**数据通信基础**

HUB

HUB上的节点处于冲突域中

HUB相连的两台机器处于冲突域中，同时只能有一台机器发送/接收数据

交换机Switch

交换机的每一个端口都是冲突域

交换机整机是广播域(Broadcast Domain)，所有子机处于广播域中

交换机的基本功能

1. 数据帧的交换

2. 终端用户的接入

3. 基本的接入安全功能（MAC地址过滤，ARP欺骗）

4. 分割冲突域

5. 二层链路的冗余，防环和负载均衡

路由器

一个接口就是一个广播域

1. 隔绝广播，实现跨三层的数据访问

2. 支持路由协议，维护路由表

3. 路径选择及数据转发

4. 广域网接入，地址转换及特定的安全功能

**OSI参考模型**

1. Physical

2. Data Link

3. Network Layer

4. Transport Layer

5. Session

6. Presentation

7. Application

其中1-4层为底层，负责网络数据传输；5-7层为高层。负责主机之间的数据传输

1.物理层：在媒介上传输比特流

1）定义接口和媒体的物理特性

2）定义比特的表示、数据传输速率、新号的传输模式（单工，半双工，全双工）

3）定义网络物理拓扑（网状、星型、环型、总线型）

4）负责把逐个的比特从一跳移动到另一跳

2. 数据链路层：将分组数据封装成帧；提供节点到节点的传输；差错检测

1）组帧、物理编址、流量控制、差错控制、接入控制

2）在不可靠的物理链路上，提供可靠的数据传输服务，吧帧从一跳移动到另一跳

3. 网络层：逻辑寻址；路由选择

1）定义了逻辑地址（三层地址）

2）分组寻址，负责将分组数据从源端传输到目的端

3）路由选择、维护路由表

4. 传输层：提供可靠或不可靠的端到端传输

1)负责将来自上层应用程序的数据进行分段和重组，并将它们组合为同样地数据流形式

2)提供端到端的数据传输服务

3)工作在传输层的协议：TCP、UDP

5. 会话层：为通信双方指定通信方式，并创建，注销会话

1）负责建立、管理和终止表示层实体之间的会话连接

2）在设备或节点之间提供会话控制

3）在系统之间协调通信过程

6. 表示层：数据和信息的转换，数据压缩解压缩，加密解密

1）数据的解码和编码

2）数据的加密和解密

3）数据的压缩和解压

4）常见的标准：ASCII、JPEG

7. 应用层：各种应用程序，协议

1）为应用软件提供接口，使应用程序能够使用网络服务

2）常见应用层协议：http、ftp、dns、telnet

TCP/IP模型

1.物理层

在媒介上传输比特；提供机械和电气的规约

2.数据链路层

将分组数据封装成帧；提供节点到节点方式的传输

3.因特尔网层

定义逻辑地址；路由的选择、将分组从源端传送到目的端

4.主机到主机层

为应用层实体提供端到端的通信功能，保证了数据包的顺序传送及数据完整性

5.应用层

对应于OSI参考模型的高层，为用户提供所需的服务，例如：FTP、Telnet、DNS、SMTP等

TCP & UDP

传输控制协议TCP

1.面向连接

2.可靠传输

3.流控及窗口机制

4.使用TCP的应用：

1）Web浏览器

2）文件传输程序

3）电子邮件

用户数据报协议UDP

1.无连接

2.不可靠传输

3.尽力而为的传输

4.使用UDP的应用：

1）视频流

2）IP语音（VoIP）

3）域名系统（DNS）

TCP三次握手

A: seq = 0, ctl = SYN

B: seq = 0, ack = 1, ctl = SYN, ACK

A: seq = 1, ack = 1, ctl = ACK

TCP四次挥手

A: seq = 101, ctl = FIN, ACK

B: seq = 301, ack = 102, ctl = ACK

B: seq = 301, ack = 102, ctl = FIN, ACK

A: seq = 102, ack = 302, ctl = ACK

ARP

ARP(Address Resolution Protocol)具有两项基本功能：

1.将IP地址解析为MAC地址

2.维护ARP映射的缓存

缺点是广播，不安全，不可靠（ARP欺骗）

Tracert

Tracert用于显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间。命令同Ping类似，但是获得的信息比Ping详细得多，包含数据包走过的全部路径，节点的IP和花费的时间。

