网络故障排除

- 中大型企业数字化转型需要多种技术,例如云计算、大数据、AI、物联网等,而以上技术又离不开数通网络的支持,一个稳定的数通网络需要在网络设计、建设、维护等方面做好充分的准备。
- 企业数通网络用到多种设备类型,设备之间使用多种物理链路连接,同时为了准确的完成数据包的转发,网络设备运行了多种网络协议。网络设备,线缆、以及网络协议都有可能产生网络故障,如何快速完成故障处理是一个高级网络工程师的基本素养。
- 本节课程主要学习网络故障处理的方法,介绍常见的网络故障,结合故障场景,构建网络工程师故障处理的能力。

什么是网络故障

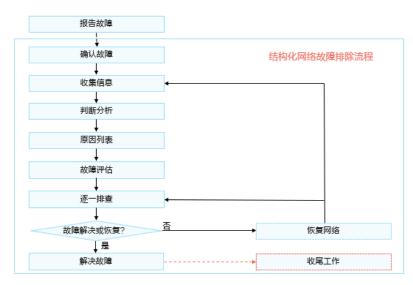
- 网络故障是指由于某种原因而使网络丧失规定功能并影响业务的现象。
- 从用户的角度出发,凡是影响业务的现象都可以定义为故障。
- 常见的故障现象和分类如下:

现象 分类	告警	环路	业务不通	业务中断	业务瞬断	됊	协议异常	协议 震荡	路由异常
硬件类	$\sqrt{}$			\checkmark		\checkmark			
配置类		\checkmark	\checkmark				\checkmark		\checkmark
网络类		$\sqrt{}$	\checkmark						
性能问题	$\sqrt{}$				\checkmark	\checkmark		\checkmark	\checkmark
软件类							\checkmark		\checkmark
对接类		$\sqrt{}$	\checkmark				\checkmark		
其他	$\sqrt{}$		\checkmark	\checkmark	\checkmark	\checkmark			

以上分类和故障现象的对应关系在不同的场景下会有所不同。



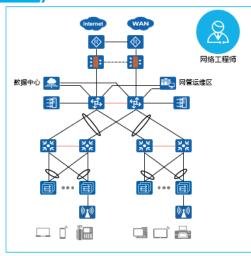
结构化的网络故障排除流程



- 如果采取非结构化的网络故障排除流程,就只是凭直觉 在这些步骤之间重复执行,虽然最终也可能找到解决故障的方 法,但没有办法保证效率。
- 在复杂的网络环境中,有可能会由于非结构化的网络故障排除流程而导致新的故障,从而使网络故障的排除变得更加困难。



报告故障



- 企业中存在多个部门,例如财务、人事、后勤、市场、研发等,这些部门之间的网络有互联互访均需求。为了保障网络的正常运行,企业可能存在如下情况:
 - 大中型企业成立网络维护部门,构建专业的网络团队。
 - 小型企业为了节省成本,一般不存在单独的网络维护部门,而 是将网络托管给专业的网络维护公司。
 - 求助设备生产商,拨打厂商的售后服务电话。

最告故章 确认故障 火集信息 判断分析 原因列表 故障评估 逐一排查 解决故障 收尾工作

 一般情况下网络故障的第一感知人员并非网络维护人员,而 是其他业务相关的各个部门人员。网络工程师经常接到各种 求助电话,例如"电脑突然无法上网"、"网页无法正常 显示"、"游戏没法玩了"……

当接到电话时,网络工程师应该如何处理呢?



故障报告者	姓名、所在的部门、职位级别、所负责的工作内容、使用电脑的位置(楼层、 房间、无线接入还是有线接入)、在使用电脑访问什么网站时发现的问题。
故障频率	故障是突发的、偶尔的、还是频繁的。
用户操作	出现故障之前和之后,用户对自己的终端做了哪些操作,如是否更改了IP地址和DNS、是否安装了桌面防火墙软件、安全控制软件等。

在电话里询问用户上面的内容,并记录在排障报告中。

- 为什么需要了解用户的职位级别、工作内容等信息?
- 在企业环境中,不同级别的用户可能会有不同的网络访问权限。

确认故障

- 确认故障的四个要素:
- 故障的主体:哪个网络业务出现了故障。
- 故障的表现:故障的现象是什么样的。
- 故障的时间:用户是什么时间发现的故障,以及专业人员推测的故障出现的真实时间。
- 故障的位置:哪个网络组件出现了故障。
- 对故障现象进行准确的描述。
- 最后应确认该故障是否属于自己的负责范围,即自己是 否被赋予了相应的权限来处理该故障。

收集信息

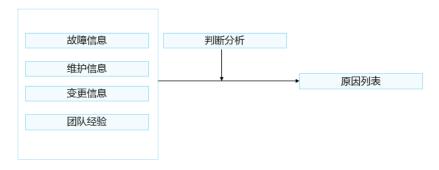
- 需要收集哪些信息:
- 收集信息阶段主要是收集与故障相关的信息,如文档、 网络变更情况等。

- 如何收集这些信息:
- 使用设备自身的操作命令;使用信息收集工具,如抓包工具、网管软件等。
- 获取授权:
- 在对信息安全要求较高的网络环境中,对信息的收集是需要得到授权的,有时需要签署书面的授权文件。
- 收集信息阶段的风险评估:
- 有些收集信息的操作,如对路由器或交换机执行"debug" 命令,会导致设备的 CPU 占用率过高,严重的情况下甚至会使设备停止响应用户的操作指令,从而引入额外的故障现象。所以在收集信息的时候应评估这些风险,平衡引入新故障的风险与解决现有故障的紧迫性之间的关系,并明确的告知用户这些风险,由用户来决定是否进行风险较大的信息收集工作。

