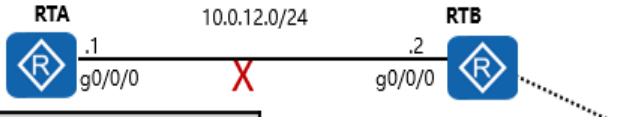
常见网络故障排除

前言

- 当网络发生故障时，最困难的不是修复网络故障本身，而是如何迅速地查出故障所在，并确定发生的原因。在本课程中，您将学习到常见网络故障的排除方法，掌握如何快速地查出问题的根源，从而排除故障，恢复网络的正常运行。

Telnet登录故障



序号	配置步骤
1	配置Telnet服务器功能及参数。
2	配置Telnet用户登录的用户界面。
3	配置Telnet类型的本地用户（AAA验证方式）。
4	从终端通过Telnet登录设备。

```
acl number 2001
 rule 5 permit source 10.0.12.1 0
 rule 10 deny #
aaa
 local-user admin1234 password cipher huawei
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
user-interface maximum-vty 8
#
user-interface vty 0 7
 acl 2001 inbound
 authentication-mode aaa
```

- 路由不可达，客户端和服务器无法建立TCP连接。
- 登录设备的用户数到达了上限。
- VTY用户界面下绑定了ACL。
- VTY用户界面下允许接入的协议不正确。如配置为protocol inbound ssh。

- Telnet 协议在 TCP/IP 协议族中属于应用层协议，通过网络提供远程登录和虚拟终端功能。以服务器/客户端（Server/

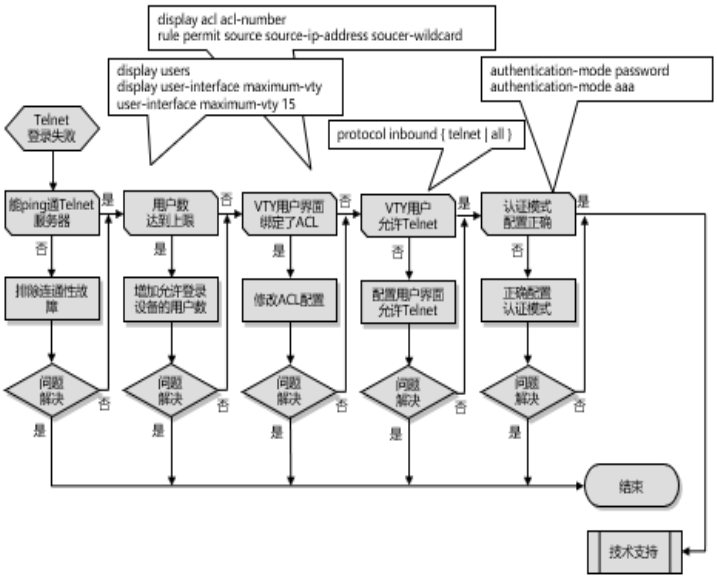
Client）模式工作，Telnet 客户端向 Telnet 服务器发起请求，Telnet 服务器提供 Telnet 服务。设备支持 Telnet 客户端和 Telnet 服务器功能。

- 缺省情况下，用户不能通过 Telnet 方式直接登录设备。

如果需要通过 Telnet 方式登录设备，可以先通过 Console 口本地登录设备，并完成以下步骤：

- 确保终端和登录的设备之间路由可达。
- 配置 Telnet 服务器功能及参数。
- 配置 Telnet 用户登录的用户界面。
- 配置 Telnet 类型的本地用户（AAA 验证方式）。
- 从终端通过 Telnet 登录设备。
- Telnet 登录故障常见原因有：
- 路由不可达，客户端和服务器无法建立 TCP 连接。
- 登录设备的用户数到达了上限。
- VTY 用户界面下绑定了 ACL。
- VTY 用户界面下允许接入的协议不正确。如配置为 protocol inbound ssh 时，使用 Telnet 将无法登录。

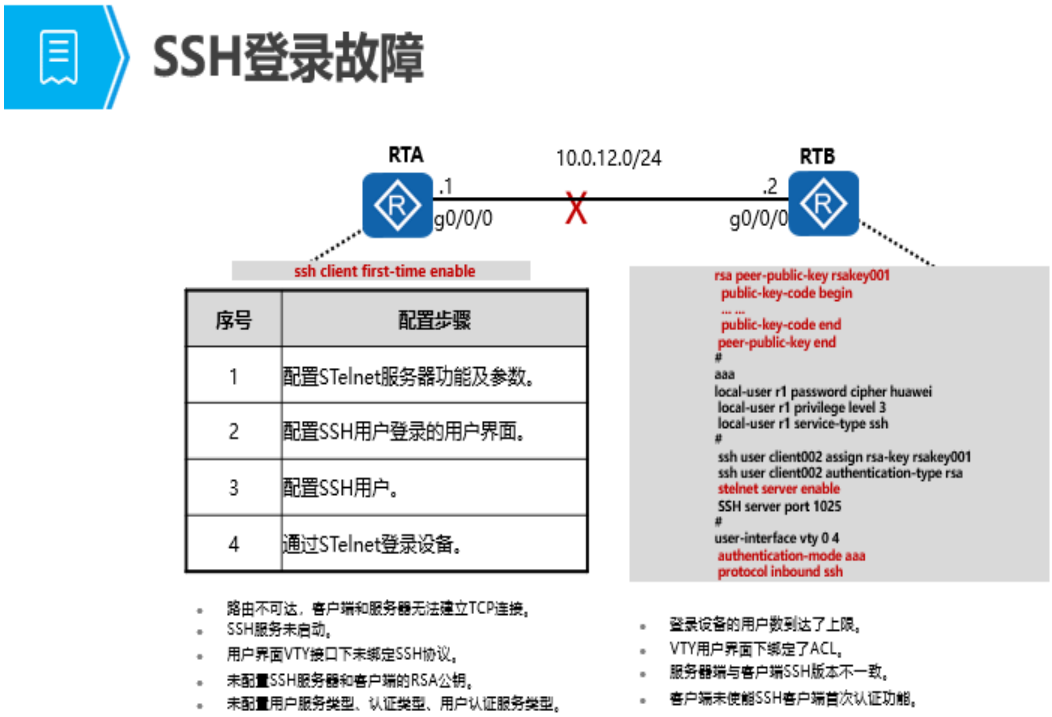
Telnet登录故障 - 排障流程



- 检查客户端能否 Ping 通服务器。
- 在客户端使用 ping 命令查看网络连接情况。如果不能 Ping 通，则 Telnet 连接也将失败。
- 如果 Ping 不通，应先排除客户端到服务器的连接性故障，使 Telnet 客户端能 Ping 通服务器端。
- 查看登录设备的用户数是否到达了上限。
- 从 Console 口登录到设备，执行命令 display users，查看当前的 VTY 通道是否全部被占用。缺省情况下，VTY 通道允许的最大用户数是 5 个，可以先执行命令 display user-interface maximum-vty，查看当前 VTY 通道允许的最大用户数。
- 如果当前的用户数已经达到上限，可以执行命令 user-interface maximum-vty 15，将 VTY 通道允许的最大用户数扩展到 15 个。
- 查看设备上 VTY 类型用户界面视图下是否配置了 ACL。
- 在 Telnet 服务器端上执行命令 user-interface vty 进入用户界面视图，执行命令 display this，查看 VTY 用户界面是否配置了 ACL 限制，如果配置了 ACL 限制，请记录该 ACL 编

号。

- 在 Telnet 服务器端上执行命令 display acl acl-number，查看该访问控制列表中是否 deny 了 Telnet 客户端的地址。如果 deny 客户端的 IP 地址，则在 ACL 视图下，执行命令 undo rule rule-id，删除 deny 规则，再执行命令 rule permit source source-ip-address soucer-wildcard，修改访问控制列表 permit 客户端的 IP 地址访问。

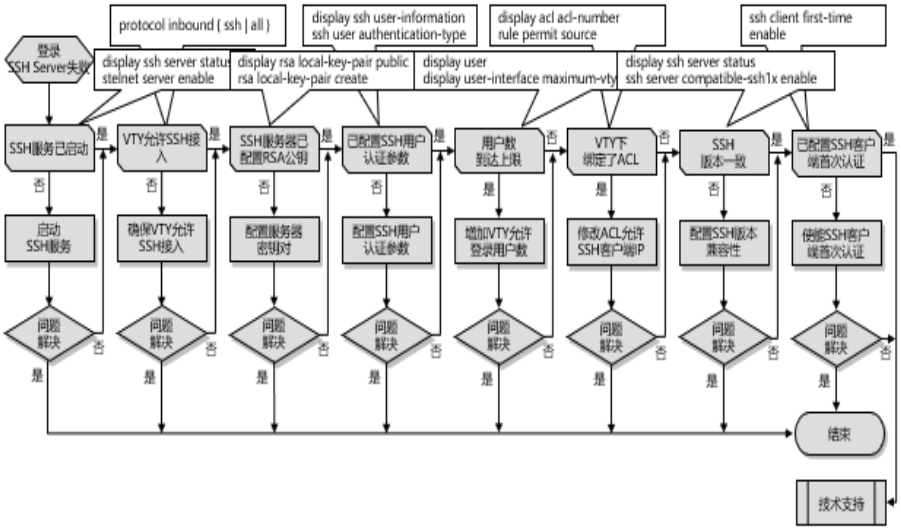


- Telnet 传输过程采用 TCP 协议进行明文传输，缺少安全的认证方式，容易招致 DoS（Denial of Service）、主机 IP 地址欺骗和路由欺骗等恶意攻击，存在很大的安全隐患。
- 相对于 Telnet，STelnet 基于 SSH2 协议，客户端和服务器端之间经过协商，建立安全连接，客户端可以像操作 Telnet 一样登录服务器端。
- 缺省情况下，用户不能通过 STelnet 方式直接登录设备。如果需要通过 STelnet 方式登录设备，可以先通过 Console 口

本地登录或 Telnet 远程登录设备，并完成以下步骤：

- 确保终端和登录的设备之间路由可达。
- 配置 STelnet 服务器功能及参数。
- 配置 SSH 用户登录的用户界面。
- 配置 SSH 用户。
- 通过 STelnet 登录设备。
- SSH 登录故障的常见原因主要包括：
- SSH Client 与 SSH Server 之间没有可达路由，无法建立 TCP 连接。
- SSH 服务未启动。
- 用户界面 VTY 接口下未绑定 SSH 协议。
- 没有配置 SSH 服务器和客户端的 RSA 公钥。
- 没有配置用户服务类型、认证类型、用户认证服务类型。
- 设备上登录用户数达到允许用户数的上限。
- user-interface vty 下绑定了 ACL 规则。
- 服务器端与客户端 SSH 版本不一致。
- 客户端未使能 SSH 客户端首次认证功能。

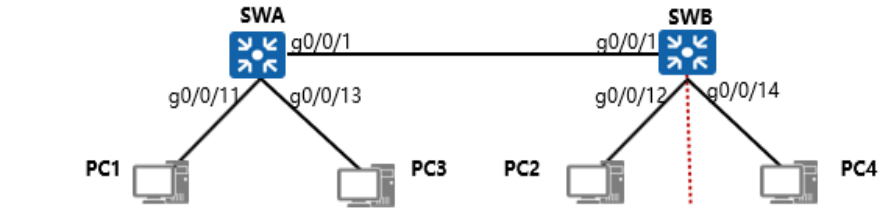
SSH登录故障 - 排障流程



- 查看 SSH 服务器端的 SSH 服务是否启动。
- 通过 Console 口或 Telnet 方式登录 SSH 服务器端，执行命令 display ssh server status，查看 SSH 服务器端配置信息。
- 如果 STelnet 没有使能，执行如下命令 stelnet server enable，使能 SSH 服务器端的 STelnet
- 服务。
- 在 SSH 服务器端上查看 VTY 类型用户界面视图下允许接入的协议配置是否正确。
- 在 SSH 服务器端上执行命令 user-interface vty 进入用户界面视图，执行命令 display this，查看 VTY 用户界面的 protocol inbound 是否为 ssh 或者 all。如果不是，执行命令 protocol inbound { ssh | all }修改配置，允许 STelnet 类型用户接入设备。
- 查看在 SSH 服务器端是否配置了 RSA 公钥。
- 设备作为 SSH 服务器时，必须配置本地密钥对。
- 在 SSH 服务器端上执行命令 display rsa local-key-pair public 查看当前服务器端密钥对信息。如果显示信息为空，则

