# 计算机网络

## 什么是计算机

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,应用系统,应用程序通过通信线路互连

实现资源共享,传递信息

## 计算机网络的功能

数据通信:pokemon中玩家之间交换精灵

资源共享:pokemon玩家共享强力队伍

增加可靠性:热备份技术可以防止设备损坏导致网络崩溃

提高系统处理能力:使用集群技术用多台设备同时处理一个事物

## 计算机网络的发展阶段

60年代

分组交换:我一次无法传输太大的文件于是我把它分成很多份分开运输

70-80年代

TCP/IP 统一天下的协议 让天下的绝大部分设备

90年代

Web技术

## 网络标准

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)

## WAN与LAN

广域网(Wide-Area Network)

--范围:几十到几千千米

--作用:用于连接远程的计算机网络

--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

# 网络设备及拓扑

## 网络设备生产商

Cisco(思科)

华为

## 网络设备

交换机

路由器

## 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

2、星型拓扑

1）优点：易于实现、易于网络扩展、易于故障排查

2）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

# 网络通信参考模型

## 网络分层

网络通信的过程很复杂

数据以电子信号的形式穿越介质到达正确的计算机然后转换成最初的形式,一边接受者能够阅读

为了降低网络设计的复杂性,将协议进行了分层设计

## OSI

国际标准化组织(ISO)