判断分析

判断分析阶段是对收集到的信息进行分析整理。

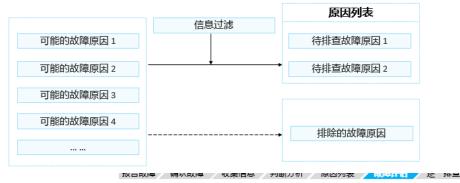
通过对故障信息、维护信息、变更信息的汇总,结合团队经验(或个人经验)进行综合的判断和分析,得到可能导致网络故障的原因列表。





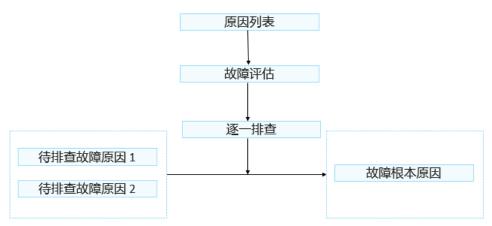
原因列表

在原因列表阶段,首先需要列出所有可能的故障原因,然后通过信息过滤,列出最可能的待排查故障原因,同时排除掉当前最不可能的故障原因,从而缩小故障的排除范围。



故障评估

需要在逐一排查前进行故障评估工作。



- 在故障评估阶段可能需要搭建临时的网络环境。
- 对复杂的网络故障,如果经过评估认为短时间内无法排除故障,而用户又需要马上恢复网络的可用性,这时可能需要 临时跳过故障节点,搭建替代的网络环境。
- 搭建临时网络环境的时候,应充分考虑到解决问题的迫切性与绕过某些安全限制措施的危险性,应与用户进行充分的沟通,并在得到许可的情况下才能执行。



逐一排查

- 在逐一排查阶段同样需要平衡解决问题的迫切性与引入新故障的风险性之间的矛盾。所以,应该明确告知用户排查工作可能带来的风险,并在得到许可的情况下才能执行操作。
- 有些情况下,通过逐一排查验证推断的过程涉及到网络变更,这时必须做好完善的应急预案和回退准备。





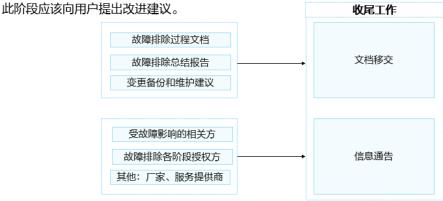
解决故障

- 如果通过逐一排查找到了故障的根本原因,并排除了故障,网络故障排除的流程就可以 结束了。
- 复杂的网络环境中,故障现象消失后仍然需要观察一段时间,一方面确认用户报告的故障已经得到了解决,另一方面确认故障排除的过程中没有引入新的故障。



收尾工作

收尾工作包括相关文档的整理、信息的通告等。需要对之前网络故障排除流程中所有进行了变更的 配置或软件进行备份,并做好故障排除文档的整理和移交工作。为了避免同样的故障再次发生,在





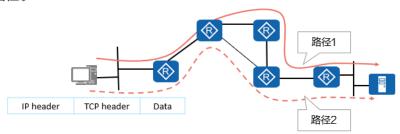
以业务流量路径为核心的故障排除思想

通常情况下,网络中业务流量的路径是在网络规划阶段就已经设计好的,只需要知道受到网络故障 影响的业务的流量往返路径,跟踪此路径,逐步排除即可。



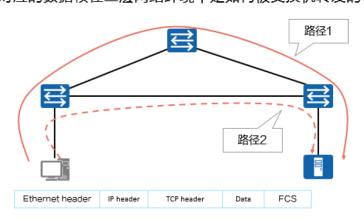
确认业务流量路径 - 网络层

在数据包转发过程中可能存在多条路径,因此需要根据报文转发过程,确认业务流量的传输路径。



确认业务流量路径 - 数据链路层

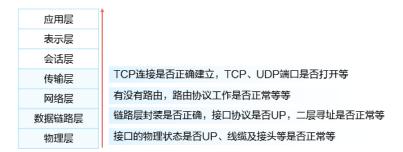
确认业务流量对应的数据帧在二层网络环境中是如何被交换机转发的。





分层故障处理法

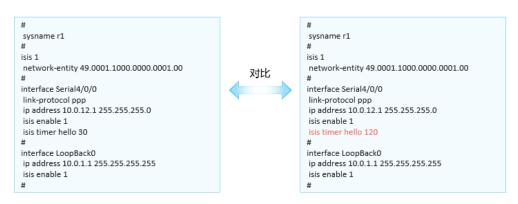
分层法很简单,所有模型都遵循相同的基本前提: 当模型的所有低层结构工作正常时,它的高层结构才能正常工作。一般建议在处理故障时,从参考模型自底向上进行故障排查。





对比配置法

- 对比配置法是指对比正常状态与故障状态下的配置、软件版本、硬件型号等内容,检查两者之间的差异。
- 经验较少的网络故障排除人员在实践中会更多的使用到这种方法。



分块故障处理法

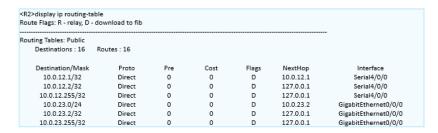
- 华为的交换机和路由器等网络设备的配置文件具有清晰的组织结构。
- 当出现一个故障案例现象时,我们可以把它归入以下某一类或某几类中,从而有助于缩减故障定位范围:
- 管理部分(路由器名称、口令、服务、日志等)
- 端口部分(地址、封装、cost、认证等)
- 路由协议部分(静态路由、RIP、OSPF、BGP、路由引入等)

- 策略部分(路由策略、策略路由、安全配置等)
- 接入部分(Console 登录、Telnet 登录、拨号等)
- 其他应用部分(DNS、DHCP、VPN配置等)



分块故障处理法 - 示例

当使用display ip routing-table命令,结果只显示出了直连路由,可能是什么原因呢?