表明没有配置服务器端密钥对，执行命令 rsa local-key-pair cr
eate 创建。

VLAN故障



序号	配置步骤
1	创建VLAN。
2	配置以太网接口的链路类型。
3	关联接口和VLAN。
4	检查配置结果。

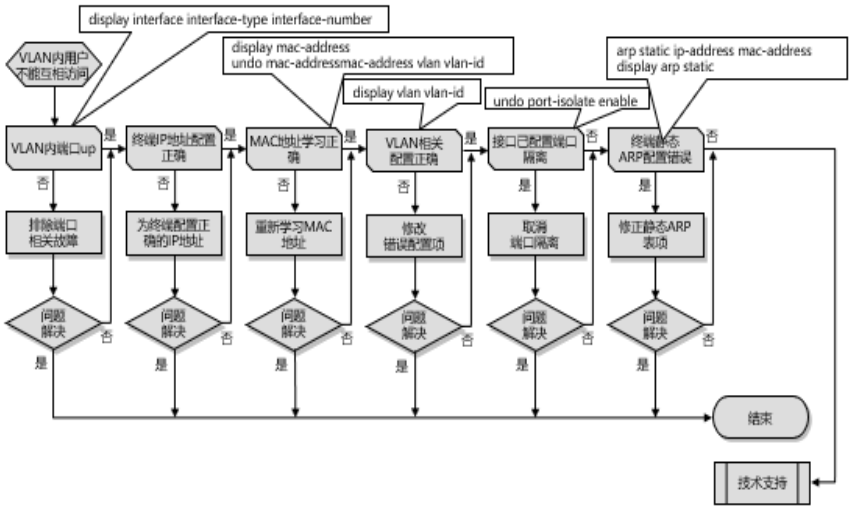
```
vlan batch 12 to 34
#
interface GigabitEthernet0/0/12
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/14
 port link-type access
 port default vlan  34
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 12 to 34
#
```

- 链路故障。
- 接口被人为shutdown或物理接口损坏。
- 交换机MAC地址学习错误。
- 交换机上配置了端口隔离。
- 主机配置了错误的静态ARP。
- 交换机上配置了错误的端口和MAC地址绑定。

- 以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detection）的共享通讯介质的数据网络通讯技术。当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至造成网络不可用等问题。通过交换机实现 LAN（Local Area Network）互连虽然可以解决冲突严重的问题，但仍然不能隔离广播报文和提升网络质量。这种情况下出现了 VLAN 技术，这种技术可以把一个 LAN 划分成多个逻辑 VLAN。每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间则不能直接互通，这样，广播报文就被限制在一个 VLAN 内。
- 配置 VLAN 的步骤为：
- 创建 VLAN。
- 配置以太网接口的链路类型。
- 关联接口和 VLAN。
- 检查配置结果。

- VLAN 故障常见原因有：
- 链路故障。
- 接口被人为 shutdown 或物理接口损坏。
- 交换机 MAC 地址学习错误。
- 交换机上配置了端口隔离。
- 主机配置了错误的静态 ARP。
- 交换机上配置了错误的端口和 MAC 地址绑定。

VLAN故障 - 排障流程

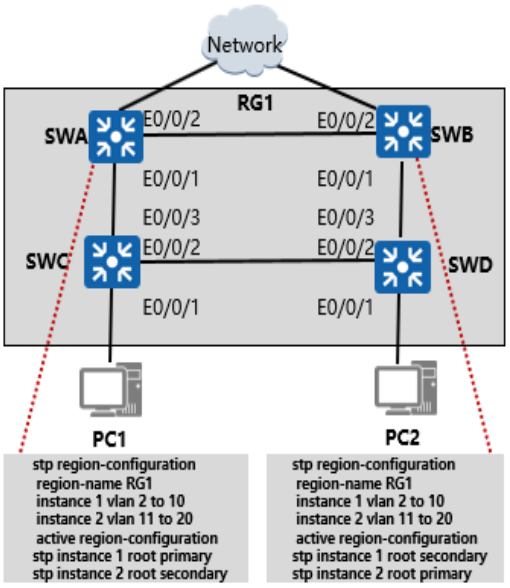


- 检查 VLAN 内需要互通的端口是否 Up。
- 在任意视图下执行 display interface interface-type interface-number 命令查看需要互通的端口的运行状态。如果接口的状态为 Down，先排除接口 Down 的故障。
- 检查需要互通的终端 IP 地址是否在同一网段，如果不是则修改为同一网段。
- 检查 Switch 上 MAC 地址表项是否正确。
- 在 Switch 上执行 display mac-address 检查设备学习到 MAC 地址、MAC 地址对应接口、所属 VLAN 是否正确，如果不正确则在接口上执行 undo mac-addressmac-address vlan

vlan-id 命令使 Switch 重新学习指定的 MAC 地址。

- 检查 VLAN 相关配置是否正确。
- 检查需要互通的端口所在的 VLAN 是否已经创建。在任意视图下执行 display vlan vlan-id 查看需要互通的端口所在的 VLAN 是否已经创建，如果未创建则在系统视图下执行 vlan 命令创建 VLAN。
- 检查需要互通的接口是否加入 VLAN。执行 display vlan vlan-id 检查需要互通的接口是否已经加入指定 VLAN，如果未加入则将接口加入指定 VLAN。如果需要互通的接口不在同一个交换机，还需要考虑交换机互联的接口允许指定的 VLAN 通过。
- 检查设备上是否配置了端口隔离。
- 在系统视图下执行 interface interface-type interface-number 进入故障接口视图，然后执行 display this 命令查看接口是否配置了端口隔离。如果配置了端口隔离，使用 undo port-isolate enable 命令取消端口上端口隔离配置。
- 检查终端设备上是否配置了错误的静态 ARP 表项，如果终端设备上配置了错误的静态 ARP 表项则修正。
- 使用 display arp static 命令查看静态 ARP 配置，使用命令 arp static ip-address mac-address 修改静态 ARP 配置。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

MSTP故障



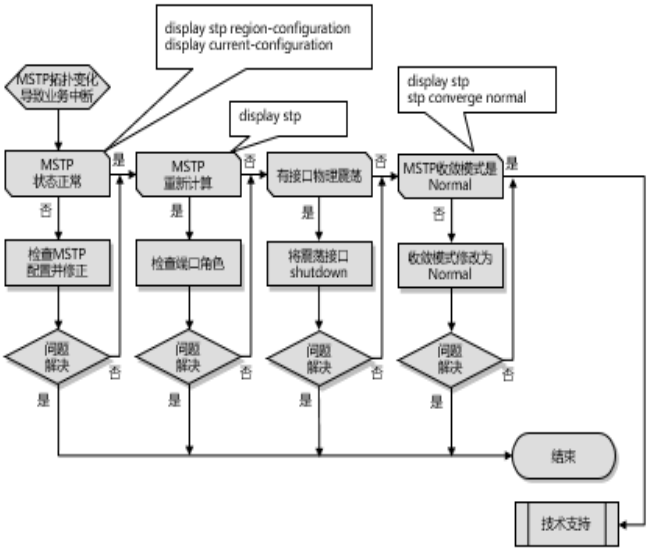
序号	配置步骤
1	配置MSTP工作模式
2	配置MST域并激活
3	（可选）配置根桥和备份根桥
4	（可选）配置交换设备在指定生成树实例中的优先级
5	（可选）配置端口在指定生成树实例中的路径开销
6	（可选）配置端口在指定生成树实例中的优先级
7	启用MSTP

- MSTP配置错误。
- 物理链路发生震荡，触发设备发送大量TC报文。
- 使能MSTP的设备收到客户端或透传的MSTP TC报文。

- 在一个复杂的网络中，由于冗余备份的需要，网络规划者一般都倾向于在设备之间部署多条物理链路，其中一条作为主用链路，其他作为备份链路。这样就难免会形成环路，若网络中存在环路，可能会引起广播风暴和 MAC 表项被破坏。为此，可以在网络中部署 MSTP 协议预防环路。MSTP 可阻塞二层网络中的冗余链路，将网络修剪成树状，达到消除环路的目的。
- MSTP 的配置步骤为：
- 配置 MSTP 工作模式。
- 配置 MST 域并激活。
- （可选）配置根桥和备份根桥。
- （可选）配置交换设备在指定生成树实例中的优先级。
- （可选）配置端口在指定生成树实例中的路径开销。
- （可选）配置端口在指定生成树实例中的优先级。
- 启用 MSTP。
- 检查配置结果。
- MSTP 故障的常见原因有：

- MSTP 配置错误。
- 物理链路发生震荡，触发设备发送大量 TC 报文。
- 使能 MSTP 的设备收到客户端或透传的 MSTP TC 报文。

MSTP故障 - 排障流程

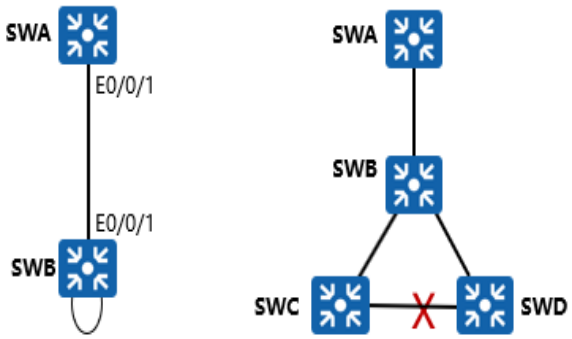


- 检查 MSTP 组网内的端口状态是否正常。
- 查看 MSTP 的端口状态，确认每个端口在每个实例的连通性。
- 检查 MSTP 配置是否正确。
- 执行命令 display stp region-configuration 检查 VLAN 与实例之间的映射关系。
- 查看 VLAN 与实例之间的映射关系是否正确。若出现映射关系错误，则执行命令 instance 将指定 VLAN 映射到指定的生成树实例上，并执行命令 active region-configuration 激活 instance 命令配置的 VLAN 与实例之间的映射关系。
- 执行命令 display current-configuration 获取设备的配置文件，查看设备上 MSTP 的相关配置。
- 查看端口配置，确认使能 MSTP 的端口是否使能了协议报文上送命令。如：bpdu enable。

- 与用户终端设备相连的端口 MSTP 是否是处于去使能状态或配置为边缘端口。
- 如果使能 MSTP 的设备上配置了 BPDU Tunnel，则确认 BPDU Tunnel 配置是否正确。
- 查看设备端口是否加入正确的 VLAN。

