

精选 Q & A

《常见问题答复集》第六期来啦！

本期主要内容：路由篇、组播篇

路由篇

Q1 在同一设备上配置的VPN网段和公网网段相同，会冲突吗？

会因为网段冲突而导致网络故障。在同一设备上配置的VPN网段和公网网段相同，其他设备在转发报文时，**优先选择直连路由的下一跳地址**，而不是为VPN网段配置的静态路由下一跳，导致ping不通。需要将直连网段地址修改为其他网段的地址才可解决该问题。

Q2 策略路由配置错误导致Ping不通故障如何排查？

配置了策略路由后，满足一定条件的报文会优先通过策略路由执行指定的操作（例如设置报文的下一跳）。如果策略路由配置错误，可能会导致报文转发失败。例如设备对本地报文应用了策略路由，在策略中指定了错误的下一跳地址，导致报文转发失败。

可通过如下步骤查看策略路由的配置，并作出相应的修改。

1. 执行**display ip policy-based-route**命令，查看已经配置的策略。如果配置了策略路由，则继续执行下一步。

2. 执行**display ip policy-based-route setup**命令，查看已经应用的策略路由信息，并分别通过如下命令查看具体类型的策略路由信息：

(1) 执行**display ip policy-based-route local**命令，查看本地策略路由的配置信息和统计信息。

(2) 执行**display ip policy-based-route interface**命令，查看接口下转发策略路由的配置信息和统计信息。

(3) 执行**display ip policy-based-route apply**命令，查看VLAN接口上应用的策略路由及其统计信息。

(4) 执行**display ip policy-based-route global**命令，查看全局策略路由的配置信息和统计信息。

(5) 执行**display ip policy-based-route egress interface**命令，查看VXLAN隧道接口出方向策略路由的配置信息和统计信息。

3. 如果策略路由的if-match子句配置了ACL匹配规则，可通过**display acl**命令查看ACL的配置和运行情况。

4. 修改策略路由，保证设备间流量正常转发。

(1) 如果是策略路由的匹配规则或apply子句导致的流量不通，则需要修改策略路由的匹配规则或apply子句。

(2) 如果是策略路由应用的接口错误，则需要先取消对应接口的策略路由配置，再重新将策略路由应用到正确的接口上。

(3) 如果应用和全局策略路由或本地策略路由，则需要先取消对应的配置。修改策略路由确保不会对正常的报文造成影响后，再重新应用策略路由。

Q3 静态路由的出接口没UP会导致Ping不通吗？

在配置静态路由时，指定的出接口需要为UP状态，否则静态路由不生效。

Q4 终端设备如果未配置网关，会导致通信故障吗？

会出现故障。如果组网环境中有多网段，为实现终端设备跨网段互相通信，则终端设备需要配置网关，并且非直连的网关设备之间需要配置到达目的网段的路由。

Q5 为什么配置的备份静态路由未及时生效？

设备上配置了到达目的网段的主用静态路由和备用静态路由，当主用链路故障时，设备可能未检测到，备用链路的静态路由不能及时生效导致流量丢失。

建议配置静态路由**关联track项**，通过track联动nqa对主用链路进行检测。当主用链路发生故障时，设备能及时发现并撤销主用静态路由，启用备用静态路由指导报文转发，将链路故障的影响降到最低。

Q6 为什么配置了静态路由关联track项，却无法通过track关联的检测模块及时检测链路故障？

请按照如下顺序进行排查：

1. 首先排查**检测模块的配置**是否正常，如果检查没问题，再进行下一步骤。

2. 检查静态路由关联track项的配置是否成功。执行**display current-configuration | include route-static**命令查看静态路由的配置情况。在配置静态路由时，应严格按照各产品命令参考里的顺序配置各个参数，否则会配置失败。其中，**description参数后面不能配置其他参数，只能输入静态路由描述信息**。

Q7 BGP邻居关系未建立的常见原因有哪些？如何处理此类故障？

本类故障的常见原因主要包括：

1. BGP报文转发不通

2. ACL过滤了TCP的179端口

3. 配置的邻居的AS号错误

4. 邻居的IP地址/IPv6地址配置错误

5. 未配置peer enable命令

6. 用Loopback口建立邻居时没有配置peer connect-interface

7. 用非直连的EBGP邻居未配置peer ebgp-max-hop

8. peer valid-ttl-hops配置错误

9. 对端配置了peer ignore

10. 两端的地址族不匹配

本类故障的处理步骤为：

1. 使用ping命令检查链路是否畅通。

2. 检查路由表中是否存在到邻居的可用路由。

3. 使用**display tcp verbose**命令或**display ipv6 tcp verbose**命令检查TCP连接是否正常。

4. 检查是否配置了禁止TCP端口179的ACL。

5. 执行**display current-configuration**命令查看当前配置，检查邻居的AS号配置是否正确。

6. 执行**display bgp peer ipv4 unicast**命令或**display bgp peer ipv6 unicast**命令检查邻居的IP地址/IPv6地址是否正确。

7. 如果使用Loopback接口，检查是否配置了peer connect-interface命令。

8. 如果是物理上非直连的EBGP邻居，检查是否配置了peer ebgp-max-hop命令。

9. 如果配置了peer ttl-security hops命令，请检查对端是否也配置了该命令，且保证双方配置的hop-count不小于两台设备实际需要经过的跳数。