根据上述的分块,该故障可能由以下三部分导致:路由协议、策略、端口。如果没有配置路由协议或配置不当,路由表就可能为空;如果访问列表配置错误,就可能妨碍路由的更新;如果端口的地址、掩码或认证配置错误,也可能导致路由表错误。



分段故障处理法

数据包转发过程中可能经过多台路由器和物理链路,每段物理连接都有可能发生故障,因此分段处理的方法是有效的。



替换法

- 替换法是检查硬件问题最常用的方法之一。
- 当怀疑是网线问题时,更换一根确定是好的网线试一试;当怀疑是接口模块有问题时,更换一个其它接口模块试一试。

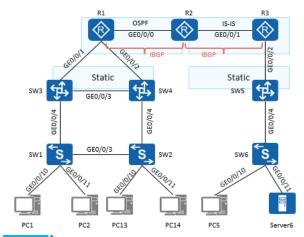


故障处理对网络维护和管理人员的要求

- 对协议要求有精深的理解。
- 能够引导客户详细描述出故障现象和相关信息。
- 充分了解自己所管理和维护的网络。
- 及时进行故障处理的文档记录和经验总结。
- 熟悉网络故障排除的方法,将多种方法结合使用。



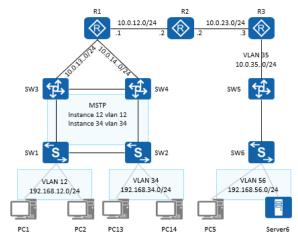
常见网络故障排除 - 拓扑介绍 (1)



- 网络工程师在进行网络维护时会遇到多种类型的网络故障,例如登录故障、路由故障、IP业务故障等,左图为网络中部分网络架构,以此图为例说明常见网络故障排除的方法和步骤。
- 路由协议介绍:
 - OSPF: R1和R2之间运行OSPF协议,R1所有接口开启OSPF协议,并且GE0/0/0属于区域0。
 - IS-IS: R2和R3之间运行IS-IS协议。
 - BGP: R1、R3分别和R2建立IBGP邻居关系,并且作为R2的路由反射器客户端。
 - · Static: SW3、SW4、SW5全部使用静态路由和路由器对接。



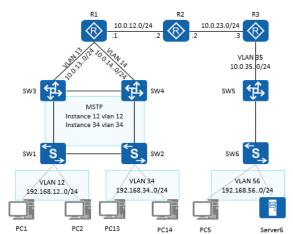
常见网络故障排除 - 拓扑介绍 (2)



- IP地址规划:
 - loopback0: R1、R2、R3分别为10.0.1.1/32, 10.0.2.2/32,10.0.3.3/32。
 - 互联接口:网段如图中所示,且IP地址最后一位为网络设备的编号。
 - 终端: 网段如图中所示。网关为同网段最大的IP地址。其中 PC5使用DHCP的方式获取IP地址,R3作为DHCP服务器。其 它终端采用静态IP地址,且IP地址最后一位为网络设备的编 号。
- 路由通告规划
 - R2部署做OSPF及IS-IS的双向路由引入,使R1、R2、R3的 LoopbackO接口IP地址可达。
 - R1将静态路由192.168.12.0/24、192.168.34.0/24引入BGP协议。
 - R3将静态路由192.168.56.0/24引入BGP协议。
- R3和SW5使用路由子接口对接。



常见网络故障排除 - 拓扑介绍 (3)



• MSTP规划:

Instance ID	VLAN ID	Root Bridge	Backup Bridge
Instance 12	VLAN 12	SW3	SW4
Instance 34	VLAN 34	SW4	SW3

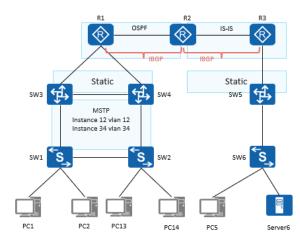
VRRP规划:

Network Segment	Master Gateway	Backup Gateway	VRID	Virtual IP
192.168.12.0/24	SW3	SW4	1	192.168.12.254
192.168.34.0/24	SW4	SW3	2	192.168.34.254

设备Telnet的用户名和密码:用户名Huawei,密码 Huawei@123。



常见网络故障排除 - 故障现象

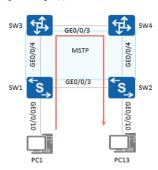


- 网络工程师遇到了以下几个故障现象:
 - PC1和PC13无法通信。
 - · Server6提供了FTP服务,但是PC1无法使用该服务。
 - · PC5不能和任何主机通信。
- 以上故障现象可能由多个原因导致,结合第一节 所学习的故障处理的方法,分别针对以上三个问 题进行故障处理的演示。
- 假设故障现象已经确认,所以后续故障处理中略 去报告故障、确认故障、收集信息、收尾工作等 步骤。



故障现象 - PC1和PC13无法正常通信 (1)

将拓扑图简化如下:



如左图所示PC1和PC13流量的规划路径,按照分层、分段、以流量路径为核心思想的故障处理流程,将PC1和PC13无法正常通信的故障原因列举如下:

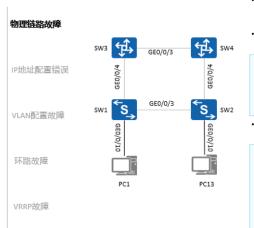
- 物理链路故障
- 。 IP地址配置错误
- 。 VLAN配置故障
- 环路故障
- VRRP故障

流量规划路径

本节故障处理旨在展示故障处理的常用方法和工具,为网络维护人员给予一定的指导,在实际场景进行故障排除时, 先后顺序可以和示例不一致。



故障现象 - PC1和PC13无法正常通信 (2)



- 在PC1、PC13上通过以下路径:控制面板\网络和Internet\网络连接\以太网 线缆、确保PC的物理线缆连接正常。(不同操作系统检查路径不一致)。
- 在交换机上查看物理接口状态(以SW1为例)。如果接口物理状态为非 "up",替换PC连接到交换机的接口。