环路故障

- 环路如果导致广播风暴会导致用户通信质量较差，甚至通信中断。

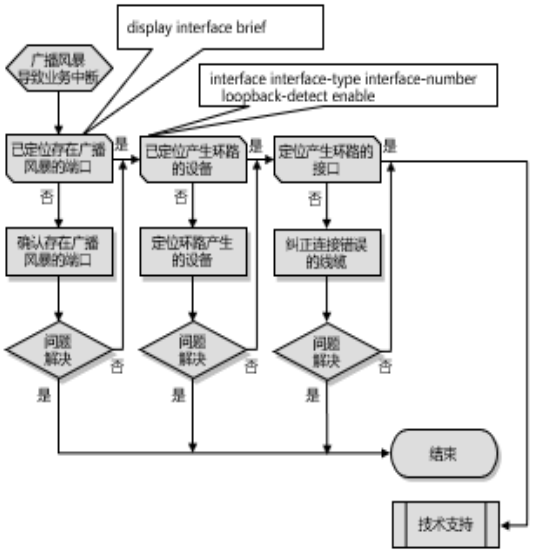


- 以太网是一个支持广播的网络，在没有环路的环境中，广播报文在网络中以泛洪的形式被送达到网络的每一个角落，以保证每个设备都能够接受到它。每台二层设备在接收到广播报文以后，都会向除接收端口以外的其他所有接口转发这个广播报文，一旦网络中有环路，这种简单的广播机制就会引发灾难性后果。
- 环路中一个广播报文被反复转发了千万次，产生了广播风暴并且很快达到或接近接口最大转发速率，并迅速消耗链路带宽。根据转发规则，这些广播报文不仅仅只是在环路上无限转发，环路设备还会向其他端口转发一份，造成整个网络中都充斥着大量重复广播报文。例如，全网络都采用千兆端口互连，出现广播风暴后，几乎每一条链路上都充斥着 1000Mbit/s 的

广播报文，正常的数据报文将很难再获得转发的机会。进而影响正常业务，导致用户通信质量较差，甚至通信中断。

- 可能会有如下现象产生：
- 设备无法远程登录。
- 在设备上使用 display interface 命令查看接口统计信息时发现接口收到大量广播报文。
- 使用串口登录设备进行操作时，操作比较慢。
- CPU 占用率超过 70%。
- 通过 ping 命令进行网络测试时丢包严重。
- 设备上发生环路的 VLAN 的接口指示灯频繁闪烁。
- PC 机上能收到大量的广播报文。
- 设备部署环路检测后，设备出现环路告警。
- 本类故障的常见原因主要为设备线缆连接错误导致环路。

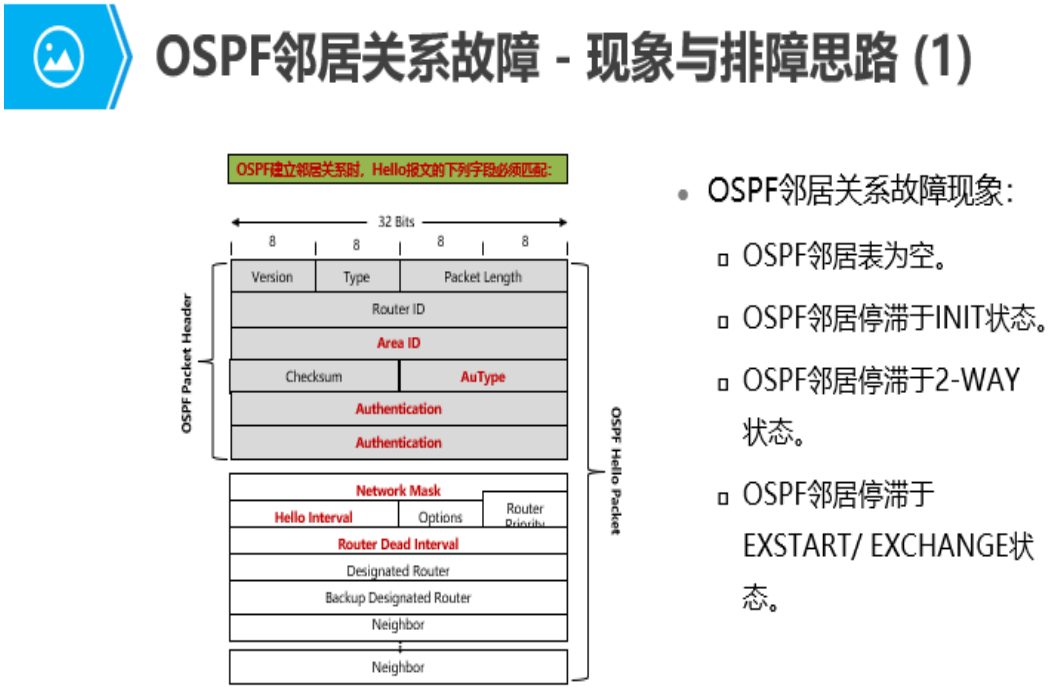
环路故障 - 排障流程



- 确认存在广播风暴的接口。
- 可以采用如下方式确认存在广播风暴的接口。
- 通过观察接口指示灯状态，如果接口指示灯频繁闪烁，

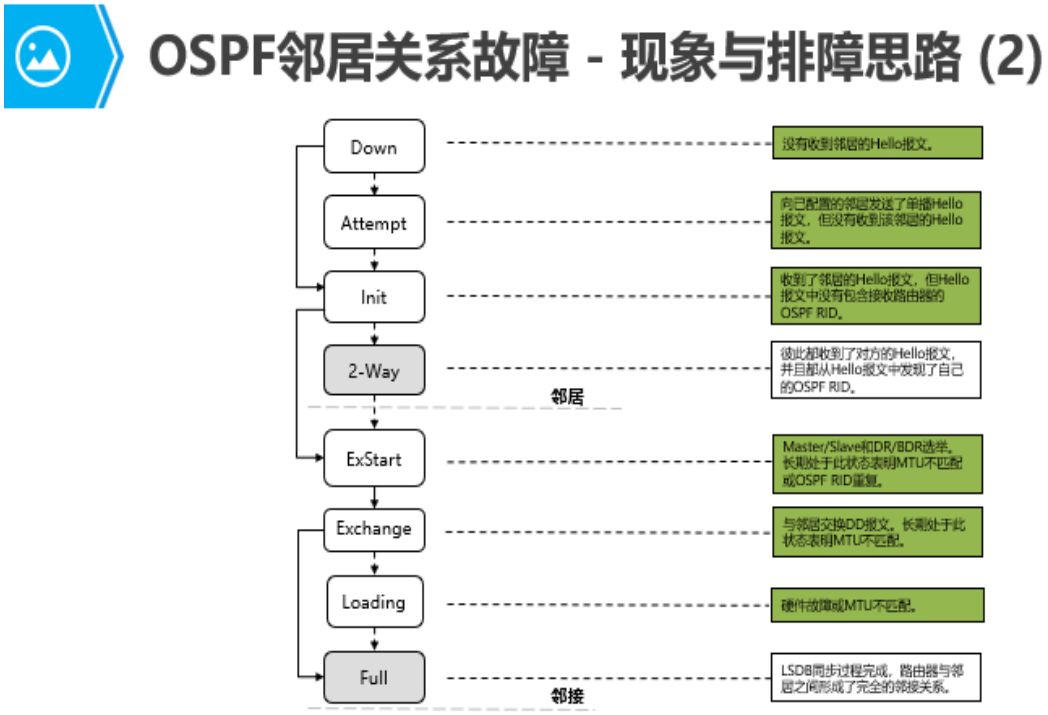
可以判断该接口可能存在广播风暴。

- 在设备上执行 display interface brief 命令查看接口接收方向和发送方向最近一段时间的带宽利用率。显示信息中“InUti”字段表示入方向上的带宽利用率，“OutUti”字段表示出方向上的带宽利用率。接口接收方向和发送方向最近一段时间的带宽利用率接近 100%的接口可能是存在广播风暴的接口。
- 判断环路产生的设备。
- 如果存在广播风暴的接口没有下连其他 Switch，此时可以判断环路发生在该 Switch 上。
- 如果存在广播风暴的接口下连其他 Switch，此时环路可能发生在该 Switch 上也可能发生在下连 Switch 上，此时可以选择如下方式进行环路检测：



- OSPF 建立邻居关系时，将检验 Hello 报文中的 Area ID、AuType、Authentication、Network Mask、Hello Interval、Router Dead Interval 字段以及可选项的值是否和接收接口上配置的对应值相匹配。如果它们不匹配，那么该数据包将被丢弃，而且邻接关系也无法建立。

- OSPF 邻居关系故障的常见现象为：
- OSPF 邻居表为空。
- OSPF 邻居停滞于 INIT 状态。
- OSPF 邻居停滞于 2-WAY 状态。
- OSPF 邻居停滞于 EXSTART/EXCHANGE 状态。

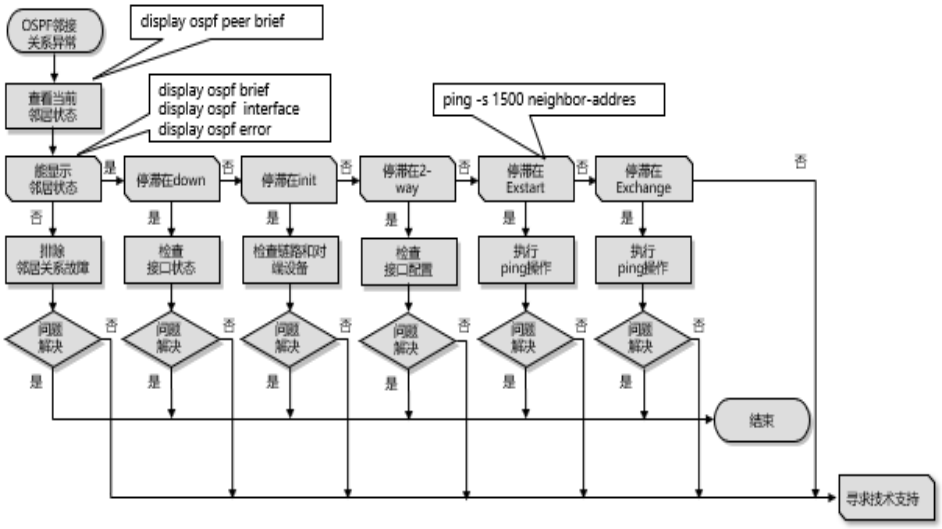


- 如果一个邻居停滞于以下某个状态并且持续很长时间，就代表着 OSPF 的邻居关系可能出现了故障。
- Down：这是邻居的初始状态，表示路由器还没有从邻居收到任何信息。停滞于此状态表明路由器没有从邻居处接收到 Hello 报文。
- Attempt：此状态只在 NBMA 网络上存在，表示路由器没有收到邻居的任何信息，但是已经周期性地向邻居发送了 Hello 报文；如果在 Router Dead Interval 的时间间隔内未收到邻居的 Hello 报文，则转为 Down 状态。停滞于此状态表明路由器向已配置的邻居发送了单播 Hello 报文，但没有收到该邻居的 Hello 报文。
- Init：表示路由器已经从邻居收到了 Hello 报文，但是自

己不在所收到的 Hello 报文的邻居列表中。这说明自己尚未与邻居建立起双向通信关系。停滞于此状态表明路由器收到了邻居的 Hello 报文，但 Hello 报文中没有包含接收路由器的 OSPF RID（Router ID）。

- 2-Way：表示路由器与邻居的双向通信关系已经建立（即已经建立起了邻居关系），但是尚未建立起邻接关系。停滞于此状态表明路由器彼此都收到了对方的 Hello 报文，并且都从 Hello 报文中发现了自己的 OSPF RID。对于以太网链路上的非 DR/BDR 路由器来说，这种状态是可以接受的。
- ExStart：邻居状态变成此状态以后，路由器开始向邻居发送 DD 报文。Master/Slave 关系是在此状态下形成的，初始 DD 序列号也是在此状态下确定的。在此状态下发送的 DD 报文不包含链路状态描述。停滞于此状态表明邻居路由器之间的 MTU 不匹配或 OSPF RID 重复。
- Exchange：在此状态下，路由器与邻居之间相互发送包含链路状态信息摘要的 DD 报文。停滞于此状态表明邻居路由器之间的 MTU 不匹配。
- Loading：在此状态下，路由器与邻居之间相互发送 LSR 报文、LSU 报文、LSAck 报文。停滞于此状态表明可能存在硬件故障或硬件故障或 MTU 不匹配。
- Full：表示 LSDB 同步过程完成，路由器与邻居之间形成了完全的邻接关系。

