**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。

HUB是一层设备，工作在物理层，作用是把一些机器连接起来组成局域网。HUB通过广播的方式共享带宽。HUB的所有接口是一个冲突域和广播域。

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。

交换机是二层设备，工作在数据链路层，作用是把一些机器连接起来形成一个局域网，交换机采用独享带宽的方式，可以过滤、转发。交换机的每一个接口是冲突域，所有的接口是广播域，可以隔离冲突域。

交换机的通信方式是广播，自己维护一个端口-发送方MAC地址数据表，具有端口记忆功能。

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

路由器是三层设备，工作在网络层。作用是连接不同的网段并找到网段中最合适的路径。路由器屏蔽了物理网络的特征，实现了跨网段转发。路由器的每一个接口都是广播域和冲突域，路由器可以隔离广播域。路由器的通信方式是单播。

单播

网络节点之间的通信就像人与人之间的对话，如果是一对一对话，那么就对应单播。单播时信息的接收和传递只在两个节点之间进行。

组播

组播传输是指在发送者和每一接收者之间实现点对多点网络连接。如果一台发送者同时给多个接收者传输相同的数据，也只需复制一份相同的数据包。它提高了数据的传送效率。减少了骨干网络出现拥塞的可能。

广播

广播是指在IP子网内广播数据包，所有在子网内部的主机都将接收到这些数据包。广播意味着网络向子网的每一个主机都投递一份数据包，无论主机是否乐意于接收这些数据包。广播的使用范围非常小，只在本地子网有效，通过路由器和交换机网络设备控制广播传输。

QOS

服务质量QOS用于评估服务方满足客户服务需求的能力。在因特网中，它主要用来评估网络转发分组的能力。通常说的QOS是对分组转发过程中带宽，吞吐量，延迟，延迟抖动，丢包率，可用性等核心需求提供支持的能力评估。

VRP QOS

在华为VRP平台中，有三种QOS服务模型：

1.尽力传送模型(Best effort)

2.集成服务模型(Int serv)

3.区分服务模型(Diff serv)

**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。

-通过向目标发送不同IP生存时间 (TTL) 值的“Internet控制消息协议(ICMP)”回应数据包，Tracert诊断程序确定到目标所采取的路由。要求路径上的每个路由器在转发数据包之前至少将数据包上的 TTL 递减 1。数据包上的 TTL 减为 0 时，路由器应该将“ICMP 已超时”的消息发回源系统。

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

-VLSM(可变长子网掩码) 是为了有效的使用无类别域间路由（CIDR）和路由汇聚(route summary)来控制路由表的大小，网络管理员使用先进的IP寻址技术，VLSM就是其中的常用方式，可以对子网进行层次化编址，以便最有效的利用现有的地址空间。

-VLSM其实就是相对于类的IP地址来说的。A类的第一段是网络号（前八位），B类地址的前两段是网络号（前十六位），C类的前三段是网络号（前二十四位）。而VLSM的作用就是在类的IP地址的基础上，从它们的主机号部分借出相应的位数来做网络号，也就是增加网络号的位数。各类网络可以用来再划分子网的位数为：A类有二十四位可以借，B类有十六位可以借，C类有八位可以借（可以再划分的位数就是主机号的位数。实际上不可以都借出来，因为IP地址中必须要有主机号的部分，而且主机号部分剩下一位是没有意义的，所以在实际中可以借的位数是在上面那些数字中再减去2，借的位作为子网部分）。

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.

-版本:RIPv1、 RIPv2和RIPng，前两者用于IPv4， RIPng用于IPv6。

-其中RIPv1为有类别路由协议，不支持VLSM和CIDR；以广播的形式发送报文；不支持认证。RIPv2为无类别路由协议，支持VLSM，支持路由聚合与CIDR；支持以广播或组播（224.0.0.9）方式发送报文；支持明文认证和MD5密文认证。

OSPF

OSPF(Open Shortest Path First开放式最短路径优先）是一个内部网关协议(Interior Gateway Protocol，简称IGP），用于在单一自治系统（autonomous system,AS）内决策路由。是对链路状态路由协议的一种实现，隶属内部网关协议（IGP），故运作于自治系统内部。

