一 网络

1 什么是计算机网络

– 硬件方面:通过线缆将网络设备和计算机连接起来

– 软件方面:操作系统,应用软件,应用程序通过通信线路互连

– 实现资源共享、信息传递

2 计算机网络的功能

数据通信

资源共享

增加可靠性

提高系统处理能力

3 计算机网络发展阶段

60年代 ---- 分组交换

70年代-80年代 ----tcp/ip

90年代至今 ----web技术

4 网络标准

1）标准化组织

– ISO(国际标准化组织)

– ANSI(美国国家标准化局)

– ITU-T(国际电信联盟-电信标准部)

– IEEE(电气和电子工程师学会)

2）WAN与LAN

• 广域网(Wide-Area Network)

– 范围:几十到几千千米

– 作用:用于连接

远距离的计算机网络

– 典型应用:Internet

• 局域网(Local-Area Network)

– 范围:1km左右

– 作用:用于连接较短

距离内的计算机

– 典型应用:企业网,

校园网

5 网络拓扑结构

1）线缆连接计算机和网络设备的布局

– 点对点

– 星型及扩展的星型

– 网状

• 点对点拓扑结构

两台设备之间有一条单独的连接

专用的广域网中电路连接的两台路由器

• 星型拓扑

– 优点

易于实现

易于网络扩展

易于故障排查

– 缺点

中心节点压力大

组网成本较高

• 网状拓扑结构

– 一个节点与其他多个节点相连

– 提供冗余性和容错性

– 可靠性高

– 组网成本高

6 分层

1）OSI的七层框架功能

应用层 网络服务与最终用户的一个接口

表示层 数据的表示、安全、压缩

会话层 建立、管理、中止会话

传输层 定义传输数据的协议端口号,以及流控和差错校验

网络层 进行逻辑地址寻址,实现不同网络之间的路径选择

数据链路层 建立逻辑连接、进行硬件地址寻址、差错校验等功能

物理层 建立、维护、断开物理连接

2）TCP/IP五层

应用层

传输层

网络层

数据链路层

物理层

3）TCP/IP 常见协议

应用层：HTTP、https、FTP、TFTP、SMTP 、SNMP、DNS

传输层：TCP、UDP

网络层：ICMP、IGMP、IP、ARP

4）PDU（协议数据单元）

传输层 数据段 segment

网络层 数据包 packet

数据链路层 数据帧 frame

物理层 比特 bit

5）相应层次的设备

应用层 计算机

传输层 防火墙

网络层 路由器

数据链路层 交换机

物理层 网卡

二 物理层

1以太网接口

1）RJ-45

– RJ是描述公用电信网络的接口,常用的有RJ-11和RJ-45

RJ-45：计算机用的

RJ-11：电话用的

2）光纤接口

– 用以稳定地但并不是永久地连接两根或多根光纤的无源组件

FC 圆形带螺纹光纤接头

ST 卡接式圆形光纤接头

SC 方型光纤接头

LC 窄体方形光纤接头 （目前主流）

MT-RJ 收发一体的方型光纤接头

缺点：维护相对较麻烦

2双绞线TP

1）特点

8根线，两两缠绕

• 双绞线TP是目前使用最广,价格相对便宜的一

种传输介质

• 由两根绝缘铜导线相互缠绕组成,以减少对邻

近线对的电气干扰

• 由若干对双绞线构成的电缆被称为双绞线电缆

• 非屏蔽双绞线UTP和屏蔽双绞线STP

屏蔽双绞线STP：线外包裹一层金属网膜，用于电磁环境非常复杂的工业环境中

长度一般是150

2）双绞线的标准

类型 传输速率

cat5 100Mbps

cat5e 100Mbps 常用

cat6 1000Mbps(1Gbps) 常用

cat7 10000Mbps(10Gbps)

