

第一部分：TCP/IP 基础

一. OSI 模型与 TCP/IP 模型分别有哪些层次，每层主要的功能？

1. OSI 分为七层：分别由低到高为物理层、数据链路层、网络层、传输层、会话层、表示层、应用层
2. TCP/IP 模型分为四层：网络接口层、网络层、传输层、应用层
3. 物理层功能：物理层涉及网络接口和传输介质的机械、电气、功能和规程方面的特性。具体包括接口和介质的物理特性。（光纤介质、铜介质、微波..）
4. 数据链路层的主要功能是管理连接在同一介质类型上的两台连网设备如何相互通信, 定义的是物理寻址（数据链路层主要的协议：以太网、PPP/HDLC、FR）
5. 网络层定义用于第 3 层的逻辑地址，基于逻辑地址的网络号寻找到达目的设备的路径，将不同的数据链路类型连接到一起，诸如以太网、FDDI、串行和令牌环（网络层主要的协议：IP、IPX 及 IP 的辅助协议：ARP、ICMP、IGMP）
6. 传输层提供端到端的通信,定义的是进程寻址（传输层主要的协议：UDP 和 TCP）
7. 会话层负责网络会话的控制。具体功能包括会话的建立、维护和交互过程中的同步。
8. 表示层负责信息的表示和转换。具体功能包括数据的加密/解密、压缩/解压缩、与标准格式间的转换等
9. 应用层负责向用户提供访问网络资源的界面。应用层包括一些常用的应用程序和服务，如电子邮件、文件传输、网络虚拟终端、WWW 服务、目录服务等

二. 请问你对 TCP 协议有什么了解？（TCP 的概念、TCP 协议有什么特点）

1. TCP 叫做传输控制协议，是传输层协议之一。能针对节点之间的连接和流量进行控制
2. TCP 是面向链接、可靠传输的协议。基于 TCP 的应用在传输数据之前必须先由 TCP 建立连接，在传输过程中由 TCP 解决可靠性、有序性，进行流量控制，传输结束后由 TCP 拆除连接（建议一定要了解清楚 TCP 的三次握手及基于连接数据传输）
3. TCP 协议拥有拥塞控制，（建议了解清楚 TCP 拥塞控制机制原理）
4. TCP 协议通过滑动窗口具有流量控制机制（了解清楚 TCP 滑动窗口工作原理）
5. TCP 拥有很强的差错控制（了解清楚如何进行差错的）

三. 请问你对 UDP 协议有什么了解？（UDP 协议有什么特点）

1. UDP 叫做用户数据报协议，是传输层协议之一。
2. UDP 是一种无链接、不可靠的协议
3. UDP 没有流量控制机制
4. UDP 只拥有最基本、最简单的差错控制
5. UDP 是无连接协议，不提供拥塞避免。

四. 请问你对 ARP 协议有什么了解？（ARP 是如何工作的？ARP 欺骗的工作原理是？及如何防御 ARP 的欺骗？）

1. ARP 叫做地址解析协议，主要用于三层 IP 地址到二层 MAC 地址的解析
2. ARP 工作原理：在同一广播域内，当设备知道目标设备的 IP，当不知道目标设备的 MAC 地址时，该设备发送一个 ARP 广播，本广播域内的所有设备均会收到。但只有目标设备收到该 ARP 请求广播，得知是需要请求自己的 MAC 地址时，才会向源设备发送一个 ARP 的回应。告之源设备自己所对应的 MAC 地址

3. ARP 欺骗主要是利用 IP 与 MAC 的绑定关系通信的原理，伪造绑定关系，从而达到欺骗的目的，ARP 的欺骗分为两种，主机欺骗及网关欺骗，主机欺骗主要是伪造局域网的某台主机的绑定关系，从而截取数据，而网关欺骗则是伪造网关的绑定关系，将所有数据导向欺骗者，还有一种欺骗为双向欺骗
4. ARP 欺骗解决方案有：ARP 静态绑定，安装 ARP 防火墙，启用交换机的动态 ARP 审查功能等

