一、局域网

组建需要使用交换机（Switch），交换机能提供多端口、高速率、无冲突的转发。

交换机工作在TCP/IP的数据链路层（2层），转发的是数据帧。

冲突域：在通信中，产生数据冲突的一个区域。

- 集线器（Hub）所有端口处于一个冲突域。
- 交换机每个端口属于单独的一个冲突域。

二、链路层

1. 传输介质

- 金属导线：双绞线、同轴电缆
- 玻璃纤维：光纤
- 电磁波：无线

2. 双绞线线序

- 568A：绿白、绿　　橙白、蓝　蓝白、橙　棕白、棕
- 568B：橙白、橙　　绿白、蓝　蓝白、绿　棕白、棕

记忆方法：先记568B的线序，再在568B的基础上进行调整，变为568A。

- 568线序：

  初始：橙白、橙　绿白、绿　蓝白、蓝　棕白、棕

  1. 先将4对线，从左到右，从浅到深排列（赤橙黄绿青蓝紫...）

     橙白、橙　　绿白、绿　　蓝白、蓝　　棕白、棕

  2. 将双绞线进行分离，将有白色的那根线，放到这对线的左边。

     橙白、橙　　绿白、绿　　蓝白、蓝　　棕白、棕

  3. 将绿色和蓝色这两根线，互换位置，得到568B线序。

     橙白、橙　　绿白、蓝　　蓝白、绿　　棕白、棕

- 568A线序：

  在568的基础上，将1、3对调，将2、6对调，得到568A的线序。

  568B：橙白、橙　　绿白、蓝　　蓝白、绿　　棕白、棕

  568A：绿白、绿　　橙白、蓝　　蓝白、橙　　棕白、棕

3. 直通线与交叉线

- 直通线：双绞线的两端，使用同样的线序，例如：568A-568A、568B-568B
- 交叉线：双绞线的两端，使用不同的线序，例如：568A-568B

如何选用直通线还是交叉线?

将能处理三层（网络层）及三层以上的设备设为A类

将能处理二层（数据链路层）及二层以下的设备设为B类

同类设备称为同种设备，不同类设备为不同种设备

同种设备使用交叉线，不同种设备使用直通线

4. 多模光纤vs单模光纤

多模光纤：

- 采用LED（发光二极管）作为光源
- 低带宽和速度
- 距离较短
- 费用/成本较低

单模光纤

- 激光发射器作为光源
- 高带宽和速度
- 距离较长
- 费用/成本较高

5. 以太网数据帧结构

Ethernet II 数据帧结构：

D.MAC	S.MAC	Type	Data	FCS
6字节	6字节	2字节	46字节-1500字节	4字节

以太网数据帧大小：64字节 - 1518字节

6. MAC地址

MAC地址共6字节，由十六进制数组成。

1 Byte = 8bits　MAC地址由48bit组成，一个十六进制数是4个bit，共有12个十六进制数

有几种表示方式：

- 0000.0c43.2e08
- 00:00:0c:43:2e:08
- 00-00-0C-43-2E-08

MAC地址前24bit为OUI（组织唯一标识符），代表厂商

后24bit由组织自己分配

单播MAC地址：第8bit为0，例：00-00-01-00-00-01

组播MAC地址：第8bit为1，例：01-80-C2-00-00-00

广播MAC地址：FFFF-FFFF-FFFF

7. 交换机MAC地址表

交换机转发数据帧，依靠MAC地址表来转发

MAC地址表存储在内容可寻址存储器（CAM）中，可实现快速的查找。

交换机学习建立MAC地址表的过程：

收到数据帧后，将数据帧的源MAC地址，和收到此数据帧的接口做一个映射，添加到MAC地址表中。

交换机MAC地址表建立，除了动态学习，也可以手工添加（静态）。

MAC地址表老化时间300s。

交换机转发行为：

- 转发 Forward：交换机收到单播帧时会转发
- 泛洪 Flood：交换机收到单播帧（未知单播帧泛洪）、组播帧、广播帧都会泛洪
- 丢弃 Discard：

三、网络层

1. IP地址的组成

IP地址是由32bit的二进制数组成，将32bit分为4个部分，每部分8bit，中间用小数点隔开，然后再将每部分转换成十进制，这种表示方式称为：点分十进制，例：192.168.0.1。

IP地址由网络位（Network ID）和主机位（Host ID）组成

网络位：标识这个地址属于哪个网络，类似街道

主机位：标识这个地址在网络中的具体位置，类似建筑

当主机位全0时，表示网络地址（哪个网络）

当主机位全1时，表示广播地址

192.168.1　.1 的网络地址是多少（192.168.1.1是哪个网络的） 192.168.1.1是192.168.1.0这个网络的

192.168.1.1是由网络位和主机位组成

假设，192.168.1是网络位，.1是主机位，问192.168.1.1的网络地址是多少?

