

# 什么是 SNMP

文档版本

01

发布日期

2019-05-31



版权所有 © 华为技术有限公司 2020。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI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默示的声明或保证。

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.....

2 SNMP 系统组成.....

3 SNMP 查询.....

4 SNMP 设置.....

5 SNMP Traps.....

6 SNMP 端口号.....

7 使用 SNMP 的相关信息.....

1

2

5

11

14

18

19

# 1 简介

---

简单网络管理协议SNMP（Simple Network Management Protocol）用于网络设备的管理。网络设备种类多种多样，不同设备厂商提供的管理接口（如命令行接口）各不相同，这使得网络管理变得愈发复杂。为解决这一问题，SNMP应运而生。SNMP作为广泛应用于TCP/IP网络的网络管理标准协议，提供了统一的接口，从而实现了不同种类和厂商的网络设备之间的统一管理。

SNMP协议分为三个版本：SNMPv1、SNMPv2c和SNMPv3。

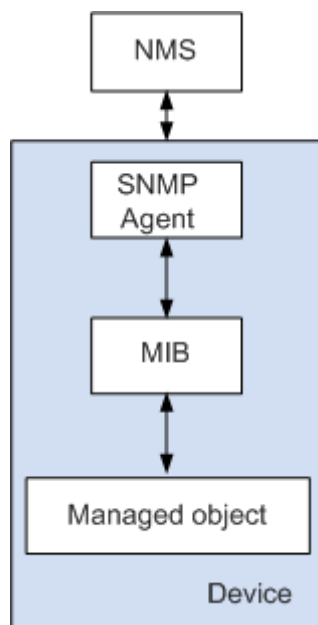
- SNMPv1是SNMP协议的最初版本，提供最小限度的网络管理功能。SNMPv1基于团体名认证，安全性较差，且返回报文的错误码也较少。
- SNMPv2c也采用团体名认证。在SNMPv1版本的基础上引入了GetBulk和Inform操作，支持更多的标准错误码信息，支持更多的数据类型（Counter64、Counter32）。
- SNMPv3主要在安全性方面进行了增强，提供了基于USM（User Security Module）的认证加密和基于VACM（View-based Access Control Model）的访问控制。SNMPv3版本支持的操作和SNMPv2c版本支持的操作一样。

# 2 SNMP 系统组成

SNMP系统由网络管理系统NMS（Network Management System）、SNMP Agent、被管对象Management object和管理信息库MIB（Management Information Base）四部分组成。NMS作为整个网络的网管中心，对设备进行管理。

每个被管理设备中都包含驻留在设备上的SNMP Agent进程、MIB和多个被管对象。NMS通过与运行在被管理设备上的SNMP Agent交互，由SNMP Agent通过对设备端的MIB进行操作，完成NMS的指令。

图 2-1 SNMP 系统组成



## NMS

NMS是网络中的管理者，是一个采用SNMP协议对网络设备进行管理/监视的系统，运行在NMS服务器上。

- NMS可以向设备上的SNMP Agent发出请求，查询或修改一个或多个具体的参数值。
- NMS可以接收设备上的SNMP Agent主动发送的SNMP Traps，以获知被管理设备当前的状态。

## SNMP Agent

SNMP Agent是被管理设备中的一个代理进程，用于维护被管理设备的信息数据并响应来自NMS的请求，把管理数据汇报给发送请求的NMS。

- SNMP Agent接收到NMS的请求信息后，通过MIB表完成相应指令后，并把操作结果响应给NMS。
- 当设备发生故障或者其它事件时，设备会通过SNMP Agent主动发送SNMP Traps给NMS，向NMS报告设备当前的状态变化。

## Managed Object

Managed object指被管理对象。每一个设备可能包含多个被管理对象，被管理对象可以是设备中的某个硬件，也可以是在硬件、软件（如路由选择协议）上配置的参数集合。