五. 你对 ICMP 和 IGMP 协议有什么了解？（自己找资料解决）

六. 常见的协议端口。

应用	TCP 端口号	应用	TCP 端口号
FTP-Data	20	BGP	179
FTP	21	HTTPS	443
SSH	22	RTSP	554
Telnet	23	SOL Server	1433
SMTP	25	Oracle	1521
Tacacs+	49	H323	1720
HTTP	80	PPTP	1723
POP3	110	MMS	1755
文件共享	139、445	远程桌面	3389

应用	UDP 端口号	应用	UDP 端口号
WINS	42	NetBIOS	137、138、139
DNS	53	IPSec NAT-T	500、4500
DHCP(bootps)	67	Syslog	514
DHCP(bootpc)	68	RIP	520
TFTP	69	L2TP	1701
NTP	123	Radius	1812、1813
SNMP	161、162	Radius cisco	1645、1646

第二部分：交换部分

一. 交换机的工作原理是？

1. 交换机具有最基本的学习和转发功能；
2. 学习功能：当交换机从一个端口收到以太网数据帧，会首先查看该数据帧的源 MAC

地址，将该 MAC 与对应的端口编号放进 MAC 地址表中；如果 MAC 地址表中已经存在该 MAC 条目，则更新计时器（MAC 地址老化时间为 300S）

3. 转发功能：当交换机从一个端口收到以太网数据帧，查看该数据帧的目的 MAC，根据 MAC 中所对应的 MAC 地址条目，从相应的接口转发出去；如果 MAC 地址表中没有该 MAC 地址的条目，则从除接受端口外的所有端口洪泛出去。

二. 你对 VLAN 有什么了解？（VLAN 的概念、VLAN 的意义、VLAN 的特点）

1. VLAN（Virtual Local Area Network）的中文名为"虚拟局域网"。VLAN 是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的新兴数据交换技术
2. 通过划分 VLAN 可以起到分割广播域，减少网络广播影响，以及实现二层业务隔离的作用。
3. 一个 VLAN 就是一个单独广播域，一个 VLAN 就是一个子网
4. 同一个 VLAN 可以直接通过二层访问，不同的 VLAN 间必须通过三层实现访问，因此说 VLAN 实现了二层业务的隔离。

三. 你对 trunk 有什么了解？（trunk 的作用，trunk 的应用，trunk 的封装模式）

1. trunk 叫做中继链路，它主要的作用就是能在同一个物理链路上同时承载多个 VLAN 的流量
2. trunk 主要的封装模式有：ISL 和 802.1Q 协议
3. ISL 叫做内部交换机链路，它是思科私有的 TRUNK 协议，封装的以太网数据添加了 26 字节的头部和 4 字节的 CRC 字段，因此数据帧开销大
4. 802.1Q 协议是 IEEE 公有标准，通过插入一个 4 字节的 TAG 字段，区分所承载的不同 VLAN。

四. 你对 STP 有什么了解？（STP 的概念、STP 的作用、STP 的端口角色选举原则）

1. STP 叫做 Spanning Tree,生成树协议；
2. STP 产生的背景：（为什么需要 STP 技术，自己查资料补充）
3. STP 主要的作用：在一个原本物理成环的二层网络上，通过运行树状算法，计算出一个或者多个逻辑阻塞端口进行阻塞，打破了物理环路，计算出一个无环的物理结构，从而避免了二层广播风暴和 MAC 地址抖动的问题
4. STP 端口角色的选举：选择根网桥、选择根端口、选择指定端口、选择阻塞端口
5. 根网桥选举：选择根网桥的依据是网桥 ID，网桥 ID 由网桥优先级和网桥 MAC 地址组成。网桥的默认优先级是 32768，网桥 ID 值小的为根网桥，当优先级相同时，MAC 地址小的为根网桥（选择根网桥主要是用于其他选择其他端口角色的参照物）
6. 根端口的选举：每个非根交换机选择一个根端口。选择顺序为：到根网桥最低的根路径成本，如果根路径开销一样，则选择发送网桥 ID，越小越优先。如果网桥 ID 一样，则选择最小的发送端口 ID
7. 指定端口的选举：在每一段链路上都要选出一个指定端口，用于向下游交换机转发 BPDU。选举原则为：在端口比较发送的 BPDU 与接收的 BPDU，如果发送的 BPDU 优于接受的 BPDU，则该端口为指定端口，反之为阻塞端口。