OSPF邻居关系故障 - 排障流程

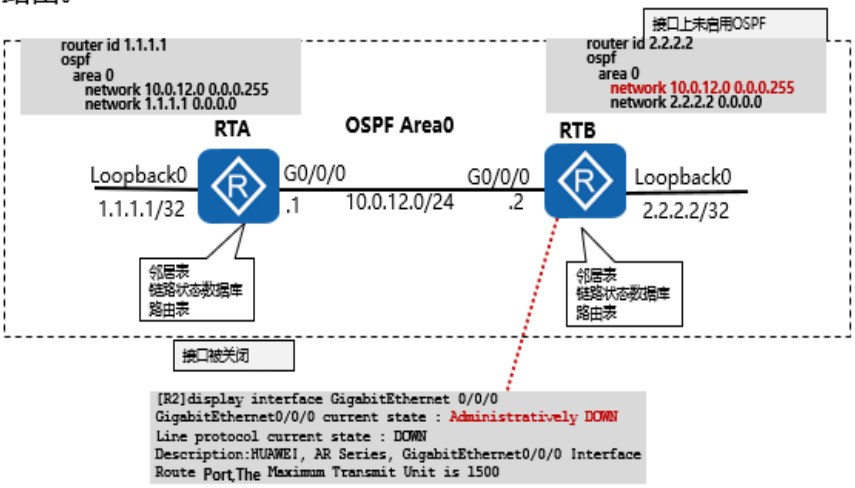


- 无法显示 OSPF 邻居：
- 执行 display interface [interface-type [interface-number]]命令查看接口物理层状态，检查设备链路是否故障（包括传输设备故障）。
- 如果接口连接的是广播网络或 NBMA 网络，检查两端 IP 地址是否在同一网段。
- 如果在接口上使能了 ospf mtu-enable，则要求接口的 MTU 一致，否则 OSPF 邻居无法协商成功。在接口视图下执行 mtu mtu 命令，修改链路两端的 MTU 值为一致。
- 对于 Broadcast 和 NBMA 类型的网段，各接口的优先级至少有一个是非零的，以确保能够正确的选举出 DR，否则两边的邻居状态只能达到 2-Way。执行命令 display ospf interface，查看接口的优先级。
- 检查两端 OSPF 的配置是否有错误：
- 检查两端 OSPF RouterID 配置是否相同：display ospf brief。如果相同则执行 ospf router-idrouter-id 命令修改配置使 Router ID 在 AS 域内唯一。

- 检查两端 OSPF Area 配置是否一致：display ospf inter face。
- 检查两端 OSPF 的其他配置是否一致：每 10 秒钟执行一次命令 display ospf error，持续 5 分钟。

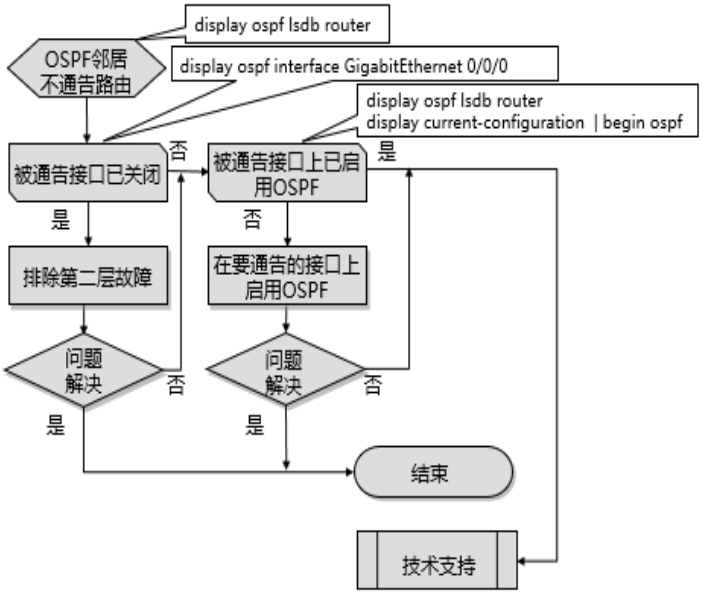
OSPF域内路由故障 - 现象与排障思路

- OSPF的域内路由故障常表现为邻居路由器不通告部分或全部路由。



- OSPF 的域内路由故障常表现为邻居路由器不通告部分或全部路由。可能的原因通常为：
- 拟通告的接口上未启用 OSPF。
- 拟通告接口被关闭。
- OSPF 是一种基于链路状态的内部网关路由协议，存在链路状态数据库。在运行了 OSPF 的路由器中需要重点关注邻居表、链路状态数据库（通常也会把它叫做“链路状态表”）、路由表。如果邻居不通告某条路由，那么这条路由将无法显示在本地路由器的路由表和 OSPF 链路状态数据库中。同时，这也表示邻居没有把这条路由包含到它自己的 OSPF 链路状态数据库中。

OSPF域内路由故障 - 排障流程



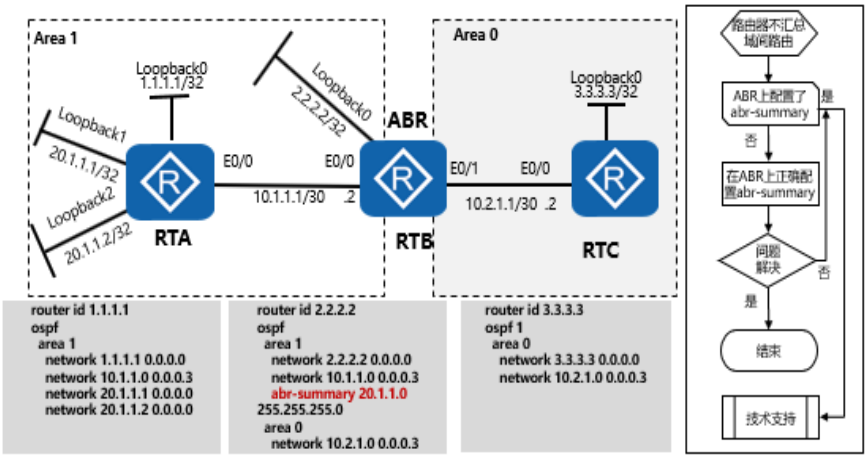
- 检查被通告接口是否被关闭。
- OSPF 不会通告断开的网络。所以如果一个接口被关闭了，那么分配给这个接口的网络不会被 OSPF 通告给邻居路由器。
- 使用命令 display ospf lsdb router 检查链路状态数据库中是否存在此网络的条目。
- display ospf interface GigabitEthernet 0/0/0 命令的输出结果可以显示链路协议状态。
- 解决方法是启用被关闭的接口、排除第二层的故障。
- 检查被通告接口上是否已启用 OSPF。
- 只有在接口上启用了 OSPF 的时候，链路状态数据库中才会包括这个接口的网络。network 语句的缺失或者配置错误都会导致链路状态数据库中缺少这个接口所在网络的路由。
- 使用命令 display ospf lsdb router 可以看到链路状态数据库中是否缺少某个网络的信息。
- 使用命令 display current-configuration | begin ospf 显示 OSPF 的配置命令，可以检查其中的 network 语句是否配

置正确。

- 如果故障无法排除，收集如下信息，联系上级支持工程师。
- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

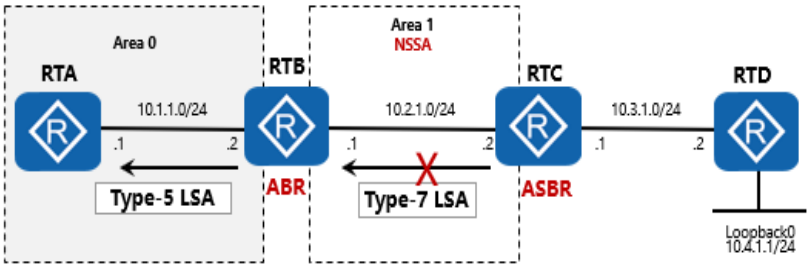
OSPF域间路由故障 - 现象与排障流程

- OSPF区域间路由故障常表现为ABR路由器不能正常完成路由汇总功能。

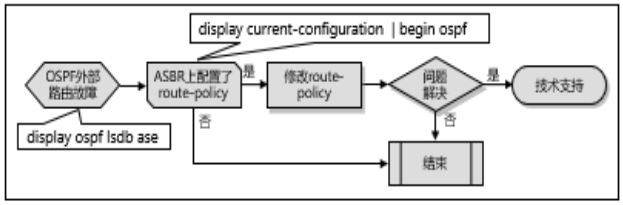


- OSPF ABR 路由器同时属于多个区域，并为它所连接的每个区域维护一个 LSDB。ABR 路由器会将所连接的非骨干区域内的链路状态信息（Router LSA 和 Network LSA）抽象成路由信息（Network Summary LSA），并将此路由信息发布到骨干区域中，再由骨干区域进一步发布到其他非骨干区域中。同时，ABR 也会将骨干区域的链路状态信息抽象成路由信息，并将此路由信息发布到所连接的非骨干区域中。
- OSPF 区域间路由故障常表现为 ABR 路由器不能正常完成路由汇总功能。此时需要使用命令 display current-configuration | begin ospf 检查 ABR 上是否正确配置了 abr-summary 命令。

OSPF域外路由故障 - 现象与排障流程

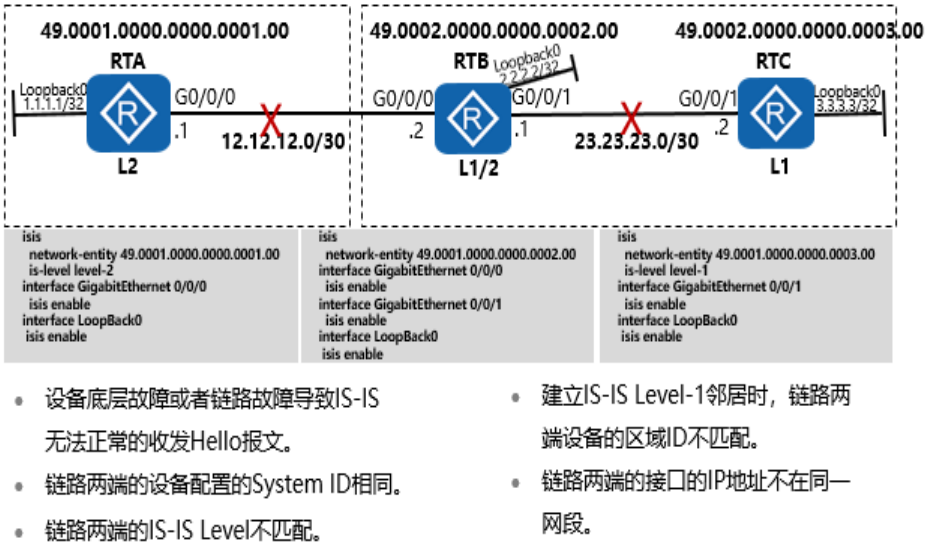


- ASBR不通告被重发布的路由。



- NSSA 区域中的 ASBR 可以引入外部路由，并通过 Type-7 LSA（NSSA LSA）在本区域内进行宣告。NSSA 区域中的 ASBR 不能产生并宣告 Type-5 LSA（AS External LSA），只能产生并宣告 Type-7 LSA（NSSA LSA）。在区域边界，NSSA 区域的 ABR 会将该 Type-7 LSA 转换成一条 Type-5 LSA，并向所有的其他区域进行泛洪。
- OSPF 域外路由故障常表现为 NSSA 区域的 ASBR 不通告被重发布的路由。可以使用命令 display ospf lsdb ase 显示 OSPF 的 AS 外部连接状态数据库信息。当 ASBR 上配置的 filter-policy 阻止了 OSPF 将外部路由安装到链路状态数据库时，需要通过修改访问控制列表来解决。

