbor） - 不交互LSA



* 邻接（Adjacency） - 交互LSA

Down状态：尚未收到hello包，开始发送hello包给邻居

Init状态：收到了邻居的hello包，但邻居的hello包的邻居列表中没有本路由器

Two-way：收到了hello包，邻居的hello包列表中包含自己的Router-ID

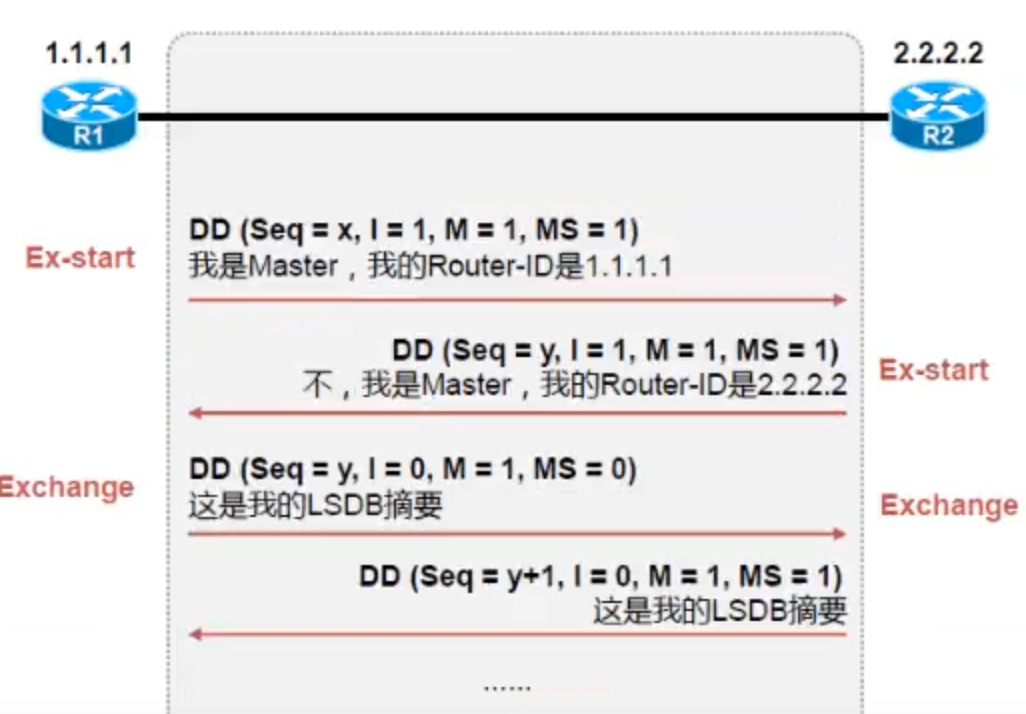
--- 接下来为邻接特有状态 ---

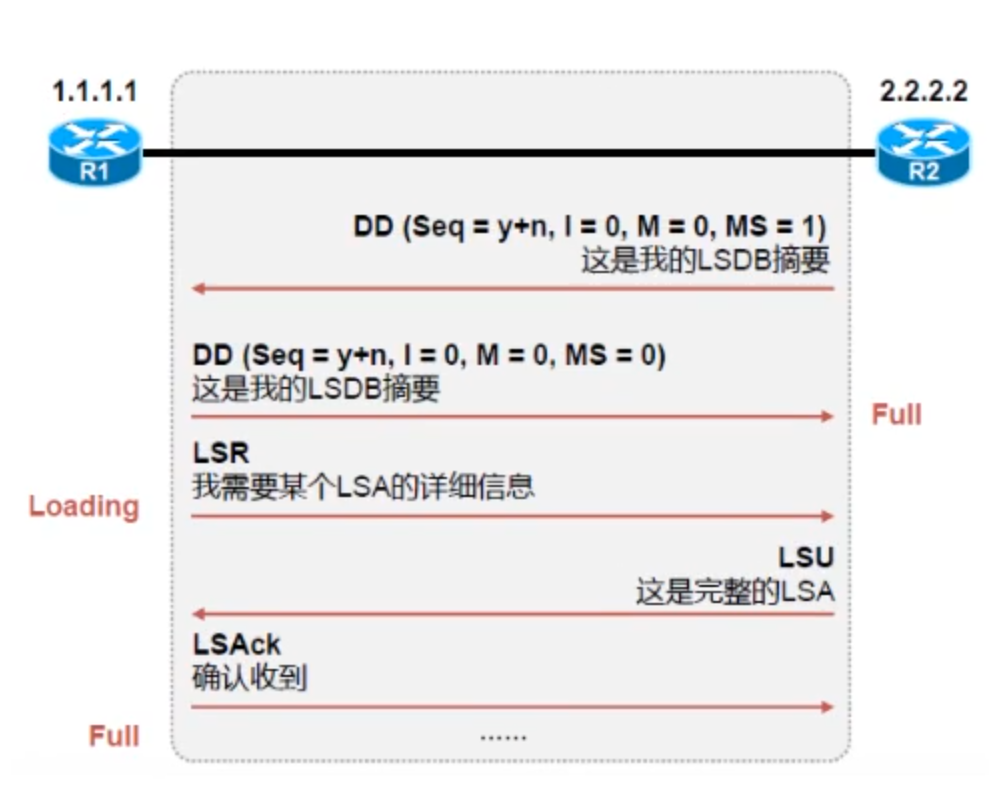
Ex-start状态：选举主从，选举Router-ID更大的为主设备。

Exchange状态：交换DD报文。seq序列号使用主设备的序列号。

Loading状态：请求LSR，将收到回复LSU，收到LSU后回复LSAck。

Full状态：双方LSDB同步，进入了邻接状态。





2. ISIS（Intermediate System to Intermediate System，中间系统到中间系统）。

##### EGP

外部网关路由协议Exterior Gateway Protocol，在运营商之间运行

- EGP，比较老

- **BGP**（Border Gateway Protocol），现网使用

针对不同IGP，优先级/管理距离（AD值，Administrative Distance）越小越优先；