五. 你对 RSTP 有什么了解？（RSTP 的概念、RSTP 的特点、RSTP 快速收敛机制）

1. RSTP 叫做 Rapid Spanning Tree，快速生成树，IEEE802.1W 标准，它在 IEEE802.1D 标准上针对 STP 收敛速度很慢的问题进行的一种改良。因此它的选举机制仍然与

802.1D 一致。

2. RSTP 增加了一些端口角色（根端口、指定端口、替代端口、备份端口）
3. RSTP 修改了一些端口状态（丢弃状态、学习状态、转发状态）
4. RSTP 通过引入边缘端口，加速了终端用户的接入；
5. RSTP 通过引入替代端口，融合了思科的 Uplinkfast 特性，加快了根端口的切换；
6. RSTP 通过引入 P/A 机制，加快了指定端口的快速收敛；
7. RSTP 通过修改了拓扑变更机制，加快了拓扑变更收敛。

六. 你对 MSTP 有什么了解？（MSTP 的概念、MSTP 的特点）

1. MSTP 叫做多实例生成树；它是允许将多个 VLAN 映射到同一个实例，每个实例是一棵生成树，基于实例来实现负载；
2. 每个实例一棵生成树，减少了 BPDU 对网络资源的占用；
3. 每个实例是一棵 RSTP，通过 RSTP 的机制实现快速收敛；

七. 你对 HSRP 有什么了解？（HSRP 的概念、HSRP 的作用、HSRP 的工作原理）

1. HSRP 叫做热备份路由协议（Hot Standby Router Protocol），是思科私有的一种提供网关冗余，提高网关可靠性的协议；
2. 工作原理：HSRP 通过建立一个 HSRP 组，每个组里有多 HSRP 设备角色：虚拟路由器、活跃路由器、备份路由器；负责转发数据包的路由器称之为主动路由器（Active Router）。一旦主动路由器出现故障，HSRP 将激活备份路由器（Standby Routers）取代主动路由器
3. HSRP 协议提供了一种决定使用主动路由器还是备份路由器的机制，并指定一个虚拟的 IP 地址作为网络系统的缺省网关地址。如果主动路由器出现故障，备份路由器（Standby Routers）承接主动路由器的所有任务，并且不会导致主机连通中断现象。
4. HSRP 的失效检测机制：周期性的发送 HELLO 包，每 3S 发送一次；在 3 个 hello 时间内没有收到对方的 Hello 则判定对方失效，进行角色的切换。

八. 你对 VRRP 有什么了解？（VRRP 的概念、VRRP 的作用、VRRP 的工作原理）

1. VRRP 叫做虚拟路由冗余协议；它是由 IEEE 所制定的公有标准，适用于任何厂商；用于提供网关冗余，提高网关可靠性；
2. VRRP 工作原理：VRRP 通过建立一个 VRRP 组，每个组里有多 HSRP 设备角色：虚拟路由器、活跃路由器、backup 路由器；活跃路由器负责本组内数据的实际转发，备份路由器负责监控活跃路由器的状态。当检测到活跃路由器失效时，备份路由器可以成为新的活跃路由器，进行数据的转发
3. VRRP 的失效检测机制：周期性的由活跃设备发送 VRRP 通告报文，每 1S 发送一次，在 3 个时间周期内没有收到对方的 VRRP 通告报文，则 backup 路由器判为活跃设备出现故障，进行切换。

九. HSRP 与 VRRP 有什么区别？

1. HSRP 与 VRRP 都是网关冗余协议，但是 HSRP 是思科私有技术，和 VRRP 是由 IEEE 所定义的公有标准；
2. 组成员类型的区别：HSRP 组中有活跃设备、备份设备及成员设备；而 VRRP 组中角色只有活跃设备、backup 设备（组中除活跃设备外，其他设备都可以是 backup 设备）

3. 报文类型的区别：HSRP 报文类型有 hello 报文、辞职消息、政变消息；而 VRRP 报文只有一种：VRRP 通告消息
4. 基于的底层区别：HSRP 基于传输层 UDP 作为底层，端口 1985；VRRP 基于 IP 协议作为底层，协议号为 112；
5. 组播更新地址的区别：HSRP 为 224.0.0.2，VRRP 为 224.0.0.18

