计算机网络的功能

数据通信、资源共享、增加数据可靠性、提高系统处理能力

计算机网络的发展

60年代:分组交换

70-80年代:TCP/IP

90年后:Web技术

标准：一致同意的规则

ISO（国际标准化组织）在网络通信中创建了OSI（开放系统互联）模型。

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）

按照网络规模和使用范围分类为

WAN：广域网 LAN:局域网

网络设备

交换机、路由器

网络设备生产厂商：cisco思科，华为。

网络拓扑结构

1. 点对点

两台设备之间有一条单独的连接，通常用于广域网连接

1. 星型拓扑
2. 优点：易于实现、易于网络扩展、易于故障排查
3. 缺点：中心节点压力大、组网成本较高

3、网型拓扑结构

1. 各个节点至少与其他两个节点相连
2. 可靠性高、组网成本高

OSI

1. 国际标准化组织（ISO）

开放系统互连参考模型OSI

OSI是一个开放式体系结构，它规定将网络分为七层

2、协议分层

为了降低网络设计的复杂性，将协议进行了分层设计

应用层：网络服务与最终用户的一个接口

表示层：数据的表现形式，如加密、压缩。

会话层：建立、管理、中止会话，例如断点续传。

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通信。

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。

TCP/IP协议族的组成

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

传输层：TCP、UDP

网络层：ICMP、IGMP、IP、ARP

PDU（协议数据单元）

传输层 段 segment

网络层 包 packet

数据链路层 帧 frame

物理层 比特 bit

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

接口

以太网接口：

RJ-45水晶头

光纤接口：

FC 、ST、SC

LC 窄体方形光纤接头（目前主流）

MT-RJ

双绞线

1. 双绞线分类：

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

非屏蔽双绞线 （UTP）

1. 双绞线标准与分类 ：

Cat5五类双绞线，适用于100Mbps的网络

Cat 5e衰减更小，适用于100Mbps的网络，串扰更少，性能优于5类线 （超五类）

Cat 6适用于1000Mbps的网络

Cat 7适用于10000Mbps的网络

4、双绞线的连接规范

1）线序

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

2）线缆的连接：

标准网线（直连线或直通线）：用于连接不同设备（A-A，B-B）

交叉网线：用于连接相同设备 （A-B）

全反线 ：不用于以太网的连接，主要用于计算机的串口和路由器或交换机的console（控制口）相连

例外情况：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。

5、物理层设备

网卡、中继器

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

交换机的工作模式：

Switch>用户模式

Switch>enable

Switch#特权模式

Switch#configure terminal

Switch(config)#全局配置模式

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#接口模式

exit返回上一模式

end直接退到特权模式

命令输入错误被卡住时同时按键盘ctrl+shift+6这三个按键

常用命令：

Switch(config)#hostname S1修改主机名为S1

Switch#show running-config查看配置信息

配置enable明文口令

全局配置模式：enable password *123*

保存交换机的配置

特权： copy running-config startup-config

或 write

恢复设备出厂默认值

特权：erase startup-config

重启：reload

设备配置的准备工作

空闲一段时间后，重回初始界面的问题

switch(config)#line con 0

switch(config-line)#exec-timeout 0 0

配置输出日志同步

Switch(config)#line console 0

Switch(config-line)#logging synchronous

禁用DNS查询

switch(config)#no ip domain-lookup

数据链路层

MAC地址

用来识别一个以太网上的某个单独的设备或一组设备

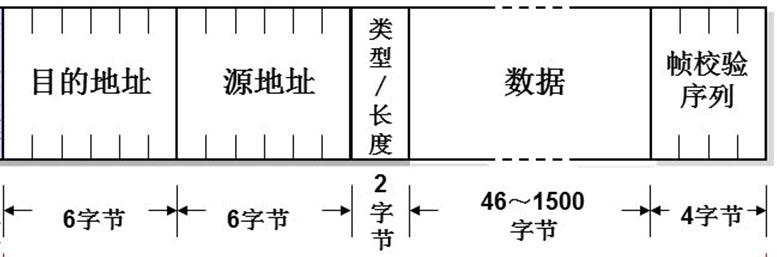
MAC地址长度48位(6个字节)，前24位代表厂商，后24位代表网卡编号，

MAC 地址的第8位为0时表示该MAC地址为单播地址，为1时表示组播地址。48位都为1表示广播地址。

Ipconfig /all 查看MAC地址

注：一块物理网卡的地址一定是一个单播地址，也就是第8位一定为0

数据链路层的帧格式



交换机

1、交换机是用来连接局域网的主要设备，可以实现数据帧的转发

2、交换机的工作原理

学习，广播，转发，更新

3、广播域

广播域指接收同样广播消息的节点的集合，交换机的所有端口默认属于同一个广播域

交换机的基本配置

1、常用命令

1）查看MAC地址表

特权：show mac-address-table

1. 什么是VLAN

虚拟局域网

1. VLAN的优势