IP地址

1.IP地址在网络中用于标识一个节点

2.IP地址用于IP分组在网络中的寻址

3.一个IPv4地址有32位，通常用“点分十进制”表示

Netmask网络掩码

1.网络掩码为32位

2.网络掩码在二进制上是一堆连续的1，以连续的0结尾

3.值为1的bit对应IP地址的网络位，值为0的bit对应IP地址的主机位

192.168.1.1 255.255.255.0 = 192.168.1.1/24

IP地址分类

网络地址：

指代网络的地址。在网络的IPv4地址范围内，最小地址保留为网络地址，此地址的主机部分每个主机位均为0.

广播地址：

用于向网络中所有主机发送数据的特殊地址。广播地址使用该网络范围内的最大地址。即主机部分各bit全为1的地址

主机地址：

可分配给网络中终端设备的地址

VLSM

为什么要划分子网

1.将一个网络号划分为多个子网，每个子网能够分配一个独立的广播域

2.广播域缩小，网络规划更加合理

3.IP地址得到了合理利用

如何进行子网划分

1.判断类别，找出掩码

2.变更掩码，找子网

3.得出子网号

4.得出主机段

5.得出广播号

环路问题

1.网络中如存在二层环路，一旦出现广播数据帧，该帧会被交换机不断地泛洪，造成广播风暴。

2.广播风暴对网络的危害很大，会严重消耗网络带宽和设备资源。

3.交换机可能从自身的不同接口接收到数据帧，MAC地址表会不断变化，也称MAC表的紊乱。

STP

Spanning-tree技术能够在网络中有二层环路时，通过阻塞特定端口来打破环路，并在网络拓扑出现变更时及时地收敛，从而保证网络的冗余性。

STP流程

1每个广播域选择一个根桥

2每个非根桥选择一个根端口

根端口：具有最低根路径的接口。如果交换机上有多个拥有相同的到根的开销，则进一步比较候选接口上所收BPDU的优劣。

3每个段选择一个指定端口

指定端口：具有最低根路径的接口。如果一个链 拥有相同的到根的开销，则进一步比较候选接口上所收BPDU的优劣。（根桥的所有端口都是指定端口，不会被阻塞）

4选出非指定端口

BPDU

BPDU是网桥协议数据单元Bridge Protocol Data Unit

依靠BPDU的泛洪，STP得以正常工作

BPDU重要参数

Root ID

发送此BPDU的交换机所认为根交换机的交换机标识

Path Cost

从发送此BPDU的交换机到达根交换机到达根交换机的最短路径总开销，含交换机根端口的开销

Bridge ID

发送此BPDU的交换机的STP交换机标识

Port ID

发送此BPDU的交换机端口的STP端口标识

比较顺序

Root ID> Path Cost> Bridge ID> Port ID

Bridge ID

桥ID共8个字节，由2个字节的优先级和6个字节的MAC地址构成

-桥优先级默认为32768，可以手工修改

-MAC地址为交换机的背板MAC

PS：优先级以4096递增，MAC是唯一。两者均越小越优。

Path Cost

路径开销是一个端口量，是用于选择链路的参考值。

路径开销的默认值及取值范围由选定的路径开销算法决定，路径开销与端口的带宽成反比。

华为路径开销计算标准为802.1d-1998， 802.1t，legacy。默认选择802.1t。

STP的端口状态

Disable

端口不仅不转发BPDU报文，也不转发用户流量。

Blocking

端口仅仅接收并处理BPDU，不转发用户流量。不学习MAC地址。如果MAX AGE计时器到期时该接口仍然没有收到BPDU则切换到Listening状态。

Listening

不接收也不转发用户流量，接收且发送BPDU，不学习MAC地址。确定端口角色，将进行选举动作。

Learning

不接收也不转发用户流量，接收并发送BPDU，学习MAC地址。

Forwarding

接收并转发帧，接收并发送BPDU，学习MAC地址。

ARP

ARP(Address Resolution Protocol)地址解析协议，它为IP地址到对应的硬件地址提供相应的动态关系。

也即在三层转发流程中，查找路由表找到下一跳的IP地址，但是IP地址是一个虚拟的地址，必须找到其对应的物理地址才能真正发送。建立与维护这一IP-MAC对应关系的表项（ARP表），就是ARP模块的主要任务。