开放系统互联参考模型OSI

OSI是一个开放式体系结构,它规定将网络分为七层

协议分层

应用层

表示层

会话层

传输层

网络层

数据链路层

物理层

物理层:建立,维护,断开物理连接,定义了接口及介质,实现了比特流的传输。

数据链路层:建立逻辑链接,进行硬件地址寻址,差错校验等功能,通过 mac 地址实现数据的通信,帧包装,帧传输,帧同步。交换机工作在数据链路层。

网络层:进行逻辑地址寻址,实现不同网络之间的通信,定义了 ip 地址,为数据传输选择最佳路径,路由器工作在网络层。

传输层:定义传输数据的协议端口号,以及流控和差错校验,实现了程序与程序的互连,可靠与不可靠的传输。

会话层:建立,管理,中止会话,例如断点续传。

表示层:数据的表现形式,如加密,压缩。

应用层:网络服务与最终用户的一个借口。

## TCP/IP

应用层

传输层

网络层

数据链路层

物理层

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

传输层：TCP、UDP

网络层：ICMP、IGMP、IP、ARP RARP

## 什么是协议

为了使数据可以在网络上从源传递到目的地,网络上所有设备需要讲相同的语言

描述网络通信中语言规范的一组规则就是协议

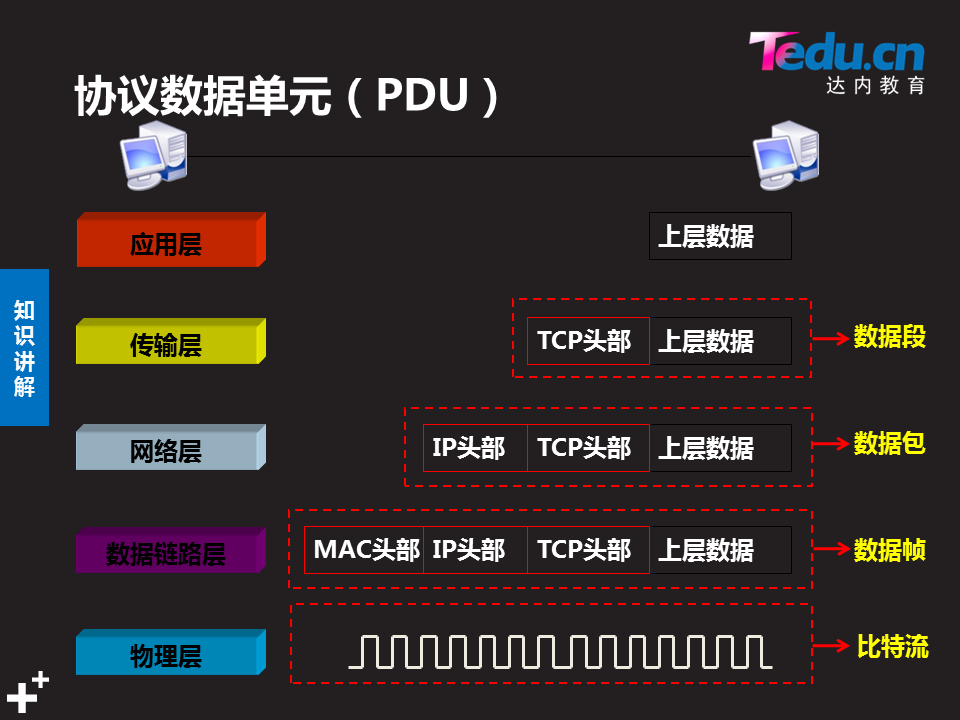
PDU（协议数据单元）

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

## 物理层-网络的基础

物理层是TCP/IP模型的最底层

为数据端设备提供传送数据的通路

就像马路是汽车的基础一样

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）

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

双绞线的连接规范

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

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。

物理层设备

网络接口卡

--连接计算机和网络硬件

--有一个唯一的网络节点地址

--按照速率可分为10/100M,100/1000M自动适应网卡

--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

## 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

一个MAC地址有48位(6字节),前24位是供应商标识,后24位是网卡编号

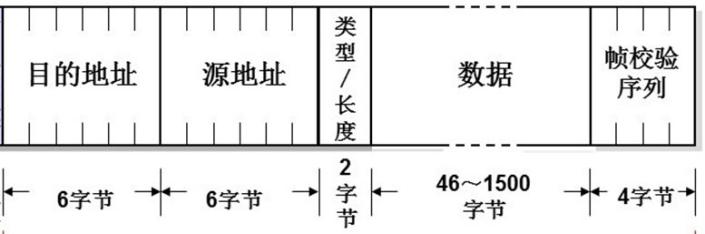
MAC 地址的第8位为0时表示该MAC地址为单播地址，为1时表示组播地址。48位都为1表示广播地址。

windows系统查看MAC地址命令 ipconfig /all

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

数据帧格式



什么是交换机

交换机是用来连接局域网的主要设备

--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

交换机的工作原理

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

广播域

--广播域指接收同样广播消息的节点的集合,如:在该集合中的任何一个节点传输一个广播帧,则所有其他能收到这个帧的节点都被认为是该广播帧的一部分

--交换机的所有接口默认属于同一个广播域

## 网络层

网络层的功能

--定义了基于IP协议的的逻辑地址

--连接不同的媒介类型

--选择数据通过网络的最佳路径

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检测双向通路的连接性

Ping命令使用ICMP协议

--ping [-t] [-l字节数] [-c次数] [-W不通时的超时时间] [-i ping之间的间隔时间] 目标IP

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

## 传输层

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

传输层的协议

TCP(Transmission Control Protocol)

--传输控制协议

--可靠地,面向连接的协议

--传输效率低

UDP(User Datagram Protocol)