3）线缆的连接

• T568A:白绿、绿、白橙、蓝、白蓝、橙、白棕、棕

• T568B:白橙、橙、白绿、蓝、白蓝、绿、白棕、棕

– 标准网线

– 交叉网线

– 全反线 初次配置路由、交换机时使用，其他情况不用

• 其他情况:版本较新设备可以随意使用标准与交叉网线而不受限制,设备本身具备自动识别功能。

直通线：两端接口类型一样

交叉线：两端接口类型不一样

技巧：与交换机连接的都是直通线，其他都是交叉线

长度一般是150

楼与连接一般是双绞线

4）物理层的设备

• 网络接口卡

连接计算机和网络硬件

有一个惟一的网络节点地址

按照速率可分为10/100M、100/1000M自适应网卡

按照扩展类型可分为USB网卡、PCI网卡

按照提供的线缆接口类型可分为RJ-45接口网卡、光纤网卡等

• 中继器

– 放大信号

– 延长网络传输距离

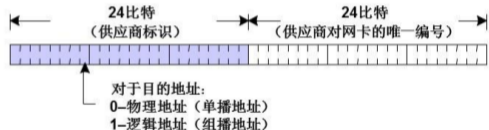
三 数据链路层

1 基础

1)MAC地址

作用：用来识别一个以太网上的某个单独的设备或一组设备

48位比特





2）数据帧

--单位

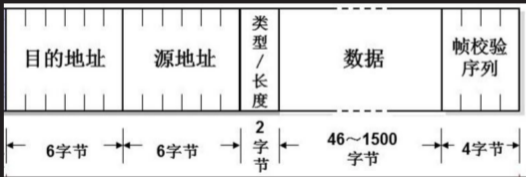
数据存储最小单位字节byte(B)

网速即传输单位为比特bit(b) ,比特流大量的0和1

1byte (字节) = 8bit (比特)

--作用

数据链路层的协议数据单元



标准数据帧： 46-1500字节

巨帧 ：大于1500字节 如150000字节

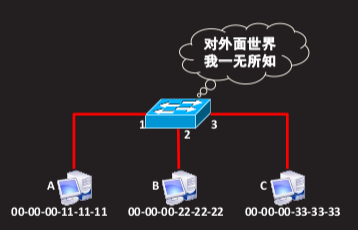
3）交换机

特点：交换机是用来连接局域网的主要设备

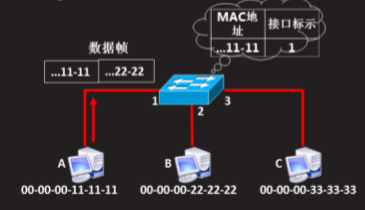
作用：交换机能够根据以太网帧中目标地址智能的转发数据,因此交换机工作在数据链路层