路由器的工作内容

1.路由器知道目标地址

2.发现到达目标地址的可能路径

3.选择最佳路径

4.维护路由信息

5.转发IP数据

路由条目的来源

1.直连路由

路由器本地接口所在的网段

2.静态路由

手工配置的路由条目

3.动态路由

路由器之间动态学习到的路由

Loopback接口

1.Loopback接口，也称为回环口，是一个逻辑，虚拟的接口

2.Loopback接口在手工创建后是不会Down的，非常稳定

3.Loopback接口常用于

1模拟路由器的直连网段，用于测试

2用于设备管理

3供其它协议使用

4作为SNMP traps消息的源地址

距离矢量路由选择协议

路由器收敛完成的标志

-当所有路由表包含相同网络可达性信息

-网络进入一个稳态

路由器继续交换路由信息

-当无新路由信息被更新时收敛结束

-网络在到达收敛前无法完全正常工作

距离矢量路由选择协议防环机制

-定义最大度量防止计数至无穷大(定义16跳为不可达)

-水平分割

-路由中毒

-毒性逆转

-抑制计时器

-触发更新

RIP

RIP(Routing Information Protocols,路由信息协议)是应用较早，使用普遍的内部网关协议。适用于小型网络，是典型的距离矢量协议。它基于UDP，端口为520，在华为设备上优先级为100.

OSPF

OSPF(Open Shortest Path First)开放最短路径协议。它是一种链路状态路由协议。Open意味着开放公邮，使得所有厂商都能够支持OSPF。在华为设备上优先级为10。

基本特点

-适应范围广

支持各种规模的网络

-快速收敛

在网络拓扑变化后立即发送更新报文，在自治系统中同步

-无自环

依靠链路状态用最短路径树算法计算路由，保证无自环

-区域划分

允许自治系统网络划分为多个区域进行管理，减小LSDB的规模，从而降低对交换机内存和CPU的消耗

OSPF Route ID

-OSPF Route ID用于在OSPF domain中唯一地表示一台OSPF设备

-可以通过手工配置的方式进行设备，或者通过协议自动选取。在实际网络中，建议手工配置OSPF Route ID

-在路由器运行OSPF并由系统自动选定Route ID后，如果该接口down掉，或者出现一个更大的IP，OSPF仍然保持原Route ID，该ID是非抢占的，即使重启OSPF进程，Route ID也不会发生改变。只有手工配置Route ID，并重启进程，才会改变。此外，如果对应接口的IP地址消失并重启OSPF进程，则Route ID也会变化。

OSPF Cost

-OSPF使用cost作为路由度量值

-OSPF中接口cost=100M/接口带宽，其中100M可以修改

-每一个激活的OSPF接口都有一个cost值

-一条OSPF路由的cost等于从起源一路到达本地所有接口cost值之和

OSPF Table

-Peer table

OSPF是一种可靠的路由协议，它要求在路由器传输链路状态通告之前，需要先建立起OSPF邻居关系，hello报文用于发现直连路由上的其他OSPF路由器，经过一系列交互，最终建立起全毗邻的邻居关系。

-Link-state database

OSPF使用LSA(Link state advertisement链路状态通告)来描述网络拓扑信息，然后OSPF路由器用链路状态数据库来存储网络的LSA。OSPF将自身和邻居通告的LSA搜集并存储在LSDB中。

-Routing table

基于LSDB使用Dijkstra算法计算出路由表。

OSPF Message

-Hello 建立和维护邻居关系

-DBD 链路状态数据库描述信息

-LSR 链路状态请求

-LSU 链路状态更新(含有一条或多条完整LSA)