IS-IS邻居关系故障 - 现象与排障思路

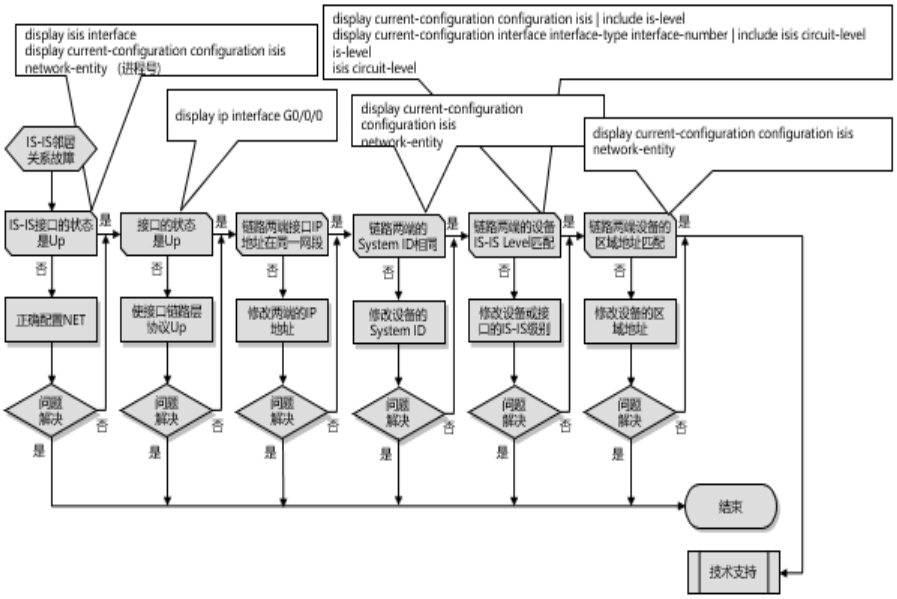


- 设备底层故障或者链路故障导致IS-IS无法正常的收发Hello报文。
- 链路两端的设备配置的System ID相同。
- 链路两端的IS-IS Level不匹配。
- 建立IS-IS Level-1邻居时，链路两端设备的区域ID不匹配。
- 链路两端的接口的IP地址不在同一网段。

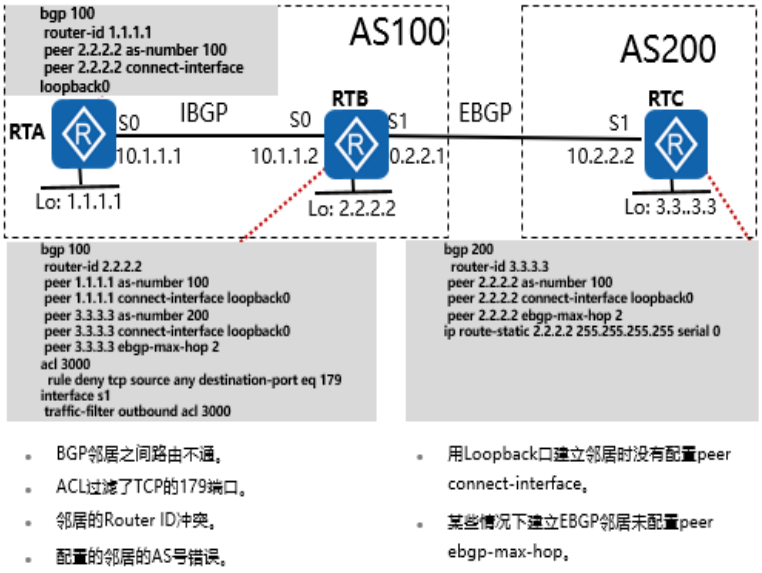
- IS-IS 网络采用了骨干区域与非骨干区域两级分层结构。IS-IS 路由器分为：Level-1 路由器，Level-2 路由器，Level-1/2 路由器（L1 路由器，L2 路由器，L1/2 路由器）。L1 路由器负责区域内的路由，只与属于同一区域的 L1 和 L1/2 路由器形成 L1 邻居关系，属于不同区域的 L1 路由器之间不能形成邻居关系。L2 路由器负责区域间的路由，可以与位于同一区域或者不同区域的 L2 和 L1/2 路由器形成 L2 邻居关系。L1/2 路由器同时属于 L1 和 L2 的路由器称为 L1/2 路由器，可以与同一区域的 L1 和 L1/2 路由器形成 L1 邻居关系，也可以与同一或者不同区域的 L2 路由器形成 L2 邻居关系，还可以与同一或不同区域的 L1/2 路由器形成 L2 的邻居关系。
- IS-IS 邻居关系故障的可能原因如下所述，在这里我们重点关注前面五种原因。
- 设备底层故障或者链路故障导致 IS-IS 无法正常的收发 Hello 报文：
- 链路两端的设备配置的 System ID 相同；
- 链路两端的 IS-IS Level 不匹配；

- 建立 IS-IS Level-1 邻居时，链路两端设备的区域地址不匹配；
- 链路两端的接口的 IP 地址不在同一网段；
- 链路两端的接口的 MTU 设置不一致或者接口的 MTU 小于发送的 Hello 报文的长度；
- 链路两端的 IS-IS 接口认证方式不匹配。

IS-IS邻居关系故障 - 排障流程



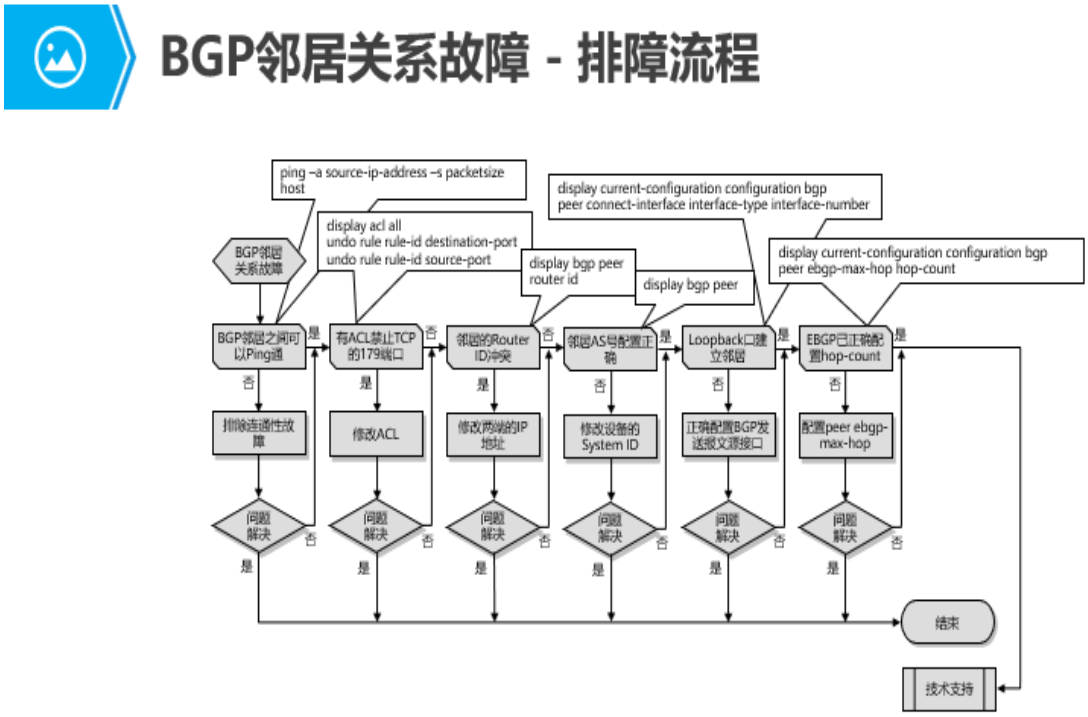
BGP邻居关系故障 - 现象与排障思路



- BGP 按照运行方式分为 EBGP（External/Exterior BGP）和 IBGP（Internal/Interior BGP）。运行于不同 AS 之间的 BGP 称为 EBGP。为了防止 AS 间产生环路，当 BGP 设备接收 EBGP 对等体发送的路由时，会将带有本地 AS 号的路由丢弃。运行于同一 AS 内部的 BGP 称为 IBGP。为了防止 AS 内产生环路，BGP 设备不将从 IBGP 对等体学到的路由通告给其他 IBGP 对等体，并与所有 IBGP 对等体建立全连接。BGP 邻居无法建立是指 BGP 邻居状态无法到达 Established 状态。
- BGP 邻居关系故障的常见原因主要包括：
- BGP 报文转发不通。
- ACL 过滤了 TCP 的 179 端口。
- 邻居的 Router ID 冲突。
- 配置的邻居的 AS 号错误。
- 用 Loopback 口建立邻居时没有配置 peer connect-interface。
- 用 Loopback 口建立 EBGP 邻居未配置 peer ebgp-max-h

op。

- 对端发送的路由数量是否超过 peer route-limit 命令设定的值。
- 对端配置了 peer ignore。
- 两端的地址族不匹配。
- 后三种故障并不是很常见，在这里我们重点关注前面六种 BGP 邻居关系故障的解决方法。

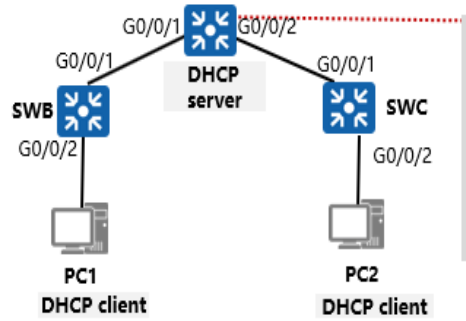


- 使用 ping 命令检测 BGP 邻居之间是否可以 Ping 通。
- 使用命令 ping –a source-ip-address –s packetsize host 来检测两端的互通性，因为带源地址可以同时检测两端路由是否正常，指定 ping 的字节可以检查大包在链路上传输是否正常。
- 如果可以 Ping 通，则说明 BGP 邻居之间有可达的路由并且链路传输也没有问题。
- 检查是否配置 ACL 禁止 TCP 的 179 端口。
- 在两端执行 display acl all 命令查看是否禁止 TCP 的 179 端口。如果有禁止 TCP 的 179 端口的 ACL，执行 undo rule r

ule-id destination-port 和 undo rule rule-id source-port 命令取消配置。

- 检查邻居的 Router ID 是否冲突。
- 在两端分别查看无法建立的 BGP 邻居的情况，执行 display bgp peer 命令查看 Router ID 是否冲突。
- 如果 Router ID 冲突，在 BGP 视图下运行命令 router id 将 Router ID 修改为不同（一般会用 Loopback 口的地址作为本端的 Router ID）。

DHCP Server故障



序号	配置步骤
1	配置全局地址池
2	配置接口工作在全局地址池模式
3	（可选）静态配置DHCP客户端的DNS服务
4	（可选）静态配置DHCP客户端的NetBIOS服务
5	（可选）配置全局地址池DHCP自定义选项
6	（可选）配置防止IP地址重复分配功能
7	（可选）配置DHCP数据保存功能

