SNMP 常见故障处理

文档版本 01

发布日期 2021-08-03

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

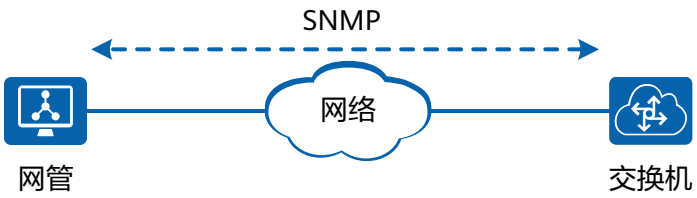
网址： https://e.huawei.com

目 录

1 简介

SNMP是广泛应用于TCP/IP网络的网络管理标准协议。网管系统可以通过SNMP协议对网络设备（包括交换机、路由器、防火墙等）进行监测和管理。

图 1-1 SNMP 网络架构



如上图所示，SNMP网络的组成包括网管、被纳管设备、中间网络，这几部分都有可能导致网管与被纳管设备之间的SNMP交互异常。

本文档主要介绍网管通过SNMP协议对交换机进行监测、管理中的常见故障处理方法，主要包括以下几方面：

- **2 网管无法通过SNMP纳管交换机**
- **3 网管接收不到交换机上的告警**

2 网管无法通过 SNMP 纳管交换机

网管无法通过SNMP纳管交换机，或者说网管无法与交换机进行SNMP对接，通常是因为网络或者SNMP配置原因导致。您可以从以下几方面进行排查和处理：

- **检查网络是否可以ping通**
- **检查SNMP是否有应用ACL**
- **检查交换机上是否有undo snmp-agent protocol source-status all-interface配置**
- **检查交换机上是否有SNMP认证失败等日志**
- **检查交换机和网管的SNMP版本是否一致**
- **针对SNMPv2c版本，检查交换机和网管的团体名是否一致**
- **针对SNMPv3版本，检查用户的安全级别是否正确**
- **针对SNMPv3版本，检查用户的认证+加密的模式及密码是否和网管侧一致**
- **检查防火墙是否允许SNMP报文通过**
- **检查网络中是否有重复的SNMP引擎ID**

检查网络是否可以 ping 通

网络可以互通是SNMP对接的前提，您可以通过ping命令检查交换机和网管能否互通。如果不能互通，请检查交换机、中间网络或网管上的路由配置是否正确，确保交换机和网管能够ping通。

需要注意的是，即使交换机和网管之间能够ping通，也并不意味着交换机和网管一定能够正常接收到对端发送的SNMP报文。因为ping是ICMP报文，而SNMP是UDP报文，可能会因为ACL的应用，或者网络中有防火墙等原因，导致SNMP报文被过滤，无法通过网络正常转发。

您可以在网络设备上进行流量统计或者镜像抓包等方法确认SNMP报文是否被正常发送、接收。因为不同网络设备的流量统计或镜像抓包方法不尽相同，本文不再赘述，您可以参考相应的产品文档。

检查 SNMP 是否有应用 ACL

如果交换机上的SNMP配置里有应用ACL，那么网管的IP地址必须在ACL规则允许通过的列表中。如果检查网管IP地址没有被放通，需要修改ACL规则，放通网管IP地址。

```
#
acl number 2001
```



```
 rule 5 permit source 192.168.1.0 0.0.0.255  //网管IP地址必须在允许通过的列表中
#
snmp-agent community write cipher xxx acl 2001  //SNMPv2c版本应用ACL的配置示例
#
snmp-agent group v3 huawei_group privacy write-view alliso acl 2001  //SNMPv3版本应用ACL的配置示例
#
```

检查交换机上是否有 undo snmp-agent protocol source-status all-interface 配置

CloudEngine交换机从V200R019C10版本开始，缺省情况下，交换机会关闭SNMP协议使用所有接口响应网管请求的功能，即有如下配置：

```
#
undo snmp-agent protocol source-status all-interface
undo snmp-agent protocol source-status ipv6 all-interface
#
```

如果交换机上有上述配置，需要打开SNMP协议使用所有或者部分接口响应网管请求的功能。

- 打开SNMP协议使用所有接口响应网管请求的功能。
  ```
  [~HUAWEI] snmp-agent protocol source-status all-interface
  [~HUAWEI] snmp-agent protocol source-status ipv6 all-interface
  ```
- 打开指定的接口响应网管请求的功能。
  ```
  [~HUAWEI] snmp-agent protocol source-interface meth 0/0/0
  ```