-LSAck 对LSU中得LSA进行确认

OSPF 网络类型

-P2P

PPP链路，Lapb链路，HDLC链路

-Broadcast

以太网链路

-NBMA

帧中继链路，ATM链路

-P2MP

手工指定

DR，BDR

-为减小多路访问网络中的OSPF流量，OSPF会在每一个MA(多路访问)网络选举一个指定路由器DR和一个备用路由器BDR。

-DR选举规则

最高OSPF优先级拥有者被选举为DR，如果优先级相等，则有最高OSPF Route ID的路由器被选举为DR，并且DR具有非抢占性。

-DR

负责使用该变化信息更新其它所有OSPF路由器(DR Other)。

-BDR

监控DR状态，当DR发生故障时接替该角色。

OSPF邻居关系建立宏观

-发现直连路径上的OSPF路由器，建立双向关系

-协商主/从关系，交换LSA头部摘要信息

-同步LSA，请求发送LSU

-完成同步，进入OSPF全毗邻

OSPF路由器角色

-区域路由器Internal Router

-区域边界路由器Area Border Router

-骨干路由器Backbone Router

-AS边界路由器AS Boundary Router

OSPF Processor ID

进程号取值范围为1-65535，只标识OSPF在本路由器内的一个进程。可以在一个路由器上运行多个不同的OSPF进程，它们彼此独立。

不同进程之间的路由交互相当于不同协议之间的路由交互。进程号是本地有效的。

AS

-AS(Autonomous System)自治系统是指在一个实体管辖下的拥有相同选路策略的IP网络。

BGP网络中每一个网络AS都有唯一的AS号。AS号分为2字节(1-65535)和-4字节(1-4294967295)。

-电信163：4134

-电信CN2：4809

-网通：9929

BGP

BGP(Border Gateway Protocol，边界网管协议)用于在AS之间实现路由信息的交互。

-BGP能够承载大批量的路由前缀

-支持MPLS/VPN应用，传递客户VPN路由

-具备强大的路由策略能力，定义了丰富的路径属性

-支持多协议的扩展

BGP协议特征

-BGP使用传输层协议TCP，端口为179。BGP路由器之间基于TCP建立会话，BGP的对等体无需直连。

-运行BGP的路由器称为BGP Speaker。两台BGP路由器需建立对等体关系(EBGP,IBGP)才能交互BGP路由。

-在对等体关系建立后路由器只能发送增量更新或触发更新

-BGP有丰富的路径属性和强大的策略工具。

-BGP能承载大量的路由前缀，用于大规模网络中。

-主要版本为V4以及MP-BGP。

BGP消息类型

-Open

建立TCP连接后的第一个消息，用于建立BGP对等体之间的邻接关系。

-Keepalive

周期性地向对等体发出该消息以保持连接的有效性。

-Update

用于在对等体之间交换路由消息。

-Notification

用于在检测到错误状态时中断BGP连接。

-Route-refresh

用于要求对等体重新发送指定地址族的路由信息。

BGP对等体

-BGP对等体关系也称为BGP邻居关系，两台BGP路由器建立BGP对等关系才能交换BGP路由。

-BGP会话基于TCP建立。建立对等体关系的BGP路由器无需直连。

BGP邻居建立过程

-空闲(Idle):为初始状态，发起 TCP连接，并倾听远程对等体所发起的连接，同时转向Connect状态。。

-连接(Connect):开始TCP连接并等待TCP连接成功的消息。如果TCP连接成功，则进入OpenSent状态；如果TCP连接失败，进入Active状态。

-行动(Active):BGP总是试图建立TCP连接，若连接计时器超时，则退回到Connect状态，若TCP连接成功就转为Open sent状态。

-OPEN发送(Open sent):TCP连接已建立， 已发送第一个OPEN报文，等待接收对方的Open报文，并对报文进行检查，若发现错误则发送Notification消息报文并退回到Idle状态。若无误则发送Keepalive消息报文,Keepalive计时器开始计时，并转为Open confirm状态。

