MAC 地址

扩展问题 1：如何识别一个 MAC 地址是单播，组播还是广播？
查看 MAC 地址是否为全 1，即 FF-FF-FF-FF-FF-FF，是则为广播 MAC 地址，不是则看 MAC 地址的第 8 位是否为 0，为 0 则为单播 MAC，为 1 则为组播 MAC。

扩展问题 2：交换机处理数据帧的行为？
转发：从一个接口接收到的数据从同一 VLAN 的另一个接口发出；收到单播帧，并且其目的 MAC 地址在 MAC 地址表中有对应的转发表项。
泛洪：从一个接口收到的数据帧从其他所有端口发出；收到未知单播帧、组播帧、广播帧时。
丢弃：该帧小与 64 字节（数据帧不完整）或者大于接口 MTU 时；从该接口收到数据帧，该数据帧又要从该接口发出时。

扩展问题 3：交换机收到一个数据帧，如何判断是二层转发还是三层转发？
根据数据帧目的 MAC 地址，如果目的 MAC 地址为交换机的 MAC 地址，进行三层转发；如果不是交换机本身的 MAC 地址，则进行二层转发。

扩展问题 4：常见的组播 MAC 地址有哪些？
01-80-C2-00-00-00：STP 发送的目的 MAC 地址；
01-80-C2-00-00-14：ISIS L1 LAN IIH 报文；
01-80-C2-00-00-15：ISIS L2 LAN IIH 报文；
01-00-5E-0X-XX-XX：用于 IPV4 组播地址映射到组播 MAC 地址；
33-33-XX-XX-XX-XX：用于 IPV6 组播地址映射到组播 MAC 地址；

扩展问题 5：三层交换机收到广播 MAC 数据帧会如何处理？
处理并泛洪

扩展问题 6：交换机收到组播 MAC 数据帧一定会进行泛洪？
不一定；例如：在开启 igmp snooping 表的场景

扩展问题 7：MAC 表和 ARP 表的生成方式有什么不同？:
MAC 表主要是交换机上的，主要根据接收数据帧的源 MAC 地址生成，记录 MAC 和接口、Vlan 的对应关系；
ARP 表主要主机和三层网络设备上的，主要根据 ARP 的报文生成，记录是报文中源 IP 和源 MAC 的对应关系。

ARP 协议

扩展问题 1：哪些设备存在 ARP 表项？:
主机或三层网络设备上会维护一张 ARP 表。

扩展问题 2：免费 ARP 和普通的 ARP 有什么区别？
免费 ARP 报文中的 sender IP 和 target IP 是一致的，而普通的 ARP 报文 sender IP 和 targetIP 是不一致。

扩展问题 3：IPV4 的重复地址检测和 IPV6 的重复地址检测有什么区别？
1.IPV4 中使用的是免费 ARP 报文，而 IPV6 中使用的是 ICMP V6 报文；
2.免费 ARP 报文是二层广播发送的，而 ipv6 中是三层组播发送的，即目的 IPV6 地址为被请求节点组播地址；

扩展问题 4：IPV4 的的地址解析和 IPV6 的地址解析有什么区别？

1.使用的协议不同　ARP NDP
2.目的地址不同　广播（二层广播）、组播（被请求节点组播组地址）
3.工作环境不同　二层　三层

扩展问题 5：什么时候会触发 ARP 请求？
1.要访问的目的 IP 地址在本设备没有对应的 ARP 表项；
2.设备上动态 ARP 表项到达老化超时时间后，设备会发送 ARP 请求报文；（默认老化超时时间为 20 分钟、老化探测次数为 3 次、老化探测模式为前两次是单播，最后一次是广播）

扩展问题 6：ARP 请求一定是广播发送的吗？
一般情况下是，除了动态 ARP 表项老化超时之后，进行老化探测是会单播发送。

扩展问题 7：设备收到 ARP 请求会如何处理？
1.查看 target IP 是否为自己的接口 IP，是则回复 ARP 应答并记录 sender IP 和 sender MAC 的对应关系在 ARP 缓存表中；
2.不是自己，设备如果开启了 proxy ARP，则会进行相应的检查（查找路由表、ARP 表项），再判断丢弃或者回复；没有开启 proxy ARP，则直接丢弃；