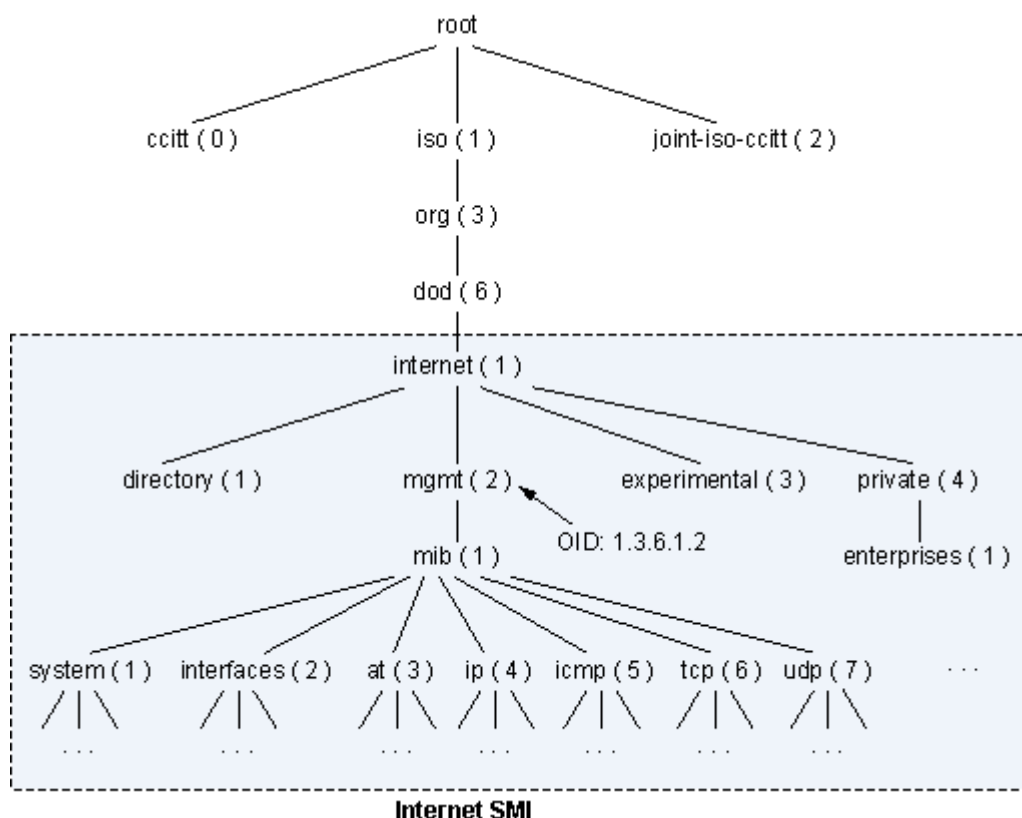
## MIB

MIB是一个数据库，指明了被管理设备所维护的变量。MIB在数据库中定义了被管理设备的一系列属性：对象的名称、对象的状态、对象的访问权限和对象的数据类型等。MIB也可以看作是NMS和SNMP Agent之间的一个接口，通过这个接口，NMS对被管理设备所维护的变量进行查询/设置操作。

MIB是以树状结构进行存储的，如图2-2所示。树的节点表示被管理对象，它可以用从根开始的一条路径唯一地识别，这条路径就称为OID，如system的OID为1.3.6.1.2.1.1，interfaces的OID为1.3.6.1.2.1.2。

子树可以用该子树根节点的OID来标识。如以private为根节点的子树的OID为private的OID——{1.3.6.1.4}。

图 2-2 OID 树结构



用户可以配置MIB视图来限制NMS能够访问的MIB对象。MIB视图是MIB的子集合，用户可以将MIB视图内的对象配置为exclude或include。exclude表示当前视图不包含该MIB子树的所有节点；include表示当前视图包含该MIB子树的所有节点。

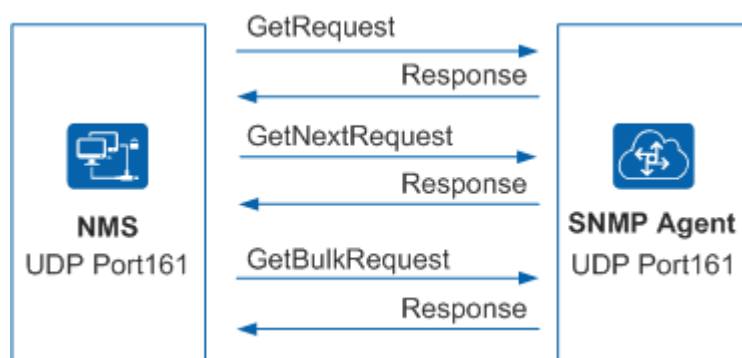
# 3 SNMP 查询

SNMP查询是指NMS主动向SNMP Agent发送查询请求，如图3-1所示。SNMP Agent接收到查询请求后，通过MIB表完成相应指令，并将结果反馈给NMS。