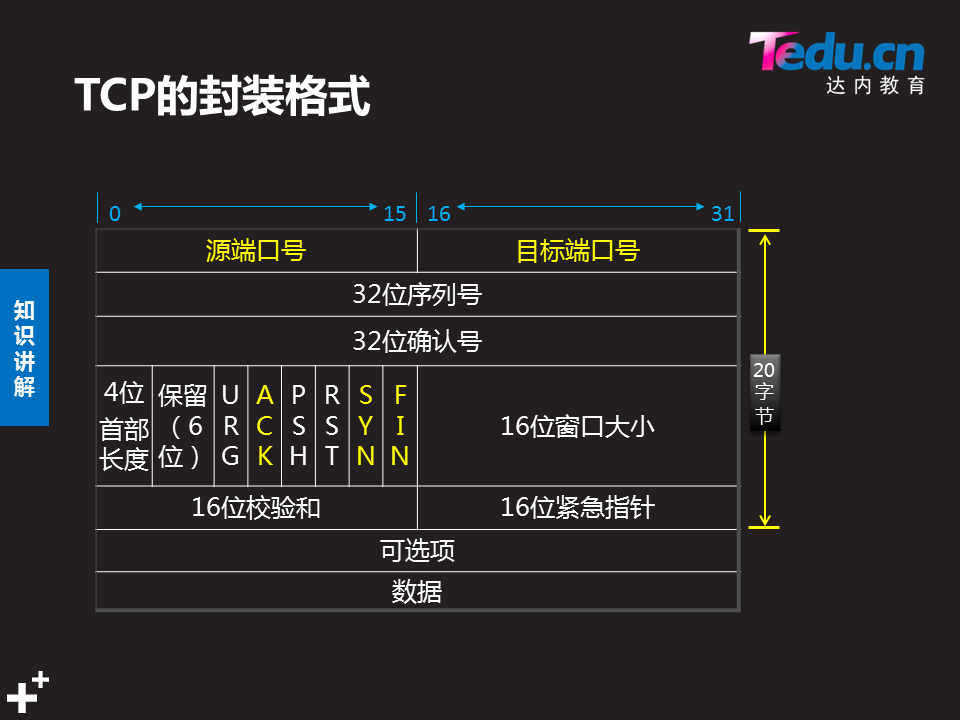
--用户名数据报协议

--不可靠的,无连接的服务

--传输效率高

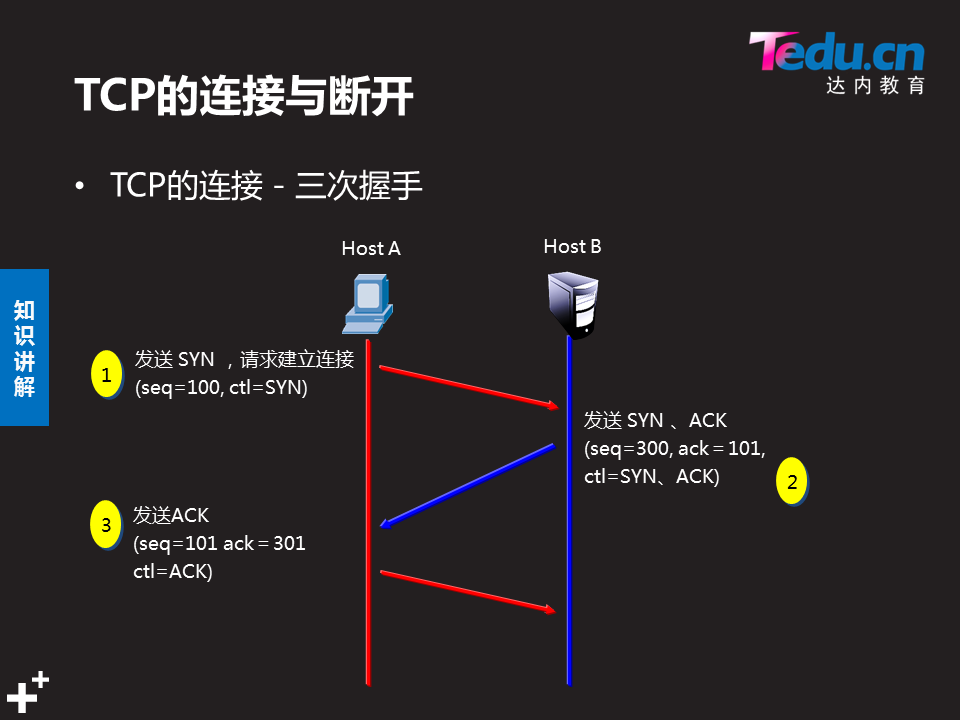
TCP协议

TCP的封装格式

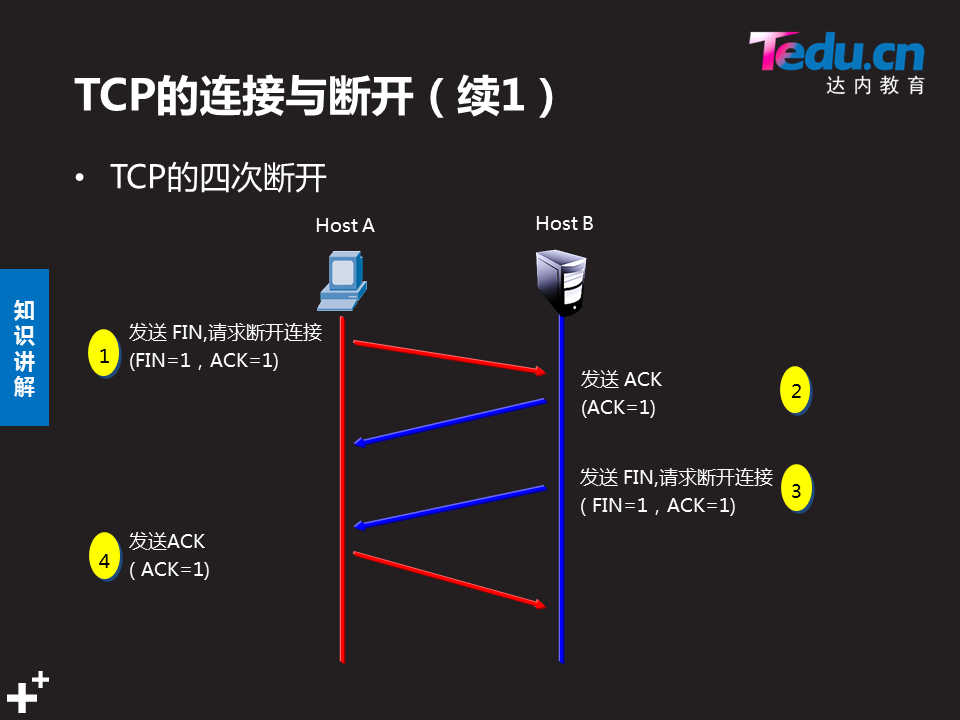


TCP的连接与断开

TCP连接--三次握手



TCP的四次断开



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

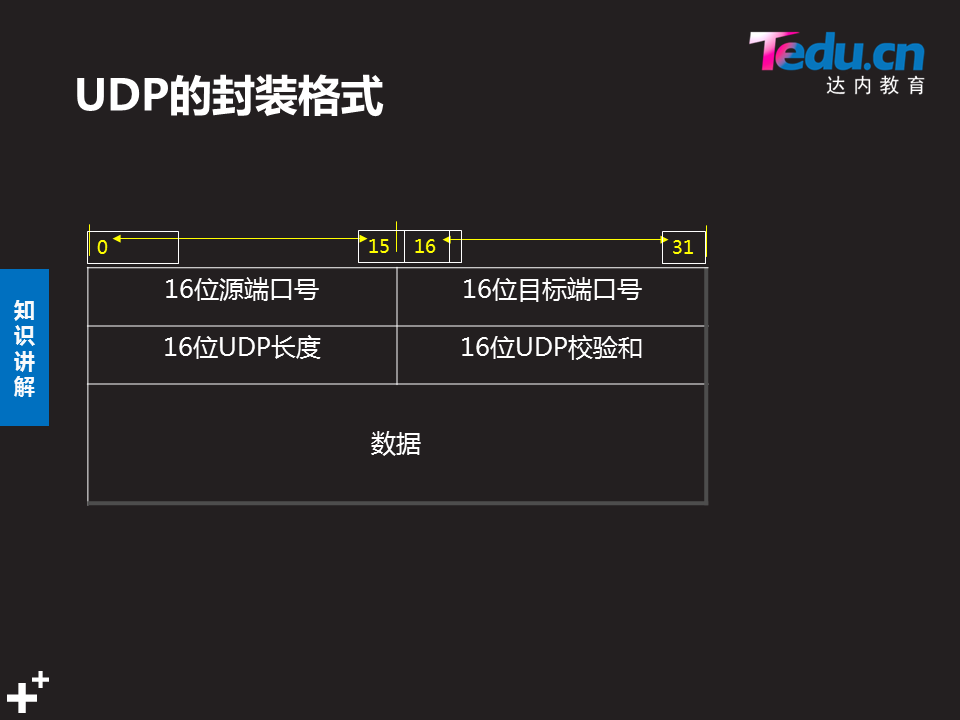
25 SMTP SMTP服务器开放的端口，用于发送邮件

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

UTP协议

UTP的封装格式



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

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

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

# 交换机的命令行模式

## 配置前的连接

Console电缆

物理连接

计算机COM口

交换机/路由器Console口

软件连接

超级终端

其他软件

## Cisco交换机的命令行

用户模式

Switch>

特权模式(一般用于查看配置信息)

Switch>enable

Switch#

全局变量模式(对整个设备进行配置)

Switch#configure terminal

Switch(config)#

接口模式

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#

--Interface : 关键字

--fastethernet : 接口类型(百兆)

--0/1 : “0”表示模块号, “1”表示接口号

模式间的转换

exit : 返回上层

end : 回到特权模式

<Ctrl-Z>退出到特权模式

命令输入错误被卡住时同时按键盘ctrl+shift+^这三个按键

配置主机名

Switch>en

Switch#conf t

Switch(config)#hostname pokemon

pokemon(config)#