针对相同IGP，度量值（网速越高越低）越低越优先，入接口累加。

##### 路由匹配顺序

最长掩码匹配（掩码25比24高，越精细越优先） – 管理距离 – 度量值

##### 动态路由更新机制

广播，目的IP地址255.255.255.255，交换机给每个接口的每个路由器都发，可能造成资源浪费，需要拆开看是否是对应协议，不是就扔掉

单播，一对一

组播，一对多，只有运行EIGRP的才会接受，目的IP224.0.0.10，但交换机不认识组播IP地址，所以还是会每个接口都发一份，而路由器可以通过IP地址判断不收

##### 路由更新方式

周期更新，定期进行收敛，保证路由真实性

触发更新，网络拓扑出现变化才更新

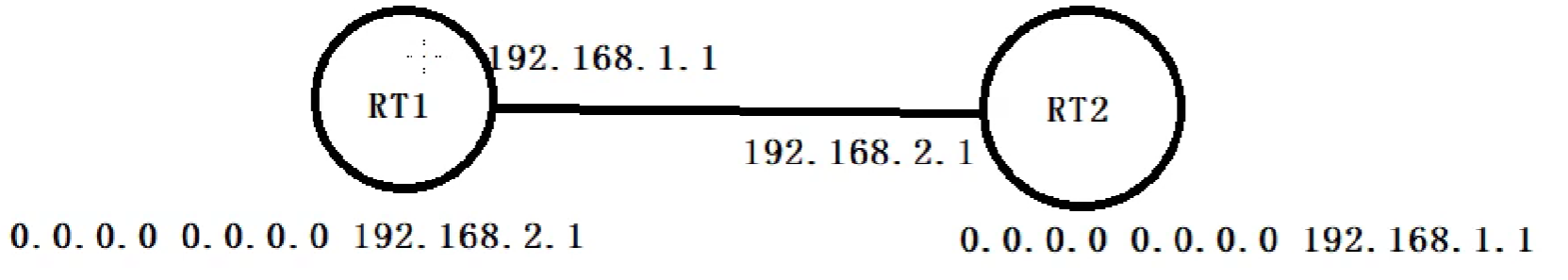
### 协议

#### ICMP协议

Internet control message protocol, 网际控制报文协议 eg. ping baidu.com

两种数据包类型：ICMP请求（源IP+目的IP+内容为ICMP请求），ICMP应答（源IP+目的IP+内容为ICMP应答）

两种情况不能通信：ICMP超时（没有收到ICMP应答（禁ping）；或者电脑没有网络），ICMP不可达（TTL-Time To Live变为0，数据包失效；路由环路）