扩展问题 8：设备收到免费 ARP 报文后，会如何处理？
1．如果免费 ARP 报文中源 IP 地址和自己的 IP 地址相同，则周期性的广播发送免费 ARP 应答报文，告知此 IP 地址在网络中存在冲突，直到冲突解除。
2．如果免费 ARP 报文中源 IP 地址和自己的 IP 地址不同，免费 ARP 报文是在 VLANIF 接口收到的，并且设备上已经有免费 ARP 报文中源 IP 地址对应的动态 ARP 表项，则进行 ARP 学习，即根据收到的免费 ARP 报文更新该 ARP 表项。其余情

况收到免费 ARP 报文后均不进行 ARP 学习。

iStack CSS

扩展问题 1：放在汇聚层可以实现网关冗余，那么放在接入层不能实现冗余？
答：网关放在接入也可以实现冗余。将两台接入交换机做堆叠，接入的服务器上使用双网卡，一个网卡接到主交换机上，一个网卡接到备交换机上。

扩展问题 2：下层设备需要支持双网卡，是指什么设备？
答：服务器。

扩展问题 3：PC 连接在主设备上，如果主设备故障了，PC 还能访问 internet 吗？
答：如果 PC 是有双网卡的，并且另外一个网卡连接在备交换机上，那么 PC 仍然能够上网。

扩展问题 4：备份的技术有哪些？
答：设备的备份技术有 VRRP 和堆叠。
链路的备份技术有链路聚合、stp、smart-link。

扩展问题 4：华为实现堆叠的方式有哪些？
答：盒式设备使用 istack，框式设备的堆叠用 CSS。

STP 与 RSTP 的不同点

协议简介
STP 不能快速迁移，即使是在点对点链路或边缘端口（边缘端口指的是该端口直接与用户终端相连，而没有连接到其它设备或共享网段上），也必须等待 2 倍的 Forward Delay 的时

间延迟，端口才能迁移到转发状态。
RSTP（Rapid Spanning Tree Protocol，快速生成树协议）是 STP 协议的优化版。其“快速”体现在，当一个端口被选为根端口和指定端口后，其进入转发状态的延时在某种条件下大大缩短，从而缩短了网络最终达到拓扑稳定所需要的时间。

1 协议编号

STP　：IEEE　802.1d
RSTP：IEEE　802.1w
MSTP：IEEE　802.1s

Protocol Version Identifier 协议版本标识符，STP 为 0，RSTP 为 2，MSTP 为 3。

2 端口角色

STP：　RP DP BP(blocking port)
RSTP: RP DP BP(Backup port) AP(Alternate port) EP(edged port)

3 端口状态

STP:disabled ,
blocking ,listening ,learning ,forwarding

disabled：说明端口未启用 STP 协议；
blocking：阻塞状态，属于 AP 端口正常状态，进行根桥的选举；
listening:侦听状态，进行端口角色的确定；
learning:学习状态，学习 mac 地址表；
forwarding：转发状态，转发数据，学习 mac 地址；

RSTP:discarding , learning ,forwarding

表 1 STP 与 RSTP 端口状态角色对应表

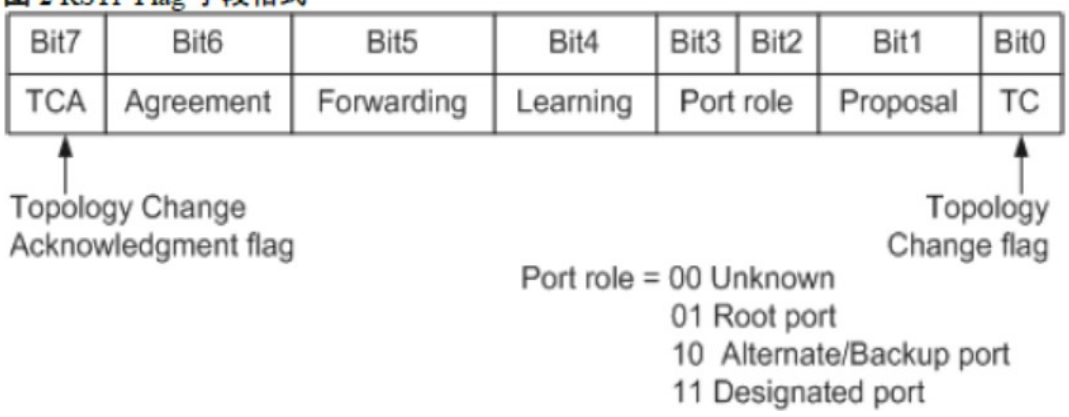
STP 端口状态	RSTP 端口状态	端口在拓扑中的角色
Forwarding	Forwarding	包括根端口、指定端口
Learning	Learning	包括根端口、指定端口
Listening	Discarding	包括根端口、指定端口
Blocking	Discarding	包括 Alternate 端口、Backup 端口
Disabled	Discarding	包括 Disable 端口