<sw1>display interface brief include up</sw1>							
Interface	PHY	Protocol	InUti	OutUti	inErrors	outErrors	
GigabitEthernet0/0/3	up	up	0%	0%	0	0	
GigabitEthernet0/0/4	up	up	0%	0%	0	0	
GigabitEthernet0/0/10	up	up	0%	0%	0	0	
GigabitEthernet0/0/11	up	up	0%	0%	0	0	

在PC1上ping 192.168.34.13,同时观察接口收发数据包数量是否增加。发现Input数据包递增。说明物理链路无故障,否则更换接口或者网线。



- 以 Windows10 系统为例进行 PC 物理连接状态的检查。
- InUti(Input bandwidth utilization): Inbound bandwidth u sage,输入带宽利用率。
- OutUti(Output bandwidth utilization): Outbound bandwidth usage,输出带宽利用率。



故障现象 - PC1和PC13无法正常通信(3)



- 查询PC1物理IP地址是否设置为192.168.12.1,并且确保网关设置为192.168.12.254。
- 在SW3和SW4上查看IP地址状态,确保IP地址配置正常(VLANIF接口没有IP 地址不会up,无法完成三层转发)。

Interface	IP Address/Mask	Physical	Protocol
MEth0/0/1	unassigned	down	down
NULL0	unassigned	up	up(s)
Vlanif1	unassigned	up	down
Vlanif12	192.168.12.3/24	up	up
Vlanif34	192.168.34.3/24	up	up
<sw4>display ip i</sw4>	nterface brief		
Interface	IP Address/Mask	Physical	Protocol
Interface MEth0/0/1	IP Address/Mask unassigned	Physical down	Protocol down
	,		
MEth0/0/1	unassigned	down	down
MEth0/0/1 NULL0	unassigned unassigned	down up	down up(s)

• 由以上结果得知SW3和SW4接口IP地址配置正确。



故障现象 - PC1和PC13无法正常通信 (4)

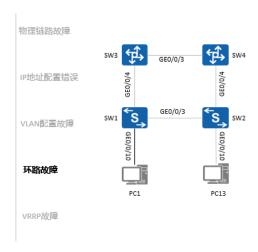


• 查询交换机端口和VLAN配置。



- 根据以上信息得知SW1的GE0/0/10和GE0/0/11 VLAN信息配置错误,将以 上错误数据进行修改。同时对另外三台交换机做校验。
- 交换机VLAN配置正确后,验证PC1和同网段的其它IP地址是否正常通信, 例如在PC1上执行命令ping 192.168.12.13,结果发现有丢包,并且延时较大。
- GE0/0/10 接口同时属于 VLAN 12、34,并且是 Tagged 模式,说明该接口配置为了 Trunk 接口,同时 PVID 不是 VLA N 12。

故障现象 - PC1和PC13无法正常通信 (5)



在交换机上查看MSTP工作状态,发现SW4所有端口都处于转发状态。

<sw4>display stp brief</sw4>							
MSTID	Port	Role	STP	State			
0	GigabitEthernet0/0/2	DESI	FORWARDING	NONE			
0	GigabitEthernet0/0/3	DESI	FORWARDING	NONE			
0	GigabitEthernet0/0/4	DESI	FORWARDING	NONE			
12	GigabitEthernet0/0/2	DESI	FORWARDING	NONE			
12	GigabitEthernet0/0/3	DESI	FORWARDING	NONE			
12	GigabitEthernet0/0/4	DESI	FORWARDING	NONE			
34	GigabitEthernet0/0/2	DESI	FORWARDING	NONE			
34	GigabitEthernet0/0/3	DESI	FORWARDING	NONE			
34	GigabitEthernet0/0/4	DESI	FORWARDING	NONE			

· MSTP故障的原因可能是域名配置错误、Instance和VLAN绑定错误、端口 绑定VLAN错误等。在SW4设备上检查MSTP配置。



- 将SW4域名修改为正确配置,继续使用PC1 ping 192.168.12.13发现在某些时间段仍然会有丢包。
- 二层环路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%。

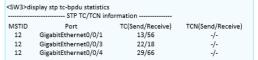
- 通过 ping 命令进行网络测试时丢包严重。
- 设备上发生环路的 VLAN 的接口指示灯频繁闪烁。
- PC 机上能收到大量的广播报文。
- 设备部署环路检测后,设备出现环路告警。



故障现象 - PC1和PC13无法正常通信 (6)



经过观察,故障现象主要发生在上下班时间,并且在故障现象发生时通过查看MAC地址表,发现MAC地址表不稳定,查看STP统计数据



上下班时间,交换机端口频繁UP/DOWN,会发送大量TC报文,因此将交换机连接主机的端口设置为边缘端口。

 开启 STP 的交换机在收到 STP TC 报文后会清空 MAC 地址表进行重新学习,在此期间,数据转发会出现短暂的中断, 从而产生丢包现象。



故障现象 - PC1和PC13无法正常通信 (7)



 为了验证网络的可靠性,维护人员将sw3设备的GE0/0/4端口关闭,此时在 PC1设备上发现无法ping通PC13,导致短时间内大量丢包。并且在sw3重启 成功后,sw3设备出现如下告警。

<SW3>
ARP/4/ARP_DUPLICATE_IPADDR(I)[0]:Received an
ARP packet with a duplicate IP address from the interface.
(IpAddress=192.168.12.254, InterfaceName=Vlanif12, MacAddress=0000-5e00-0101)

 由于该IP地址是虚拟IP地址,因此怀疑VRRP出现故障。同时分别在SW1 的GE0/0/10和SW2的GE0/0/3端口捕获报文。标红色的为源MAC和源IP。 SW2未捕获到数据包。

[SW1]capture-packet interface GigabitEthernet 0/0/10 destination terminal Packet: 6