192.168.1. 00000000 = 192.168.1.0

2. IP地址的分类

A类：前8bit是网络位，后24bit是主机位，且最高位固定为0，范围：0.0.0.0 - 127.255.255.255

B类：前16bit是网络位，后16bit是主机位，且前2bit固定为10，范围：128.0.0.0 - 191.255.255.255

C类：前24bit是网络位，后8bit是主机位，且前3bit固定为110，范围：192.0.0.0 - 223.255.255.255

D类：组播地址，给组播使用

E类：保留，用于科研

3. 私有地址/公有地址

A类私有地址：10.0.0.0/8

B类私有地址：172.16.0.0/12（172.16.0.0-172.31.255.255）

C类私有地址：192.168.0.0/16

172.17.1.1

4. 特殊地址

0.0.0.0：未指定地址，代表还没获取到IP地址

255.255.255.255：本地广播地址

127.x.x.x：测试地址，测试本地TCP/IP协议栈是否工作正常

5. 子网掩码

子网掩码（NetMask)：用于让计算机识别IP地址的网络位以及主机位

子网掩码由32bit的二进制数组成，格式与IPv4地址一样

子网掩码的1代表网络位，子网掩码的0代表主机位

主机判断网络位的方法：

192.168.1.1 255.255.255.0

1. 将IPv4地址用二进制表示

   192.168.1.1

   11000000.10101000.00000001.00000001
2. 将子网掩码用二进制表示

   255.255.255.0

   11111111.11111111.11111111.00000000
3. 将IPv4地址与子网掩码地址做“与”运算（1和0相与为0，1和1相与为1，0和1相与为0，0和0相与为0）

   11000000.10101000.00000001.00000001

   11111111.11111111.11111111.00000000

   对位相与

   11000000.10101000.00000001.00000000

   192.168.1.0

A类地址的默认子网掩码：255.0.0.0，简化为/8

B类地址的默认子网掩码：255.255.0.0，简化为/16

C类地址的默认子网掩码：255.255.255.0，简化为/24

192.168.1.1 255.255.255.0

可以写作：192.168.1.1/24

6. 子网划分

子网划分的意义：节约地址空间、便于管理

通过VLSM（可变长子网掩码）来进行子网划分

子网划分有两种分类：

- 按子网数划分
- 按主机数划分

按子网数划分

示例：有3个部门，A、B、C

A：30台主机

B：20台主机

C：10台主机

给定网络为192.168.1.0/24，划分出3个子网，分别给三个部门。

192.168.1.　　00000000

255.255.255.　00000000

给定的网络是192.168.1.0/24，网络位已经固定为192.168.1，三个不同的网络意思就是三个网络的网络位不同。

因为网络位已经固定，没有多余的网络位可用，所以需要向主机位去借位，作为网络位来使用。

题目中要划分3个部门，需要借2位，借完之后，网络位就有26位，主机位6位。

192.168.1.　　00　000000

255.255.255.　11　000000

借完2位后：

00：192.168.1.0/26

01：192.168.1.64/26

10：192.168.1.128/26

11：192.168.1.192/26

A部门：192.168.1.0/26

　　可用地址范围：192.168.1.1/26 - 192.168.1.62/26

　　网络地址：192.168.1.0/26　广播地址：192.168.1.63/26

B部门：192.168.1.64/26

可用地址范围：192.168.1.65/26 - 192.168.1.126/26

网络地址：192.168.1.64/26 广播地址：192.168.1.127/26

C部门：192.168.1.128/26

可用地址范围：192.168.1.129/26 - 192.168.1.190/26

网络地址：192.168.1.128/26 广播地址：192.168.1.191/26

按主机数划分

先满足主机数目最多的子网，最后满足主机数目最小的子网。

借多少位作为网络位，需要根据实际情况来计算。

示例：给定的网络为192.168.1.0/24，有4个部门，A、B、C、D，划分4个子网，分配给4个部门：

A部门：80台

B部门：60台

C部门：30台

D部门：10台

先考虑A部门，如果借位，那么剩余的主机位数，要满足80台主机，设剩余的主机位数为n，2的n次方 - 2 大于等于 80，n = 7，

即主机位为7，借1位作为网络位。

192.168.1. 0 0000000

255.255.255. 1 0000000

0：192.168.1.0/25 A部门

1：192.168.1.128/25

192.168.1.128/25

再考虑B部门，如果借位，那么剩余的主机位数，要满足60台主机，设剩余的主机位数为n，2的n次方 - 2 大于等于 60，n = 6，

即主机位为6，借1位作为网络位。

192.168.1. 1 0 000000

255.255.255. 1 1 000000

10：192.168.1.128/26 B部门

11：192.168.1.192/26

192.168.1.192/26

再考虑C部门，如果借位，那么剩余的主机位数，要满足30台主机，设剩余的主机位数为n，2的n次方 - 2 大于等于 30，n = 5，

即主机位为5，借1位作为网络位。

192.168.1.　1 1 0 00000

255.255.255.　1 1 1 00000

110：192.168.1.192/27　C部门

111：192.168.1.224/27

192.168.1.224/27

最后考虑D部门，如果借位，那么剩余的主机位数，要满足10台主机，设剩余的主机位数为n，2的n次方 - 2 大于等于 10，4 = 5，

即主机位为4，借1位作为网络位。

192.168.1.　1 1 1 0 0000

255.255.255.　1 1 1 1 0000

1110：192.168.1.224/28　D部门

1111：192.168.1.240/28

7. 默认网关

不同网络的主机想要实现通信，需要找到离开自己网络的”大门“，网关就是网络的大门，网关用于实现不同网络主机进行通信。

网关设备通常由路由器、三层交换机、防火墙等设备来充当。

8. DNS

DNS：域名系统服务

配置地址时，还需配置DNS服务器，DNS服务器是用于做域名解析的。

域名：www.baidu.com、www.163.com

DNS服务用于将域名解析为IP地址。

例如：主机A访问www.cisco.com

1. 主机A在浏览器中输入www.cisco.com，主机就会向www.cisco.com发出请求，获取网页资源。
2. 因为www.cisco.com是域名，并不是IP地址，所以主机A发送一个域名解析的请求，发送给DNS服务器，向