4 Flags 字段

STP：STP 中只使用了 flag 中最高位和最低位。最低位是 TC，最高位是 TCA

RSTP：RSTP 使用了在 STP 保留的中间 6 位

图 2 RSTP Flag 字段格式



Bit3 和 Bit2：端口角色
00：未知
01：根端口
10：Alternate / Backup
11：指定端口

5 生成树保护

STP 没有保护 ，RSTP 有 4 种保护

1 BPDU 保护：保护边缘端口在收到了 BPDU 以后，会将该端口 error-down，同时通知网管。
只能针对与边缘端口保护
配置：stp bpdu-protection //在系统视图下

2 根保护：当该端口收到更优的 RST BPDU 后，端口进入 Discarding 状态，不再转发报文。若一段时间内端口未收到更优的 RST BPDU，则会自动恢复到正常的 Forwarding 状态
只能在指定端口上保护
配置：stp root-protection //在接口试图下

3 环路保护 loop-protection . 在启动了环路保护功能后，如果

根端口或 Alternate 端口长时间收不到来自上游设备的 BPDU 报文，则向网管发出通知信息（此时根端口会进入 Discarding 状态，角色切换为指定端口），而 Alternate 端口则会一直保持在阻塞状态（角色也会切换为指定端口），不转发报文，从而不会在网络中形成环路。
只在根端口或 Alternate 端口上生效
配置：stp loop-protection //在接口试图下

4 TC-BPDU 泛洪保护：当设备收到 TC-BPDU 以后，在单位时间内会有一个限制的次数。
配置：stp tc-protection threshold 在系统视图下+可处理的报文数量

6 RSTP 边缘端口 edged port

1 接入设备进入转发，不等 30s
2 边缘端口进入转发时不产生 TC BPDU
3 生成树拓扑变化时，P/A 收敛不会阻塞边缘端口
4 收到 TC 不删除 mac 地址
5 不向边缘端口发送 TC BPDU
6 如果边缘端口收到 BPDU 将变为普通端口，参与生成树选举

7 端口快速切换机制

STP 在任何的情况端口从阻塞到转发最少需要 30S。RSTP 在以下的场景下，端口从阻塞到转发不需要转发延迟：

① 根端口快速切换机制
如果网络中一个根端口失效，那么网络中最优的 Alternate 端口将成为根端口，直接进入 Forwarding 状态，无需任何转发延迟。

② 边缘端口机制
边缘端口不参与 RSTP 运算，可以由 Disable 直接转到 Forwarding 状态，且不经历时延。
③Proposal/Agreement 机制
当一个端口被选举成为指定端口之后，在 STP 中，该端口至少要等待一个 Forward Delay（Learning）时间才会迁移到 Forwarding 状态。而在 RSTP 中，此端口会先进入 Discarding 状态，再通过 Proposal/Agreement 机制快速进入 Forwarding 状态。这种机制必须在点到点全双工链路上使用。

======
如果网络中一个根端口失效，那么网络中最优的 Alternate 端口将成为根端口，进入 Forwarding 状态。因为通过这个 Alternate 端口连接的网段上必然有个指定端口可以通往根桥。
RP 出现问题，AP 会变成 RP
DP 出现问题，BP 会变成 DP