SNMP查询操作有三种：Get、GetNext和GetBulk。SNMPv1版本不支持GetBulk操作。

- Get操作：NMS使用该操作从SNMP Agent中获取一个或多个参数值。
- GetNext操作：NMS使用该操作从SNMP Agent中获取一个或多个参数的下一个参数值。
- GetBulk操作：基于GetNext实现，相当于连续执行多次GetNext操作。在NMS上可以设置被管理设备在一次GetBulk报文交互时，执行GetNext操作的次数。

图 3-1 SNMP 查询操作

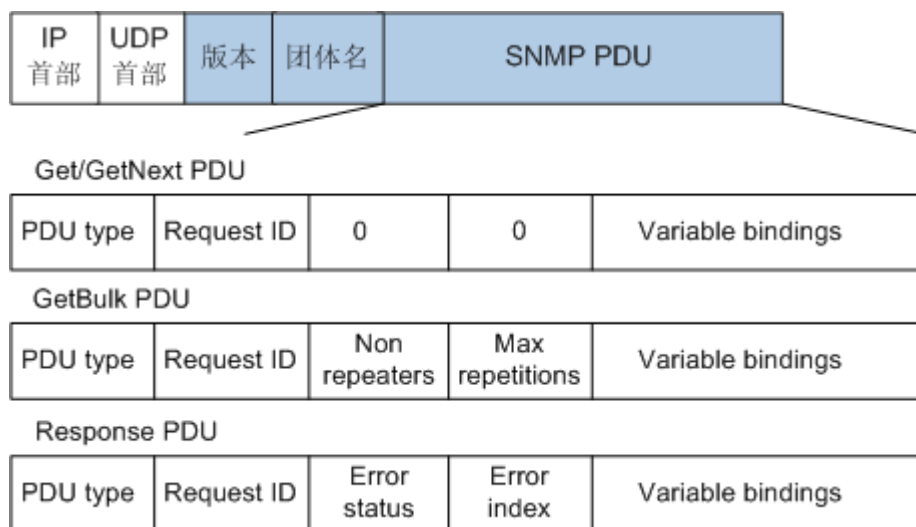


## SNMP 查询操作的报文

SNMPv1和SNMPv2c查询报文格式如图3-2所示。SNMPv1和SNMPv2c的报文主要由版本、团体名、SNMP PDU组成。各类SNMP操作的报文封装在SNMP PDU中。



图 3-2 SNMPv1/SNMPv2c 查询操作报文格式



报文中的主要字段如下：

- 版本：表示SNMP的版本，如果是SNMPv1报文则对应字段值为0，SNMPv2c则为1。
- 团体名：用于在SNMP Agent与NMS之间完成认证，字符串形式，用户可自行定义。团体名包括“read”和“write”两种，执行SNMP查询操作时，采用“read”团体名进行认证；执行SNMP设置操作时，则采用“write”团体名进行认证。
- Request ID：用于匹配请求和响应，SNMP给每个请求分配全局唯一的ID。
- Non repeaters/Max repetitions：GetBulk操作基于GetNext操作实现，相当于多次执行GetNext操作，这两个参数用于设置执行GetNext操作次数。
- Error status：用于表示在处理请求时出现的状况。
- Error index：差错索引。当出现异常情况时，提供变量绑定列表（Variable bindings）中导致异常的变量的信息。
- Variable bindings：变量绑定列表，由变量名和变量值对组成。

通过捕获报文工具获取设备发送的SNMPv2c版本Get请求报文如[图3-3](#)所示，SNMPv2c版本GetNext请求报文如[图3-4](#)所示。SNMPv2c版本GetBulk请求报文如[图3-5](#)所示。

图 3-3 SNMPv2c 版本 Get 请求报文

```

> Frame 106: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
> Ethernet II, Src: 00:ff:5a:77:11:81 (00:ff:5a:77:11:81), Dst: HuaweiTe_9b:59:66 (10:1b:54:9b:59:66)
> Internet Protocol Version 4, Src: 192.168.240.225, Dst: 192.168.33.175
> User Datagram Protocol, Src Port: 51659 (51659), Dst Port: 161 (161)
< Simple Network Management Protocol
  version: v2c (1)
  community: private
  < data: set-request (3)
    < set-request
      request-id: 8
      error-status: noError (0)
      error-index: 0
      < variable-bindings: 1 item
        < 1.3.6.1.2.1.1.5.0: 687561776569
          Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
          < Value (OctetString): 687561776569
            Variable-binding-string: huawei