DNS服务器询问，www.cisco.com的IP地址是多少

3. 服务器收到后，查询域名与IP的对应关系，找到www.cisco.com的IP地址，并回复给主机A。
4. 主机A收到回复后，访问对应的IP地址，获取网页资源。

9. IPv4头部

Ver：版本

IHL：头长度，范围20Byte - 60Byte

Service Type：做QoS用

Total Length：总长度，头部长度+数据长度

Identification：标识，用于标识属于一个数据包的分片

Flag：标记

- R：保留
- DF：如果为1，则不允许分片；如果为0，允许分片
- MF：如果为1，后续还有分片；如果为0，后续没有分片

Fragment Offset：片偏移，用于按序重组

TTL：生存时间，用于减小环路对网络造成的影响，没经过一台3层设备，TTL值减1，减为0时，数据包将被丢弃掉。

Protocol：标识上层使用什么协议

Header Checksum：校验完整性

Source Address：源IP地址

Destination Address：目的IP地址

Options：可选项

Padding：填充

四、传输层

1. 传输层特点：

1. 会话的多路复用
2. 标识不同的应用

   通过端口号进行区分上层协议，端口号范围 0 - 65535，1024及以下称为知名端口号，已经分配给固定协议使用，1024以上称为随机端口号，部分没有固定分配的。

   HTTP：80（TCP）

   HTTPS：443（TCP）

   FTP：文件传输协议，20、21（TCP），登录FTP服务器时,需要提供用户名和密码。

SSH：加密的管理远程设备，22（TCP）

Telnet：不加密的管理远程设备，23（TCP）

DNS：53（TCP）、（UDP）

TFTP：简单文件传输协议，69（UDP），登录TFTP服务器时，不需要提供用户名和密码。

SNMP：简单网络管理协议，161（UDP）

3. 分段
4. 流量控制
5. 面向连接/面向非连接
6. 提供可靠/不可靠传输

2. TCP

TCP称为传输控制协议，它是一个面向连接的协议，提供可靠的传输机制。

TCP的通信过程可以简单的分为三步：

- 建立连接：三次握手的过程
- 传输数据：通过序列号、确认号提供可靠传输，通过窗口大小提供流控
- 断开连接：四次挥手的过程

3. UDP

UDP称为用户数据报协议，它是一个无连接的协议，没有可靠传输机制，如果需要，由上层应用程序提供。

对于一些延时比较敏感的流量，需要使用UDP，例如：语音、视频流量

五、ICMP

ICMP称为互联网消息控制协议，主要用于排查网络错误，提供错误信息。

ICMP的应用：

Ping：测试网络连通性，使用ICMP的两个报文，echo-request、echo-reply。

Traceroute：测试报文去往目的地所经过的路径。

六、IOS操作

1. 模式

用户模式：Switch>，执行有限的命令，主要都是类似Ping这种基本的命令。

特权模式：Switch#，执行大部分的命令，在此模式下的操作权限比用户模式更高。

全局配置模式：Switch(config)#，全局配置模式，可对设备进行配置，例如，改名。

接口模式：SW1(config-if)#，接口配置模式，可对接口进行配置，例如，配置IP地址。Router(config)#interface e0/0

2. 常用操作

命令支持简写：例如，SW1#configure terminal = SW1#conf t

补全命令：Tab键

帮助：问号?

- show ?，指以show命令开头，后边能跟哪些命令
- s?，指以s开头的命令，有哪些

快捷键：

- 上翻命令：方向键上
- 下翻命令：方向键下
- 光标移到行首：Ctrl + a
- 光标移到行尾：Ctrl + e
- 返回特权模式：end

3. 常用命令

退出：exit，返回上一级

进入特权模式：SW1>enable

特权模式返回用户模式：SW1#disable

进入全局配置：SW1#configure terminal

改名：SW1(config)#hostname Sw1

查看当前配置：Sw1#show running-config （此命令只能在特权模式下执行，如果再其他模式下想要执行，前面加do）

保存命令：

- SW1#copy running-config startup-config
- SW1#write

进入接口模式：Router(config)#interface e0/0

配置IP地址：Router(config-if)#ip address 192.168.1.1 255.255.255.0

配置接口描述信息：R1(config-if)#description xxx

开启接口：Router(config-if)#no shutdown（思科设备中，所有三层接口，默认关闭）

查看系统版本：Router>show version

查看接口IP地址摘要信息：Router#show ip interface brief

查看接口详细信息：Router#show interface e0/0

设置特权模式密码：

- SW1(config)#enable password 12345（以明文形式在配置文件中显示，不够安全）
- SW1(config)#enable secret 12345（以密文形式在配置中文件中显示，比较安全）
- 同时配置以上密码，secret比password优先，会以secret密码为准

启用系统自带的加密功能：SW1(config)#service password-encryption（配置文件中所有的密码都会以密文显示，此加密方式容易被破解），关闭此功能后，对之后的操作不再加密，之前已经加密过的，不会解密。

Console线路认证：

密码认证：

SW1(config)#line console 0

SW1(config-line)#password 123

SW1(config-line)#login

用户名+密码认证：

SW1(config)#username user1 privilege 15 password 123

SW1(config)#line console 0

SW1(config-line)#login local

七、路由表

1. 查看路由表：show ip route

路由表项的含义：

每一横行称为一个路由条目，或者一条路由。

第一列：字母，表示这一条路由是如何进入到路由表当中的，即这条路由的来源。

- C：代表直连路由，路由器自己直连接口UP以后，感知到的路由。
- S：代表静态路由，管理员手工添加到路由表中的路由。
- R：代表动态路由协议RIP学习到的路由。
- O：代表动态路由协议OSPF学习到的路由。
- D：代表动态路由协议EIGRP学习到的路由。