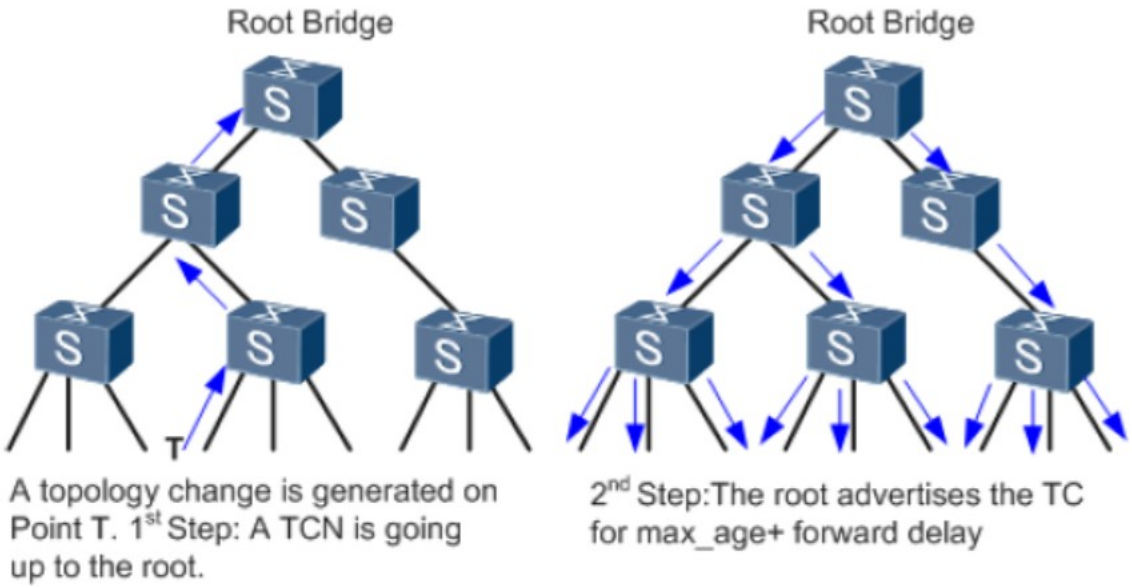
故障恢复
STP 直连故障 30，非直连故障　50
RSTP 直连故障 立即，非直连故障　3 倍 BPDU 时间，6 连续丢 3 个 BPDU 报文，RSTP 就认为链路出再故障，要进行切换

8 P/A 机制　分段
Proposal/Agreement 机制
当一个端口被选举成为指定端口之后，在 STP 中，该端口至少要等待一个 Forward Delay（Learning）时间才会迁移到 Forwarding 状态。而在 RSTP 中，此端口会先进入 Discarding 状态，再通过 Proposal/Agreement 机制快速进入 Forward 状态。这种机制必须在点到点全双工链路上使用。

1 上游设备发送 Proposal 报文，启动等待定时器。
2 下游设备堵塞全部其它端口，回应上游 Agreement 报文。
3 上游设备收到 Agreement 报文，端口进入转发状态。
通过一层一层的往下游请求，下游同意快速收敛，上游进入转发，实现整个 RSTP 网络快速收敛。

9 TC 处理机制

在标准 STP 中检测拓扑是否发生变化的标准为有端口 down/Up，而在 RSTP 中检测拓扑是否发生变化只有一个标准：一个非边缘端口迁移到 Forwarding 状态。
标准 STP 一旦检测到拓扑发生变化，非根桥交换机先触发 TCN 给到根桥交换机，在由根桥交换机触发 TC，此机制过于繁琐并且效率低下。
而 RSTP 一旦检测到拓扑发生变化，将进行如下处理：
① 为本交换设备的所有非边缘指定端口启动一个 TC While Timer，该计时器值是 Hello Time 的两倍（4s ）。在这个时间内， 清空状态从 Discarding 到 Forwarding 的端口上学习到的 MAC 地址。
② 同时，由这些端口向外发送 RST BPDU，其中 TC 置位。一旦 TC While Timer 超时，则停止发送 RST BPDU。
③ 其他交换设备接收到 RST BPDU 后，清空所有端口学习到 MAC 地址，除了收到 RST BPDU 的端口。同时也为自己所有的非边缘指定端口和根端口启动 TC While Timer，重复上述过程