广播控制、安全性、带宽利用、延迟

创建VLAN的方法

在全局配置模式中：vlan 2（创建vlan2）

Name 名字（给vlan2命名）

接口加入vlan

1）进入将要加入vlan的接口然后输入

switchport access vlan 3

2）、同时将多个接口加入vlan 2

全局： interface range f0/1 – 10

switchport access vlan 2

5、查看vlan信息

特权：show vlan brief

trunk中继链接

1、作用：实现交换机之间的单一链路传递多个vlan的信息

2、链路类型：

接入链路(access): 可以承载1个 vlan

中继链路(trunk)：可以承载多个 vlan

3、vlan的标识

1）ISL(cisco私有的标记方法)

2）IEEE 802.1q(公有的标记方法)

4、trunk的配置

接口模式：switchport mode trunk(配置为中继链路)

5、查看接口模式

特权模式：show interface f0/5 switchport

EthernetChannel（以太网通道）

1、功能：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

2、以太网通道的配置：

全局：interface range f0/6 – 8

switchport mode trunk

channel-group 1 mode on

查看以太网通道的配置： show etherchannel summary

路由器原理及静态路由

1、路由

跨越从源主机到目标主机的一个互联网络来转发数据包的过程

2、路由表

路由器根据路由表做路径选择

3、路由表的获得

1）、直连路由：配置IP地址，端口UP状态，形成直连路由。

2）、非直连网段：需要静态路由或动态路由，将网段添加到路由表中。

4、静态路由

1）、特点：

由管理员手工配置的，是单向的，因此需要在两个网络之间的边缘路由器上需要双方对指，否则就会造成流量有去无回，缺乏灵活性，适用于小型网络。

2)、配置

全局模式：

ip route 目标网络ID 子网掩码 下一跳IP

缺省路由（默认路由）

缺省路由是一种特殊的静态路由

简单地说,缺省路由就是在没有找到任何匹配的具体路由条目的情况下才使用的路由，适用于只有一个出口的末节网络（比如企业的网关出口）

全局:ip route 0.0.0.0 0.0.0.0 下一跳

查看路由表

特权：show ip route

C直连路由

S静态路由

S\*默认路由

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

三层交换技术

1、作用

使用三层交换技术实现VLAN间通信

三层交换=二层交换+三层转发

2、虚拟接口（SVI）

三层交换机上配置的VLAN接口为虚接口

3、三层交换机的配置

1）、在三层交换机启用路由功能

全局：ip routing

2）、配置虚拟接口的IP 地址

全局：interface vlan  *1*

ip address  *192.168.2.254 255.255.255.0*

no shutdown

3）在三层交换机上配置Trunk并指定接口封装为802.1q

接口模式：switchport trunk encapsulation dot1q

switchport mode trunk

4）、配置路由接口

进入接口：no switchport

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

动态路由

1、动态路由特点

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, 减少了管理任务，但占用了网络带宽

适合ISP服务商、广域网、园区网等大型网络

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

OSPF协议

* Open Shortest Path First ( 开放式最短路径优先）
* OSPF区域
  + 为了适应大型的网络，OSPF在AS内划分多个区域
  + 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

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*

TCP和UDP协议

1、TCP

传输控制协议

可靠的、面向连接的协议

传输效率低

2、UDP

用户数据报协议

不可靠的、无连接的服务

传输效率高

1. TCP的三次握手与四次断开

TCP的应用

|  |  |  |
| --- | --- | --- |
| 端口 | 协议 | 说　　明 |
| 21 | FTP | FTP服务器所开放的控制端口 |
| 23 | TELNET | 用于远程登录，可以远程控制管理目标计算机 |
| 25 | SMTP | SMTP服务器开放的端口，用于发送邮件 |
| 80 | HTTP | 超文本传输协议 |
| 53 | DNS | 域名服务，当用户输入网站的名称后，由DNS负责将它解析成IP地址，这个过程中用到的端口号是53 |

三、UDP

1、UDP首部格式

|  |  |
| --- | --- |
| 源端口号（16） | 目标端口号（16） |
| UDP长度（16） | UDP校验和（16） |

UDP长度：用来指出UDP的总长度

校验和：用来完成对UDP数据的差错检验，它是UDP协议提供的唯一的可靠机制

2、UDP端口及应用

|  |  |  |
| --- | --- | --- |
| 端口 | 协议 | 说明 |
| 69 | TFTP | 简单文件传输协议 |
| 123 | NTP | 网络时间协议 |
| 53 | DNS | 域名服务 |