环形路由：

TTL默认值：Windows 64，Linux 255

## 传输层

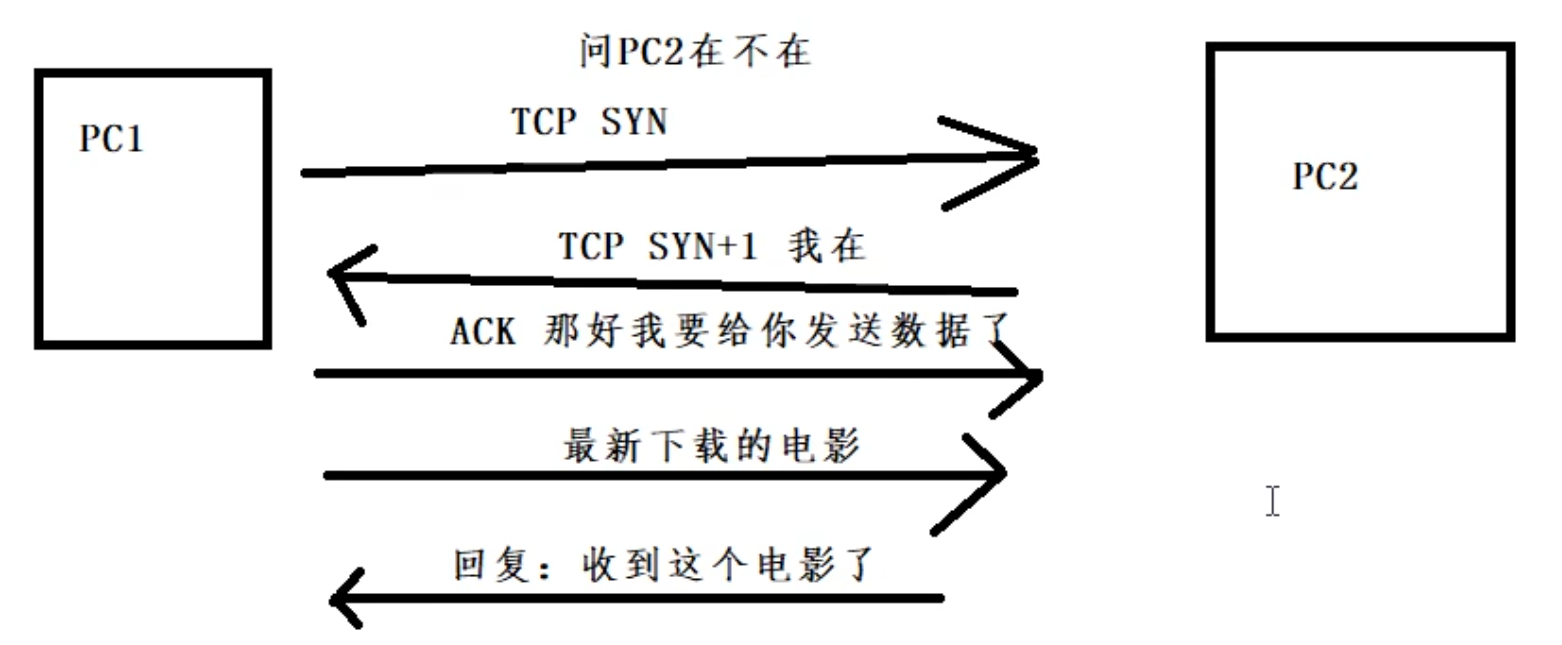
端口号 – 区分应用/服务

两种协议：TCP（可靠，贵），UDP（速度慢，便宜）

### TCP

Transmission Control Protocol，字节流传输，没有边界

面向连接，通信前三次握手（Three-way Handshake）建立连接



1. 客户端 → 服务器：发送 SYN=1（Synchronize Sequence Number同步序列号），并选择一个随机初始序列号 Seq = x；
2. 服务器 → 客户端：发送 SYN=1, ACK=1，Seq = y，Ack = x+1；

目的：服务器确认收到客户端的请求（Ack = x+1），并告诉客户端“我也想建立连接，我的序列号是 y”。

1. 客户端 → 服务器：发送 ACK=1，Ack = y+1。

目的：客户端确认收到了服务器的回应，连接建立成功。

如果没有收到回复，等待一段时间之后再发一次。

断连时需要四次握手：

1. 客户端 → 服务端：FIN，进入 FIN-WAIT-1 状态。
2. 服务端 → 客户端：ACK，服务端确认收到了关闭请求，但服务端可能还有数据没发完，进入 CLOSE-WAIT 状态。
3. 服务端 → 客户端：FIN，服务端也发完数据了，主动关闭自己这边，进入LAST-ACK状态。
4. 客户端 → 服务端：ACK，客户端确认服务端的关闭请求，进入TIME-WAIT状态，等待 2MSL（Maximum Segment Lifetime报文最大生存时间）后彻底关闭。