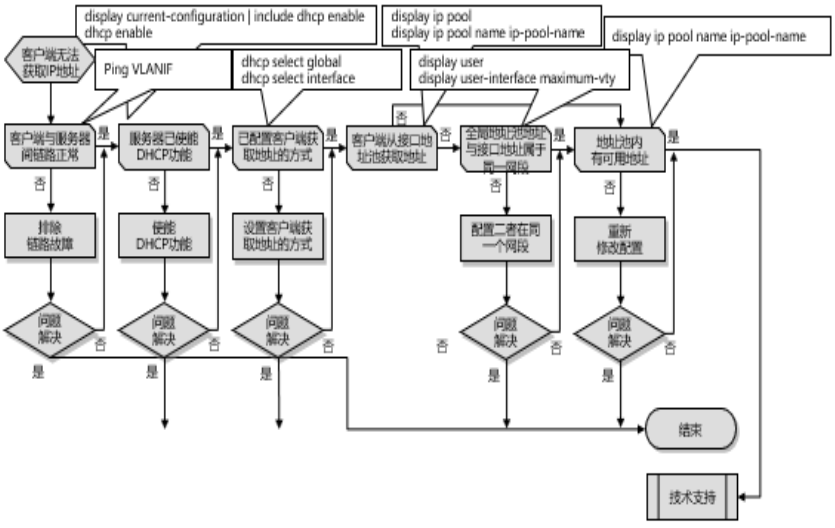
- 客户端与服务器之间的链路故障。
- 未使能DHCP功能。
- VLANIF接口下没有选择DHCP分配地址的方式。
- 全局地址池中的IP地址与VLANIF接口的IP地址不在同一个网段中。
- 地址池中没有可用的IP地址可分配。

- 随着网络规模的扩大和网络复杂度的提高，网络配置变的越来越复杂，再加上计算机数量剧增且位置不固定（如移动便携机或无线网络），引发了 IP 地址变化频繁以及 IP 地址不足的问题。为了实现网络可以动态合理地分配 IP 地址给主机使用，需要用到动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）。
- DHCP 是一种用于集中对用户进行动态管理和配置的技术。DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请（包括 IP 地址、子网掩码、缺省网关等参数），

服务器根据策略返回相应配置信息。DHCP 技术实现了计算机快速、动态地获取 IP 地址功能，提高了 IP 地址的使用效率。

- DHCP 故障的常见原因主要包括：
- 客户端与服务器之间的链路有故障。
- 设备未使能 DHCP 功能。
- 设备 VLANIF 接口下没有选择 DHCP 分配地址的方式。
- 当选择从全局地址池中分配 IP 地址时：
- 如果客户端与服务器在同一个网段内，中间没有中继设备时，全局地址池中的 IP 地址与设备 VLANIF 接口的 IP 地址不在同一个网段中。
- 如果客户端与服务器不在同一个网段内，中间存在中继设备时，全局地址池中的 IP 地址与中继设备的 VLANIF 接口的 IP 地址不在同一个网段中。
- 地址池中没有可用的 IP 地址可分配。

DHCP Server故障 - 排障流程

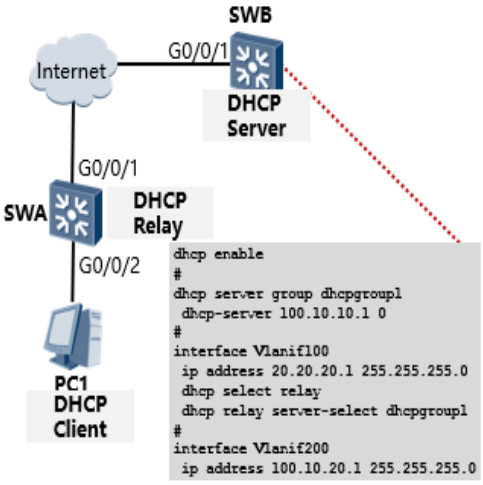


- 检查客户端与 DHCP 服务器之间的链路是否有故障。
- 客户端与服务器在同一个网段内，中间没有中继设备时，在客户端与服务器连接的网卡上配置 IP 地址，确保该 IP 地址

与服务器用户侧的 VLANIF 接口的 IP 地址在同一网段，从客户端 Ping VLANIF 接口的 IP 地址。 如果 Ping 不通，先排除链路的故障。

- 客户端与服务器不在同一个网段内，中间存在中继设备时，分别 Ping 客户端与中继设备、中继设备与服务器之间的链路状态。如果 Ping 不通，先排除链路的故障。
- 检查 DHCP 功能是否处于使能状态。
- 执行命令 display current-configuration | include dhcp enable，检查 DHCP 功能是否已经使能。如果无任何 DHCP 相关显示信息，说明 DHCP 功能未使能，执行命令 dhcp enable，使能 DHCP 功能。缺省情况下，DHCP 功能未使能。
- 检查 VLANIF 接口下是否选择 DHCP 分配地址的方式。
- 如果 VLANIF 接口下没有选择 DHCP 分配地址的方式，则客户端不能通过当前 VLANIF 接口以 DHCP 的方式来获取 IP 地址。
- 在 VLANIF 接口视图下，执行命令 display this，检查是否选择 DHCP 分配地址的方式。
- dhcp select global：VLANIF 接口已经选择全局地址池为 DHCP 客户端分配 IP 地址。
- dhcp select interface：VLANIF 接口已经选择接口地址池为 DHCP 客户端分配 IP 地址。
- 无上述显示信息说明 VLANIF 接口没有选择 DHCP 分配地址的方式。执行命令 dhcp select global 或者 dhcp select interface，配置 VLANIF 接口选择 DHCP 分配地址的方式。

DHCP Relay故障

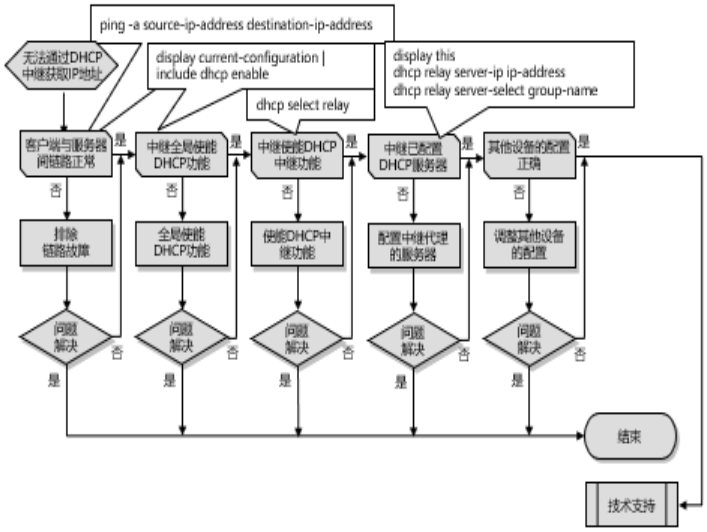


序号	配置步骤
1	配置指定接口工作在DHCP中继模式
2	配置DHCP中继转发的目的服务器组
3	配置DHCP中继接口绑定DHCP服务器组
4	（可选）配置DHCP中继请求DHCP服务器释放客户端的IP地址
5	（可选）配置DHCP中继对Option82信息的处理策略

- 客户端与DHCP服务器之间的链路有故障。
- 未全局使能DHCP功能，导致DHCP功能没有生效。
- 未使能DHCP中继功能，导致DHCP中继功能没有生效。
- DHCP中继没有配置所代理的DHCP服务器。
- 链路上其他设备配置错误。

- 当设备作为 DHCP 中继时，客户端可以通过 DHCP 中继与其他网段的 DHCP 服务器通信，从 DHCP 服务器的全局地址池中获取 IP 地址及其他配置信息。这样，多个网段的 DHCP 客户端可以使用同一个 DHCP 服务器，既节省了成本，又便于集中管理。
- DHCP Relay 故障的常见原因主要包括：
- 客户端与 DHCP 服务器之间的链路有故障。
- 客户端与 DHCP 中继之间的链路有故障。
- DHCP 中继与 DHCP 服务器之间的链路有故障。
- 设备未全局使能 DHCP 功能，导致 DHCP 功能没有生效。
- 设备未使能 DHCP 中继功能，导致 DHCP 中继功能没有生效。
- DHCP 中继没有配置所代理的 DHCP 服务器。
- DHCP 中继没有配置所代理的 DHCP 服务器的 IP 地址。
- DHCP 中继 VLANIF 接口没有绑定 DHCP 服务器组，或者绑定的 DHCP 服务器组中没有配置所代理的 DHCP 服务器。
- 链路上其他设备配置错误。

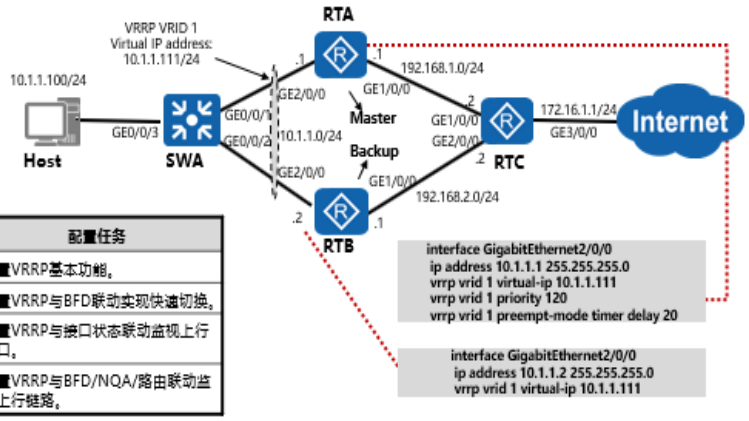
DHCP Relay故障 - 排障流程



- 检查客户端与 DHCP 服务器之间的链路是否有故障。
- 检查客户端与 DHCP 中继之间的链路是否有故障。在客户端手工配置与 DHCP 中继用户侧 VLANIF 接口位于同一网段的 IP 地址（不能与已经分配的 IP 地址冲突），然后在任一侧 ping 对端检查两者之间的链路是否有故障。如果 Ping 不通，先排除链路的故障。
- 检查 DHCP 中继与 DHCP 服务器之间的链路是否有故障。在 DHCP 中继上执行命令 ping -a source-ip-address destination-ip-address，source-ip-address 为 DHCP 中继用户侧接口的 IP 地址，destination-ip-address 为 DHCP 服务器的 IP 地址。如果 Ping 不通，先排除链路的故障。
- 检查 DHCP 中继是否全局使能 DHCP 功能。
- 执行命令 display current-configuration | include dhcp enable，检查 DHCP 功能是否已经使能。如果无任何显示信息，说明 DHCP 功能未使能，执行命令 dhcp enable，使能 DHCP 功能。缺省情况下，DHCP 功能未使能。
- 检查 DHCP 中继是否处于使能状态。

- 如果 DHCP 中继未使能，则客户端无法跨网段来获取 IP 地址。
- 如果同时选择了 global/interface 和 relay 功能，则设备优先选择 DHCP Server 角色，当 DHCP Server 分配 IP 地址失败后，则会切换到 DHCP Relay 角色，开始 DHCP Relay 功能。
- 在 VLANIF 接口视图下，执行命令 display this，检查 DHCP 中继是否处于使能状态。如果显示 dhcp select relay，说明 DHCP 中继已经处于使能状态，如果无上述显示信息，说明 DHCP 中继处于未使能状态，执行命令 dhcp select relay，使能 DHCP 中继功能。

VRRP备份组震荡故障



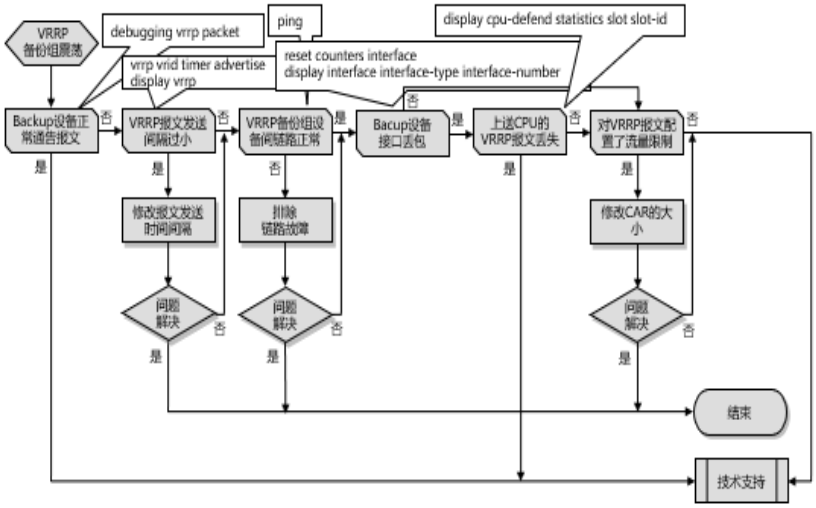
序号	配置任务
1	配置VRRP基本功能。
2	配置VRRP与BFD联动实现快速切换。
3	配置VRRP与接口状态联动监视上行接口。
4	配置VRRP与BFD/NQA/路由联动监视上行链路。