第二列：目标网络及掩码，指明这一条的路由的目的地。

第三列：管理距离，简称AD。代表这条路由的优先级，用于比较不同路由协议，去往相同目的时使用，AD值越小越优先。

- C：0
- S：1
- R：120
- O：110
- D：90

第四列：度量值，用于比较同一协议，去往同一网络时使用。度量值数值越小越好，不同的协议的度量标准不同。

第五列：下一跳，指的数据包去往目标网络，下一次把包交给哪个地址。

第六列：时间，指学习到此路由，到查看路由表时，已存在的时间。

第七列：出接口，指去往目标网络，从哪个接口向外发送。

2. 路由器路由表中有多条路由可以去往相同目的地时，查表的顺序（依据）

1. 最长匹配原则，先选掩码长度最长的路由。
2. 如果掩码长度一样，再比较AD值，选小的。
3. 如果AD值一样，再比较度量值，选小的。
4. 如果以上都一样，则负载分担。

八、静态路由

1. 配置

Router(config)#ip route 目标网络 掩码 下一跳

举例：R1(config)#ip route 192.168.2.0 255.255.255.0 12.1.1.2

2. 静态路由负载分担

配置多个下一跳，实现路由的备份，提高冗余性、可靠性。

ip route 192.168.2.0 255.255.255.0 12.1.1.2
ip route 192.168.2.0 255.255.255.0 21.1.1.2

3. 浮动静态路由

通过修改某条静态路由的AD值，来实现路由备份，可以使流量在默认情况下走高速链路，当高速链路失效，走备用链路

ip route 192.168.2.0 255.255.255.0 12.1.1.2
ip route 192.168.2.0 255.255.255.0 21.1.1.2 10（管理距离）

4. 默认路由（缺省路由）

通常在企业出口路由器上配置缺省路由，指向运营商（ISP）。

ip route 0.0.0.0 0.0.0.0 21.1.1.2（下一跳）

去往任意网络，都将数据包发给下一跳地址。

当路由表中有明细路由时，按照明细路由转发，当没有明细路由时，按照默认路由转发。

5. 静态路由注意事项

配置静态路由有两种方法：

1. 指定下一跳，例如：ip route 192.168.2.0 255.255.255.0 12.1.1.2
2. 指定出接口，例如：ip route 192.168.2.0 255.255.255.0 s0/0

当接口是以太接口（e、fa、g），只能配置下一跳；当接口是串行接口（s口），可以配置下一跳，或出接口。

九、动态路由协议概念

AS：自治系统，由同一个组织机构管理的设备/协议的集合，例如：联通、电信。

1. 按作用范围分：

AS内：IGP，内部网关协议，RIP、OSPF、IS-IS、EIGRP

AS间：EGP，外部网关协议、BGP

2. 按算法分：

距离矢量路由协议：RIP、EIGRP

链路状态路由协议：OSPF、IS-IS

路径矢量路由协议：BGP

十、RIPv2

1. 特点

1. RIP称为路由信息协议，它是距离矢量路由协议，属于内部网关协议。
2. RIP适合小型网络，不适合大型网络。
3. RIP以跳数（hops）衡量去往目标网络的距离，每经过一台设备算作“1跳”，最大支持“15跳”，超过15认为网络不可达。
4. RIP的报文是UDP封装的，UDP端口号520代表RIP。
5. RIP有两种报文，请求（request），响应（response）
6. RIP周期性的发送更新，每隔30s一次。
7. RIPv1使用广播发送报文（255.255.255.255），RIPv2支持组播（224.0.0.9）和广播（兼容v1情况下）
8. 容易引起环路，通过水平分割，毒性逆转、触发更新等来防止环路：
    - 水平分割：从一个接口收到的路由，不会再从此接口发送回去。默认开启水平分割，如果开启毒性逆转，毒性逆转优先。
    - 毒性逆转：从一个接口收到的路由，将此路由的跳数设置为16（认为不可达），再发送回去。
    - 触发更新：当路由失效时，立即发送更新，而不等待计时器。
9. RIP有两个版本：
    - v1不支持VLSM、不支持认证功能，使用广播地址发送报文
    - v2支持VLSM、支持认证功能，支持组播和广播
10. RIP默认开启自动汇总，在不连续子网的情况下，需要关闭自动汇总
    - R1(config)#router rip
      R1(config-router)#no auto-summary （关闭自动汇总）

2. 配置

R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.1.0

network 接口的主网络号

比如：接口地址为192.168.1.1，则network 192.168.1.0；接口地址为10.1.1.1，则network 10.0.0.0

十一、OSPF

1. 特点

1. OSPF称为开放最短路径优先协议，它是链路状态路由协议，属于内部网关协议。
2. OSPF适合中大型网络。
3. OSPF支持划分多个区域，好处是减小LSDB，使计算更快，优化网络。
4. OSPF必须要有一个骨干区域，骨干区域号码为0，即Area 0就是骨干区域。如果有多个区域，要求非骨干区域必须和骨干区域直连。用于区域间防环。

5. OSPF的报文直接封装在IP报文中，协议号89。
6. OSPF使用组播地址：225.0.0.5、224.0.0.6
7. OSPF衡量目标网络的远近是以cost（开销）作为度量值的。cost与接口带宽有关，接口带宽越大，cost越小。