### UDP

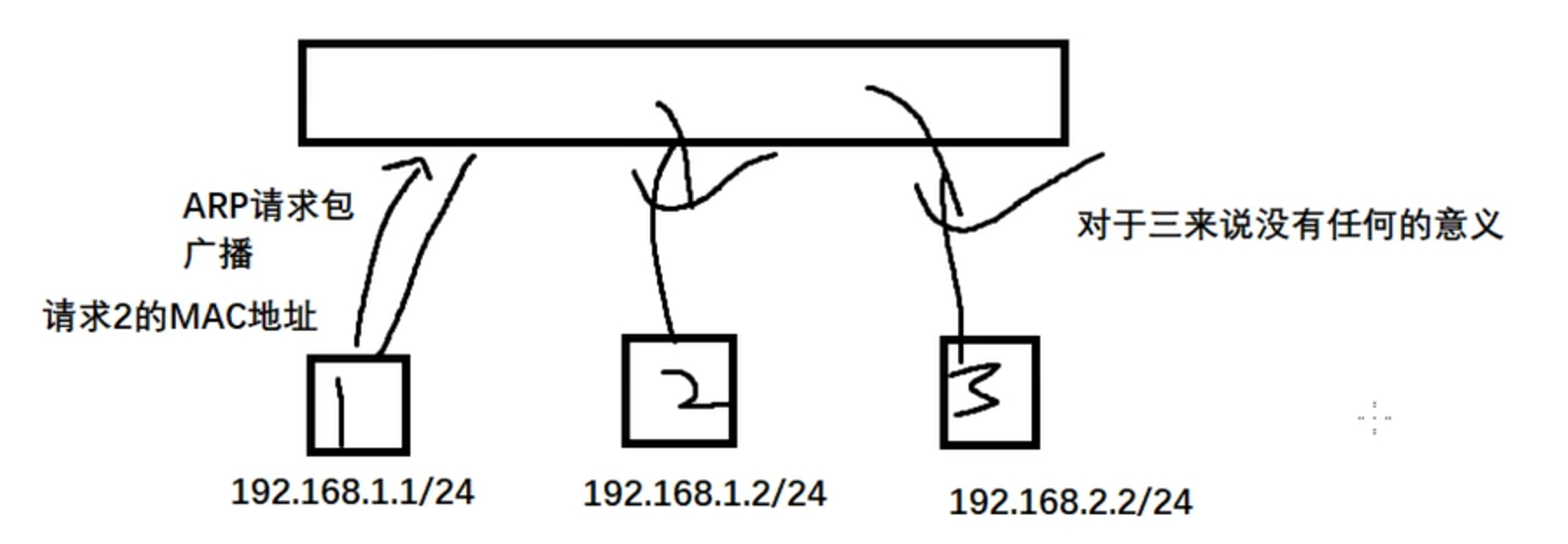
User Datagram Protocol

无连接，报文传输，保留边界，不保证可靠性，速度快

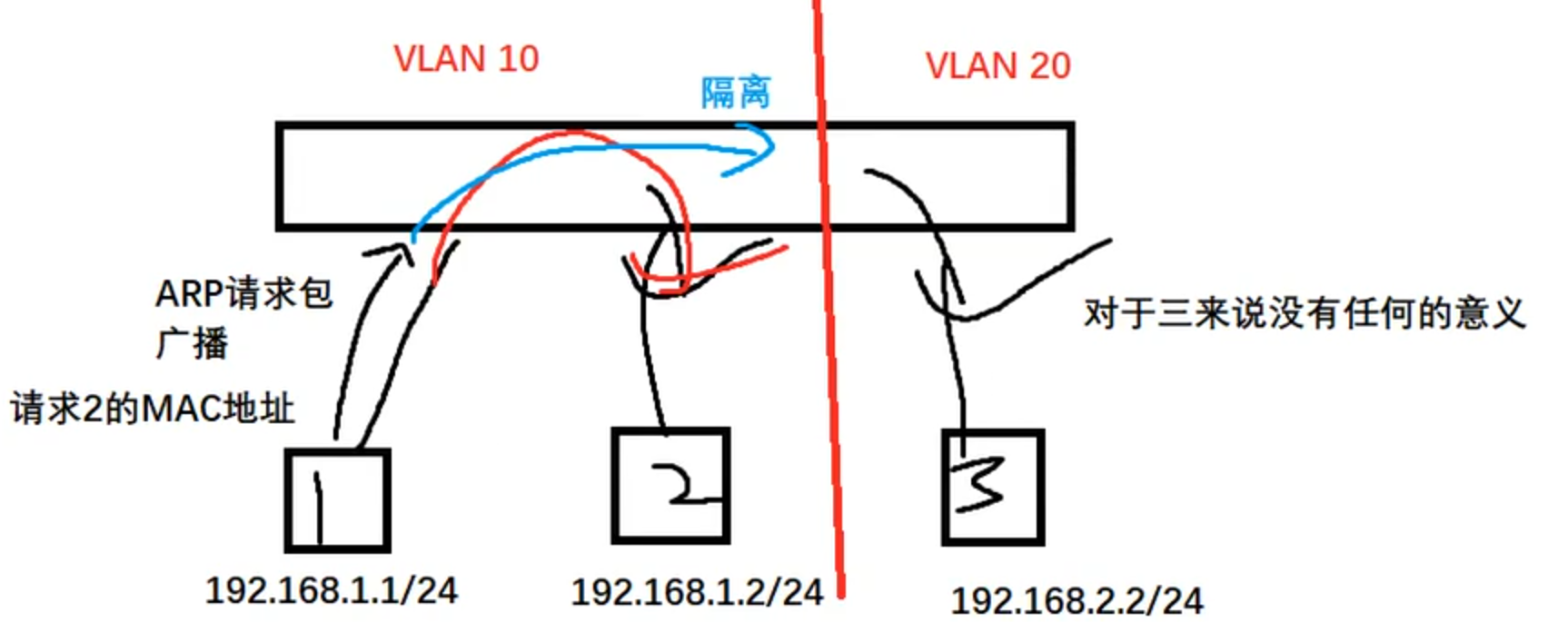
## V-LAN

Virtual Local Area Network虚拟局域网。WAN广域网。

传统局域网的问题：不能合理隔绝广播流量。



把一台交换机虚拟切成两台使用，隔绝广播流量，不同的VLAN不能通信。



默认交换机所有接口都能通信 – 默认都在VLAN1 – 本征VLAN（Native VLAN），数据包不存在标签，其他VLAN在交换机接口收到数据包后会加上对应VLAN的标签

### 交换机的三种接口类型

Access – 连接PC、路由器，在接收数据时打标签，发送数据时拨开标签（路由器和PC不认识带标签的数据包，不剔除标签就会直接扔掉）。默认所有接口都是access接口。