--交换机的转发原理

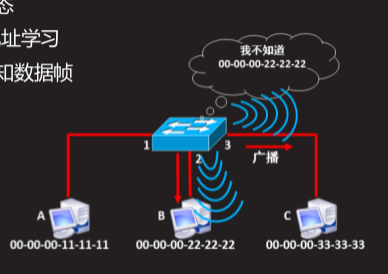
----初始状态



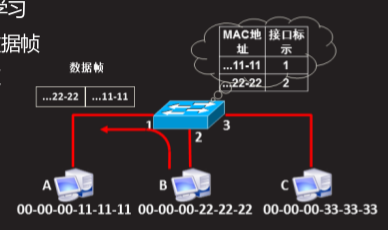
----MAC地址学习



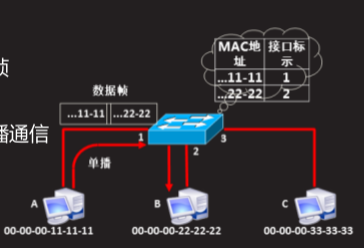
----广播未知数据帧



----接收方回应



----交换机实现单播通信



--总结

• 学习

– MAC地址表是交换机通过学习接收的数据帧的源MAC地址来形成的

• 广播

– 如果目标地址在MAC地址表中没有,交换机就向除接收到该数据帧的接口外的其他所有接口广播该数据帧

• 转发

– 交换机根据MAC地址表单播转发数据帧

• 更新

– 交换机MAC地址表的老化时间是300秒

– 交换机如果发现一个帧的入接口和MAC地址表中源MAC地址的所在接口不同,交换机将MAC 地址重新学习到新的接口

4）vlan基础

--什么是VLAN

Virtual LAN(虚拟局域网)是物理设备上连接的不受

物理位置限制的用户的一个逻辑组。

--为什么引入VLAN

交换机的所有接口默认属于同一个广播域

随着接入设备的增多,网络中广播增多,降低了网络的效率

为了分割广播域,引入了VLAN

特点：VLAN分割广播域

--作用

广播控制

增加安全性

提高带宽利用

降低延迟

--分类

基于接口划分的静态VLAN 常用

基于主机mac地址划分的动态VLAN

--vlan配置

vlan0-vlan4095 提示vlan0保留，vlan1默认已经创建

----创建vlan

sw1(config)#vlan vlan名称 创建vlan

sw1(config)#no vlan vlan名称 删除vlan

例子：

sw1(config)#vlan 2 创建2

----将接口加入到相应的vlan中

(config)# interface f0/1 进入接口0/1

sw1(config-if)#switchport access vlan vlan-id 添加接口到vlan

sw1(config-if)# no switchport access vlan vlan-id 删除vlan中的接口

sw1(config)# interface range f0/1 – 10 同时将多个接口添加到某个VLAN中

sw1(config-if-range)#switchport access vlan vlan-id 添加接口到vlan

sw1(config-if-range)# no switchport access vlan vlan-id 删除vlan中的接口

----验证vlan

sw1#show vlan brief 查看vlan信息

sw1#show vlan id vlan数字 查看指定vlan信息

5）trunk(中继链路)

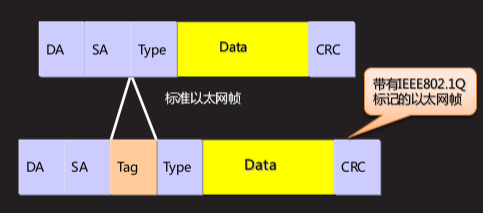
trunk 中继链路 承载多个vlan

acces 接入链路 承载1个vlan

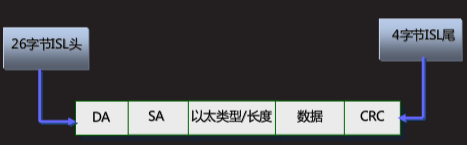
--VLAN标识的种类

ISL和802.1Q 的异同

--IEEE 802.1Q(标准，常用)



--ISL(Cisco私有协议)



• 相同点

都是显式标记,即帧被显式标记了VLAN的信息

• 不同点

IEEE 802.1Q是公有的标记方式,ISL是Cisco私有的

ISL采用外部标记的方法,802.1Q采用内部标记的方法

ISL标记的长度为30字节,802.1Q标记的长度为4字节

--配置

sw1(config)# interface range fastEthernet 0/1 – 2 要捆绑在一起的接口

sw1(config-if-range)#switchport mode trunk 设置为trunk模式

6）以太通道

--以太通道概述

• 也称为以太接口捆绑、接口聚集或以太链路聚集。英文名EtherChannel

• 以太通道为交换机提供了接口捆绑的技术,允许两个交换机之间通过两个或多个接口并行连接,同时传输数据,以提供更高的带宽和可靠性

--EtherChannel-以太通道作用

多条线路负载均衡,带宽提高

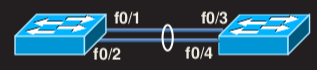
容错,当一条线路失效时,其他线路通信,不会丢包

--配置以太网通道

sw1(config)# interface range fastEthernet 0/1 – 2 要捆绑在一起的接口

sw1(config-if-range)#channel-group 1 mode on 创建组号为1的以太通道

sw1# show etherchannel summary 查看以太通道的配置



--以太通道配置指导原则

\*参与捆绑的接口必须属于同一个vlan,如果是在中继模式下,要求所有参加捆绑的接口都是在中继模式下

\*如果接口配置的是中继模式,那么应该在链路的两端将通道中的所有接口配置成中继模式

2 思科交换机命令

1）用户模式

Switch>

2 ）特权模式(一般用于查看配置信息)

Switch>enable

Switch#

3）全局配置模式(所做的配置对整个设备生效)