00 00 5e 00 01 03 54 89 98 1f 5a 8d 81 00 00 0c 08 00 45 00 00 3c 39 aa 40 00 80 01 11 b8 c0 a8 0c 01 c0 a8 22 0d 08 00 99 d1 82 3b 0a 71 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 15 147 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27

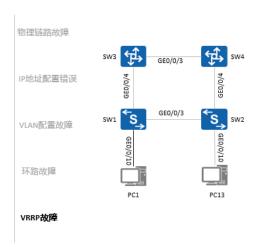
• capture-packet 命令用来在设备捕获符合设置规则的业

务报文,捕获的报文可保存为本地文件。

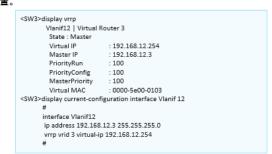
- capture-packet { interface interface-type interface-number | acl acl-number } * [vlan vlan-id | cvlan cvlan-id] * destination terminal [car cir car-value | time-out time-out-value | packet-num number | packet-len length] *
- 目前不支持捕获管理接口的报文。
- 目前只支持捕获接口入方向报文,不支持捕获接口出方向报文。



故障现象 - PC1和PC13无法正常通信 (8)



 上页结果表明丢包位置在SW1和SW2之间,且目的MAC地址为00 00 5e 00 01 03,得知VRRP的ID号为3,根据规划ID应为1。检查SW3的VRRP状态及配

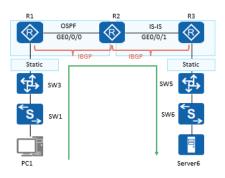


- 经过以上判断得知,由于VRID配置错误,VRRP出现双主故障,因此在 VRRP切换时会引发丢包,将SW3配置修改正确。
- 再次进行可靠性验证,发现切换时无丢包,至此故障排除。
- SW3、SW4上 VRRP 组号不一致,当 SW3 的 VRRP 检测下行链路故障时不会导致 SW4 的 VRRP 状态变化,SW4 的 VRRP 状态无变化,还是 Master,不会触发免费 ARP 刷新终端的 ARP 表项。
- 终端 PC1 发送给网关的报文其数据帧目的 MAC 地址依旧还是 00 00 5e 00 01 03。
- SW1、SW3 之间链路断开后,SW1 上不再有 00 00 5e 00 01 03 的 MAC 地址表项,无法将报文转发给 SW2。



故障现象 - PC1无法使用FTP服务 (1)

将拓扑图简化如下:

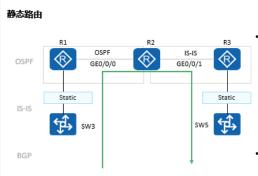


→ 流量规划路径

- 在上一故障处理中已保证PC1和SW3之间无故障,Server6和 SW5之间无故障。
- 如左图所示,将PC1无法使用FTP服务的故障原因列举如下:
 - 物理链路故障(已完成)
 - 路由故障
 - 静态路由
 - OSDE
 - BGP
 - IS-IS
 - 流量控制
 - 服务器故障(已完成)
- 本节主要处理路由故障,流量控制故障。



故障现象 - PC1无法使用FTP服务 (2)



- 数据包转发时需要进行逐跳转发,沿途所有的路由器都要有到达目的地的路由,首先检测PC1发送数据包给Server6经过的所有网络设备是否存在到达Server6的路由表项。
- 在SW3设备上检查静态路由配置。
 - 配置静态路由时:对于点到点接口,只需指定出接口;对于广播类型接口,必须指定下一跳IP。

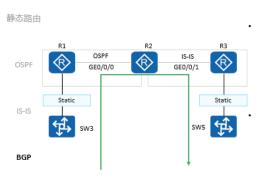
<SW3>display ip routing-table protocol static Route Flags: R - relay, D - download to fib
Destination/Mask Proto Pre Cost Flags NextHop Interface 0.0.0.0/0 Static 60 0 RD 10.0.13.1 Vlanif13

通过该步骤发现SW3静态路由配置没有问题。

──→ 流量规划路径



故障现象 - PC1无法使用FTP服务 (3)



在R1查看路由表。 <R1>display ip routing-table 192.168.56.0

由輸出结果得知,R1无到达192.168.56.0的路由。由于R1的路由应该由BGP协议获取,接下来查询R1的BGP邻居关系是否正常建立。

 <R1>display bgp peer

 BGP local router ID : 10.0.1.1

 Local AS number : 100

 Total number of peers : 1
 Peers in established state : 0

 Peer
 AS
 MsgRovd
 MsgSent
 OutQ
 Up/Down
 State
 PrefRcv

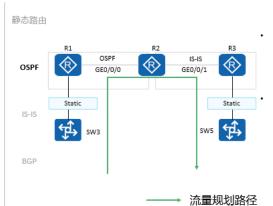
 10.0.2.2
 100
 0
 0
 0:00:05:05
 Idle
 0

由以上结果得知BGP邻居关系建立失败,BGP邻居关系建立失败的原因有:

- 。 远端设备的loopback0接口不可达
- · 本设备或远端设备AS号配置错误
- 。 非直连EBGP邻居关系未设置多跳
- Router ID冲突
- 流量规划路径 根据输出结果判断,BGP报文发送和接收数量都是0,因此怀疑是由于远端设备的loopback0接口不可达导致。



故障现象 - PC1无法使用FTP服务 (4)



· 在R1上查看到达BGP邻居IP地址的路由

<R1>display ip routing-table 10.0.2.2

由輸出结果得知,R1无到达10.0.2.2的路由。由于R1的路由应该由OSPF协议获取,接下来查询R1的OSPF邻居关系是否建立正常。

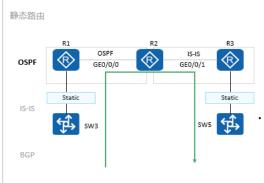
<R1>display ospf peer
OSPF Process 1 with Router ID 10.0.1.1