检查交换机上是否有 SNMP 认证失败等日志

在网管与交换机进行SNMP对接失败时，交换机上可能会记录一些SNMP异常的日志，例如：SNMP/3/SNMP_AUTHEN_FAILED。您可以执行命令**display logbuffer**查看交换机上是否有SNMP异常日志，并根据日志中记录的原因而进行相应的处理。

```
SNMP/3/SNMP_AUTHEN_FAILED: Failed to login through SNMP. (Version=[Version],
UserName=[UserName], Ip=[Ip], VpnName=[VpnName], RequestID=[RequestID], PduType=[PduType],
Reason=[Reason])
```

4.1 SNMP_AUTHEN_FAILED日志常见原因及处理列举出了常见的SNMP对接异常原因及处理方法。

检查交换机和网管的 SNMP 版本是否一致

SNMP有v1、v2c、v3几种版本，交换机侧和网管侧的SNMP版本必须保持一致，否则无法进行SNMP对接。

缺省情况下，交换机的SNMP版本为v3。您可以检查配置文件或者通过命令**display snmp-agent sys-info version**查看当前交换机的SNMP版本。如果两侧SNMP版本不一致，需要修改交换机或网管侧，使其保持一致。

例如配置交换机的SNMP版本支持v2c。

```
[~HUAWEI] snmp-agent sys-info version v2c
```

针对 SNMPv2c 版本，检查交换机和网管的团体名是否一致

团体名包括只读权限的团体名和读写权限的团体名，交换机侧和网管侧配置的团体名必须一致。

交换机上配置的SNMP团体名是以密文的形式保存的。如果忘记配置的团体名，建议重新配置团体名，使之与网管侧一致。


```
#
snmp-agent sys-info version v2c
snmp-agent community read cipher xxx   //只读权限团体名
snmp-agent community write cipher xxx   //读写权限团体名
#
```

针对 SNMPv3 版本，检查用户的安全级别是否正确

SNMPv3用户的安全级别分为三个等级，从高到低为：

- privacy：认证并加密
- authentication：认证不加密
- none：不认证不加密

SNMPv3协议规定，用户和告警主机的安全级别不能低于其所属用户组的安全级别，否则网管将无法与交换机对接。如果用户组是privacy级别，用户和告警主机就必须是privacy级别；用户组是authentication级别，用户和告警主机可以是privacy或者authentication级别。

```
#
snmp-agent sys-info version v3
snmp-agent group v3 dc-admin privacy read-view rd write-view wt notify-view nt   //组名为dc-admin，安全级别为privacy
#
snmp-agent usm-user v3 uhmroot
snmp-agent usm-user v3 uhmroot group dc-admin    //用户名为uhmroot，属于dc-admin组
snmp-agent usm-user v3 uhmroot authentication-mode sha cipher xxx    //认证模式及密码
snmp-agent usm-user v3 uhmroot privacy-mode aes128 cipher xxx       //加密模式及密码，如果用户组安全级别为privacy，用户必须同时配置authentication-mode和privacy-mode
#
```

针对 SNMPv3 版本，检查用户的认证+加密的模式及密码是否和网管侧一致

交换机侧SNMPv3用户的认证、加密的模式及密码必须和网管侧保持一致，否则无法完成SNMP对接。

交换机上配置的SNMP密码是以密文的形式保存的。如果忘记配置的密码，建议重新配置认证、加密的模式及密码，使之与网管侧一致。

```
#
snmp-agent usm-user v3 uhmroot
snmp-agent usm-user v3 uhmroot group dc-admin
snmp-agent usm-user v3 uhmroot authentication-mode sha cipher xxx   //认证模式及密码，必须和网管侧一致
snmp-agent usm-user v3 uhmroot privacy-mode aes128 cipher xxx       //加密模式及密码，必须和网管侧一致
#
```

检查防火墙是否允许 SNMP 报文通过

如果交换机和网管之间的网络中有防火墙，则可能会因为防火墙的过滤策略而导致SNMP报文无法正常通过。以Huawei防火墙为例，防火墙默认丢弃所有的报文，只有在防火墙策略中放行的报文才能正常转发。