10 收到次优 BPDU 会立即回复优质 BPDU

当一个端口收到上游的指定桥发来的 RST BPDU 报文时，该端口会将自身存储的 RST BPDU 与收到 RST BPDU 进行比较如果该端口存储的 RST BPDU 优先级高于收到的 RST BPDU ，那么该端口会直接丢弃收到的 RST BPDU ，立即回应自身存储的 RST BPDU 。当上游设备收到下游设备回应的 RST BPDU ，上游设备会根据收到的 RST BPDU 报文中相应的字段立即更新自己存储的 RST BPDU 。由此，RSTP 处理次优 BPDU 报文不再依赖于任何定时器通过超时解决拓扑收敛，从而加快了拓扑收敛。

STP 协议

扩展问题 1：STP 选举四要素？

1.根桥 ID（Root ID=根桥的优先级+mac 地址）

2.根路径开销（RPC：根据接口的带宽计算）

3.发送者桥 ID（Bridge ID=发送者交换机的优先级+mac 地址）

4.发送者端口 ID（Port ID=发送端口的优先级+端口编号）

若以上四个比较不出来：
5.接收端口的 ID（接收端口优先级+端口编号）

扩展问题 2：STP 的各种状态是如何处理 BPDU？
STP 端口状态：
Forwarding：若是 RP 端口则接收 BPDU，若是 DP 端口则发送。
Learning：若是 RP 端口则接收 BPDU，若是 DP 端口则发送。
Listening：若是 RP 端口则接收 BPDU，若是 DP 端口则发送。
Blocking：端口仅接收并处理 BPDU。
Disabled：端口不处理 BPDU 报文。

扩展问题 3：华为交换机如果接口关闭了 STP，收到 BPDU 会如何处理？
BPDU 报文发送的目的地址为 01-80-C2-00-00-00，华为交换机如果接口关闭了 STP，收到目的 MAC 地址为：01-80-C2-00-00-00 组播数据帧会接收不处理。
说明：开启了 STP 的交换机收到 01-80-C2-00-00-00 组播数据帧会进行 STP 的计算不会泛洪，计算完成之后（修改 bpdu 的发送者桥 ID 以及相应的根路径开销），再从 DP 端口发出。

扩展问题 4：边缘端口的端口角色是什么角色？
DP 端口，因为该端口没有收到更优的 BPDU，当一台运行 STP 的交换机刚启动，端口的角色为 DP 端口，只有收到比该端口优的 BPDU 才会迁移成其他的角色，边缘端口一般用于连接终端设备，不会收到 BPDU，即端口角色为 DP 端口。

扩展问题 5：如果一个端口收到比自己还要差的 BPDU 会怎么处理？
华为将这种 BPDU 称为次优 BPDU，华为交换机收到次优 BP

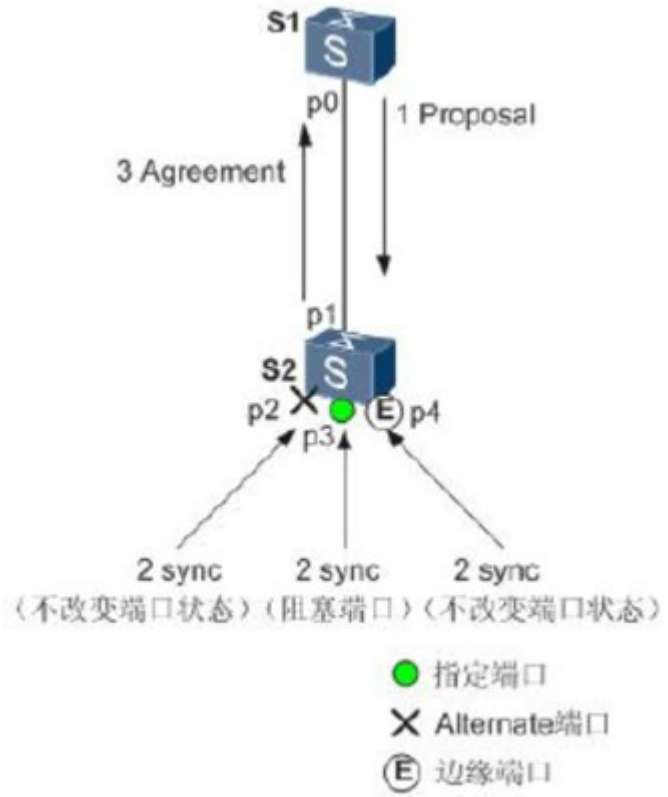
DU 会丢弃该 BPDU，并发送自己接口的最优的 BPDU（stp 与 rstp 处理行为一致）。