第三部分：路由部分

一. 路由的查找与转发原则

1. 最长掩码匹配原则；
2. 逐跳转发原则；

二. 路由条目的生成与处理过程

三. 策略路由与路由策略有什么区别？

3. 策略路由工作在转发层面，针对的对象是 IP 数据报文；它是通过用户自定义策略规则直接影响数据如何进行转发；
4. 路由策略工作在控制层面，针对的对象是路由条目；它是通过策略直接影响路由表中的路由条目，从而可以间接的影响数据转发；

四. 你对 RIP 路由协议有什么了解？（RIP 的概念、RIP 的特点、RIP 的工作原理、RIP 的防环机制）

1. RIP 叫做路由信息协议（Routing Information Protocol）
2. 典型的距离适量算法协议，因此 RIP 的路由完全依赖于邻居的传递，是一种传闻式路由；路由计算精准度不高，容易产生路由环路，因此 RIP 协议设计了 6 中防环机制；
3. RIP 因为存在 16 跳的限制，因此 RIP 协议主要定位在小型网络的路由学习管理；
4. RIP 协议基于 UDP 作为底层，端口 520；
5. RIP 的版本分为 RIPv1 和 RIPv2

五. RIPv1 与 RIPv2 有什么区别？

1. RIPv1 属于有类路由协议，路由更新时不携带子网掩码。采用接口掩码为网络默认掩码。因此 RIPv1 不支持不连续的子网
2. RIPv2 属于无类路由协议，路由更新时携带子网掩码。支持不连续的子网掩码
3. 路由通告更新的方式：RIPv1 广播更新（255.255.255.255）、RIPv2 组播更新（224.0.0.9）
4. RIPv2 支持触发更新 ,RIPv1 在 IOS12.2 以前不支持；
5. RIPv2 支持认证 ，而 RIPv1 不支持；

六. 链路状态路由协议与距离适量路由协议有什么区别？

1. 这两种算法主要是邻居之间传递的内容及路由的计算方面有区别；
2. 距离适量路由协议邻居设备之间传递的是已经计算好的路由条目，类似于二手信息；是一种传闻是传递路由方式，即第 1 个路由器将路由计算好之后，传递给下一个路由器，下一个路由器进行简单的矢量叠加，然后再将自己计算好的路由发给下一个

路由器；

3. 链路状态路由协议邻居间传递的是链路状态信息（LSA）,类似于一手信息；本区域内的路由器收到区域内的 LSA 信息后，进行 LSDB 的同步，在同步的基础上每个路由器都可以单独的运行 SPF 算法计算出最佳路由；因此链路状态路由协议路由计算非常精确，不会产生路由环路；
4. 因此可以说，距离适量的路由依赖于邻居，而链路状态路由协议路由是自己计算。

七. 你对 OSPF 路由协议有什么了解？（OSPF 的概念、OSPF 的特点、OSPF 的工作原理）

1. OSPF 叫做开放最短路由优先（Open shortest path first）是一种典型的链路状态路由协议；因此路由计算精确，不会产生路由环路；并且路由收敛速度很快
2. 主要定位于中大型网络路由学习管理，属于 IGP 路由协议；
3. 支持区域的划分，由以前传统平面式网络变成立体层次化网络；划分骨干区域和非骨干区域；
4. 支持区域间汇总、自治系统外部路由汇总及特殊区域；因此能对 OSPF 网络的路由进行进一步的优化；
5. 无类路由协议，支持可变长子网掩码 VLSM；
6. OSPF 的工作原理：在一个区域内，每个路由器都会产生一个 LSA 信息由于描述自身的链路状态信息，每个 LSA 都会在本区域内进行洪泛，最终达到 LSDB 数据库的同步；然后每个路由器会运行 SPF 算法，以自己为根，计算出最佳路由；