在检查防火墙上的安全策略时，需要注意策略中的以下几点：

- 交换机所属的安全域和网管所属的安全域之间的策略，交换机和网管的IP地址需要被放通，且双向都需要放通。
- 防火墙上连接交换机和网管的接口需要开启SNMP服务。

```
#
security-policy
```

```
 rule name policy1      //安全域策略
  source-zone trust      //源安全域
  destination-zone untrust      //目的安全域
  source-address 10.1.1.0 mask 255.255.255.0      //源IP地址，交换机或网管地址需要在此范围内
  destination-address 10.1.2.0 mask 255.255.255.0      //目的IP地址，交换机或网管IP地址需要在此范围内
  action permit
 rule name policy2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
#
interface GigabitEthernet1/0/0      //连接交换机或网管的接口
 undo shutdown
 ip address 10.1.2.1 255.255.255.0
 service-manage snmp permit      //开启SNMP服务，缺省情况下SNMP服务未开启
#
```

检查网络中是否有重复的 SNMP 引擎 ID

正常情况下，网络中每台交换机都会有一个唯一的SNMP引擎ID，用于标志一个SNMP实体。如果网络中交换机的SNMP引擎ID有重复，那么后添加的交换机将无法与网管进行对接。

```
#
snmp-agent
snmp-agent local-engineid 800007DB03D0C65B9E5D01    //SNMP引擎ID
#
```

SNMP引擎ID重复通常出现于复制其他交换机的配置文件后，再进行修改并使用的场景，容易漏修改原交换机使用的SNMP引擎ID。如果发现SNMP引擎ID有重复，可以在交换机上通过**undo snmp-agent local-engineid**恢复ID为缺省值，使其唯一。

```
[~HUAWEI] undo snmp-agent local-engineid
```


3 网管接收不到交换机上的告警

当交换机发生故障或因某些原因导致系统进入不正常的工作状态时，为帮助用户快速感知并定位问题，系统会产生事件和告警，同时触发产生相应的Trap信息。Trap信息通过SNMP协议上报到网管系统。在实际应用中，习惯把Trap直接称为告警，为便于理解，下文中的告警和Trap是同一个含义。

网管能够收到交换机告警的前提是网管已经成功纳管交换机，所以在处理网管接收不到告警的问题前，请先确保网管能够正常纳管交换机，然后从以下几方面进行排查和处理：

- **检查交换机上告警开关是否打开，或告警是否被过滤**
- **检查交换机是否有set net-manager vpn-instance配置**
- **检查交换机发送告警时使用的SNMP版本是否与全局SNMP版本一致**
- **检查交换机的SNMP告警端口号和网管侧是否一致**

检查交换机上告警开关是否打开，或告警是否被过滤

网管接收到告警的前提是交换机真实产生了告警或事件，并产生了相应的Trap信息，因此在网管接收不到告警时，首先需要确认交换机是否产生了Trap。

执行命令**display trapbuffer**查看Trap缓冲区中是否存在对应的告警信息。如果不存在，则说明交换机没有产生告警，网管也就无法收到告警，此时可以通过检查交换机的如下配置进行排查：

- 检查对应的告警开关是否开启。

  例如，接口Down的告警为：IFNET_1.3.6.1.6.3.1.1.5.3 linkdown ，IFNET为告警所属的模块。通过命令**display snmp-agent trap feature-name** *feature-name* **all**，可以查看到交换机上接口Down告警开关是否打开，其中“Current switch status”值即表示当前告警开关的开启状态。

  ```
  <HUAWEI> display snmp-agent trap feature-name ifnet all
  ------------------------------------------------------------------------------
  Feature name: IFNET
  Trap number : 4
  ------------------------------------------------------------------------------
  Trap name                Default switch status   Current switch status
  hwPhysicalAdminIfDown        on                      on
  hwPhysicalAdminIfUp          on                      on
  linkdown                 off                     off
  linkup                   off                     off
  ```

  如果告警被关闭，可以执行命令**snmp-agent trap enable feature-name** *feature-name* **trap-name** *trap-name*可以打开对应告警的开关。


```
[~HUAWEI] snmp-agent trap enable feature-name ifnet trap-name linkdown
```

或者执行命令**snmp-agent trap enable**打开所有告警的开关。

```
[~HUAWEI] snmp-agent trap enable
```

- 检查告警是否被过滤掉。

  如果交换机上配置了**info-center filter-id** { *id* | **bymodule-alias** *modname alias* }命令过滤了相应的Trap，那么即使交换机产生了该告警，也不会产生Trap信息，网管也无法收到该告警。

  ```
  #
  info-center filter-id bymodule-alias ifnet linkdown
  #
  ```

  如果有上述配置，可以执行**undo info-center filter-id** { *id* | **bymodule-alias** *modname alias* }删除该配置

  ```
  [~HUAWEI] undo info-center filter-id bymodule-alias ifnet linkdown
  ```