查看交换机配置

pokemon# show running-config

配置enable明文口令

Switch(config)#enable password 123456

明文口令可以在running-config看到

保存交换机的配置

Switch#copy running-config startup-config

Switch#write

恢复设备出厂默认值

Switch#erase startup-config

重启

Switch#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

查看MAC地址表

Swtich#show mac-address-table

# 路由原理及配置

## 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

## 路由器怎么工作

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)

## 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

## 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

使用 ip route 命令

--指定到达IP目的的网络

--基本格式

Route(config)#ip route 目标网络ID 子网掩码 下一跳IP

默认路由(缺省路由)

--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

查看路由表

Route#show ip route

C直连路由

S静态路由

S\*默认路由

# 三层交换

## 三层交换技术

--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

## 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*

三层交换机VLAN间通信的转发过程

--先通过接口进入vlan 将vlan当做路由器来转发

## 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

在三层交换机启用路由功能

Switch(config)#ip routing

配置虚拟接口的IP

Switch(config)#interface vlan *vlan-id*

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

Switch(config-if)#no shutdown

配置路由接口

Switch(config-if)#no switchport

在三层交换机配置Trunk并指定封装为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

# 动态路由

## 概述

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

--占用了网络宽带

## 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

•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

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*

# VLAN

## 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

## VLAN的作用

--广播控制

--增加安全性

--提高带宽利用

--降低延迟

## 静态VLAN的配置

配置VLAN的步骤

--创建VLAN

--将接口加入到相应的VLAN中

--验证

在全局配置模式下创建VLAN

Switch(config)#vlan *vlan-id*

删除已创建的VLAN

Switch(config)#no vlan *vlan-id*

将接口加入VlAN

Switch(config)#interface f0/1 (进入端口)

Switch(config-if)#switchport access vlan *vlan-id* (将端口加入vlan)

Switch(config-if)#no switchport access vlan *vlan-id* (将端口从vlan中删除)

Switch(config)#interface range f0/1-10 (同时进入多个端口)

验证VLAN的配置

Switch#show vlan brief

# Trunk

## 交换机之间的VLAN通信

如何实现交换机之间的VLAN通信

--每个VLAN一条链路?

--只用一条链路,那么来自多个VLAN的数据如何标识?