Trunk – 交换机和交换机之间连接，发送或接收数据包都会保留标签。两种类型：dot1q（802.1q，公有的Trunk封装协议，把标签插入到数据帧里面），ISL（思科私有的封装协议，直接把标签放在数据帧最外层，效率更高但不是公有的）。默认允许所有VLAN通过交换机进入其他交换机，可以配置。

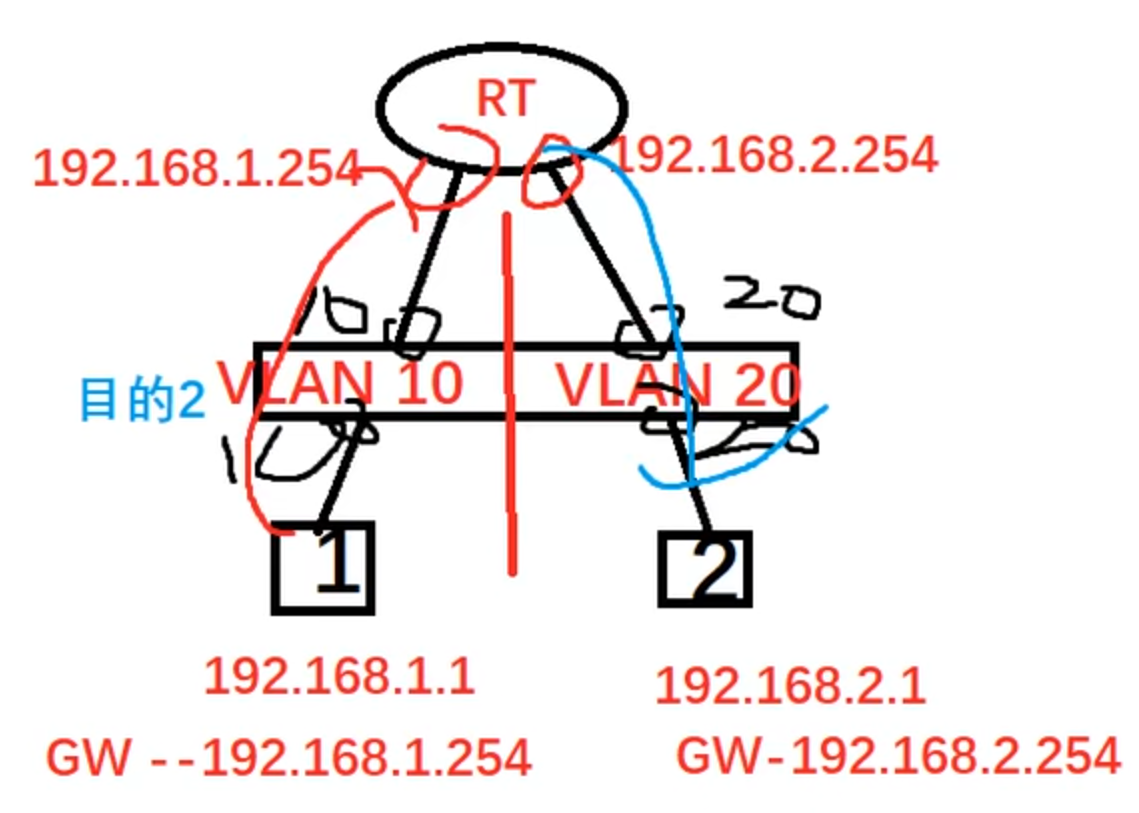


Hybrid – 混杂接口，华为私有接口，可以当成access或trunk，可以保留或剥离标签，可以随时切换