扩展问题 6：STP 中为什么要设计转发延迟时间？
STP 如果没有 forwarding delay 可能会带来的临时环路问题：在一个端口从不转发状态进入转发状态之前，需要等待一个足够长的时间，以使需要进入不转发状态的端口有足够时间完成生成树计算，并进入不转发状态
说明：RSTP 采用同步机制，避免临时环路问题。

扩展问题 7：运行 STP 的交换机是怎么感知拓扑发送变化的，为什么要发送 TCBPDU，不发会怎么样？
标准的 STP 中当一个接口 DOWN/UP 则认为拓扑发生。
拓扑发生变化之后，原有的 MAC 地址表是不能正确引导数据转发的，如果不发 TCBPDU 刷新 MAC 地址表，会导致数据流量无法正常转发，要等 300S 的 MAC 地址表老化时间后，才会刷新 MAC 地址表。

扩展问题 8：什么情况下会触发 P/A 协商？
点到点全双工链路。

扩展问题 9：P/A 协商过程？
新链路连接成功后，P/A 机制协商过程如下：



<1>p0 和 p1 两个端口马上都先成为指定端口，发送 RST BPDU

<2>S2 的 p1 口收到更优的 RST BPDU，意识到自己不是指定端口，S2 停止发送 RST BPDU

<3>S1 的 p0 进入 Discarding 状态，发送的 RST BPDU 中把 proposal 置 1

<4>S2 收到根桥发送来的携带 proposal 置位的 BPDU 时，开始将自己的所有端口进入 sync 变量置位（RP 阻塞其他非边缘端口，自己转为 forwarding 状态）

<5>p2 已经阻塞，状态不变；p4 是边缘端口，不参与运算；所以只需要阻塞非边缘指定端口 p3

<6>除了边缘端口的其他端口都进入 Discarding 状态之后，各端口的 synced 变量置位。当所有的端口都设置为 synced 后，根端口 p1 的 synced 也置位，便向 S1 返回 Agreement 位置位

的 RST BPDU 并进入 forwarding 状态。该 RST BPDU 携带和刚才根桥发过来的 BPDU 一样的信息，除了 Agreement 位置位（Proposal 位清零）
<7>当 S1 判断出这是对刚刚发出的 Proposal 的回应，端口 p0 马上进入 Forwarding 状态

以上 P/A 过程可以向下游继续传递
说明：P/A 机制要求两台交换设备之间链路必须是点对点的全双工模式。一旦 P/A 协商不成功，指定端口的选择就需要等待两个 Forward Delay，协商过程与 STP 一样。

扩展问题 10：rstp 比 stp 收敛快，快在哪里?
1、P/A 协商机制
2、AP 端口备份机制
3、边缘端口

扩展问题 12：P/A 机制的协商一定要是点到点的全双工吗？
是的，一定要是点到点的全双工

扩展问题 13：MSTP 相对于 RSTP 和 STP 的优点？
1、MSTP 支持链路负载分担，而 STP/RSTP 不支持：
RSTP 所有的 VLAN 在一棵树上即一个实例，单无法现实负载负担；
MSTP 有实例的概念，一个实例相当于一颗树，将不同实例的根设置在不同的交换机上，然后将不同的 vlan 映射到不同的实例里，实现流量负载分担，提高链路的利用率。
2、MSTP 有域的概念，而 STP/RSTP 没有：
MSTP 可以将设备分别划分到不同域中，每个域单独收敛，域中的一台设备发生变化，只会影响该域，不会应该整个网络。

扩展问题 14：如何判断设备是否在同一 MSTP 域？

1.都启动了 MSTP。

2.具有相同的域名。

3.具有相同的 VLAN 到生成树实例映射配置。

4.具有相同的 MSTP 修订级别配置。