--交换机给每个去往其他交换机的数据帧打上VLAN标识

## 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

## VALN标识的种类

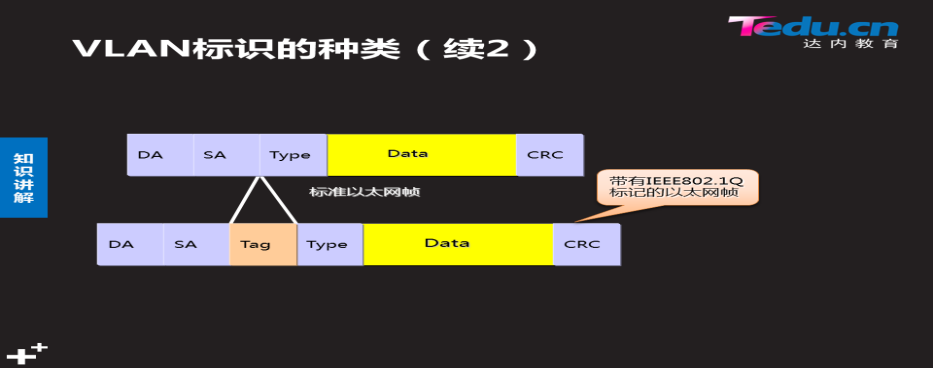
以太网上实现中继可用两种封装类型

--ISL(Cisco私有协议)