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。

Dijkstra算法

-迪杰斯特拉算法是由荷兰计算机科学家狄克斯特拉于1959 年提出的，因此又叫狄克斯特拉算法。是从一个顶点到其余各顶点的最短路径算法，解决的是有向图中最短路径问题。迪杰斯特拉算法主要特点是以起始点为中心向外层层扩展，直到扩展到终点为止。

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

-边界网关协议（BGP）是运行于 TCP 上的一种自治系统的路由协议。 BGP 是唯一一个用来处理像因特网大小的网络的协议，也是唯一能够妥善处理好不相关路由域间的多路连接的协议。 BGP 构建在 EGP 的经验之上。 BGP 系统的主要功能是和其他的 BGP 系统交换网络可达信息。网络可达信息包括列出的自治系统（AS）的信息。这些信息有效地构造了 AS 互联的拓朴图并由此清除了路由环路，同时在 AS 级别上可实施策略决策。

-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。

流分类

-流分类是指依据一定的匹配规则识别出对象。流分类是由区别地实施服务的前提。

流量监管

-对进入路由器的特定流量的规格进行监管。当流量超出规格时，可以采取限制或惩罚措施，以保护运营商的商业利益，保护网络资源不受损害。

流量整形

-一种主动调整流的输出速率的控制措施，通常是为了使流量适配下游路由器可供给的网络资源，避免不必要的报文丢弃和拥塞。

拥塞管理

-网络拥塞时必须采取的解决资源竞争的措施。通常是通过队列调度技术将报文放入队列中缓存，并采用某种调度算法安排报文的转发次序。每一种队列调度技术都会对网络性能产生特定的影响。

拥塞避免

过度的拥塞会对网络资源造成损害。拥塞避免监督网络资源的使用情况，当发现拥塞有加剧的趋势时，采取主动丢弃报文的策略，通过调整流量来解除网络的过载。VRP提供了多种拥塞避免机制来满足不同的应用，包括尾丢弃，RED(Random Early Detection)，WRED(Weighted Random Early Detection)。

集成服务模型

-一种综合服务模型，可以满足多种QOS需求。使用集成服务模型时，在发送报文前，需要通过信令向网络申请特定的服务。传送QOS请求的信令是RSVP(资源预留协议)。应用程序需要先通知网络其流量参数和需要的特定QOS请求，在收到确认信息后，网络已经为这个应用程序报文预留了资源后，发送报文。RSVP是一个QOS信令，作用是为报文流提供端到端的资源预留申请。

-集成服务模型提供两种服务：

保证服务：提供保证的带宽和时延限制来满足应用程序的需求。

负载控制服务：保证即使在网络过载的情况下，能对报文提供类似网络未过载时的服务(低延时，高通过)。

区分服务模型

-网络根据每个报文流指定的QOS来提供服务，对报文的等级进行划分，可以有不同的标准，如IP包得优先级位，报文的源地址，目的地址。网络通过这些来对报文进行分类，流量整形，流量监管和排队。

-区分服务模型通常用来为一些重要的应用提供端到端的QOS，通过CAR和队列技术来实现。

CAR(Committed Access Rate)：根据预先设置的匹配规则来进行报文的分类，同时也完成对报文的流量的度量和监管。

队列技术：PQ,CQ,WFQ,CBQ等队列技术

-使用区分服务时，边界路由器可以通过多种条件灵活地对报文进行分类，对不同的报文设置不同的标记字段，其它路由器只需要根据标记字段进行报文的分类。在IP骨干网通常采用区分服务模型。

VLAN

-基于端口

基于交换机的端口编号来划分VLAN。计算机所属的VLAN由计算机所连的网络设备端口所属的VLAN来决定。

-基于MAC地址

根据计算机的网卡MAC地址来划分VLAN

-基于网络层协议

将运行不同IP协议的计算机分为不同的VLAN

VLAN

-一个VLAN中所有的设备都是在同一个广播域内，不同的VLAN为不同的广播域；VLAN之间互相隔离，广播不能够跨越VLAN传播，因此不同的VLAN之间无法互访，不同的VLAN之间需要通过三层设备实现通信。

-一个VLAN一般为一个逻辑子网，由被配置为此VLAN成员的设备组成；

-VLAN中成员一般基于交换机的接口分配，划分VLAN就是对交换机的接口划分；

-VLAN工作于OSI参考模型的第二层；

-VLAN是二层交换机的一个根本的工作机制。

链路类型

-接入链路(Access Link)