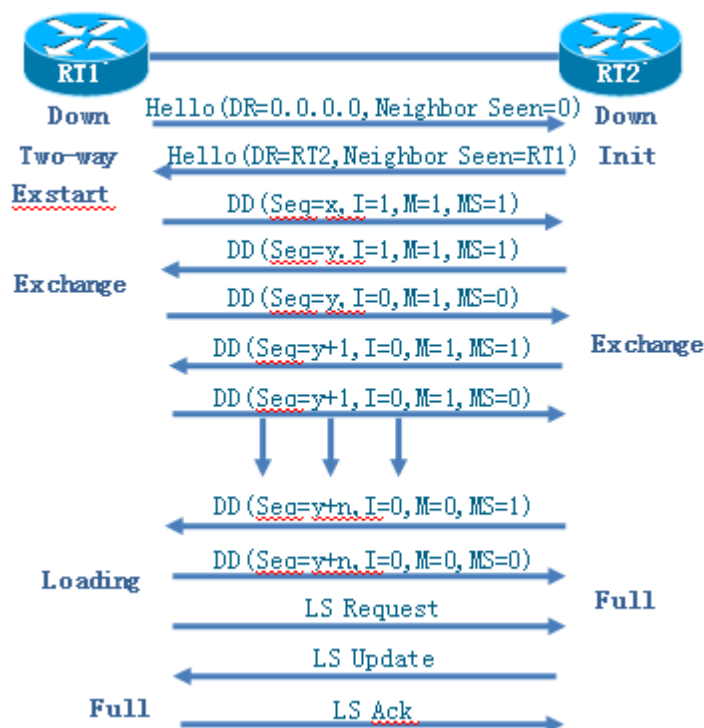
八. OSPF 有哪些网络类型，分别有什么特点？

1. OSPF 网络类型有：点对点网络、广播型网络、NBMA 型网络、点对多点或虚链路
2. POINT_TO_POINT：特点：无 DR 和 BDR，HELLO 时间间隔为 10S；
3. BROADCAST：特点：多路访问型网络，需要选取 DR 和 BDR，HELLO 时间为 10s
4. NON_BROADCAST (NBMA):特点：多路访问型网络，需要选取 DR 和 BDR，HELLO 时间为 30S, 由于底层不支持广播能力，因此需要通过 neighbor 命令手动指定邻居，采用单播建立邻居；
5. POINT_TO_MULTIPOINT:特点:需手动更改网络类型,无 DR 和 BDR 的选举;HELLO 时间间隔为 30S

九. OSPF 有哪些 LSA 类型，分别有什么特点？

1. 一类 LSA（Router-LSA）：由每个路由器生成，描述了路由器的链路状态和花费，传递到整个区域
2. 二类 LSA（Network-LSA）：由 DR 生成，描述了本网段的链路状态，传递到整个区域
3. 三类 LSA（Net-Summary-LSA）：由 ABR 生成，描述了区域内某一段的路由，传递到相关区域
4. 四类 LSA（Asbr-Summary-LSA）：由 ABR 生成，描述了到 ASBR 的一跳主机路由，传递到相关区域
5. 五类 LSA（AS-External-LSA）：由 ASBR 生成，描述了到 AS 外部的路由，传递到整个 AS（STUB 区域除外）
6. 7 类 LSA（NSSA 外部路由）：由 ASBR 生成，在 NSSA 区域中描述引入的外部路由信息，只在 NSSA 区域进行洪泛

十. OSPF 邻接关系的建立过程？



十一. OSPF 为什么要划分多区域？划分多区域有什么意义？

1. OSPF 划分区域的背景：
 - a) 在同一个区域内 OSPF 需要实现 LSDB 数据库的同步，因此如果一个区域内设备过多，则收到的 LSA 信息将会过多，导致 LSDB 和路由表过于庞大，因此需要消耗大量的设备内存，
 - b) 同一个区域的路由器出现故障时，会影响到所有的路由器，因此影响范围过大；
2. OSPF 划分区域的意义：
 - a) 通过划分多区域，可以实现区域间路由汇总；每个区域的一类 LSA 只会在本区域内进行洪泛，也只要在本区域内实现 LSDB 数据库的同步；因此极大的减少了 LSA 和路由条目的数量；
 - b) 通过进行区域间的路由汇总，可以将一个区域的故障限制在本区域，而不会去影响到其他的区域，提高网络性能的稳定性的；