2. OSPF路由器角色

- IR：内部路由器，所有接口都属于一个区域的路由器，称为IR。
- BR：骨干路由器，至少有一个接口属于骨干区域的路由器，称为BR。
- ABR：区域边界路由器，同时属于两个或两个以上区域，且至少有一个接口属于骨干区域的路由器，称为ABR。
- ASBR：自治系统边界路由器，将OSPF域外的路由引入到了OSPF域内中，这台路由器称为ASBR。

3. OSPF工作原理

建立邻居 ----> 泛洪LSA，存放到LSDB ----> 通过LSDB使用SPF算法计算去往目标网络的最佳路径 ----> 将计算的最优的路径放入到路由表中

4. Router ID

在OSPF中，每台运行OSPF协议的路由器，都会有一个Router ID，Router ID要求每台设备唯一，不能重复，用于唯一标识OSPF路由器。

Router ID的格式是IPv4地址的格式，例如：1.1.1.1、2.2.2.2。

Router ID有两种方式生成：

1. 手工配置（推荐手工配置）
2. 自动选举（如果没有手工配置则自动选举）
    - 如果有虚拟接口（Loopback接口），则使用虚拟接口IP地址最大的，作为Router ID。
    - 如果没有虚拟接口，则使用物理接口IP地址最大的作为Router ID。

5. OSPF的邻居和邻接

邻居关系：路由器之间都知道对方的存在，但是LSDB还未同步。

邻接关系：路由器之间的LSDB已经同步。

6. OSPF的报文

- Hello：用于发现、建立、维护邻居关系。
- DBD：数据库描述，主从选举，数据库摘要信息（目录）。
- LSR：链路状态请求，用于请求链路状态通告（LSA）。
- LSU：链路状态更新，用于发送LSA。

- LSAck：链路状态确认，用于对消息的确认。

7. OSPF的开销

开销 = 参考带宽（100Mbit/s） ➗ 实际带宽

如果想修改开销，有两种方法：

- 直接修改接口开销（推荐）
- 修改参考带宽值，为了统一标准，所有路由器都要设置。（不推荐）

计算去往目标网络的开销值，只计算数据包沿途路径所有出接口开销之和。

8. DR、BDR

在MA（多路访问）网络中，由于OSPF路由器之间有多个邻居关系，如果全部发展成邻接关系（LSDB同步），会产生多余的、重复的LSA，为减少重复LSA泛洪，在MA网络中，需要选举DR、BDR。

DR：指定路由器

BDR：备份指定路由器，作为DR的备份

DR、BDR选举：

1. 先比较优先级（Hello报文中），优先级值默认为1，范围0-255，数值越大越好，0没有资格参选。
2. 如果优先级一样，则比较Router ID，选大的。
3. DR、BDR不能被抢占

9. OSPF配置

在配置OSPF时，需要用到通配符掩码，通配符掩码的作用是用于匹配的。

通配符掩码的格式和子网掩码的格式一样，都是点分十进制

- 1：代表不关心、不匹配
- 0：代表关心、匹配

```
router ospf 100
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
 network 12.1.1.1 0.0.0.0 area 0
 network 13.1.1.1 0.0.0.0 area 0
```

```
R1(config)#interface e0/1
R1(config-if)#ip ospf cost 5
```

十二、EIGRP

1. EIGRP特点

- EIGRP（增强内部网关路由协议）是思科私有协议，是距离矢量路由协议，无类路由协议（支持VLSM）。
- 支持多种网络层协议：IP、IPX、Apple Talk
- 直接封装在IP报文中，协议号88
- 使用AS的概念，AS基于接口定义，一台EIGRP路由器可与属于多个AS
- 支持组播和单播，组播地址224.0.0.10
- 使用DUAL算法，无环路，收敛快。
- 支持等价和非等价负载分担
- 减少带宽的占用
- 触发更新、部分更新、边界更新

2. 三张表

- 邻居表：和路由器建立邻居关系的路由器
- 拓扑表：包含路由器学习到达目的地的所有路由条目
- 路由表：最佳路径的路由表

3. 相关术语

- FD：可行距离，到达一个目的地的最小度量值
- AD/RD：通告距离/报告距离，邻居路由器所通告的它自己到达某个目的地的最小度量值
- FC：可行性条件，AD<FD，邻居路由器到达目的地的度量值必须小于本地路由器达到目的地的度量值
- Successor：后继路由器，是一个直连的邻居路由器，它满足FC，通过它具有到达目的地的最小度量值，是去往目的地的下一跳
- Feasible Successor：可行后继路由器，是一个邻居路由器，它满足FC，当主路由不可用时，FS用来代替主路由，当做备用路由。