- 由以上结果得知OSPF邻居关系建立失败。邻居关系建立失败的原因有:
 - Router ID冲突
 - 。 区域ID不匹配
 - 网络掩码不匹配
 - MTU不一致
 - MA网络中,所有设备的DR优先级设置为0
 - 认证密码不匹配
 - · 接口被设置为silent-interface
 - 时间参数不匹配



故障现象 - PC1无法使用FTP服务 (5)

在R1查看OSPF error。



── 流量规划路径

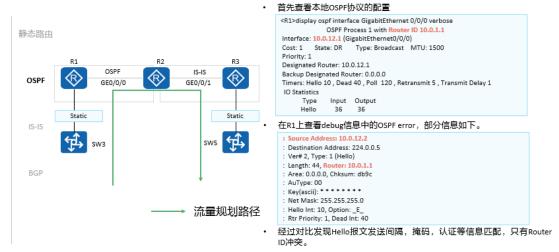
[R1]display ospf error General packet errors: 0 : IP: received my own packet 0 : Bad packet 0 : Bad checksum 0 : Bad version : Drop on unnumbered interface 0 : Bad virtual link 0 : Bad authentication type : Bad authentication key 0 : Packet size > ip length 0 : Transmit error : Interface down : Unknown neighbor 0 : Bad net segment 133 : Router id confus 0 : Extern option mismatch

由以上结果得知OSPF邻居关系建立失败的原因可能是Router ID冲突,为了更准确的确定故障原因,在R1上开启debug OSPF 功能。

<R1>terminal debugging Info: Current terminal debugging is on. <R1>debugging ospf packet interface GigabitEthernet 0/0/0



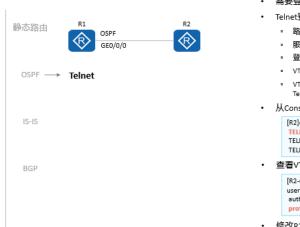
故障现象 - PC1无法使用FTP服务 (6)



• R1 上 debug 信息可以看到来自 10.0.12.2 的 hello 报文携带的 OSPF Router ID 与 R1 上 OSPF Router ID 相同,从而导致 Router ID 冲突。



故障现象 - PC1无法使用FTP服务 (7)



- 需要登录R2修改OSPF Router ID,但此时发现无法Telnet登录R2。
- 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。
 - · 服务器未开启Telnet功能。
 - 。 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。
- 从Console口登录到R1,查询设备是否开启Telnet服务。



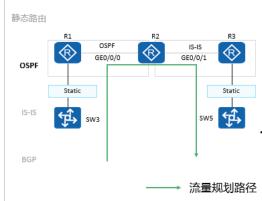
查看VTY下是否允许Telnet。

[R2-ui-vty0-4]display this
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh

• 修改R2配置,VTY下允许Telnet,经过测试发现R2可以正常登录。



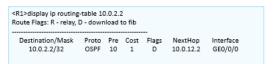
故障现象 - PC1无法使用FTP服务 (8)



在R2修改OSPF Router ID, 并且将OSPF进程重启,使Router ID生效,然后检查OSPF邻居关系状态。

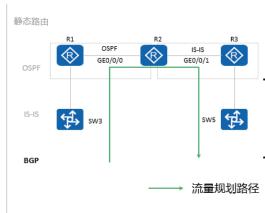


在R1上查看是否存在10.0.2.2的路由。





故障现象 - PC1无法使用FTP服务 (9)



• 在R1上查看BGP邻居状态。



在R1上查看BGP路由表中是否存在192.168.56.0/24。

```
<R1>display bgp routing-table
BGP Local router ID is 10.0.1.1
Total Number of Routes: 2

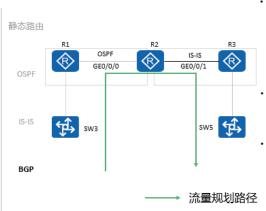
Network NextHop MED LocPrf Path/Ogn
*>192.168.12.0/24 0.0.0.0 0 0 ?
```

发现RI仍然没有路由信息,由于该路由信息是由R3引入,因此需要在R3 上查看是否将路由引入BGP协议。

```
<R3>display bgp routing-table
BGP Local router ID is 10.0.3.3
Total Number of Routes: 1
Network NextHop MED LocPrf Path/Ogn
*>192.168.56.0
0.0.0.0
0
?
```



故障现象 - PC1无法使用FTP服务 (10)



· 在R3上查看BGP邻居状态。



R3和R2的BGP邻居状态未建立,在R3上查看是否存在10.0.2.2/32的路由表项。

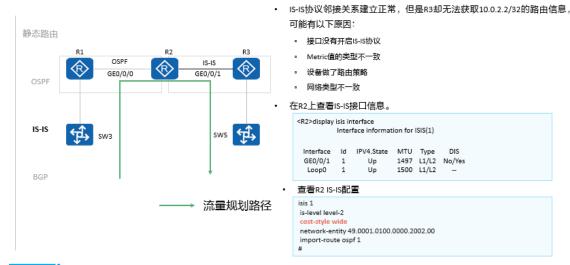
<R3>display ip routing-table 10.0.2.2

R3上无10.0.2.2/32的路由,由于R2和R3之间运行IS-IS协议,需要查看R3和R2之间是否正常建立了IS-IS邻居关系。

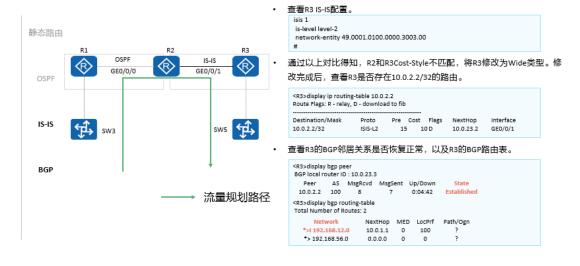
```
<R3>display isis peer
Peer information for ISIS(1)
SystemId Interface Circuitld State Type PRI
0100.0000.2002 GE0/0/1 0100.0000.2002.01 Up L2 64
```