十二. OSPF 为什么要设置特殊区域？有哪些特殊区域？分别有什么特点？

1. 设置特殊区域的意义：通过将非骨干区域设置为特殊区域，可以过滤某些特定类型的 LSA 信息，减少路由条目的数量，优化路由表；
2. 特殊区域的类型：STUB 区域、完全 STUB 区域、NSSA 区域、完全 NSSA 区域；
3. STUB 区域的特点：过滤了 4 类、5 类 LSA，即过滤了 AS 外部路由；STUB 区域不允许存在 ASBR，及不允许本区域引入外部路由；由 ABR 下发一条 3 类的默认路由实现到 AS 外部的访问；
4. 完全 STUB 区域的特点：在 STUB 区域的基础上，进一步过滤了 3 类 LSA，即过滤了 AS 外部路由和区域间路由；
5. NSSA 区域的特点：在 ABR 上过滤了 4 类和 5 类的 LSA，即过滤了 AS 外部的路由；NSSA 允许存在 ASBR，即本区域允许引入外部路由，但是以 7 类 LSA 的形式存在；

ABR 不会自动下发默认路由，需手工通过 default-information 下发默认路由；在 NSSA 区域允许出现两次汇总，即可以在 ASBR 和 ABR 上汇总；

6. 完全 NSSA 区域的特点：在 NSSA 区域的基础上，进一步过滤了 3 类 LSA，即过滤了 AS 外部路由和区域间路由；但完全 NSSA 的 ABR 会自动下发 3 类的默认路由，实现通过 ABR 去访问其他的 AS；

十三. 你对 BGP 路由协议有什么了解？（BGP 的概念、BGP 的特点、BGP 的工作原理）

1. BGP 叫做边界网关路由协议，它是唯一的 EGP 路由协议；
2. BGP 主要定位于超大型网络和因特网路由学习和管理，具有大规模路由管理的能力；并且 BGP 有丰富的路由属性，支持复杂的路由策略；因此即使网络规模不是特别大，但是所要求的路由策略非常复杂时，同样可以应用 BGP 协议来解决；
3. BGP 是典型的距离适量路由协议，它是基于 AS 为单位进行适量路由传递；因此 BGP 路由协议容易产生路由环路，需要设计相关的防环机制；
4. BGP 为了便于路由的管理，可以将网络化整为零，划分出多个 AS；
5. BGP 基于底层 TCP 协议，端口 179；由于 TCP 是一个可靠面向连接的协议，因此 BGP 将繁琐的可靠机制交由底层提供；
6. 无类路由协议，支持无类域间路由；

十四. 为什么需要 BGP 同步？BGP 同步的工作原理是？

1. 因为在一个 BGP 自治系统内，并不是所有设备都会运行 BGP，因此没有运行 BGP 协议的 IGP 路由器无法学到 AS 外部的 BGP 路由，因此可能会导致出现 BGP 路由黑洞；BGP 同步是解决路由黑洞的方案之一；
2. BGP 同步指的是 IBGP 路由与 IGP 路由的同步，即从 IBGP 邻居处学习到的路由必须也要通过 IGP 路由协议学到，否则不会将该 BGP 路由放进全局路由表，也不会将该路由发送出去；当一条路由如果通过 BGP 和 IGP 都学到了，此时称之为 BGP 达到了同步；

十五. BGP 路由优选原则有哪些？（要求按顺序）

首先，丢弃下一跳不可达的路由；在同步状态下，丢弃没有达到同步的路由

1. 选择 weight 值最高的路由（Weight 是 Cisco 私有值，不是 BGP 属性）
2. 选择 Local Preferences 最大的路由
3. 选择本地始发的路由
4. 选择 AS_Path 最短的路由
5. 选择 Origin 最小的路由 IGP<EGP<INCOMPLETE
6. 选择 MED 最小的路由
7. EBGp 路由优于联盟 EBGp 路由优于 IBGP 路由
8. 选择下一跳 IGP 开销最小的路由
9. 选择通告者 router-id 最小邻居的路由

十六. BGP 路由属性中，权重、本地优先、MED 有什么特点？

1. 权重属性：
 - a) Cisco 私有属性，用于路径选择
 - b) 它被本地化配置在路由器上，并针对每个不同的邻居

- c) 权重属性仅在本地有意义，不会被宣告给任何 BGP 邻居
- d) 权重的值可以从 0—65535；由本路由器始发的缺省权重值为 32768，其他路径的缺省权重值为 0。
- e) 到同一目的地存在多条路由时，有高权重值的路由被优选为