-OPEN证实(Open confirm):BGP等待Keepalive报文，同时复位保持计时器。如果收到了Keepalive报文，就转为Established状态，邻居关系协商完成。如果系统收到一条更新或Keepalive消息，它将重新启动保持计时器；如果收到Notification消息，BGP就退回到空闲状态。

-已建立(Established):即建立了邻居（对等体）关系，路由器将和邻居交换Update报文，同时复位保持计时器。

BGP同步规则

-BGP同步规则指出，BGP路由器不应该使用通过IBGP对等体获悉的路由或将其通告给EBGP对等体，除非该路由是本地的或又通过IGP获悉。

-华为设备默认关闭BGP同步规则。

-若同步规则关闭，BGP可以使用这样的路由并将其通告给外部BGP对等体：从IBGP对等体那获悉的且没有与IGP同步的路由。

-若同步规则开启，则路由器通过IBGP对等体获悉路由后，将等待IGP将该路由传遍整个AS，然后再将其通告给外部对等体。

VRRP

-VRRP(Virtual Router Redundancy Protocol)虚拟路由冗余协议

-利用VRRP，椅子路由器(同一个LAN中的接口)协同工作，但只有一个处于Master状态，处于该状态的路由器接口承担实际的数据流量转发任务。在一个VRRP组中的多个路由器接口共用一个虚拟IP地址，该地址被作为局域网内所有主机的缺省网关地址。

-VRRP决定哪个路由是Master，Master路由器负责接收发送至用户网关的数据包并进行转发，响应PC对其网关的ARP请求。

-Backup路由器侦听Master状态，并准备随时解题Master路由器的工作。

VRRP术语

-VRRP路由器

运行VRRP的路由器，一台VRRP的路由器的接口可以同时参与到多个VRRP组中，在不同的组中，一台VRRP路由器可以充当不同的角色。

-VRRP组

一个VRRP组由多个VRRP路由器组成，使用Group ID进行标识，属于同一个VRRP组的路由器互相交换信息，每一个VRRP组中只能有一个Master。

-虚拟路由器

对于每一个VRRP组，抽象出一个逻辑路由器，该路由器充当网关。该路由器并非真实存在。

-虚拟IP地址

虚拟IP地址用于标示虚拟路由器，该地址实际上就是网关地址。

-虚拟MAC地址

与IP地址对应的MAC也是虚拟的，该MAC地址由固定位加上VRRP组ID  
组成。当PC发ARP请求虚拟IP对应的MAC地址时，Master路由器响应该请求并告知虚拟MAC地址。

-Master路由器

在VRRP组中，仅有Master响应对虚拟地址的VRP请求。Master路由器以一定时间间隔发送VRRP消息，通知Backup路由器自己的存活情况。

-Backup路由器

在VRRP组中处于监听状态的路由器，一旦Master路由器出现故障，Backup路由器就开始接替工作。

-选举依据

先比较接口优先级，如果相等比较接口IP地址（比大）。

虚拟MAC地址

-通过VRRP形成的虚拟路由器使用虚拟IP地址和虚拟MAC与网络中的PC进行通信。虚拟MAC地址的最后一个字节的VRID表示VRRP ID号的十六进制。

Master Router

-响应PC对网关的ARP请求

-转发目的MAC地址为虚拟MAC地址的IP报文

-周期性发送VRRP组播包告知自己的存活情况

Backup Router

-持续侦听Master发送的VRRP组播包

-当Master出现问题时，接替Master

-对虚拟IP地址的ARP请求不做响应

-丢弃目的MAC地址为虚拟MAC地址的IP报文

-丢弃目的IP地址为虚拟IP地址的报文

VRRP状态机

-VRRP协议共有三种状态，分别是Initialize，Master，Backup。初始状态均为Initialize，通过比较优先级产生Master和Backup。若Backup在规定时间内没有收到Master传来的心跳报文，则切换为Master。

VRRP Preempt

-当VRRP优先级更高的设备加入网络时，如果启用了Preempt，则可立即抢占Master角色，发送VRRP Announcement消息，宣称自己为Master。

-可修改抢占延迟时间，默认是0s。