10. 检查两端设备是否配置了peer ignore，如果想建立邻居关系，执行**undo peer ignore**命令即可。

11. 请检查BGP会话两端的地址族能力是否匹配。例如，建立BGP VPNv4邻居时，需要两端都要在BGP-VPNv4地址族下配置命令peer enable。

Q8 怎么查看和配置等价路由条数？

当到达同一目的地址的多条等价路由的条数超过了设备支持的最大条数时，新增的等价路由无法和已存在的等价路由一起形成负载分担。

通过如下命令可以**查看系统当前支持的最大等价路由的条数**：

1. 执行**display max-ecmp-num**命令用来显示系统支持IPv4最大等价路由的条数。

2. 执行**display ipv6 max-ecmp-num**命令用来显示系统支持IPv6最大等价路由的条数。

通过如下命令可以**调整系统支持的最大等价路由的条数**：

1. 执行**max-ecmp-num**命令调整设备支持的最大IPv4等价路由的条数。

2. 执行**ipv6 max-ecmp-num**命令用来配置系统支持IPv6最大等价路由的条数。

Q9 不同VRF或公网与VRF如何通过三层接口实现互访？

可通过多种方式实现不同VRF之间或公网与VRF之间通过三层接口实现互相访问：

方法一、配置静态路由实现三层接口路由互通：

在执行**ip route-static vpn-instance**命令时，同时指定源和目的VPN实例，实现不同VPN实例下三层接口之间的路由互通；在执行**ip route-static vpn-instance**命令时，指定下一跳地址属于公网实例，实现公网与指定VPN实例的路由互通；在执行**ip route-static**命令时，同时指定下一跳地址属于VPN实例，实现公网与指定VPN实例的路由互通。

方法二、配置BGP路由由协议实现三层接口路由互通：

执行**import-route**命令引入不同VPN实例的IGP路由，实现三层接口路由互通。

方法三、配置路由信息引入功能实现三层接口路由互通：

在VPN实例IPv4地址族视图下执行**route-replicate**命令，将公网或其他VPN实例的路由信息引入到指定VPN实例中；在公网实例IPv4地址族视图下执行**route-replicate**命令，将指定VPN实例的路由信息引入到公网中。

Q10 如何查看设备是否支持前缀大于64位的IPv6路由？

缺省情况下，部分设备不支持前缀大于64位的IPv6路由，即使配置成功，该类型的路由也不能指导报文转发。

通过**display switch-routing-mode status**命令查看前缀大于64位的IPv6路由功能的支持情况。通过**switch-routing-mode ipv6-128**命令开启前缀大于64位的IPv6路由功能。

组播篇

Q1 组播组网，接入设备配置二层组播后，为什么网络卡顿、延迟高？

需要配置**未知组播数据报文丢弃功能**。

当未配置丢弃未知组播数据报文功能时，二层设备收到未知组播数据报文时，会在未知组播数据报文所属的**VLAN/VSI内广播**该报文。当二层设备收到大量未知组播报文时，网络中会充斥着大量的未知组播报文，从而导致网络卡顿、延迟高。

配置丢弃未知组播数据报文后，二层设备**只向其路由器端口转发**未知组播数据报文，不在VLAN/VSI内广播。如果二层设备没有路由器端口，未知组播数据报文会被丢弃，不再转发。

Q2 组播组网，二层接入设备配置了IGMP Snooping和IGMP Snooping drop-unknown功能后，为什么组播转发表项异常？

需要将二层接入设备的IGMP Snooping**版本配置为3**。

缺省情况下，二层设备开启IGMP Snooping功能后，设备上的IGMP Snooping**版本为2**。当三层设备的IGMP版本和用户主机的IGMP版本为3时，二层设备收到用户主机发送的IGMPv3的成员关系报告报文后，无法处理IGMPv3的成员关系报文，将在VLAN/VSI内广播该报文。

将二层设备的IGMP Snooping版本**修改为3后**，IGMP Snooping设备在收到IGMP成员关系报告报文时，二层设备将其通过VLAN/VSI内的**所有路由器端口转发**出去，从该报文中解析出主机要加入的组播组地址，**并对该报文的接收端口做如下处理**：

1. 如果不存在该组播组所对应的转发表项，则创建转发表项，将该端口作为动态成员端口添加到出端口列表中，并启动其老化定时器。

2. 如果已存在该组播组所对应的转发表项，但其出端口列表中不包含该端口，则将该端口作为动态成员端口添加到出端口列表中，并启动其老化定时器。

3. 如果已存在该组播组所对应的转发表项，且其出端口列表中已包含该动态成员端口，则重置其老化定时器。

Q3 什么情况下需要配置查询器？是否可以配置多个查询器？

在运行了IGMP的组播网络中，会有一台三层组播设备充当IGMP查询器。该查询器负责发送IGMP查询报文，在网络层建立并维护组播转发表项，从而正常转发组播数据。

当组播组网中没有三层设备，而二层设备不支持IGMP时，如果没有设备充当查询器，会导致无法建立组播转发表项。此时就需要在**二层设备上开启IGMP Snooping查询器功能**，从而能够在数据链路层建立并维护组播转发表项。

为了防止因单一IGMP Snooping查询器发生故障而引起组播业务中断，在同一网段、同一VLAN/VSI内可以配置多个查询器。但正常情况下，同一网段、同一VLAN/VSI内只需要一个查询器。过多的查询器会导致网络中充斥着大量的查询报文、组播接收者也会接收到多份同样的数据报文，导致网络非常拥塞。

通过在设备上开启IGMP Snooping**查询器选举功能**可以解决这个问题。选举出的IGMP Snooping查询器发生故障无法正常工作后，VLAN/VSI内各设备会重新选举出新的IGMP Snooping查询器以保证组播业务正常转发。