4. EIGRP基本配置

R1(config)#router eigrp 100

R1(config-router)#network 12.1.1.1 0.0.0.0

R1(config-router)#network 1.1.1.1 0.0.0.0

十三、VLAN

1. VLAN概念

VLAN是虚拟局域网，作用主要是缩小二层广播域。

VLAN范围0-4095，最小值和最大值保留，可用范围是1-4094。

VLAN 1默认存在，所有接口默认都属于VLAN 1，VLAN 1无法删除、修改。

2. 链路类型

Access链路：用于连接主机、终端、服务器，在发送数据时，去掉VLAN tag。

Trunk链路：用于连接交换机，转发来自不同VLAN的数据帧，发送数据时要携带标记。

思科设备Trunk链路默认允许所有VLAN通过。

3. VLAN配置

- 创建VLAN：

  SW1(config)#vlan 10

  SW1(config)#vlan 10,20,30

  SW1(config)#vlan 10-20

- 划分接口到某个VLAN

  SW1(config)#interface vlan e0/1

  SW1(config-if)#switchport mode access

  SW1(config)#switchport access vlan 10

- 将接口配置为Trunk

  SW1(config)#interface vlan e0/0

  SW1(config-if)#switchport trunk encapsulation dot1q

  SW1(config)#switchport mode trunk

- 配置Trunk链路仅允许某些VLAN通过

  SW1(config)#interface e0/0

  SW1(config-if)#switchport trunk allowed vlan 10

  或

  SW1(config)#interface e0/0

  SW1(config-if)#switchport trunk allowed vlan 10,20

4. Native VLAN（本征VLAN）

Native VLAN是一个不打标记的VLAN，默认Native Vlan为VLAN 1。

本征VLAN通常配置成一个不使用的VLAN，提高网络安全性。

SW1(config)#interface e0/0

SW1(config-if)#switchport trunk native vlan 999

5. VLAN间通信

为解决不同VLAN、不同网段间的通信，常用的主要有：

1. 单臂路由，交换机连接路由器的接口配置为Trunk，路由器需要划分子接口，将子接口配置为不同VLAN的网关.
2. 三层交换，交换机通过配置SVI接口（交换虚拟接口），将SVI接口作为VLAN内主机的网关，实现不同VLAN间通信

十四、STP

1. 二层环路带来的问题

1. 广播风暴
2. 重复数据帧
3. MAC地址表抖动

2. STP的作用

STP既可以消除环路，又可以提供冗余。

STP通过一系列的计算、比较，最终在逻辑上阻塞某个接口（接口不转发数据）来消除环路；当可用链路失效，原先被阻塞的接口恢复转发，提供冗余。

3. STP计算

STP计算步骤：

1. 在整个二层网络中，选一台交换机作为根交换机（Root Bridge）
    - 每台运行STP的交换机都有一个桥ID（BID），BID = 优先级 + MAC地址
    - 优先级范围0-61440，默认值32768，数值越小越好，配置时只能是4096的倍数
    - MAC地址指的是交换机的背板MAC（主板的MAC，不是某个接口的MAC）
    - 比较BID来选举根交换机，先比较优先级，如果优先级一样再比MAC地址，选小的。
2. 在每台非根交换机上选一个端口，作为根端口（RP）
    - 根端口RP是距离根交换机最近的端口，距离跟开销（cost）有关，开销与带宽有关，带宽越大，开销越

小。

3. 在每条链路上选一个端口，作为指定端口（DP）
    - 先在每条链路上选一台交换机作为指定交换机，指定交换机是这条链路距离根最近的交换机，指定交换机再这条链路上的端口就是指定端口DP。
4. 没被选出来的接口，阻塞掉，为阻塞端口（AP）

4. STP报文

STP协议报文称为BPDU（桥协议数据单元）。

BPDU中有4个参数用于STP计算：

- RID：Root Bridge ID，指根交换机的BID
- RPC：Root Path Cost，到根累计开销之和
- BID：指定交换机的BID
- PID：Port，端口ID。端口ID由两部分组成，PID = 优先级 + 端口号，优先级默认值128，范围0-240，配置时只能为16的倍数。端口号即E0/1、E0/2。比较时先比优先级，优先级一样，再比端口号，越小越优先。

5. 常见问题

- 根交换机上的端口一定是DP么?

  答案：不一定，有可能是阻塞端口。

- RP的对端，一定是DP么?

  答案，一定，RP的对端一定是DP。

- DP的对端，一定是RP么?

  答案：不一定，DP的对端有可能是阻塞端口。

6. STP版本

公有：

STP：802.1D

RSTP：快速生成树，802.1w

MSTP：多生成树，802.1s

思科私有：

PVST+：每VLAN生成树，思科默认使用的STP版本。

RPVST+：快速每VLAN生成树。

7. STP端口状态

Disabled：禁用状态，指端口未启用，或未开启STP协议。

Blocking：阻塞状态，阻塞端口的最终状态。

Listening：侦听状态，确立端口角色。

Learning：学习状态，学习MAC地址，建立MAC地址表。

Forwarding：转发状态，转发数据。

从Lstening -- > Learning 要经历一个转发延时（Forward Delay）的时间，15s。

从Learning --> Forwarding要经历一个转发延时的时间，15s。

十五、EtherChannel

1. 链路聚合的优点

- 增大带宽
- 提供负载分担
- 提供链路冗余

2. 链路聚合的实现方法

- 动态协商：LACP协议、Pagp协议（思科私有协议）
- 手工配置：

3. 手工配置命令

SW1(config)#interface range e0/0 - 1

SW1(config-if-range)#shutdown

SW1(config-if-range)#channel-group 1 mode on

SW1(config)#interface Port-channel 1

SW1(config-if)#switchport trunk encapsulation dot1q

SW1(config-if)#switchport mode trunk

SW1(config)#interface range e0/0 - 1

SW1(config-if-range)#no shutdown

4. LACP配置命令

SW1(config)#interface range e0/0 - 1

SW1(config-if-range)#shutdown

SW2(config-if-range)#channel-group 1 mode active（或者passive）

SW1(config)#interface Port-channel 1

SW1(config-if)#switchport trunk encapsulation dot1q

SW1(config-if)#switchport mode trunk

SW1(config)#interface range e0/0 - 1

SW1(config-if-range)#no shutdown

十六、广域网

1. 广域网概念

WAN是一种运行地理范围比LAN更大的数据通信网络。要实现WAN，企业需要使用服务提供商或运营商（例如电话公司或有线网络公司）的设施。运营商可以将企业自己的各个位置互连，以及将其连接到其他企业的位置、外部服务和远程用户。WAN可传输多种类型的流量，例如语音、数据和视频。