- IS-IS 邻居关系无法正常建立的原因有:
- 区域 ID 不一致。(只会影响 level-1)
- 运行级别不一致。(注:在华为中如果系统级别和接口 电路级别不同,以系统级别为准)
- 接口认证不一致。
- system-id 长度不一致或者 system-id 冲突。
- IP 地址不在同一个网段。(IS-IS 在广播网中是开启源检查的,但是可以关闭)

故障现象 - PC1无法使用FTP服务 (11)

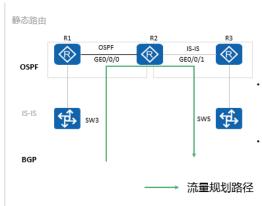


故障现象 - PC1无法使用FTP服务 (12)





故障现象 - PC1无法使用FTP服务 (13)



 R3已正确发布路由,且已经学习到192.168.12.0/24的路由。继续在R1查看 是否存在到达目的地192.168.56.0/24的路由。

<R1>display bgp routing-table
BGP Local router ID is 10.0.1.1

Network NextHop MED LocPrf Path/Ogn
*-192.168.12.0 0.0.0.0 0 0 ?
I 192.168.56.0 10.0.3.3 0 100 ?

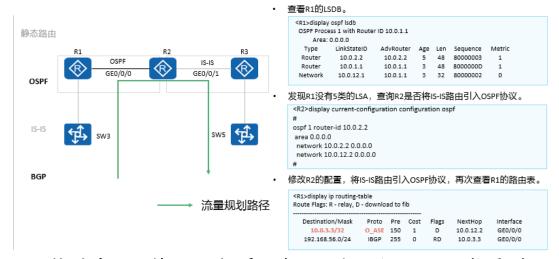
R1已收到R3发送的BGP路由,但是该路由不可用,可能因为下一跳不可达,继续在R1查看是否存在到达10.0.3.3/32的路由表项。

<R1>display ip routing-table 10.0.3.3

- 发现R1路由表中不存在10.0.3.3/32的路由,由于该路由条目应由R1从IS-IS 向OSPF引入,因此可能有以下原因导致R1无路由:
 - 。 R1配置了路由策略
 - R2没有将IS-IS路由引入OSPF
 - · R2接口出方向做了5类LSA的过滤



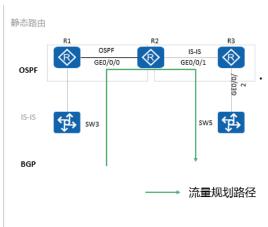
故障现象 - PC1无法使用FTP服务 (14)



• 修改完 R2 的配置之后,在 R1 上已经可以正常看到 10.0. 3.3/32 的路由表项。



故障现象 - PC1无法使用FTP服务 (15)



在PC1设备Traceroute 192.168.56.6。

traceroute to 192.168.56.6, 8
1 192.168.12.3 63 ms 46 ms 47 ms
2 10.0.13.1 78 ms 63 ms 62 ms
3 10.0.12.2 94 ms 63 ms 78 ms
4 10.0.23.3 94 ms 62 ms 63 ms
5 * * *

发现数据包到达R3之后没有返回响应,在R3的GE0/0/2接口开启流量统计,查看R3是否将数据包从GE0/0/2口发出。

E名 (R3) acl 3000

[R3] acl 3000

[R3-acl-adv-3000] rule 5 permit ip source 192.168.12.1 0 destination 192.168.56.6 0

[R3-acl-adv-3000] quit
[R3] traffic classifier trafficSta
[R3-classifier-trafficSta] if-match acl 3000

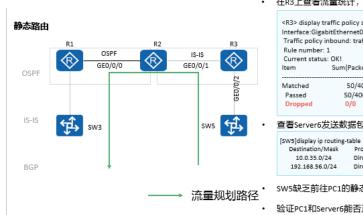
[R3-classifier-trafficSta] quit
[R3] traffic behavior trafficSta
[R3-behavior-trafficSta] statistic enable
[R3-behavior-trafficSta] quit
[R3] traffic policy trafficSta
[R3-trafficpolicy-trafficSta] quit
[R3] trafficpolicy-trafficSta] quit
[R3] interface GigabitEthernet0/0/2.35
[R3-digabitEthernet0/0/2.35] traffic-policy trafficSta outbound

- R1 上正常学习到路由之后,PC1 依然无法访问 Server6 提供的 FTP 服务,此时通过 traceroute 排查到 Server6 的连通性在何处中断。
- 基于流量统计,可以分析如下问题:
- 流量是否到达设备入口,进而判断上游设备是否丢包;
- 流量是否被转发到设备出口,进而判断设备是否丢包;
- 流量在设备入口二三层信息是否正确,进而判断上游设备转发封装是否正常;
- 流量在设备出接口二三层信息是否正确,进而判断设备 转发封装是否正常;
- 是否存在 MAC 漂移、路由变化、IP 冲突等导致的流量 瞬间漂移。
- 流量统计的配置步骤:
- 配置 ACL 规则,匹配需要统计的流量。
- 配置流分类,根据 ACL 规则匹配不同的流量,从而区分不同数据流量。
- 配置流行为,在流行为中配置流量统计。
- 配置流策略,绑定以上流分类和流行为,实现对不同用户报文的流量统计。

在接口出方向或入方向调用流策略。



故障现象 - PC1无法使用FTP服务 (16)



在R3上查看流量统计,发现R3无丢包。

<R3> display traffic policy statistics interface GigabitEthernet0/0/2.35 outbound Interface: GigabitEthernet0/0/2.35
Traffic policy inbound: trafficSta
Rule number: 1
Current status: OK!
Item Sum(Packets/Bytes)