检查交换机是否有 set net-manager vpn-instance 配置

通常情况下，交换机上配置SNMP发送告警信息时，除了指定目标网管外，还会使用**snmp-agent trap source** *interface-type interface-number*命令指定发送告警的源接口。这样在网管上可以进行告警源识别。

但是交换机上若同时配置了**set net-manager vpn-instance** *vpn-instance*命令，且该VPN和**snmp-agent trap source** *interface-type interface-number*命令指定的源接口绑定的VPN不是同一个，那么交换机会优先使用**set net-manager vpn-instance** *vpn-instance*命令指定的VPN里的某个接口作为源接口，这样会导致网管无法接受到正确源地址的告警。

例如交换机上有以下配置。那么交换机发送告警至网管时，源接口将是vpn1里的LoopBack2，而不是LoopBack1。

```
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface LoopBack2
 ip binding vpn-instance vpn1
 ip address 2.2.2.2 255.255.255.255
#
set net-manager vpn-instance vpn1     //如果配置该命令，优先使用该命令指定的VPN里的接口来发送告警
#
snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname uhmroot v3 privacy     //指定接收告警的目标网管
#
snmp-agent trap source LoopBack1     //指定发送告警的源接口
#
```

若产生了上述冲突场景，可以采用下面其中一种方法解决：

- 执行**undo set net-manager vpn-instance**删除该配置。

  删除该配置前，请先确认对其他业务模块的影响，因为该命令不仅仅会影响SNMP模块，还会对FTP、SFTP、Info Center、SSH、TACACS等业务模块产生影响。

- 在**snmp-agent target-host trap**命令中指定源接口。该命令中指定的源接口参数**source** *interface-type interface-number*具有最高优先级。

  ```
  [~HUAWEI] snmp-agent target-host trap address udp-domain 10.1.1.1 source loopback1 params securityname uhmroot v3 privacy
  ```


检查交换机发送告警时使用的 SNMP 版本是否与全局 SNMP 版本一致

交换机上**snmp-agent target-host trap**命令指定的发送告警时使用的SNMP版本，需要与**snmp-agent sys-info version**指定的全局SNMP版本一致，否则交换机无法正常发送出告警。在配置**snmp-agent target-host trap**命令时，如果不指定SNMP版本，则默认使用SNMPv1。

例如以下配置中，全局SNMP协议使能的是v3版本，而未指定发送告警时所使用的SNMP版本，使用默认的v1版本，两者的版本不一致，因此交换机无法正常发送出告警。

```
snmp-agent sys-info version v3      //仅使能SNMPv3版本
snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname uhmroot //未配置交换机发送告警所使用的SNMP版本，默认使用SNMPv1版本
```

需要在**snmp-agent target-host trap**命令中指定发送告警时使用的SNMP版本，使其和全局的版本一致。

```
[~HUAWEI] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname uhmroot v3 privacy
```

检查交换机的 SNMP 告警端口号和网管侧是否一致

按照SNMP协议规范，SNMP使用目的端口号162来发送告警信息。因此，网管通常使用端口号162来处理告警信息，例如Huawei的eSight网管系统。

如果交换机上**snmp-agent target-host trap**配置里指定了目的端口号（缺省情况下为162），且与网管侧不一致，则会导致网管无法正常接收告警信息。

```
#
snmp-agent target-host trap address udp-domain 10.1.1.1 udp-port 161 params securityname uhmroot v3 privacy
#
```

建议使用默认的目的端口号。

```
#
snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname uhmroot v3 privacy
```


4 附录

4.1 SNMP_AUTHEN_FAILED 日志常见原因及处理

SNMP/3/SNMP_AUTHEN_FAILED: Failed to login through SNMP. (Version=[Version], UserName=[UserName], Ip=[Ip], VpnName=[VpnName], RequestID=[RequestID], PduType=[PduType], **Reason**=[Reason])