2. WAN具有以下三个主要特征：

- WAN通常连接比LAN更大的地理区域中分布的设备。
- WAN使用运营商（例如电话公司、电缆公司、网络运营商）提供的服务。
- WAN使用各种类型的连接来在大范围地理区域内提供带宽访问能力。

3. PPP

PPP称为点对点协议，它是公有协议，是目前使用最多的广域网封装协议。（思科设备默认广域网接口封装协议为HDLC）

它能提供认证、地址协商等功能。

PPP共有两大组件：

- LCP：链路控制协议，负责链路的建立与拆除。
- NCP：网络控制协议，负责协商网络层的参数，例如：协商IP地址，协商对端接口的路由。

PPP链路建立过程：LCP --> 认证阶段（可选）--> NCP

4. 认证

PPP支持明文和MD5密文认证，明文认证使用的是PAP认证协议，密文认证使用CHAP认证协议。

明文认证PAP：由被认证方向认证方以明文形式发送用户名、密码，认证方进行认证，认证通过则链路可以建立。

密文认证CHAP：由被认证方向认证方以密文形式发送密码，认证方进行认证，认证通过则链路可以建立。

5. 配置

R1(config)#interface s1/0

R1(config-if)#encapsulation ppp

明文PAP认证配置：

- 认证方：

  R2(config)#username user1 password 123456

  R2(config)#interface s1/0

  R2(config-if)#ppp authentication pap
- 被认证方：

  R1(config)#interface s1/0

  R1(config-if)#ppp pap sent-username user1 password 123456

密文CHAP认证配置：

- 认证方：

  R2(config)#username user1 password 123456

  R2(config)#interface s1/0

  R2(config-if)#ppp authentication chap
- 被认证方：

  R1(config)#interface s1/0

  R1(config-if)#ppp chap hostname user1

  R1(config-if)#ppp chap password 123456

十七、访问控制列表

1. 概念

1. 访问控制列表简称ACL，是一种匹配流量的工具，可以用于流量过滤、流量选择。
2. ACL由一些列permit和deny语句组成
3. ACL按自上而下的顺序执行
4. 匹配上某条ACL后则执行相应动作，并停止进一步的匹配（不再向下匹配）
5. 在每个ACL的末尾都有一个隐式deny all语句
6. 默认第一条序号为10，第二条20，以此类推

2. ACL的种类

- 标准ACL：只能匹配数据包源IP地址，无法匹配目的IP、协议、端口等。
- 扩展ACL：不仅可以匹配数据包源IP地址，还能匹配目的IP、协议、端口等。

3. ACL的配置方法

- 编号：以编号形式创建ACL
    - 标准ACL：1-99，1300-1999
    - 扩展ACL：100-199，2000-2699
- 命名：以命名形式创建ACL，在创建ACL时定义标准或扩展

4. 部署原则

- 标准ACL在部署时，离目的越近越好
- 扩展ACL在部署时，离源越近越好
- ACL只能过滤穿越或到达自己的流量，不能过滤自己始发的流量

5. 配置：

- 需求1：

  R2(config)#access-list 1 deny host 10.1.1.2

  R2(config)#access-list 1 permit any

  R2(config)#interface e0/1

  R2(config-if)#ip access-group 1 out

- 需求2：配置之前，先清除需求1的配置

  Telnet配置：

  R3(config)#username user1 password 123

  R3(config)#line vty 0 4

R3(config-line)#login local

R3(config-line)#transport input all

ACL配置：

R3(config)#ip access-list extended TR3

R3(config-ext-nacl)# deny   icmp host 10.1.1.1 host 23.1.1.3 echo

R3(config-ext-nacl)# permit tcp host 10.1.1.1 host 23.1.1.3 eq telnet

R3(config-ext-nacl)# permit ip any any

R3(config)#interface e0/0

R3(config-if)#ip access-group TR3 in

测试：

R1#ping 23.1.1.3

R1#telnet 23.1.1.3

十八、NAT

1. NAT作用

NAT称为网络地址转换，它允许私网用户访问公网，通过将私网地址转换为单个或多个公网IP地址，

NAT的需求主要来自：

- IPv4地址空间有限，公网IP地址紧缺
- 私网地址在公网路由器上不能路由

2. NAT分类

- 静态NAT：一对一的转换，NAT转换表一直存在，可以由外向内主动发起访问
- 动态NAT：多对多的转换，NAT转换表动态产生，有一定老化时间，不能由外向内主动发起访问
- PAT：多对一的转换，不仅转换IP地址，还将端口号一起做转换，NAT转换表动态产生。可以做静态的端口转换，也可以做动态的端口转换。