2. 本地优先属性：

- a) 本地优先属于周知自选属性；
- b) 本地优先属性实际上是给路由设置优先级，越大越优先；
- c) 默认的本地优先值为：100
- d) 本地优先影响的范围：在一个自治系统内有效，即可以在 IBGP 邻居之间传递；

3. MED 属性

- a) MED 叫做多出口鉴别器，属性可选非传递属性；
- b) MED 就是 BGP 的度量值 (Metric) ,越小越优先。
- c) MED 只允许在一个 AS 内进行传递，即 IBGP 邻居之间。不允许将收到的路由 MED 属性传递给其他的 AS；
- d) 默认情况下，从其他 BGP 对等体接受的路由，MED 为零；从 IGP 重发布进 BGP 的路由，会默认继承 IGP 路由数值；

十七. Mpls 标签控制与分发原则

1. 标签分配模式：

- a) DOD (下游按需标记分发)：上游 LSR 先向下游 LSR 发送标签请求消息，下游 LSR 收到标签请求后为此 FEC 分配标签，并将分配的标签通过标签映射消息反馈给上游 LSR ；
- b) DU (下游自主标记分发)：下游 LSR 在 LDP 会话建立成功，主动向其上游 LSR 发布标签映射消息，无需等待上游请求

2. 标签控制模式：

- a) 有序模式：上游设备只有收到它的下游返回的标签映射消息后才向其更上游发送标签映射消息
- b) 独立模式：不管有没有收到其下游返回的标签映射消息，都立即向其上游发送标签映射消息

3. 标签保留模式：

- a) 保守模式：只保留来自下一跳邻居的标签，丢弃所有非下一跳邻居发来的标签
- b) 自由模式：保留来自邻居的所有标签

十八. 你对标签的分发协议有什么了解？以及标签是如何进行分发的？

1. 针对 IGP 路由的分发：

- a) 标记分发协议 (TDP)：cisco 开发并实施的第一种标签分发协议 (私有)
- b) 资源预留协议 (RSVP)：只被 MPLS TE 所使用
- c) 标签分发协议 (LDP)

2. 针对 BGP 路由的分发：

- a) MP-BGP: BGP 路由协议能够同时传递路由前缀和分发标签。BGP 最主要的是用来在 MPLS VPN 网络中进行标签分发

十九. 你对 MPLS VPN 有什么了解？(mpls vpn 的意义，mpls vpn 的工作原理)

- 1. mpls vpn 最主要的意义是，能允许在同一张物理网上同时承载多种业务，每一种业务之间又可以实现相互隔离。类似于每一种业务一张逻辑的专网；因此既可以保证

业务安全，又可以节省网络建设成本；

二十. 你对 VRF 有什么了解？RD 和 RT 有什么区别？

1. VRF 叫做 VPN 路由转发实例；它实际上是在一个物理设备上通过创建 VRF，创建出几个虚拟的路由器；每一个 VRF 拥有自己独立的 IP 编址、独立的接口、独立的路由表、独立的路由协议；通过 VRF 可以实现本地路由的隔离；
2. RD：叫做路由区分器，主要用于相同的 IPV4 路由的区分；在 IPV4 路由前加上一个 8 字节的 RD，变成唯一的 VPNv4 路由。VPNv4 路由只在 PE 于 PE 之间存在；
3. RT：路由目标，是 BGP 的扩展团体属性，主要用于 BGP 路由的取舍和选择。接受设备通过 RT 来判断把路由导入进相应的 VRF 路由表；

第四部分：网络安全（由于时间问题，接下来的请各位鸟人整理）

- 一. 网络安全中常见的攻击及攻击原理？
- 二. 局域网常见的攻击原理及防范？
- 三. 你对网络安全有什么了解？（常见的安全解决方案）
- 四. 你对防火墙有什么了解？（防火墙的主体功能）
- 五. 你对防火墙的种类有什么了解？（防火墙的种类、及每种防火墙的工作原理特点）
- 六. 你对 VPN 有什么了解？（VPN 的概念、VPN 的特点、VPN 的种类）
- 七. 你对远程接入 VPN 有什么了解？（远程接入 VPN 主要应用、远程接入 VPN 的种类特点）
- 八. 你对站点到站点 VPN 有什么了解？（站点到站点 VPN 的主要应用、站点到站点 VPN 的种类特点）