Matched 50/400
Passed 50/400
Dropped 0/0

查看Server6发送数据包方向上设备的路由信息,检查SW5路由表。

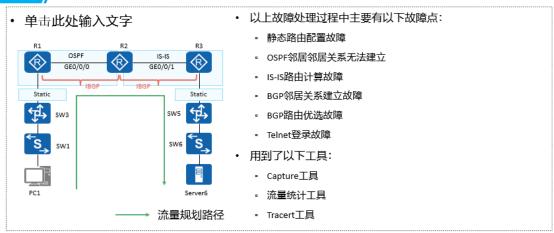
 [SWS] display ip routing-table
 Destination/Mask
 Proto
 Pre
 Cost
 Flags
 NextHop
 Interface

 10.03.5.0/24
 Direct
 0
 0
 D
 10.0.35.5
 Vlanif35

 192.168.56.0/24
 Direct
 0
 0
 D
 192.168.56.5
 Vlanif35

- ス・ SW5缺乏前往PC1的静态路由,在SW5上配置静态路由。
 - 验证PC1和Server6能否正常通信,以及正常使用FTP服务。
 - 完成以上工作后该故障处理完成。

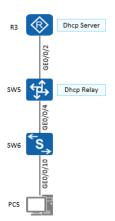
故障现象 - PC1无法使用FTP服务总结





故障现象 - PC5无法和任何主机通信 (1)

将拓扑图简化如下:



- 由于PC5不能和任何主机进行通信,因此怀疑PC5物理链路或者IP地址获取异常。
- · 检查PC5获取IP地址的状态,发现PC5未能获取IP地址。

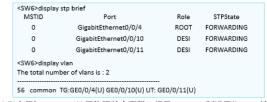
PC>ipconfig
IPv4 address 0.0.0.0
Subnet mask 0.0.0.0
Gateway 0.0.0.0
Physical address 54-89-98-39-22-87
DNS server 0.0.0.0

- PC5使用DHCP的方式获取IP地址,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。
 - · 地址池中没有可用的IP地址可分配。
 - 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:
 - 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。
 - DHCP中继没有配置所代理的DHCP服务器。
 - nuco由機和nuco服务要素可決

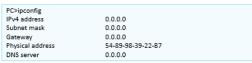


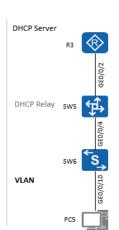
故障现象 - PC5无法和任何主机通信 (2)

- 检查PC5物理链路是否正常(略)。
- 检查交换机SW6是否出现二层环路,以及相关VLAN配置。



- 由以上得知GE0/0/10接口物理状态正常,但是GE0/0/10别设置为Trunk端口,在SW6设备上修改配置,将GE0/0/10设置为Access端口,并且VLAN设置为56。
- 修改完毕后继续查看PC5是否正常获取IP地址。

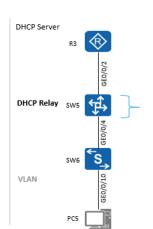






故障现象 - PC5无法和任何主机通信 (3)

• SW5为DHCP中继设备,接下来查询SW5的全局配置。



- <SW5>display current-configuration dhcp enable # interface Vlanif35 ip address 10.0.35.5 255.255.255.0 dhcp select relay dhcp relay server-ip 10.0.35.3 #
- sw5已开启DHCP服务,并且已完成中继配置,但是由于PC5发送的数据包经过SW6之后,SW6转 发时会添加TAG56,因此SW5配置的DHCP中继接口错误。
- 按照如下命令,修改SW5的配置。

[SW5]interface Vlanif 56 [SW5-Vlanif56]dhcp select relay [SW5-Vlanif56]dhcp relay server-ip 10.0.35.3

· 修改完成后,在PC5设备上发现仍然无法获取IP地址。



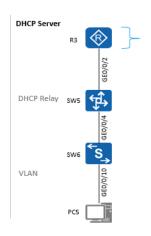
故障现象 – PC5无法和任何主机通信 (4)

• 查询SW5的DHCP Relay状态。





故障现象 - PC5无法和任何主机通信 (5)



R3和SW5对接使用的是子接口,因此需要在子接口下开启DHCP Server服务,而不是物理接口GE0/0/2。

[R3]interface GigabitEthernet 0/0/2.35 [R3-GigabitEthernet0/0/2.35]dhcp select global 在R3上完成如上配置后,检查R3 DHCP Server的状态。 <R3>display dhcp server statistics DHCP Server Statistics: Client Request Dhcp Discover Dhcp Request Server Reply Dhcp Offer Bad Messages 在PC5上查看IP地址获取状态: PC>ipconfig 192.168.56.253 IPv4 address Subnet mask 255.255.255.0 192.168.56.254 Gateway

PC5已获取到IP地址,并且验证可以和所有主机通信,故障处理完成。

54-89-98-39-22-B7 192.168.1.1

思考题:

(多选题)在结构化的网络故障排除流程的收尾工作中,信息需要通告给哪些相关方?

Physical address

DNS server

- 受故障影响的相关方。
- 故障排除各阶段授权方。
- 厂家、服务提供商。
- 对故障根源感兴趣的其他无关人员。
- (判断题)在大规模网络中对比法是处理故障最有效的方法。

参考答案:

ABC

错

思考题:

- (多选题)OSPF 邻居关系无法建立,有可能是以下哪种原因?
- Router ID 冲突
- 区域 ID 不匹配
- 接口掩码不匹配

- 进程号不一致
- (判断题)运行 IS-IS 协议的路由器,如果接口下的路由器层级和全局路由器层级不一致,以接口路由器层级为准。
- (多选题)二层环路可能会产生哪些故障现象?
- 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%

参考答案:

ABC

错

ABCD