Switch#configure terminal

Switch(config)#

4 ）接口模式

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#

– interface:关键字

– fastethernet:接口类型

– 0/1:“0”表示模块号,“1”表示接口号

5）常见错误及解决

--命令错误

----真机

真机直接关掉DNS 查询 命令：sw1(config)#no ip domain-lookup

----模拟器

直接关掉DNS 查询 命令：sw1(config)#no ip domain-lookup

按ctrl + shift + 6

3 命令集合

1）用户模式

sw1>en 进入特权模式

提示：en => enable

2）特权模式

sw1#show mac-address-table 查看MAC地址表

sw1#configure terminal 进入全局配置模式

sw1#w 保存当前配置

提示：w => wite => copy running-config startup-config

sw1#show running-config 查看当前配置

sw1#reload 重启

sw1# erase startup-config 恢复设备出厂默认值(清空startup-config )

3） 全局配置模式

sw1(config)#hostname 名称 修改主机名称

sw1(config)#no ip domain-lookup 配置禁用DNS查询

sw1(config)#enable password 密码 设置进入密码

--控制台消息打断输入的命令

sw1(config)#line console 0 进入line

sw1(config-line)#logging synchronous 配置输出日志同步

sw1(config-line)#exec-timeout 0 0 配置控制台会话的时间，分 秒 0 0：永不超时

4）接口模式

四 网络层

转发对象：数据包

1 网络层基础

1）网络层的功能

定义了基于IP协议的逻辑地址

连接不同的媒介类型

选择数据通过网络的最佳路

2）ICMP协议

• ICMP通过IP数据报传送,用来发送错误和控制信息

• ICMP定义了很多信息类型,例如:

– 目的地不可达

– TTL 超时

– 信息请求

– 信息应答

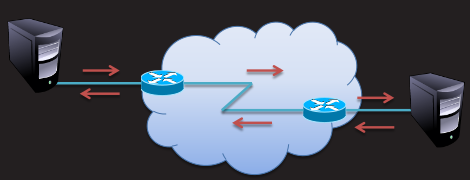
– 地址请求

– 地址应答

• ICMP检测双向通路的连通性

• Ping命令使用ICMP协议

– Ping [-t] [-l 字节数] 目标IP或主机名



• 常见的ping反馈结果

– 连接建立成功,Reply from 目标地址 .. ..

– 目标主机不可达,Destination host unreachable.

– 请求时间超时,Request timed out.

3）ip地址基础

A类：1-127 255.0.0.0

B类：128-191 255.255.0.0

C类：192-223 255.255.255.0

网络位 主机位

192.168.0.0/24 网络ID

192.168.0.255/24 广播地址

2路由器基础

1）什么是路由

--将数据包从一个网络发送到另一个网络

需要依靠路由器来完成

路由器只关心网络的状态,决定最佳路径

2）路由器怎么工作

隔离广播

--主要完成下列事情

\*识别数据包的目标IP地址

\*识别数据包的源IP地址(主要用于策略路由)

\*在路由表中发现可能的路径

\*选择路由表中到达目标最好的路径

\*维护和检查路由信息

--根据路由表选择最佳路径

\*每个路由器都维护着一张路由表,这是路由器转发数据包的关键

\*每条路由表记录指明了:到达某个子网或主机应从路由器的哪个物理接口发送,通过此接口可到达该路径的下一个路由器的地址(或直接相连网络中的目标主机地址)

3）如何获得路由表

--静态、默认路由

由管理员在路由器上手工指定

适合分支机构、家居办公等小型网络

--动态路由

根据网络拓扑或流量变化,由路由器通过路由协议自动设置

适合ISP服务商、广域网、园区网等大型网络

4）静态路由

--主要特点

由管理员手工配置,为单向条目

通信双方的边缘路由器都需要指定,否则会导致数据包有去无回

--配置静态路由

----直连路由C

命令：

rt1(config)# in g0/0 #进入该接口

rt1(config-if)#ip address 192.168.1.1 255.255.255.0 #配置路由接口地址

rt1(config-if)#no shutdown #开启路由接口

----静态路由S

使用 ip route 命令-->指定到达IP目的网络

基本格式:Router(config)#ip route 目标网络ID 子网掩码 下一跳

例子：

----默认路由

默认路由是一种特殊的静态路由

默认路由的目标网络为 0.0.0.0 0.0.0.0,可匹配任何目标地址

只有当从路由表中找不到任何明确匹配的路由条目时,才会使用默认路由,一般在企业网关出口使用

5）动态路由

--动态路由

基于某种路由协议实现

--动态路由特点

减少了管理任务

占用了网络带宽

--动态路由协议OSPF

全称为Open Shortest Path First ( 开放式最短路径优先)