- 链路原因：
  - 传输VRRP通告报文的链路震荡。
  - 报文拥塞导致VRRP报文被随机过滤掉。
- 协议原因：
  - 通告报文的发送时间间隔过小。
- 其他原因：
  - Backup设备接口丢包。

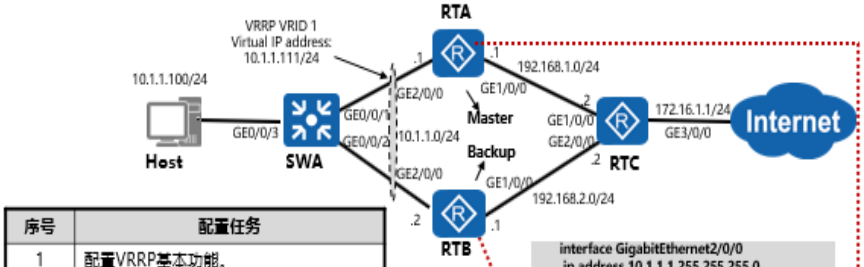
- VRRP 能够在不改变组网的情况下，采用将多台路由设备组成一个虚拟路由器，通过配置虚拟路由器的 IP 地址为默认网关，实现默认网关的备份。当网关设备发生故障时，VRRP 机制能够选举新的网关设备承担数据流量，从而保障网络的可靠通信。

- VRRP 备份组震荡的可能原因有：
- 传输 VRRP 通告报文的链路震荡。
- 通告报文的发送时间间隔过小。
- Backup 设备接口丢包。
- 报文拥塞导致 VRRP 报文被随机过滤掉。

VRRP备份组震荡故障 - 排障流程



VRRP备份组双主故障



序号	配置任务
1	配置VRRP基本功能。
2	配置VRRP与BFD联动实现快速切换。
3	配置VRRP与接口状态联动监视上行接口。
4	配置VRRP与BFD/NQA/路由联动监视上行链路。

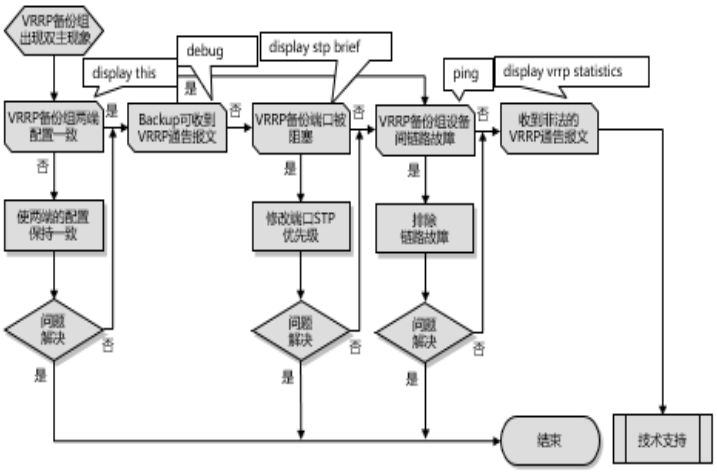
```
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 20
```

```
interface GigabitEthernet2/0/0
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
```

- 链路原因：
  - 传输VRRP通告报文的链路故障。
  - 链路形成环路。
- 配置原因：
  - 两端的VRRP备份组配置不一致。
- 协议原因：
  - 低优先级的VRRP备份组将收到的VRRP通告报文被作为非法报文丢弃。

- VRRP 备份组将两台设备虚拟成一台网关设备，虚拟网关设备具有虚拟 IP 地址和虚拟 MAC 地址，主机只感知这个虚拟网关设备的存在，以它为网关与外部进行通信。正常情况下，用户侧的流量通过 Master 设备转发。当 Master 设备出现故障时，通过 VRRP 协商，从 Backup 设备中选举出新的 Master 设备，继续承担流量转发工作。
- VRRP 备份组双主的可能原因有：
- 两端的 VRRP 备份组配置不一致。
- 传输 VRRP 通告报文的链路故障。
- 链路形成环路。
- 低优先级的 VRRP 备份组将收到的 VRRP 通告报文作为非法报文丢弃。

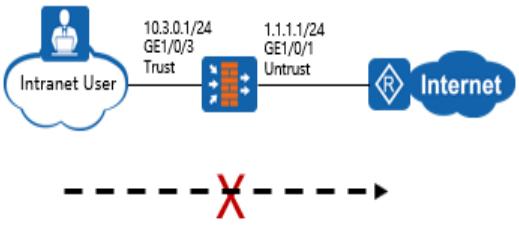
VRRP备份组双主故障 - 排障流程



- 检查 VRRP 备份组两端的配置是否一致。
- 在配置 VRRP 备份组两端的 VLANIF 接口上，执行 display this 命令，查看备份组两端的如下配置：
- ip address：接口 IP 地址是否在同一网段，如果 IP 地址不在同一网段，执行 ip address 来修改配置。
- vrid：接口上的备份组 ID 是否相同，如果不同，执行 vrrp vrid virtual-router-id virtual-ip virtual-address 命令修改配置。
- Virtual IP：VRRP 组的虚拟 IP 地址是否相同，如果不同，执行 vrrp vrid virtual-router-id virtual-ip virtual-address 命令修改配置。
- TimerRun：VRRP 中通告报文时间间隔是否相同，如果不同，执行 vrrp vrid virtual-router-id timer advertise adver-interval 命令修改配置。
- Auth Type：VRRP 报文认证方式是否相同，如果不同，执行 vrrp vrid virtual-router-id authentication-mode { simple key | md5 md5-key }命令修改配置。
- 查看 Backup 设备是否能够收到 VRRP 通告报文。

- 打开 Backup 设备的 debug 开关，查看是否有如下显示信息。
- *Aug 27 19:45:04 2010 Quidway VRRP/7/DebugPacket:
- Vlanif45 | Virtual Router 45:receiving from 45.1.1.4, priority = 100,timer = 1,
- auth type is no, SysUptime: (0,121496722)
- 默认情况下 Master 设备都是 1 秒发送 1 个通告报文。

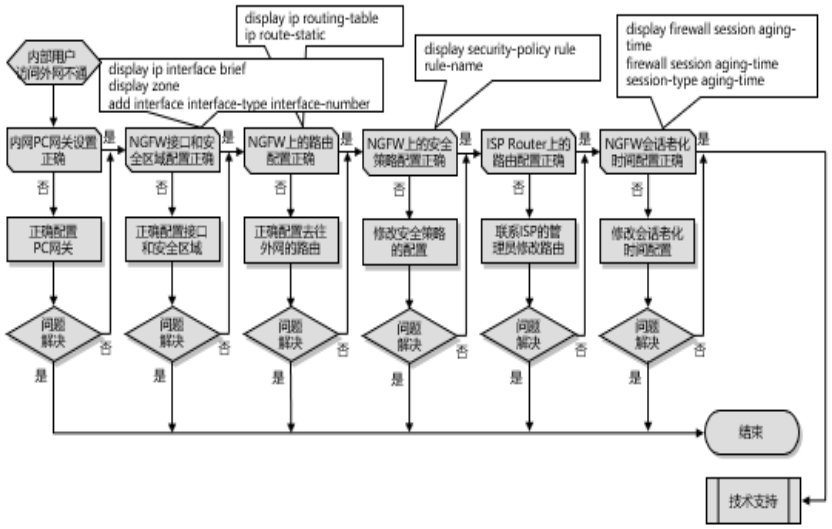
内网对外访问故障



- 内网用户所使用PC上的网关设置有误。
- NGFW上的接口和安全区域配置有误。
- NGFW上的路由配置有误。
- NGFW上的安全策略配置有误。
- ISP Router上的路由配置有误。
- NGFW上的会话老化时间配置有误。

- NGFW 可以作为企业的出口网关，部署在网络边界处。企业内部网络中的用户通过 NGFW 提供的 NAT 功能来访问 Internet。配置完成后，如果发现企业内部网络中的用户不能访问 Internet，可能的原因有：
- 内网用户所使用 PC 上的网关设置有误。
- NGFW 上的接口和安全区域配置有误。
- NGFW 上的路由配置有误。
- NGFW 上的安全策略配置有误。
- ISP Router 上的路由配置有误。
- NGFW 上的会话老化时间配置有误。

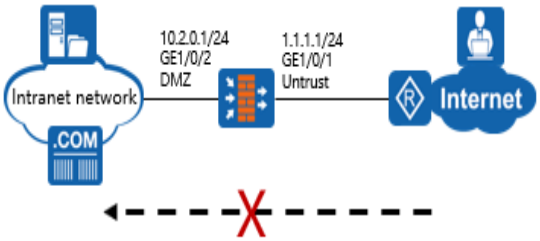
内网对外访问故障 - 排障流程



- 检查 PC 的网关是否设置为 NGFW 连接内部网络的接口的 IP 地址。
- 检查 NGFW 上连接内部网络和 Internet 的接口是否配置了正确的 IP 地址并加入安全区域。
- 在 NGFW 的 CLI 环境中使用 display ip interface brief 命令查看接口是否配置了正确的 IP 地址。
- 检查 IP Address 一列的信息，如果配置有误，在接口视图下使用 ip address ip-address mask 命令重新配置 IP 地址。
- 使用 display zone 命令查看接口是否正确的加入安全区域。
- 如果配置有误，在安全区域视图下使用 add interface interface-type interface-number 命令将接口加入安全区域。
- 检查 NGFW 上是否存在去往 Internet 的路由。
- 在 NGFW 的 CLI 环境中使用 display ip routing-table 命令查看路由表项。
- 如果配置有误，请使用 ip route-static 命令重新配置路由。
- 检查 NGFW 上配置的安全策略以及安全策略所引用的配

置文件是否正确。

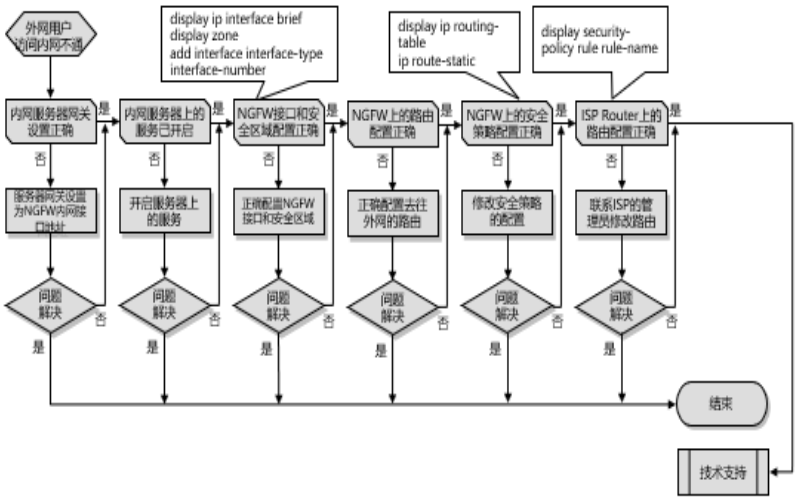
外网对内访问故障



- 内网服务器上的网关设置有误。
- 内网服务器上的服务没有开启。
- NGFW上的接口和安全区域配置有误。
- NGFW上的路由配置有误。
- NGFW上的安全策略配置有误。
- ISP Router将报文丢弃。