该日志中记录了交换机与网管通过SNMP对接失败的部分原因，具体内容如下：

表 4-1 失败原因及处理建议

失败原因	含义	处理建议
Version is incorrect	网管侧和交换机侧配置的SNMP版本不一致。	执行命令**display snmp-agent sys-info version**查看交换机配置的SNMP版本是否与网管侧使用的SNMP协议版本一致。如果不一致，请在系统视图下执行命令**snmp-agent sys-info version**配置交换机所支持的SNMP协议版本。
Packet is too large	网管发送的报文太大，超过交换机设置的阈值。	在系统视图下执行命令**snmp-agent packet max-size**增大报文阈值。
Community is incorrect	网管侧和交换机侧配置的团体名不一致。	用户配置的SNMP团体名是以密文的形式保存的。如果忘记配置的团体名，建议在系统视图下执行命令**snmp-agent community** { **read** | **write** } *community-name*重新配置团体名，使之与网管侧配置一致。
ACL denied	该IP地址被ACL禁止。	请在对应的ACL视图下执行命令**rule**，配置允许网管IP地址访问交换机。 如果网管在某个VPN中，但是ACL规则中没有绑定VPN实例名，请在对应的ACL视图下执行命令**rule**，在配置ACL规则时绑定VPN实例。

失败原因	含义	处理建议
UsmUser Name is incorrect	网管侧和交换机侧配置的SNMPv3 USM用户名或者AAA本地用户名不一致。	请修改网管侧的配置或者重新配置交换机的SNMPv3 USM用户名/AAA本地用户名，使网管侧和交换机侧配置的用户名保持一致。
Wrong Protocol Parameter	协议参数错误，SNMPv3用户安全级别低于SNMPv3用户组的级别。	在系统视图下执行命令**snmp-agent usm-user v3** *user-name* **authentication-mode** { **md5** | **sha** }配置SNMPv3用户的认证密码；在系统视图下执行命令**snmp-agent usm-user v3** *user-name* **privacy-mode** { **3des168** | **aes128** | **aes192** | **aes256** | **des56** }配置SNMPv3用户的加密密码。
Wrong Privacy Parameters for USM User	网管侧SNMPv3 USM用户使用的加密方式或加密密码与交换机侧配置不一致。	在系统视图下执行命令**snmp-agent usm-user v3** *user-name* **privacy-mode** { **3des168** | **aes128** | **aes192** | **aes256** | **des56** }重新配置SNMPv3 USM用户的加密方式和加密密码，使之与网管侧的保持一致。
Wrong Authentication Parameters for USM User	网管侧SNMPv3 USM用户使用的认证方式或认证密码与交换机侧配置不一致。	请在系统视图下执行命令**snmp-agent usm-user v3** *user-name* **authentication-mode** { **md5** | **sha** }重新配置SNMPv3 USM用户的认证方式和认证密码，使之与网管侧的保持一致。

失败原因	含义	处理建议
Wrong Security level for USM User	网管侧SNMPv3 USM用户使用安全级别高于交换机侧SNMPv3 USM用户的安全级别。	在任意视图下执行命令**display snmp-agent usm-user**查看SNMPv3 USM用户是否配置认证或者加密方式，如果： ● 交换机SNMPv3 USM用户没有配置认证方式和加密方式，表示交换机SNMPv3 USM用户的安全级别为noauthentication，而网管侧SNMPv3 USM用户使用的安全级别为authentication。此时可以进行以下任一操作： – 在系统视图下执行命令**snmp-agent usm-user v3** *user-name* **authentication-mode** { **md5** | **sha** }配置交换机SNMPv3 USM用户的认证密码，并保证认证密码与网管侧的一致。 – 修改网管侧SNMPv3 USM用户使用的安全级别，使之与交换机保持一致。 ● 交换机SNMPv3 USM用户配置了认证方式，表示交换机SNMPv3 USM用户的安全级别为authentication，而网管侧SNMPv3 USM用户使用的安全级别为privacy。此时可以进行以下任一操作： – 在系统视图下执行命令**snmp-agent usm-user v3** *user-name* **privacy-mode** { **3des168** | **aes128** | **aes192** | **aes256** | **des56** }配置交换机SNMPv3 USM用户的加密密码，并保证加密密码与网管侧的一致。 – 修改网管侧SNMPv3 USM用户使用的安全级别，使之与交换机保持一致。
Wrong Authentication Parameters for Local User	网管侧AAA本地用户使用的认证密码和交换机侧配置不一致。	在系统视图下执行命令**snmp-agent local-user v3** *user-name* { **authentication-mode** { **md5** | **sha** } **privacy-mode** { **3des168** | **aes128** | **aes192** | **aes256** | **des56** } }重新配置SNMPv3 AAA本地用户的认证密码和加密密码，使之与网管侧保持一致。
Wrong Privacy Parameters for Local User	网管侧AAA本地用户使用的加密密码与交换机侧配置不一致。	

失败原因	含义	处理建议
Pipeline is full	网管发送的SNMP请求报文过多，导致管道线已满。	减少网管发送SNMP请求报文的数目。