连接用户主机和交换机之间的链路为接入链路。接入链路上通过的帧为不带Tag的以太网帧。

-干道链路(Trunk Link)

连接交换机和交换机之间的链路为干道链路。干道链路上通过的帧通常为带Tag的以太网帧。

端口类型

-在802.1Q中定义VLAN帧后，设备的有些端口可以识别VLAN帧，有些端口不能识别。VRP支持基于端口的VLAN划分方式，也即根据交换机的端口编号来划分VLAN。计算机所属的VLAN由端口的VLAN决定。

Access端口

-Access端口是交换机上用于连接用户主机的端口，只能连接接入侧。Access端口只允许一个VLAN帧通过。从主机接收帧时，给帧加上Tag标记；向主机发送帧时，将Tag中的帧标记剥除。

Trunk端口

-Trunk端口是交换机上用来和其他交换机连接的端口，它只能连接干道链路。Trunk端口允许多个VLAN帧通过，在接收和发送帧时保留Tag标记。

Hybrid端口

-Hybrid端口是交换机上既可以连接用户主机，又可以连接其他交换机的端口。它可以视为是Access端口和Trunk端口的混合体。它允许多个VLAN通过，并可以在出端口方向将某些VLAN帧的Tag剥除。

Q in Q端口

-Q in Q端口是交换机上和其他交换机相连的，并且只能够处理携带双层Tag标记的VLAN端口。Q in Q端口可以给以太网帧加上双重Tag。可以支持多达4096\*4096个VLAN。

链路聚合

-一个网络中，某些关键链路承载的流量可能非常大，链路的负载很高，带宽容易成为数据传输的瓶颈，而增加带宽会提高硬件成本。以太网链路聚合是一种通用的以太网技术，它能够将多条以太网链路进行“捆绑”，捆绑后这些链路形成了逻辑上的一条新链路，不仅增加了带宽，还同时提供了负载均衡和链路冗余。

-链路聚合技术能够用在交换机之间、防火墙之间等等，是一种部署非常广泛的技术。

缺省VLAN

-在交换机上，每个Access，Hybrid，Q in Q端口可以配置一个缺省VLAN。端口类型不同，缺省VLAN的含义也有所不同。

1.Accsess和Hybrid端口的缺省VLAN

-当收到不带Tag的帧时，交换机会在帧上加上Tag标记，将Tag中得VID值设置为端口所属的缺省VLAN编号。

-对于从这两种端口发送出的帧，如果Tag的VID值为缺省VLAN编号，则交换机会剥除该帧中的Tag标记。

2.Q in Q缺省VLAN

-对于Q in Q端口接收的帧，无论该帧是否带有Tag标记，交换机都会在帧上加Tag，并将Tag中的VID字段设置为端口所属的缺省VLAN编号。

-对于Q in Q端口发送的帧，如果最外层Tag的VID字段的值等于缺省VLAN编号，交换机会将帧最外层的Tag剥除。

VLAN基本通信原理

-为了提高通信效率，交换机内部的数据帧一律带有Tag，以统一方式处理。当一个数据帧进入交换机端口时，如果没有带Tag，且该端口上配置了PVID(Port VLAN ID)，那么该数据帧就会标上该端口的PVID。如果数据帧已经带有了Tag，那么及时该端口已经配置了PVID，交换机也不会再给数据帧标记Tag。