--IEEE 802.1Q

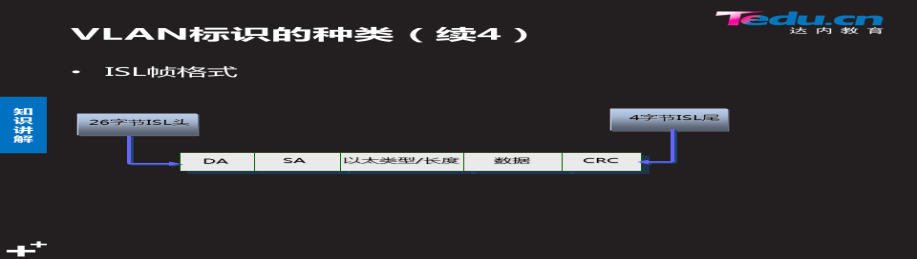
IEEE802.1Q帧格式

在地址后加入4字节



ISL帧格式

在头加入26字节在尾加入4字节



ISL和802.1Q的异同

--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

## Trunk命令

配置接口为Trunk模式

Switch(config)#interface *interface-id*

Switch(config-if)#switchport mode trunk

恢复端口默认模式

Switch(config)#interface *interface-id*

Switch(config-if)#switchport mode dynamic auto

或

Switch(config-if)#no switchport mode trunk

查看接口模式

Switch#show interface *interface-id* switchport

# 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合,英文名EtherChanel

--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

## 配置以太通道

EtherChannel -- 以太通道

--多条线路负载均衡,宽带提高

--容错,当一条线路失效时,其他线路通信,不会丢包

配置端口为以太通道模式

Switch(config)#interface range fastEthernet 0/1-2

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

查看以太通道的配置

Switch# show etherchannel summary

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

# ACL

## 访问控制列表作用

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

## 访问控制列表的工作原理

访问控制列表在接口应用的方向

--出:已经过路由器的处理,正离开路由器接口的数据包

--入:已达到路由器接口的数据包,将被路由器处理

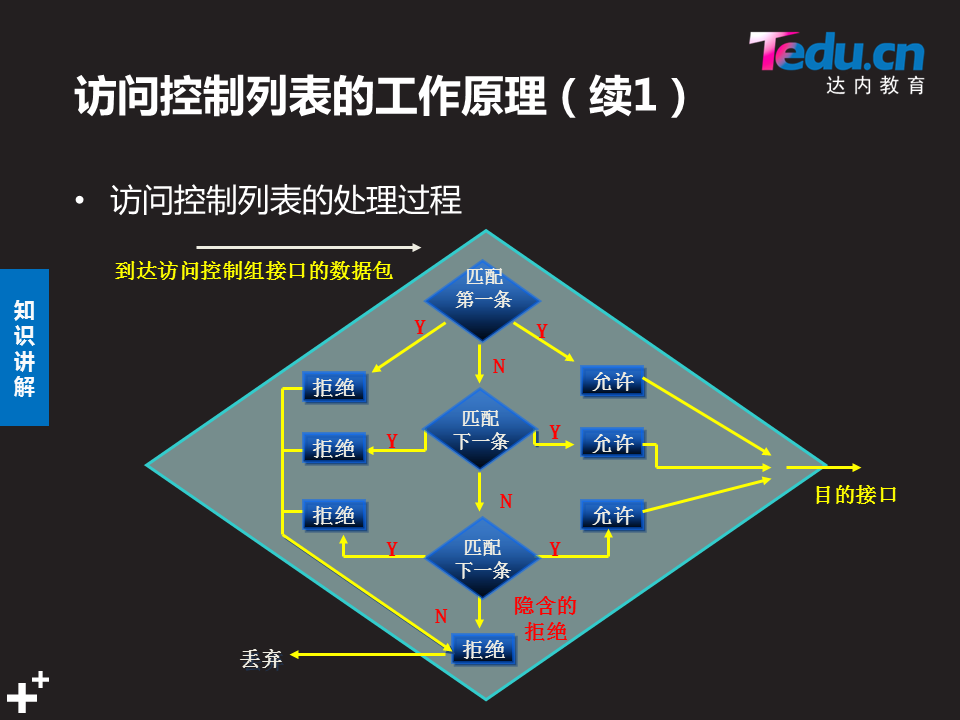
列表应用到接口的方向与数据方向有关

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。



注: 默认拒绝

## 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

2）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

## 标准访问控制列表的配置

创建ACL

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

应用实例:

Router(config)#access-list 1 deny 192.168.1.1 0.0.0.0

Router(config)#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：

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

关键字

--host

--any

将ACL应用于接口

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

在接口上取消ACL的应用

Router(config-if)#no ip access-group *access-list-number*{in|out}

查看访问控制列表

Router#show access-lists

删除ACL

Router(config)#no access-list *access-list-number*

## 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]

应用实例:

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

# NAT

## NAT概述

NAT的作用

NAT

--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。

NAT的特性

优点

--节省公有合法IP地址

--处理地址重叠

--安全性

缺点

--延迟增大

--配置和维护的复杂性

NAT实现方法

--静态转换(Static Translation)

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

## 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

Router(config)#ip nat inside source static *local-ip* *globbal-ip*

*local-ip* 内部的机器

*globbal-ip* 到外部的IP

在内外接口上启用NAT：

出口配置：ip 　nat 　outside

入口配置：ip 　nat 　inside

NAT端口映射配置

建立NAT端口映射关系

将192.168.1.1的web映射到100.0.0.2上

Router(config)#ip nat inside source static tcp 192.168.1.1 80 100.0.0.2 80

## 端口多路复用(PAT)

PAT的作用

--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,及配置默认路由

Router(config-if)#ip nat outside

Router(config-if)#ip nat inside

跟踪NAT

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

## STP生成树算法

在网络中存在物理环路,会产生广播风暴

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

## STP配置

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

PVST+的配置命令

启用生成树命令 (此命令可以不用输入，默认交换机会开启)

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

指定根网桥（主根或次根）

改优先级

Router(config)#spanning-tree vlan 1 priority 优先级的值

注意： 优先级的值是4096的倍数

或指定主次

Router(config)#spanning-tree vlan 1 {primary|secondary}

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

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

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+实现网络的负载平衡

# HSRP

## HSRP概述

热备份路由选择协议（Hot Standby Routing Protocol）

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。

## HSRP配置

首先要进入vlan中并给vlan配置IP地址

配置为HSRP的成员

Switch(config-if)#standby HSRP备份组号 ip 虚拟网关IP

Switch(config-if)#standby 1 ip 192.168.1.254

配置HSRP的优先级

Switch(config-if)#standby HSRP备份组号 priority 优先级

Switch(config-if)#standby 1 priority 105

优先级范围0-255，越大越优先，默认为100

查看HSRP摘要信息

Switch#show standby brief

HSRP占先权

--当本身优先级大于其他设备是立刻抢占活跃路由器身份

--HSRP占先权配置

Switch(config-if)#standby 备份组号 preempt