```

图 3-4 SNMPv2c 版本 GetNext 请求报文

```

> Frame 62: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
> Ethernet II, Src: 00:ff:5a:77:11:81 (00:ff:5a:77:11:81), Dst: HuaweiTe_9b:59:66 (10:1b:54:9b:59:66)
> Internet Protocol Version 4, Src: 192.168.240.225, Dst: 192.168.33.175
> User Datagram Protocol, Src Port: 50073 (50073), Dst Port: 161 (161)
< Simple Network Management Protocol
  version: v2c (1)
  community: public
  < data: get-next-request (1)
    < get-next-request
      request-id: 10
      error-status: noError (0)
      error-index: 0
      < variable-bindings: 1 item
        < 1.3.6.1.2.1.1.4.0: Value (Null)
          Object Name: 1.3.6.1.2.1.1.4.0 (iso.3.6.1.2.1.1.4.0)
          Value (Null)

```

图 3-5 SNMPv2c 版本 GetBulk 请求报文

```

> Frame 362: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
> Ethernet II, Src: 00:ff:5a:77:11:81 (00:ff:5a:77:11:81), Dst: HuaweiTe_9b:59:66 (10:1b:54:9b:59:66)
> Internet Protocol Version 4, Src: 192.168.240.225, Dst: 192.168.33.175
> User Datagram Protocol, Src Port: 62695 (62695), Dst Port: 161 (161)
< Simple Network Management Protocol
  version: v2c (1)
  community: public
  < data: getBulkRequest (5)
    < getBulkRequest
      request-id: 11
      non-repeaters: 0
      max-repetitions: 10
      < variable-bindings: 1 item
        < 1.3.6.1.2.1.1.4.0: Value (Null)
          Object Name: 1.3.6.1.2.1.1.4.0 (iso.3.6.1.2.1.1.4.0)
          Value (Null)

```

SNMPv3查询报文格式如图3-6所示，SNMPv3报文主要由版本、MsgID、MaxSize、Flags、Security Model、Security Parameters、Context EngineID、Context Name和SNMP PDU组成。SNMPv3报文的SNMP PDU的格式与SNMPv2c的一致。SNMPv3版本的报文可以使用鉴权机制，会对Context EngineID、Context Name和SNMP PDU进行加密。

图 3-6 SNMPv3 报文格式

IP 首部	UDP 首部	版本	MsgID	Max Size	Flags	Security Model	Security Parameters	Context EngineID	Context Name	SNMP PDU
----------	-----------	----	-------	-------------	-------	-------------------	------------------------	---------------------	-----------------	----------

报文中的主要字段定义如下：

- 版本：表示SNMP的版本，如果是SNMPv3报文则对应字段值为3。
- MsgID：请求报文的序列号。
- MaxSize：消息发送者所能够容纳的消息最大字节，同时也表明了发送者能够接收到的最大字节数。
- Flags：消息标识位，占一个字节，有三个特征位：reportableFlag，privFlag和authFlag。
  - reportableFlag=1，在能够导致Report PDU生成的情况下，SNMPv3报文接收方必须向发送方发送Report PDU；reportableFlag=0，SNMPv3报文接收方不发送Report PDU。只有在SNMP PDU部分不能被解密时（比如由于密钥错误导致解密失败等）才会用到Report。
  - privFlag=1，对SNMPv3报文进行加密；privFlag=0，不对SNMPv3报文进行加密。
  - authFlag=1，对SNMPv3报文进行鉴权；authFlag=0，不对SNMPv3报文进行鉴权。

除了privFlag=1，authFlag=0的情况外，其他任意组合都可以，所以在配置SNMPv3的安全级别的时候需要注意：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。
- SecurityModel：消息采用的安全模型，发送方和接收方必须采用相同的安全模型。
- SecurityParameters：安全参数，包含SNMP实体引擎的相关信息、用户名、鉴权参数、加密参数等安全信息。
- Context EngineID：SNMP唯一标识符，和PDU类型一起决定应该发往哪个应用程序。
- Context Name：用于确定Context EngineID对被管理设备的MIB视图。