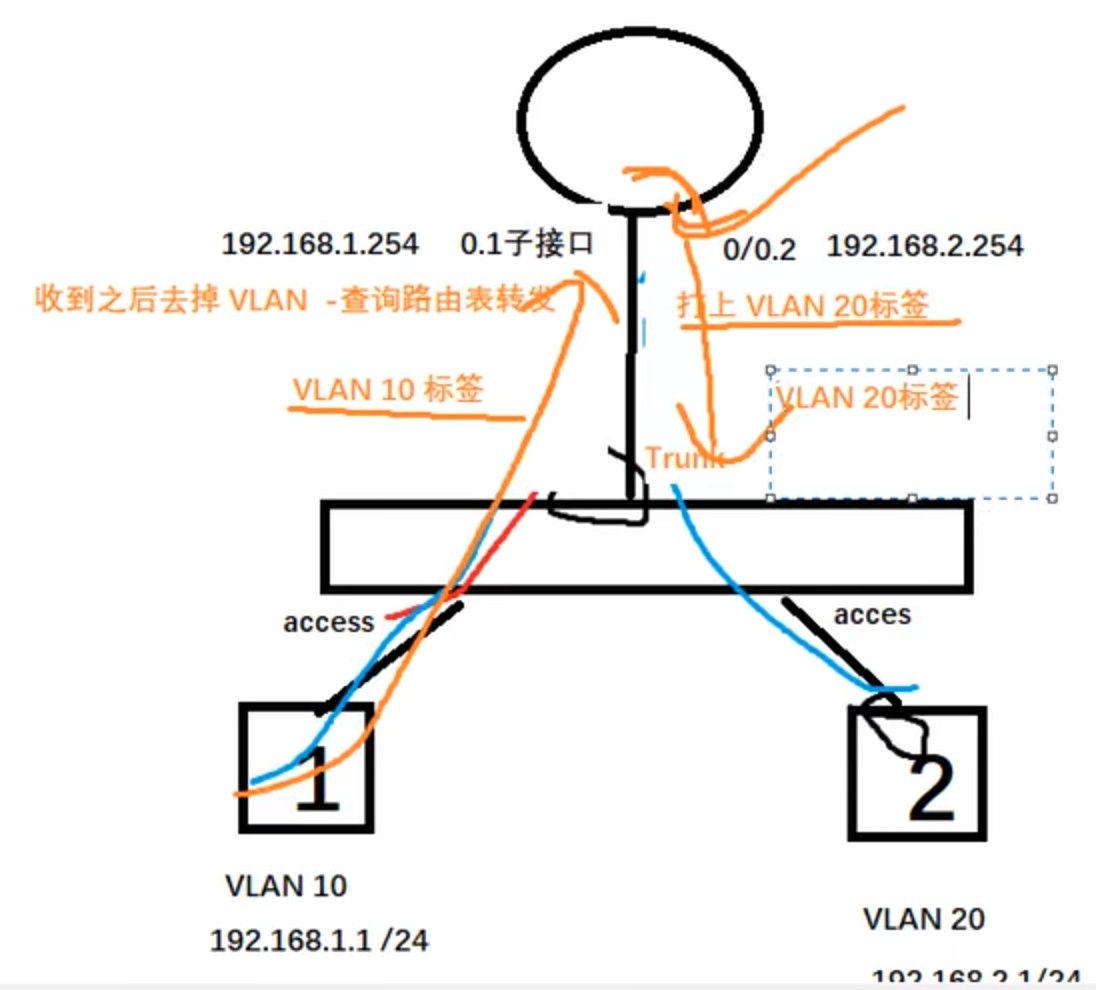
### 跨VLAN通信

#### 接一台路由器

路由器查询路由表后转发，缺点：浪费交换机和路由器的接口，路由器一般只有两个接口（内网和外网），添加接口卡很贵



#### 单臂路由



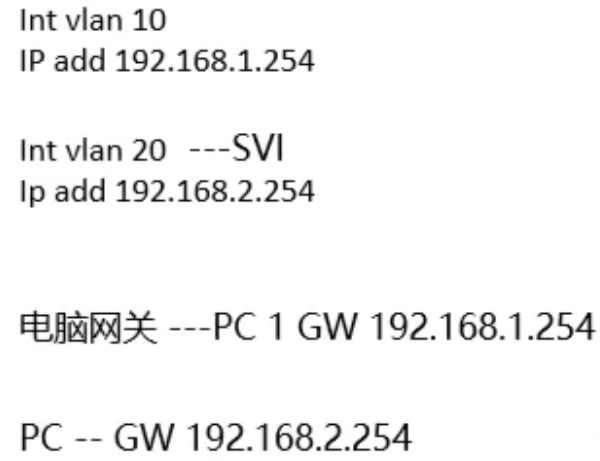
只需要路由器的一个接口，在接口上封装dot1q协议能够识别特定VLAN的标签。设置虚拟子接口0/0.1和0/0.2，配置IP地址当作网关。