- 如果发现企业内部网络中的用户不能访问 Internet，可能的原因有：
- 内网服务器上的网关设置有误。
- 内网服务器上的服务没有开启。
- NGFW 上的接口和安全区域配置有误。
- NGFW 上的路由配置有误。
- NGFW 上的安全策略配置有误。
- ISP Router 将报文丢弃。

外网对内访问故障 - 排障流程

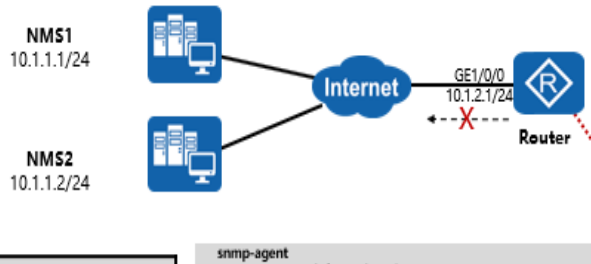


- 检查内网服务器的网关是否设置为 NGFW 连接内部网络的接口的 IP 地址。
- 检查内网服务器上的服务是否开启。
- 检查 NGFW 上连接内部网络和 Internet 的接口是否配置了正确的 IP 地址并加入安全区域。
- 在 NGFW 的 CLI 环境中使用 display ip interface brief 命令查看接口是否配置了正确的 IP 地址。如果配置有误，则在接口视图下使用 ip address ip-address mask 命令重新配置 IP 地址。
- 使用 display zone 命令查看接口是否正确的加入安全区域。如果配置有误，则在安全区域视图下使用 add interface interface-type interface-number 命令将接口加入安全区域。
- 检查 NGFW 上的路由配置。
- 在 NGFW 的 CLI 环境中使用 display ip routing-table 命令查看路由表项。如果配置有误，使用 ip route-static 命令重新配置路由。
- 检查 NGFW 上配置的安全策略以及安全策略所引用的配

置文件是否正确。

- 在 NGFW 的 CLI 环境中使用 display security-policy rule rule-name 命令查看安全策略的配置信息。
- 检查安全策略的匹配条件是否可以正确匹配到外网用户访问内网服务器的流量，此处的目的地址应该是内网服务器的私网地址，同时查看安全策略的动作是否为 permit。如果配置有误，则在安全策略规则视图下使用 source-address 命令调整安全策略规则的源地址，或者使用命令 action 调整安全策略规则的动作。
- 如果安全策略中引用了内容安全的配置文件，使用 display profile type { app-control | av | data-filter | file-block | ips | mail-filter | url-filter } name name 命令查看内容安全配置文件的配置信息，是否将外网用户与内网服务器之间的流量阻断。

SNMP无法连接故障



序号	配置任务
1	配置SNMPv2c的基本功能。
2	（可选）限制网管对设备的管理权限。
3	（可选）配置向网管发送告警。
4	（可选）配置SNMP扩展错误码功能。

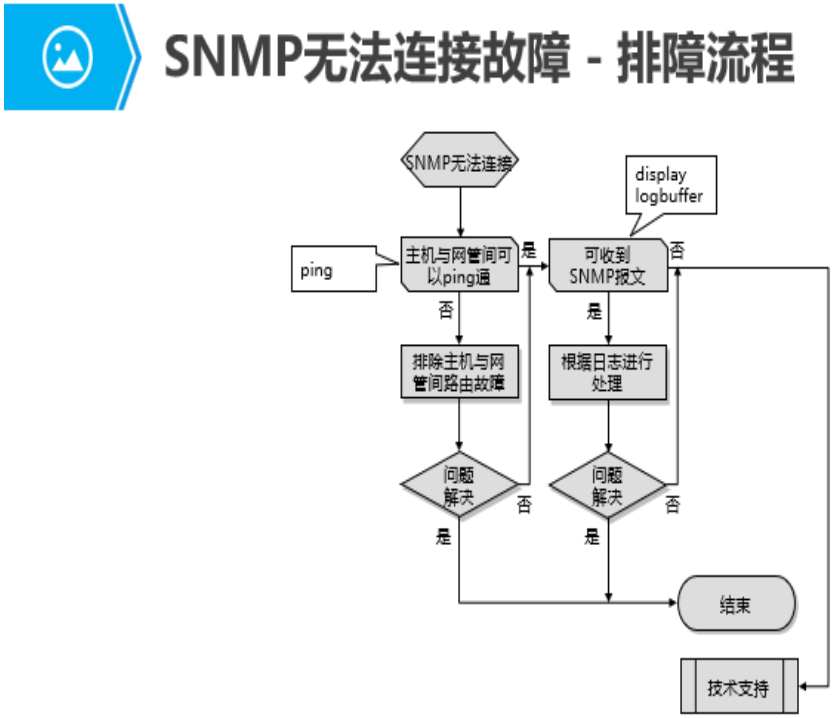
```
snmp-agent
snmp-agent sys-info version v2c
acl 2001
 rule 5 permit source 10.1.1.2 0.0.0.0
 rule 6 deny source 10.1.1.1 0.0.0.0
snmp-agent mib-view dnsmib include 1.3.6.1.4.1.2011.5.25.194
snmp-agent community write adminnms2 mib-view dnsmib acl 2001
snmp-agent target-host trap-paramsname trapnms2 v2c securityname adminnms2
snmp-agent target-host trap-hostname nms2 address 10.1.1.2 trap-paramsname trapnms2
snmp-agent trap queue-size 200
snmp-agent trap life 60
snmp-agent trap enable
snmp-agent sys-info contact call Operator at 010-12345678
```

- 报文不可达造成无法连接。
- 配置原因造成无法连接。

- 简单网络管理协议 SNMP 是广泛用于 TCP/IP 网络的网络管理标准协议。SNMP 提供了一种通过运行网络管理软件的中心计算机（即网络管理工作站）来管理网元的方法。共有三个版本 SNMPv1、SNMPv2c 和 SNMPv3，用户可以根据情

况选择配置一个或多个版本。

- 要在组网中配置 SNMP 协议，需要在管理端配置 SNMP 管理程序 NMS，同时在被管理设备端配置 SNMP 代理程序 Agent。网络管理系统 NMS 可以通过 Agent 在任何时候及时地获得设备的状态信息，实现远端控制被管理设备；Agent 可以及时地向 NMS 报告设备的当前状态信息。
- SNMP 无法连接故障的常见原因主要包括：
- 报文不可达造成无法连接。
- 配置原因造成无法连接。

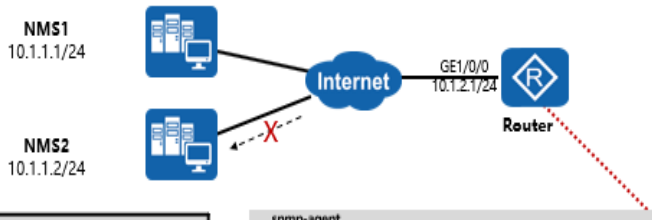


- 执行 ping 命令查看主机和网管之间是否可以 Ping 通。
- 如果可以 Ping 通，说明主机和网管之间有可达的路由。
- 如果无法 Ping 通，先排除链路的故障。
- 执行 display logbuffer 命令查看主机上是否有提示登录失败的日志。
- Failed to login through SNMP, because the version was incorrect. (Ip=[STRING], Times=[ULONG]) (主机不支持网管发送登录请求所使用的

SNMP 协议版本）。

- 执行 display snmp-agent sys-info version 命令查看主机是否支持网管发送登录请求所使用的 SNMP 协议版本。
- 执行 snmp-agent sys-info version 命令配置主机所支持的 SNMP 协议版本。
- Failed to login through SNMP, because the packet was too large. (Ip=[STRING], Times=[ULONG])（设备接收到的报文超过设备所设置的阈值）。
- 执行 snmp-agent packet max-size 命令增大报文阈值。
- Failed to login through SNMP, because the community was incorrect. (Ip=[STRING], Times=[ULONG])（团体字配置错误）。
- 执行 display snmp-agent community 命令查看主机配置的团体字。
- 执行 snmp-agent community 命令配置读写团体名，使之与网管端配置一致。
- Failed to login through SNMP, because of the ACL filter function. (Ip=[STRING], Times=[ULONG])（该 IP 被 ACL 禁止）。
- 执行 display acl 命令查看主机 ACL 配置，如果网管端发送请求所使用的 IP 被 ACL 禁止访问，则执行 rule 命令配置允许网管端 IP 访问主机。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

收不到SNMP告警故障



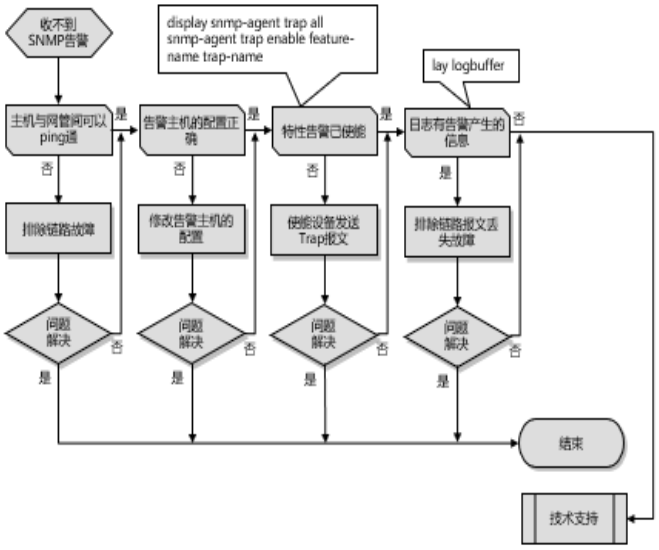
序号	配置任务
1	配置SNMPv2c的基本功能。
2	（可选）限制网管对设备的管理权限。
3	（可选）配置向网管发送告警。
4	（可选）配置SNMP扩展错误码功能。

```
snmp-agent
snmp-agent sys-info version v2c
acl 2001
 rule 5 permit source 10.1.1.2 0.0.0.0
 rule 6 deny source 10.1.1.1 0.0.0.0
snmp-agent mib-view dnsmib include 1.3.6.1.4.1.2011.5.25.194
snmp-agent community write adminnms2 mib-view dnsmib acl 2001
snmp-agent target-host trap-paramsname trapnms2 v2c securityname adminnms2
snmp-agent target-host trap-hostname nms2 address 10.1.1.2 trap-paramsname trapnms2
snmp-agent trap queue-size 200
snmp-agent trap life 60
snmp-agent trap enable
snmp-agent sys-info contact call Operator at 010-12345678
```

- 报文丢失。
- 主机侧SNMP配置错误。
- 主机侧业务模块没有产生告警，或者产生的告警格式错误。

- 收不到 SNMP 告警故障的常见原因主要包括：
- 报文丢失造成网管主机无法接收到这条告警。
- 主机侧 SNMP 配置错误，造成告警无法发送。
- 主机侧业务模块没有产生告警，或者产生的告警格式错误导致告警无法发送。

收不到SNMP告警故障 - 排障流程



- 确保主机与网管间可以 ping 通。
- 检查设备上告警主机的配置是否正确。 如果告警主机配置错误，参考产品文档的配置说明进行修改。
- 查看告警的使能情况。
- 执行 display snmp-agent trap all 命令查看到所有特性下的告警的使能情况。如果特性告警没有使能，执行 snmp-agent trap enable feature-name trap-name 命令使能设备发送 Trap 报文，并设置 Trap 的相关参数。
- 取主机上的日志，检查是否有告警产生的信息。如果存在期望获取的告警的记录，说明告警已经产生但是网管没有收到，则需要查看链路上是否存在报文丢失的情况。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

思考题

1. 下述哪些原因可能引起BGP邻居关系故障?

   A. ACL过滤了TCP的179端口。

   B. 邻居的Router ID冲突。

   C. 用Loopback口建立EBGP邻居未配置peer ebgp-max-hop。

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

- 1、答案：ABCD。