3、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

需要上层协议来提供差错控制：例如TFTP协议

访问控制列表概述

1、访问控制列表（ACL）：

读取第三层、第四层包头信息

根据预先定义好的规则对包进行过滤

1. 访问控制列表的处理过程

如果匹配第一条规则，则不再往下检查，路由器将决定该数据包允许通过或拒绝通过。

如果不匹配第一条规则，则依次往下检查，直到有任何一条规则匹配。

如果最后没有任何一条规则匹配，则路由器根据默认的规则将丢弃该数据包。

3、访问控制列表的类型：

1. 标准访问控制列表

基于源IP地址过滤数据包

列表号是1～99

1. 扩展访问控制列表

基于源IP地址、目的IP地址、指定协议、端口等来过滤数据包

列表号是100～199

二、标准访问控制列表

1、标准访问控制列表的创建

全局：access-list 1 deny 192.168.1.1 0.0.0.0

全局：access-list 1 permit 192.168.1.0 0.0.0.255

通配符掩码：也叫做反码。用二进制数0和1表示，如果某位为1，表明这一位不需要进行匹配操作，如果为0表明需要严格匹配。

隐含拒绝语句：

access-list 1 deny 0.0.0.0 255.255.255.255

1. 将ACL应用于接口

接口模式：ip access-group 列表号 in或out

注：access-list 1 deny 192.168.1.1 0.0.0.0或写为

access-list 1 deny host 192.168.1.1

access-list 1 deny 0.0.0.0 255.255.255.255或写为

access-list 1 deny any

1. 删除已建立的访问控制列表

全局：no access-list 列表号

1. 接口上取消ACL

接口模式：no ip access-group 列表号in 或out

1. 查看访问控制列表

特权：show access-lists

5、删除ACL

全局：no access-list 列表号

注：不能删除单条ACL语句，只能删除整个ACL。

1. NAT（网络地址转换）
2. 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。
3. 优点：

节省公有合法IP地址

处理地址重叠

安全性

3、NAT的缺点

延迟增大

配置和维护的复杂性

4、NAT实现方式

1. 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：

配置接口IP及路由

全局：

Ip nat inside source static 192.168.1.1 61.159.62.131

在内外接口上启用NAT：

出口配置：ip 　nat 　outside

入口配置：ip 　nat 　inside

1. 端口多路复用（PAT）

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的配置：

全局：ip nat inside source list 1 interface f0/1 overload

5、NAT两种实现方式的区别：

静态转换的对应关系一对一且不变，并且没有节约公用IP，只隐藏了主机的真实地址。

端口多路复用可以使所有内部网络主机共享一个合法的外部IP地址，从而最大限度地节约IP地址资源。

开启nat排错功能

Router#debug ip nat

S表示源地址

D表示目的地址

192.168.1.2->61.159.62.130表示将192.168.1.2转换为61.159.62.130

关闭nat排错功能

Router#undebug ip nat

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

选择根网桥

选择交换网络中网桥ID最小的交换机成为根网桥，网桥ID是一个八字的字段，前两个字节十进制数为网桥优先级，后六个字是网桥的MAC地址，优先级小的被选择为根网桥，如优先级相同则MAC地址小的为根网桥。

网桥优先级的取值范围0-65535默认值为32768

查看交换机mac地址

Switch#show version

Base ethernet MAC Address : 0001.9751.0467

VLAN与STP（生成树）之间的关系：

PVST+（增强的每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

四、PVST+的配置命令

1、启用生成树命令 (此命令可以不用输入，默认交换机会开启)

全局：spanning-tree vlan 2

2、指定根网桥（主根或次根）

改优先级

全局：spanning-tree vlan  *1*  priority *优先级的值*

注意： 优先级的值是4096的倍数；

或者在全局模式（推荐此方式）：spanning-tree vlan  *2*  root primary

spanning-tree vlan  *2*  root secondary

3、查看某个vlan的生成树的配置

特权：show spanning-tree vlan 1

Root ID Priority 20481 表示根网桥的优先级

Bridge ID Priority 24577 表示当前设备的优先级

BLK 表示阻塞接口

FWD 表示转发接口

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

一、热备份路由选择协议（HSRP）

1. 作用：Cisco私有协议 ，确保了当网络边缘设备或接入链路出现故障时，用户通信能迅速并透明地恢复，以此为IP网络提供冗余性。通过使用同一个虚拟IP地址和虚拟MAC地址，LAN网段上的两台或者多台路由器可以作为一台虚拟路由器对外提供服务。HSRP使组内的cisco路由器能互相监视对方的运行状态。（Cisco私有协议）

2、HSRP组成员

活跃路由器、备份路由器、虚拟路由器（即该lan上的网关）、其他路由器

HSRP的配置

1、配置为HSRP的成员

进入路由器的网关接口

standby 1 ip 虚拟网关IP

2、配置HSRP的优先级

standby *1*  priority *优先级*

*优先级范围0-255，默认为100*

3、查看HSRP摘要信息

特权： show standby brief

4、HSRP端口跟踪

standby 1 track f0/1

5、HSRP占先权

standby *1*  preempt