缺点：单点故障，这个接口坏了会造成整个公司网络瘫痪，已经淘汰。

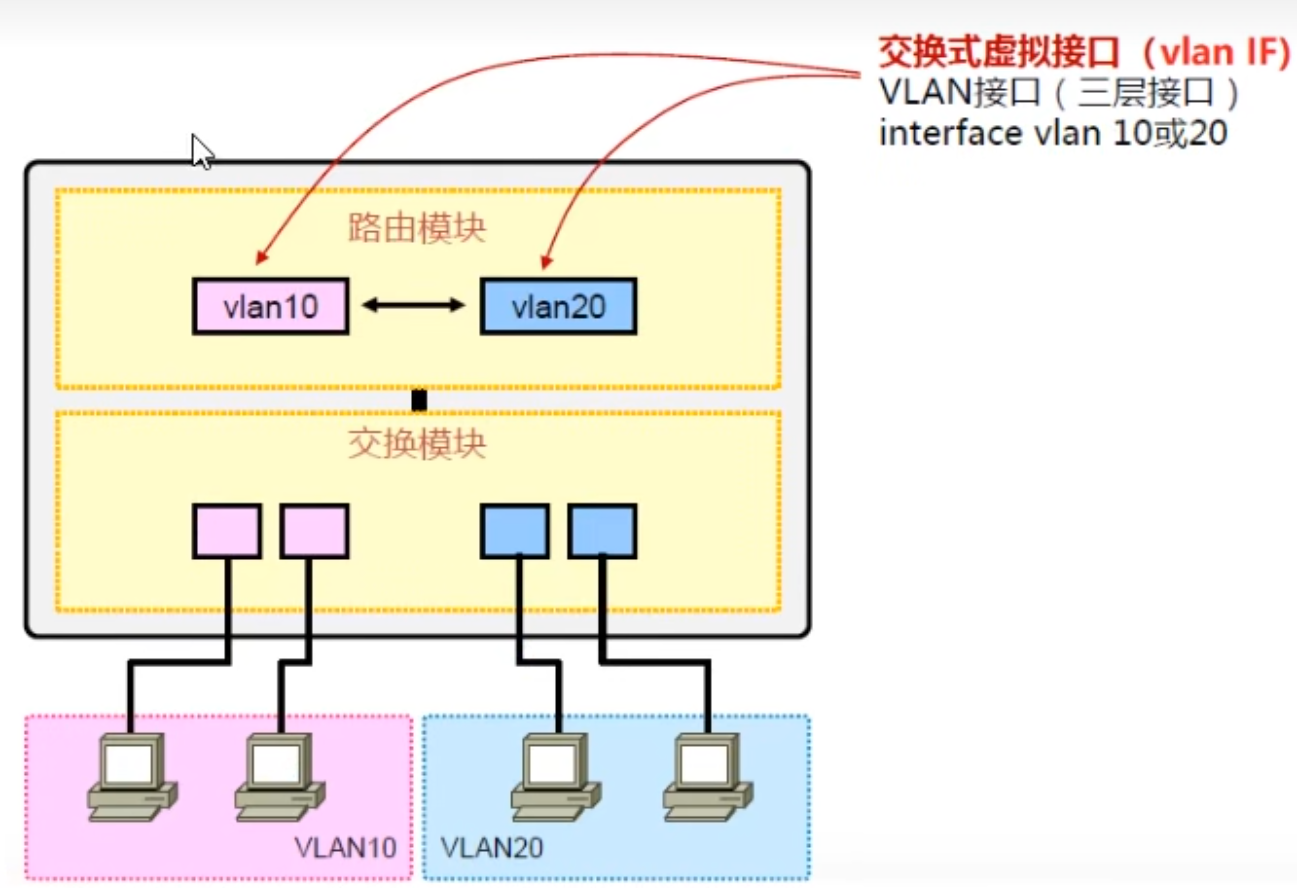
#### SVI（Switched Virtual Interface，华为：VLAN IF）交换虚拟接口

只有三层交换机支持，能路由转发。二层交换机只支持MAC地址表转发。

给VLAN配IP地址，电脑的网关就是SVI接口。



三层交换机内部结构：



路由模块查询路由表，交换模块进行转发。

# 实验

## 命令行等级

Router> 用户模式，查看部分配置，不能操作

Router> enable 进入特权模式(ena)