-PVID也即端口缺省VLAN ID，一个端口缺省属于的VLAN，通常为1。

Access端口处理帧的过程

1.收到一个二层帧

2.判断是否有VLAN Tag

-没有Tag，标记上Access端口的PVID

-有Tag，与Access端口的PVID一致则进行下一步处理，不一致则丢弃

3.二层交换机根据帧的MAC地址和VLAN ID查找配置信息，决定从哪一个端口发出

4.交换机根据出接口发送数据帧

-当数据从Access端口发出时，剥除VLAN Tag

-当数据从Trunk端口发出时，直接发出

-当数据从Hybrid端口发出时，先判断该VLAN在端口是Tag还是UnTag，若是Untag则剥离VLAN Tag再发出，若是Tag则直接发出。

Trunk端口处理帧的过程

1.收到一个二层帧

2.判断是否有VLAN Tag

-没有Tag，标记上Trunk端口的PVID

-有Tag，判断Trunk端口是否允许该VLAN帧进入，不允许则丢弃

3.二层交换机根据帧的MAC地址和VLAN ID查找配置信息，决定从哪一个端口发出

4.交换机根据出接口发送数据帧

-当数据从Access端口发出时，剥除VLAN Tag

-当数据从Trunk端口发出时，直接发出

-当数据从Hybrid端口发出时，先判断该VLAN在端口是Tag还是UnTag，若是Untag则剥离VLAN Tag再发出，若是Tag则直接发出。

Hybrid端口处理帧的过程

1.收到一个二层帧

2.判断是否有VLAN Tag

-没有Tag，标记上Hybrid端口的PVID

-有Tag，判断Hybrid端口是否允许该VLAN帧进入，不允许则丢弃

3.二层交换机根据帧的MAC地址和VLAN ID查找配置信息，决定从哪一个端口发出

4.交换机根据出接口发送数据帧

-当数据从Access端口发出时，剥除VLAN Tag

-当数据从Trunk端口发出时，直接发出

-当数据从Hybrid端口发出时，先判断该VLAN在端口是Tag还是UnTag，若是Untag则剥离VLAN Tag再发出，若是Tag则直接发出。

光纤接头

常见光纤接头：ST,SC,LC,FC

FC型光纤连接器：外部加强方式是采用金属套，紧固方式为螺丝扣。一般在ODF侧采用。配线架上用得最多。

SC型光纤连接器：连接GBIC光模块或普通光纤收发器的连接器，它的外壳呈矩形，紧固方式是插拔闩式，无须旋转。在交换机路由器上用的最多。

ST型光纤连接器：常用于光纤配线架，外壳呈圆形，紧固方式为螺丝扣。

LC型光纤连接器：连接SFP模块的连接器，它采用操作方便的模块化插孔机制。路由器常用。

BFD

-BFD(Bidirectional Forwarding Detection)双向检测转发。

-它是一个简单的Hello协议，它和很多路由协议的邻居检测部分相似。一对系统在它们之间所建立的会话通道上周期性地发送检测报文。如果某个系统长时间没有收到对端的检测报文，则认为在这条到相邻系统的双向通道的某个部分发生了故障。

异步模式

-在异步模式下，两个系统相互周期性地发送BFD控制报文，如果某个系统在检测时间内没有收到对端发来的BFD控制报文，就宣布会话为Down。

查询模式

-在查询模式下，假定每一个系统都有一个独立的方法用于确认它连接到其他的系统。一旦BFD会话建立，系统停止发送BFD报文，除非某个系统需要显示地验证连接性。在此情况下，系统发送一个短系列的BFD控制包，如果在检测时间内没有收到返回的报文就宣布会话为Down，如果收到对端回复报文，则保持沉默。

回声功能

-本地发送一系列BFD回声报文，远端系统通过它的转发通道将他们环回回来。如果本地系统连续几个回声报文都没有收到，那么会话被宣布为Down。

AR

-AR系列企业路由器是集路由、交换、无线、语音、安全为一体的新一代业务路由网关设备。

-AR一般位于企业网内部网络与外部网络的连接处，是内部网络和外部网络之间数据流的唯一出入口，能将多种业务部署在同一设备上，极大地降低了企业网络建设初期投资与长期运维成本。用户可以根据企业用户的规模选择不同的AR路由器作为出口网关设备。

IP地址

-IP地址在网络中用于标识一个节点或网络设备的接口。

-IP网络中数据包的寻址是基于IP地址进行的，IP地址就像现实生活中的门牌号。

-IP协议定义了数据分组的格式，也定义了数据分组寻址的方式。主要是IPv4和IPv6。

-一个IPv4地址有32位。

-IPv4地址通常使用点分十进制，例如192.168.1.1。

十进制与二进制的转换

-点分十进制易于理解网络，但是网络设备在实际运用时是使用二进制。

-192.168.10.1对应11000000.10101000.00001010.00000001

IP地址的分类

-IPv4地址一共有五类：

-A类地址：第一个八位组首位为0，区间为1.0.0.0~127.255.255.255.其中127.0.0.1/8为本地回环。

- B类地址：第一个八位组首位为10，区间为128.0.0.0~191.255.255.255.

- C类地址：第一个八位组首位为110，区间为192.0.0.0~223.255.255.255.