适合大中型网络使用

• 邻居列表

• 链路状态数据库

• 路由表

• OSPF区域

– 为了适应大型的网络,OSPF在网络内部划分多个区域

– 每个OSPF路由器只维护所在区域的完整链路状态信息

• 区域ID

– 区域ID可以表示成一个十进制的数字

– 也可以表示成一个IP

• 骨干区域Area 0

– 负责区域间路由信息传播

--OSPF基本配置

----启动OSPF路由进程

Router(config)# router ospf process-id

----指定OSPF协议运行的接口和所在的区域

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

--路由器向下宣告默认路由

Router(config-router)#default-information originate

3.三层交换机

1）虚接口概述

在三层交换机上配置的VLAN接口为虚接口

使用SVI(交换虚拟接口)实现VLAN间路由

Switch(config)# interface vlan vlan-id 虚接口的引入使得应用更加灵活

2）三层交换机的配置

• 创建所需VLAN

• 为每个VLAN配置IP地址

• 启用SVI接口

• 启用三层交换机的IP路由功能

• 如果需要,配置三层交换机的动态或静态路由

--命令

----启用路由功能

Switch(config)# ip routing #在三层交换机启用路由功能

----配置虚接口的IP

Switch(config)# interface vlan vlan-id

Switch(config-if)# ip address ip\_address netmask

Switch(config-if)# no shutdown

提示：三层交换机接口转路由接口(思科设备专属) ，其他华为等交换机不支持，还是要配置虚拟接口ip

Switch(config-if)#no switchport

– 在三层交换机上配置Trunk并指定接口封装为802.1q

Switch(config)#interface fastEthernet 0/24

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#switchport mode trunk

--三层交换机上的路由接口

三层交换机的物理接口默认是二层接口

可以转换为三层接口

转换为三层接口后,该接口不属于任何VLAN

可以像路由器接口一样使用

五 传输层

1基础

1）传输层的作用

网络层提供点到点的连接

传输层提供端到端的连接

2）传输层的协议

--TCP(Transmission Control Protocol)

传输控制协议

可靠的、面向连接的协议

传输效率低

--UDP(User Datagram Protocol)

用户数据报协议

不可靠的、无连接的服务

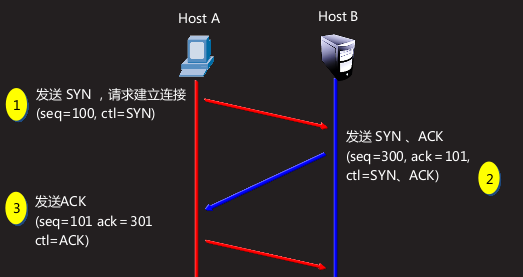
传输效率高

2 TCP

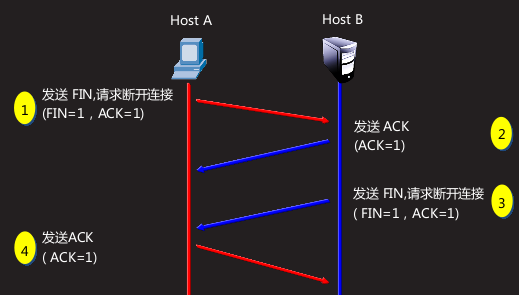
1)TCP的封装格式



2)TCP的连接-三次握手



2)TCP的四次断开



3 UDP

1)UDP的封装格式



2)UDP的应用



2)UDP的流控和差错控制

UDP缺乏可靠机制

UDP只有校验和来提供差错控制

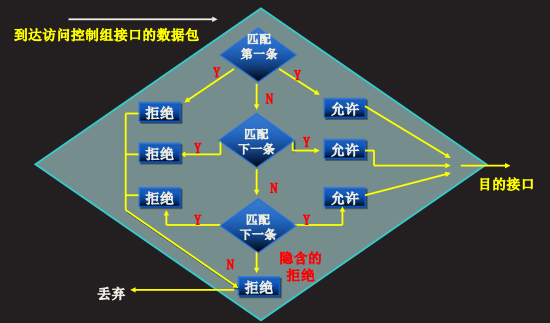
4 ACL

--访问控制列表(ACL)