SNMPv3提供了鉴权机制，推荐用户使用SNMPv3版本。通过捕获报文工具获取设备发送的SNMPv3版本加密的Get请求报文如图3-7所示，SNMPv3版本不加密的Get请求报文如图3-8所示。

图 3-7 SNMPv3 版本加密的 Get 请求报文

```

> Frame 114: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0
> Ethernet II, Src: 00:ff:5a:77:11:81 (00:ff:5a:77:11:81), Dst: HuaweiTe_9b:59:66 (10:1b:54:9b:59:66)
> Internet Protocol Version 4, Src: 192.168.240.225, Dst: 192.168.33.175
> User Datagram Protocol, Src Port: 55372 (55372), Dst Port: 161 (161)
< Simple Network Management Protocol
  msgVersion: snmpv3 (3)
  > msgGlobalData
  > msgAuthoritativeEngineID: 800007db034857029a8eed
  msgAuthoritativeEngineBoots: 38
  msgAuthoritativeEngineTime: 12281
  msgUserName: user1
  msgAuthenticationParameters: 6d097a7de96e7f9bb09170de
  msgPrivacyParameters: 000000c800000021
  < msgData: encryptedPDU (1)
    encryptedPDU: 49b25d4847208f3eb30b9a481e7d971bcc3f778449293d88...

```

图 3-8 SNMPv3 版本不加密 Get 请求报文

```

> Frame 112: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
> Ethernet II, Src: 00:ff:5a:77:11:81 (00:ff:5a:77:11:81), Dst: HuaweiTe_9b:59:66 (10:1b:54:9b:59:66)
> Internet Protocol Version 4, Src: 192.191.240.225, Dst: 192.91.33.175
> User Datagram Protocol, Src Port: 55372 (55372), Dst Port: 161 (161)
< Simple Network Management Protocol
  msgVersion: snmpv3 (3)
  > msgGlobalData
  msgAuthoritativeEngineID: <MISSING>
  msgAuthoritativeEngineBoots: 0
  msgAuthoritativeEngineTime: 0
  msgUserName:
  msgAuthenticationParameters: <MISSING>
  msgPrivacyParameters: <MISSING>
  < msgData: plaintext (0)
    plaintext
      contextEngineID: <MISSING>
      contextName:
      < data: get-request (0)
        get-request
          request-id: 15
          error-status: noError (0)
          error-index: 0
          variable-bindings: 0 items

```

## SNMP 查询操作的工作原理

不同版本的SNMP查询操作的工作原理基本一致，唯一的区别是SNMPv3版本增加了身份验证和加密处理。下面以SNMPv2c版本的Get操作为例介绍SNMP查询操作的工作原理。

假定NMS想要获取被管理设备MIB节点sysContact的值，使用可读团体名为public，过程如下所示：

1. NMS：向SNMP Agent发送Get请求报文。报文中各字段的设置如下：版本号所使用的SNMP版本；团体名为public；PDU中PDU类型为Get类型，绑定变量填入MIB节点名sysContact。
2. SNMP Agent：首先对报文中携带版本号和团体名进行认证，认证成功后，SNMP Agent根据请求查询MIB中的sysContact节点，得到sysContact的值并将其封装到

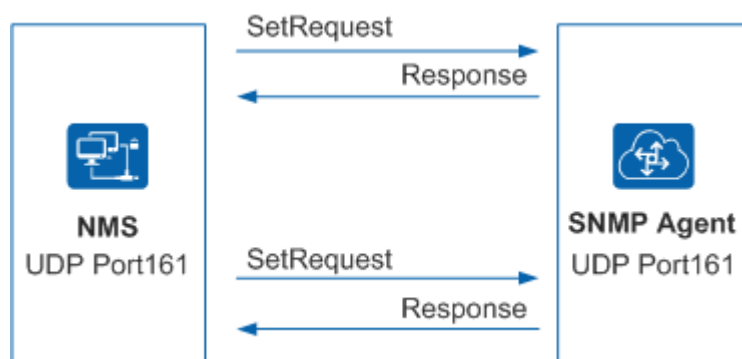
Response报文中的PDU，向NMS发送响应；如果查询不成功，SNMP Agent会向NMS发送出错响应。

# 4 SNMP 设置

SNMP设置是指NMS主动向SNMP Agent发送对设备进行Set操作请求，如图4-1所示。SNMP Agent接收到Set请求后，通过MIB表完成相应指令，并将结果反馈给NMS。