Router# 特权模式，查看所有配置，不能配置

Router# configure 进入全局模式

Router(config)# 全局模式，可以做任何操作，不能查看配置

Router(config)# interface g0/0 进入接口配置模式

Router(config-if)# exit 返回上一级

## 静态路由

设置静态路由：目标网段+目标掩码+下一跳地址/出接口

Eg. 192.168.1.0 255.255.255.0 e0/1

## 动态路由

路由器自动同步路由表，网络拓扑发生变化的时候自动收敛（路由的增加和减少）

OSPF动态路由协议

路由配置规定：

不同接口不能配置同一个IP地址

不同接口不能配置同一个网段

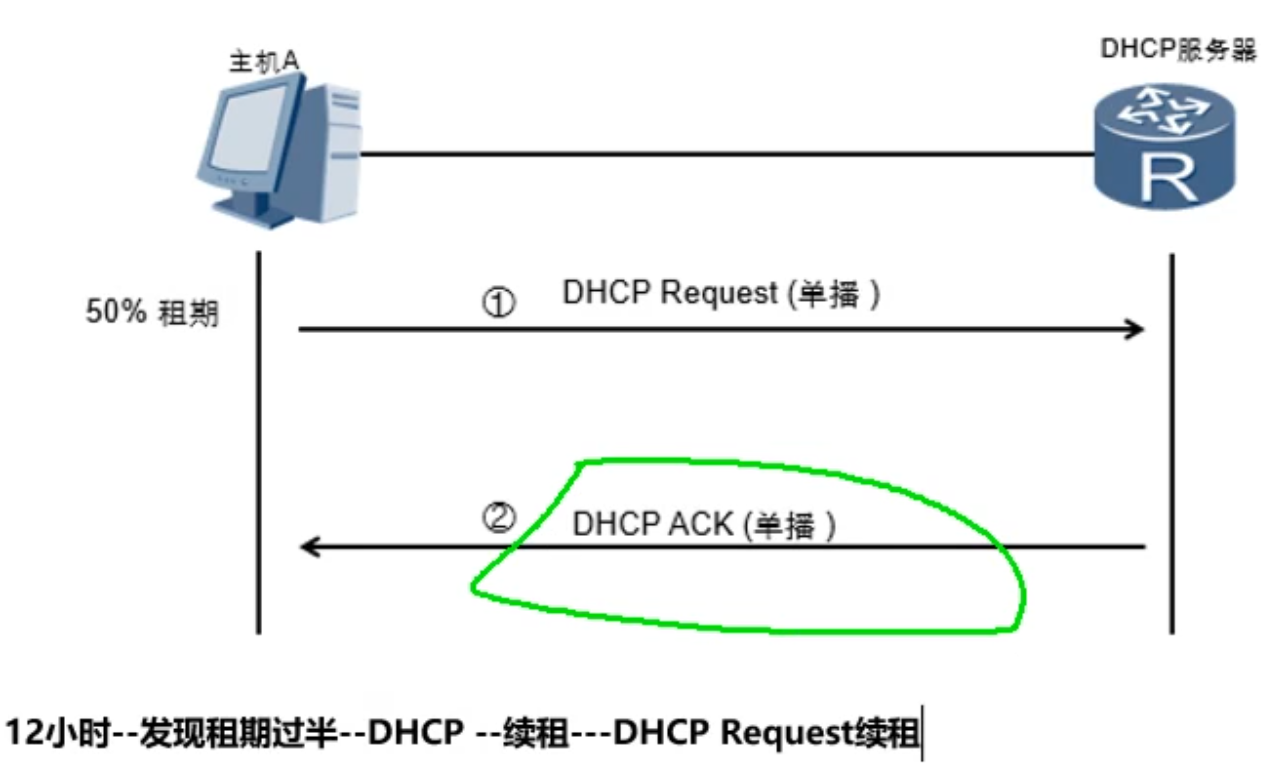
## DHCP

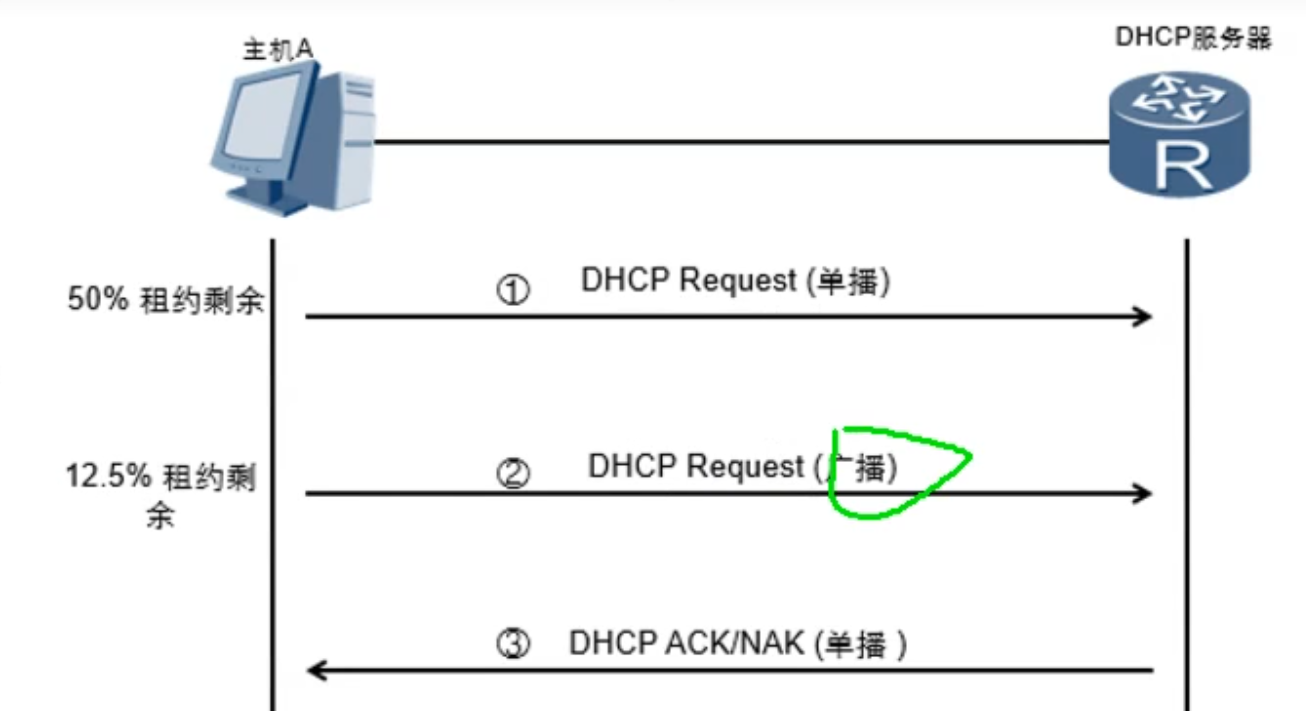
Dynamic Host Configuration Protocol，动态主机配置协议



Offer（IP地址+GW+DNS+租期（默认一天））先到的先采用

最后主机需要发送一个免费ARP – 以自己地址为目的请求MAC地址，自己回复自己，如果其他人应答，则发生了IP地址冲突

续租（Renewing state）流程 同意ACK，不同意NAK

如果原DHCP服务器没有应答 – 重绑定（Rebinding state）

DHCP release 释放地址，通知服务器

网络层（TCP/IP）四个协议：ARP, ICMP(Internet control message protocol, 网际控制报文协议）， IGMP(Internet group management protocol, 网际组管理协议）， IP（Internet protocol）