读取第三层、第四层 头部信息

根据预先定义好的规则对数据进行过滤

--访问控制列表的处理过程



--访问控制列表的类型

----标准访问控制列表

基于源IP地址过滤数据包

标准访问控制列表的访问控制列表号是1~99

----扩展访问控制列表

基于源IP地址、目的IP地址、指定协议、端口来过滤数据包

扩展访问控制列表的访问控制列表号是100~199

--标准访问控制列表的配置

Router(config)#access-list access-list-number { permit | deny } source [ source-wildcard ] 创建ACL

例子：允许192.168.1.0/24和主机192.168.2.2的流量通过

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

Router(config)# access-list 1 permit 192.168.2.2 0.0.0.0

隐含的拒绝语句

Router(config)# access-list 1 deny 0.0.0.0 255.255.255.255

--将ACL应用于接口

Router(config-if)# ip access-group access-list-number {in|out} 将ACL应用于接口

Router(config-if)# no ip access-group access-list-number {in |out} 在接口上取消ACL的应用

Router(config)# Show access-lists 查看访问控制列表

Router(config)# no access-list access-list-number 删除ACL

--扩展访问控制列表的配置

创建ACL

Router(config)# access-list access-list-number { permit | deny } protocol { source source-wildcard destination destination-wildcard } [ operator operan ]

例子：

Router(config)# access-list 101 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 80

Router(config)# access-list 101 permit ip any any

提示：1、拒绝192.168.1.0/24网段访问192.168.2.2的web(tcp 80)服务

2、允许所有主机访问所有主机的所有服务

5 NAT

1）基础

Network Address Translation,网络地址转换

--作用

通过将内部网络的私有IP地址翻译成全球唯一的公网IP地址,使内部网络可以连接到互联网等外部网络上。

--IP地址分类

A类： 1-127 255.0.0.0

B类： 128-191 255.255.0.0

C类： 192-223 255.255.255.0

网络位 主机位

192.168.0.0/24 网络ID

192.168.0.255/24 广播地址

私有IP地址分类:

A类 10.0.0.0~10.255.255.255

B类 172.16.0.0~172.31.255.255

C类 192.168.0.0~192.168.255.255

--NAT的优点

节省公有合法IP地址

处理地址重叠

安全性

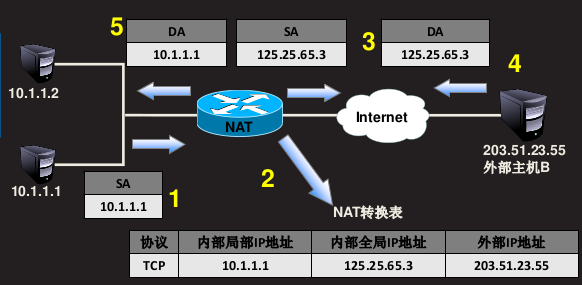
--NAT的缺点

延迟增大

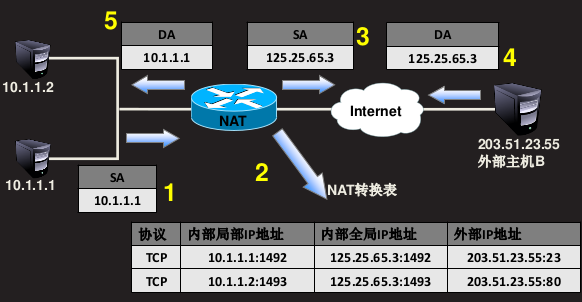
配置和维护的复杂性

--NAT实现方式

静态转换(Static Translation) ------服务器



端口多路复用(Port Address Translation,PAT) ----------员工



2）静态转换

IP地址的对应关系是一对一,而且是不变的,借助静态转换,能实现外部网络对内部网络中某些特设定服务器的访问

--静态NAT配置步骤

接口IP地址配置

决定需要转换的主机地址

决定采用什么公有地址

在内部和外部接口上启用NAT

--设置外部接口的IP地址:

Router(config)#interface g0/1

Router(config-if)#ip address 100.0.0.1 255.0.0.0

Router(config-if)#no shut

--设置内部接口的IP地址:

Router(config)#interface g0/0

Router(config-if)#ip address 192.168.1.254 255.255.255.0

Router(config-if)#no shut

--建立静态地址转换

Router(config)#ip nat inside source static 192.168.1.1 100.0.0.2

--在内部和外部接口上启用NAT

Router(config)#interface g0/1

Router(config-if)#ip nat outside

Router(config)#interface g0/0

Router(config-if)#ip nat inside

--NAT端口映射配置

用途：控制外网访问内网服务

例子：

Router(config)#ip nat inside source static tcp 192.168.1.6 80 61.159.62.133 80

3）端口多路复用PAT

--PAT(端口多路复用)

通过改变外出数据包的源IP地址和源端口并进行端口转换,内部网络的所有主机均可共享一个合法IP地址实现互联网的访问,节约IP。

--PAT配置步骤

接口IP地址配置

使用访问控制列表定义哪些内部主机能做PAT

确定路由器外部接口,在内部和外部接口上启用NAT

–定义内部ip地址

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

–设置复用动态IP地址转换

Router(config)#ip nat inside source list 1 interface g 0/1 overload

--在内部和外部接口上启用NAT

Router(config)#interface g0/1

Router(config-if)#ip nat outside

Router(config)#interface g0/0

Router(config-if)#ip nat inside

--跟踪NAT

R1#debug ip nat debug ip nat命令跟踪NAT操作

R1#undebug ip nat

6 网络检测命令

1)ping

2)traceroute

路由跟踪，检测网络中出现问题的节点

3）arp

linux： arp #查看mac地址

windows：arp -a  #查看mac地址

六 常见网络问题

1 STP生成树算法

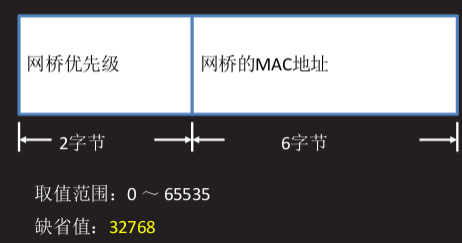
作用：解决广播风暴

1）STP简介

STP - Spanning Tree Protocol(生成树协议)逻辑上断开环路,防止广播风暴的产生当线路故障,阻塞接口被激活,恢复通信,起备份线路的作用

2）网桥ID(BID)

网桥ID是唯一的,交换机之间选择BID值最小的交换机作为网络中的根网桥



提示：必须是4096的倍数，32768是默认值

3）基本配置

--启用生成树命令(默认开启)

Switch(config)#spanning-tree vlan vlan-list

--指定根网桥

Switch(config)#spanning-tree vlan vlan-list priority Bridge-priority 实际中使用

或

Switch(config)#spanning-tree vlan vlan-list root { primary| secondary } 没有修改过网络中有效

--查看生成树的配置

Switch#show spanning-tree

--查看某个VLAN的生成树详细信息

Switch#show spanning-tree vlan vlan-id

4）PVST+

PVST+ ：每vlan生成树

--PVST+配置的意义

配置网络中比较稳定的交换机为根网桥

利用PVST+实现网络的负载分担

2 HSRP

ttl=1

1）概念

--热备份路由选择协议

HSRP(Hot Standby Routing Protocol)

HSRP ----思科私有

VRRP ----公有，华为设备，H3C能有

2）HSRP原理

3）HSRP的配置命令

--配置为HSRP的成员

Switch(config-if)#standby group-number ip virtual-ip-address #进入vlan配置,虚拟网关

--配置HSRP的优先级

Switch(config-if)#standby group-number priority priority-value

priority-value：范围0~255,默认100 越大优先级越高

--HSRP占先权配置

Switch(config-if)#standby group-number preempt #当本身优先级大于其他设备时立刻抢占活跃路由器身份，设置这项会立刻抢占

--查看HSRP摘要信息

Switch(config-if)#show standby brief

--查看HSRP信息

MS2#show standby brief