3. NAT配置

- 配置Inside及Outside接口：

  R1(config)#interface e0/0

  R1(config-if)#ip nat inside

  R1(config)#interface e0/1

  R1(config-if)#ip nat outside

- 静态NAT配置：

  R1(config)#ip nat inside source static 192.168.1.1 200.1.1.11

- 动态NAT配置：

  R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255

  R1(config)#ip nat pool NAT 200.1.1.11 200.1.1.13 netmask 255.255.255.0

  R1(config)#ip nat inside source list 1 pool NAT

- PAT配置：

  R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255

  R1(config)#ip nat pool NAT 200.1.1.11 200.1.1.13 netmask 255.255.255.0

  R1(config)#ip nat inside source list 1 pool NAT overload

  或

  R1(config)#R1(config)#ip nat inside source list 1 interface e0/1 overload

  主要用于只有一个公网IP地址，或公网IP地址不固定的情况

- 查看及清空NAT转换表

  R1#show ip nat translations

  R1#clear ip nat translation *

十九、IPv6

1. IPv6地址格式

IPv6地址共128bit，使用十六进制数表示（每个16进制数为4bit），共分8段，每段之间用冒号“：”隔开。

IPv6地址分为网络前缀和接口ID，网络前缀类似IPv4地址的网络位，接口IP类似IPv4地址的主机位。

例：2001 : 0123 : 0000 : 0000 : 00CD : 34F0 : 0000 : 0132

地址压缩：

1. 每段的“前导0”可以省略
2. 连续多个0，可以省略为“::”，但是只能出现一次

例：2001 : 123 :: CD : 34F0 : 0 : 132

2. IPv6地址分类

单播：

组播：

任播：地址范围和单播地址范围一样，任播地址可以相同，理解任播实际上是一种服务，可以提供冗余、负载分担等功能。

- 全局单播：2000::/3，由互联网编号指派机构（IANA）分配并在公共网络上使用。它们等效于IPv4全局（公有）地址。
- 链路本地地址：fe80::/10，一个在接口上自动配置的IPv6地址，范围仅限于物理链路。
- 唯一本地地址：fc00::/7，唯一本地单播地址，类似于私有IPv4地址，它们用于本地通信。
- 环回地址：::1，类似127.0.0.1
- 未指定地址：::，未获取到地址

3. EUI-64规则

通过EUI-64规则，可以自动生成64bit的接口ID，步骤如下：

1. 将MAC地址的前24bit和后24bit中间，插入FF FE
2. 将高7位（从最高位数第7bit）由0变为1，由1变为0

4. 配置

R1(config)#ipv6 unicast-routing

R1(config)#interface e0/0

R1(config-if)#ipv6 enable

R1(config-if)#ipv6 address 2012::1/64

R1(config-if)#no shutdown

R1(config)#ipv6 route 3003::/64 2012::2

R1(config)#ipv6 route ::/0 2012::2

R1#ping ipv6 3003::3 source loopback 0

二十、思科设备管理

1. 设备硬件组成

- CPU
- 主板
- 接口
- 存储器
  - RAM：随机访问存储器，断电即丢失，用于存储路由器的当前运行配置文件（running config）。
  - NVRAM：非易失性随机访问存储器，断电保留，用于存储路由器启动配置文件（startup config）。
  - ROM：只读存储器，断电保留，初始化硬件并引导IOS软件，Mini OS（类似BIOS）。
  - Flash：闪存，断电保留，存储IOS镜像。

#####

2. 备份配置文件、系统（模拟器中路由器和交换都可以做，路由器2911，交换机2950T）

- 备份系统文件

  R1#copy flash: tftp:

  Source filename []? c2900-universalk9-mz.SPA.151-4.M4.bin

  Address or name of remote host []? 192.168.1.100

  Destination filename [c2900-universalk9-mz.SPA.151-4.M4.bin]?

- 备份配置文件
  R1#copy startup-config tftp:

  Address or name of remote host []? 192.168.1.100

  Destination filename [R1-confg]?

  Writing startup-config...!!

  [OK - 700 bytes]

3. 升级系统（模拟器中建议使用交换机来做）

- 下载新的镜像文件

  Switch#copy tftp: flash:
  Address or name of remote host []? 192.168.1.100
  Source filename []? c2950-i6q4l2-mz.121-22.EA8.bin
  Destination filename [c2950-i6q4l2-mz.121-22.EA8.bin]?

  Accessing tftp://192.168.1.100/c2950-i6q4l2-mz.121-22.EA8.bin...
  Loading c2950-i6q4l2-mz.121-22.EA8.bin from 192.168.1.100: !!!
  [OK - 3117390 bytes]

  3117390 bytes copied in 0.042 secs (74223571 bytes/sec)

- 删除旧的镜像文件

Switch#delete flash:c2950-i6q4l2-mz.121-22.EA4.bin
Delete filename [c2950-i6q4l2-mz.121-22.EA4.bin]?
Delete flash:/c2950-i6q4l2-mz.121-22.EA4.bin? [confirm]

- 重启设备

  Switch#reload
  System configuration has been modified. Save? [yes/no]:y
  Building configuration...
  [OK]
  Proceed with reload? [confirm]

4. 故障恢复（模拟器中使用路由器做）

路由器进入Mini OS系统：开机时，按Ctrl + c

交换机进入Mini OS系统：开机按住Mode键，大约13秒

rommon 1 > IP_ADDRESS=192.168.1.1
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > DEFAULT_GATEWAY=192.168.1.254
rommon 4 > TFTP_SERVER=192.168.1.100
rommon 5 > TFTP_FILE=c2900-universalk9-mz.SPA.151-4.M4.bin
rommon 6 > tftpdnld

5. 密码恢复

register：寄存器

0x2102：表示开机加载NVRAM Startup config

0x2142：表示开机不加载NVRAM Startup config

1. 重启设备，进入Mini OS
2. 修改寄存器值，并重启

   rommon 1 > confreg 0x2142

   rommon 2 > reset
3. 将Startup config复制到Running config

   R1#copy startup-config running-config
4. 删除或重置密码，并保存

   R1(config)#enable secret 123

或

R1(config)#no enable secret

5. 重启设备，进入Mini OS
6. 修改寄存器值，并重启

   rommon 1 > confreg 0x2102

   rommon 2 > reset