- D类地址：第一个八位组首位为1110，区间为224.0.0.0~239.255.255.255.这个类别的地址专门用于组播。

-剩下的是E类地址，保留作为研究使用。

IP地址类型

-网络地址：指代网络的地址。一个IP地址中主机位全0的地址，也称为网络号。

-广播地址：用于向网络中所有的主机发送数据的特殊地址。广播地址使用该范围内的最大地址。即主机部分各比特位全部为1 的地址，也称为广播号。

-主机地址：可分配给网络中终端设备的地址。

网络掩码

-网络掩码也为32位，在二进制上是一堆连续的1接着后面连续的0。

-值为1的位对应IP地址中的网络位，值为0的位对应IP地址中的主机位。

-通常用掩码长度来表示一个IP地址+掩码：

192.168.1.1 255.255.255.0 等同于 192.168.1.1/24

IP路由

-在一个IP网络中，路由是非常主要的概念。网络的基本功能，是让处于网络中的两个节点能够互相通信。通信实际上就是数据交互的过程。数据交互需要网络设备帮助我们在两个通信节点之间进行传输。当路由器收到一个数据包，路由器会找出IP头部的目的IP地址，然后依据目的IP到自己的路由表中进行查找，找到最匹配的路由条目后，将数据包根据路由条目所指示的出接口或下一跳IP转发出去，这就是路由。

-每台路由器都会在本地维护一个路由表，路由表中装载着路由器通过各种途径获取的路由条目。每一条路友条目由路由前缀、路由信息来源、出接口或下一跳IP、优先级、开销等元素组成。路由器通过直连、静态、动态方式获取路由条目并维护自己的路由表。路由表是支持数据转发的依据和基础，每一个需要执行数据转发或路由动作的设备都需要维护一张路由表。

路由优先级

-路由器可以通过多种途径获知路由条目：如静态手工配置或通过各种动态路由协议学习等等。当路由器从两种不同的途径获得去往同一目的地的两条下一跳不同的路由时，路由器会比较这两条路由的优先级，优先选择Pre小的路由。如果Pre相同，就进一步比较开销Cost。

动态路由协议的分类

-根据作用范围，可分为

内部网关协议IGP：在一个自治系统内运行。

外部网关协议BGP：运行在不同自治系统之间。

-根据使用的算法，可分为

距离矢量协议RIP、BGP。

链路状态协议OSPF、IS-IS。

路由策略

-路由策略是一种比基于目标网络进行路由更加灵活的数据包路由转发机制。应用了路由策略，路由器将通过路由图决定如何对需要路由的数据包进行处理，路由图决定了一个数据包的下一跳转发路由器。

-路由策略是控制层面的行为，操作的对象是路由条目，匹配的是路由，具体是指目标网段、掩码、下一跳、度量值、Tag、Community等。

Router policy用途

-路由重分发期间关联router policy进行路由过滤或执行策略

-应用于策略路由

-应用于NAT

-应用于BGP中的策略部署

-其他用途

策略路由

-策略路由，是一种比基于目标网络进行路由更加灵活的数据包路由转发机制。路由器将通过路由图决定如何对需要路由的数据包进行处理，路由图决定了一个数据包的下一跳转发路由器。

防火墙

-防火墙的主要作用是划分网络安全边界，实现关键系统与外部环境的安全隔离，保护内部网络免收外部攻击。

-与路由器相比防火墙提供了更丰富的安全防御策略，提高了安全策略下数据报文的转发速率。

-由于防火墙用于安全边界，通常兼具NAT、VPN功能。

防火墙分类

-包过滤防火墙

利用定义的特定规则过滤数据包，防火墙直接获得数据包的源、目的IP地址，TCP/UDP的源端口。

-代理型防火墙

使得防火墙作为一个访问的中间节点，对客户端来说防火墙是一个服务器，对于服务器来说防火墙是一个客户端。

-状态检测型防火墙

检查应用层协议信息并监控基于连接的应用层协议状态。

安全区域

-安全区域是一个安全概念，大部分的安全策略都基于安全区域实施。通常在防火墙上创建安全区域，并定义该安全区域的安全级别，然后将防火墙的接口关联到一个安全区域，那么该接口连接的网络，就属于这个安全区域。属于同一个安全区域的用户具有相同的安全属性。

预设的安全区域

-非受信区域(Untrust)：低级的安全区域，安全优先级为5

通常用于定义Internet等不安全的区域。

-非军事化区(DMZ)：中度级别的安全区域，安全优先级为50

通常用于定义内网服务器所在的区域。这种设备虽然部署在内网，但是经常要被外网访问，存在较大的安全隐患，同时一般不允许其访问外网。

-受信区(Trust)：较高级别的安全区域，安全优先级为85

通常用于定义内网终端用户所在区域。

-本地区域(Local)：最高级别的安全区域，安全优先级为100

定义的是设备本身，包括设备的各个接口本身。凡是由设备构造并主动发出的报文均可认为是从Local区域中发出，凡是需要设备响应并处理的报文均可认为是由Local区域接受。

安全区域的规划

-用于可自定义安全区域，也可使用系统自带的安全区域，防火墙的一个接口只能属于一个特定区域，一个区域可以包含多个接口，接口只有划分到区域中才能正常处理报文。

-Local Zone指的是设备本身，包括设备的各个接口。凡是发给防火墙的都可以认为是发向Local的，防火墙发出的数据可以认为是来自Local的。

-内部网络应该安排在安全级别较高的区域。

-外部网络应该安排在安全区域最低的区域。

-一些可对外部提供有条件服务的网络应安排在安全级别中等的DMZ区域中。

安全区域的限制

-防火墙不能有两个拥有相同安全级别的区域

-防火墙的一个物理接口只能属于一个安全区域

-防火墙的多个接口可以同时属于一个区域

-系统自带的安全区域不能删除

-相同区域内不同接口间的报文不过滤直接转发

-一个报文如果在进、出端口时相同则会被丢弃

-接口没有加入安全区域前不能转发报文

区域间

-安全域间这个概念用于描述流量的传输通道，它是两个区域间的唯一道路。如果希望对此通道的流量进行控制，则需要在通道上设置安全策略。对于不需要经过该通道的流量，在该安全域间的安全策略是不起作用的。任何两个安全区域都构成一个安全域间，并具有单独的安全域间视图。

防火墙工作模式

-路由模式

防火墙的每一个接口连接一个网络，防火墙的接口地址是所连接子网的网关；

报文首先通过入接口信息找到进入域信息，然后查找转发表，根据出接口找到出口域，再根据这两个域确定域间关系，最后按照配置在这个域间关系上的安全策略进行操作。

-透明模式

防火墙的接口不配置IP地址，可被看做是一台二层交换机。

透明模式的防火墙支持ACL规则检查、ASPF状态过滤、防攻击检查、流量监控等。

透明模式可以配置系统管理IP。

混合模式

-防火墙一部分接口工作在透明模式，一部分接口工作在路由模式。混合模式主要是为了解决防火墙在透明模式下无法双机热备的问题，因为双机热备需要在接口上配置IP地址。

ACL

-访问控制列表ACL是由permit或deny语句组成的一系列有顺序规则的集合，它通过匹配报文的相关字段实现对报文的分类。

-ACL本身只是一组规则，只能区分某一类报文，无法实现过滤报文的功能。对这类报文的处理方法，需要由引用ACL的具体引用来决定。

-ACL是一个使用非常广泛的基础性工具，能够被各种应用所调用。

ACL应用

-过滤IP流量(源目IP，源目端口，协议类型)

-在NAT中调用

-在路由策略中调用

-在VPN中调用

-在防火墙部署策略中调用

-其他

ACL分类

-基本ACL

基本ACL只能针对IP数据包中IP头的源IP地址进行匹配。如果在防火墙上布置ACL过滤来源于192.168.1.0/24这个子网的IP流量，实际上就是过滤掉源IP地址为192.168.1.0/24的子网IP的报文。

-高级ACL

高级ACL能针对数据包的源IP地址、目的IP地址、协议类型、TCP源目的端口或UDP源目的端口等元素进行匹配。它的功能较基本ACL丰富。

NAT

-技术背景

NAT是缓解IPv4地址枯竭的重要方法。在IP地址中定义私有和公有IP。私有IP只能在本地网络中使用，不能出公网。NAT技术能对IP报文中的源或目的地址进行转换，从而使得当源地址为私有IP地址空间的数据包到达网络出口时，由NAT设备对私有地址进行转换，转换成一个合法的IP并将数据包发到公网，当数据包返回时，又将目的IP修改为初始的私有IP地址。