SNMP设置操作只有一种Set，NMS使用该操作可设置SNMP Agent中的一个或多个参数值。

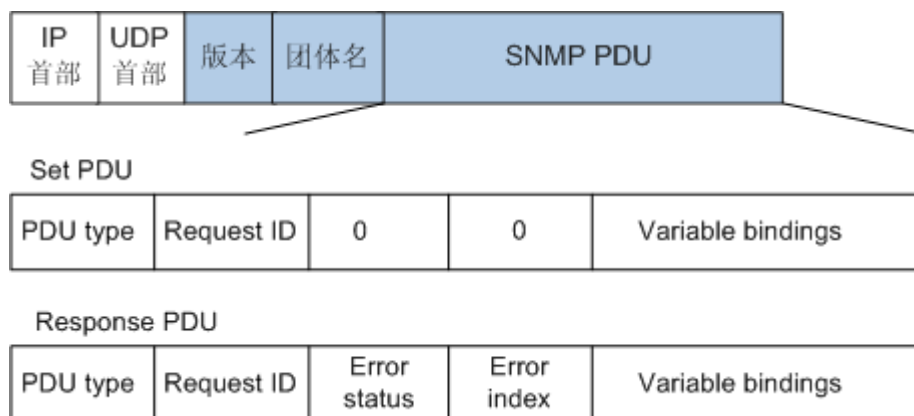
图 4-1 SNMP Set 操作



## SNMP Set 操作的报文

SNMPv1和SNMPv2c的Set操作报文格式如图4-2所示。一般情况下，SNMPv3的Set操作信息是经过加密封装在SNMP PDU中，其格式与SNMPv2c的Set操作报文格式一致。

图 4-2 SNMPv1/SNMPv2c Set 操作报文格式



报文中主要字段的含义如下：

- Request ID：用于匹配请求和响应，SNMP给每个请求分配全局唯一的ID。
- Error status：用于表示在处理请求时出现的状况。
- Error index：差错索引。当出现异常情况时，提供变量绑定列表（Variable bindings）中导致异常的变量的信息。
- Variable bindings：变量绑定列表，由变量名和变量值对组成。

通过捕获报文工具获取设备发送的SNMPv2c版本Set请求报文如图4-3所示。

图 4-3 SNMPv2c 版本 Set 请求报文

```

> Frame 106: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
> Ethernet II, Src: 00:ff:5a:77:11:81 (00:ff:5a:77:11:81), Dst: HuaweiTe_9b:59:66 (10:1b:54:9b:59:66)
> Internet Protocol Version 4, Src: 192.168.240.225, Dst: 192.168.33.175
> User Datagram Protocol, Src Port: 51659 (51659), Dst Port: 161 (161)
+ Simple Network Management Protocol
  version: v2c (1)
  community: private
  + data: set-request (3)
    + set-request
      request-id: 8
      error-status: noError (0)
      error-index: 0
    + variable-bindings: 1 item
      + 1.3.6.1.2.1.1.5.0: 687561776569
        Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
        + Value (OctetString): 687561776569
          Variable-binding-string: huawei
  
```

## SNMP Set 操作的工作原理

不同版本的SNMP Set操作的工作原理基本一致，唯一的区别是SNMPv3版本增加了身份验证和加密处理。下面以SNMPv3版本的Set操作为例介绍SNMP Set操作的工作原理。

假定NMS想要设置被管理设备MIB节点sysName的值为HUAWEI，过程如下所示：

1. NMS：向Agent发送不带安全参数的Set请求报文，向SNMP Agent获取Context EngineID、Context Name和安全参数（SNMP实体引擎的相关信息）。
2. SNMP Agent：响应NMS的请求，并向NMS反馈请求的参数。

3. NMS: 再次向SNMP Agent发送Set请求, 报文中各字段的设置如下:
  - 版本: SNMPv3
  - 报文头数据: 指明采用鉴权、加密方式。
  - 安全参数: NMS通过配置的算法计算出鉴权参数和加密参数。将这些参数和获取的安全参数填入相应字段。
  - PDU: 将获取的Context EngineID和Context Name填入相应字段, PDU类型设置为Set, 绑定变量填入MIB节点名sysName和需要设置的值HUAWEI, 并使用已配置的加密算法对PDU进行加密。
4. SNMP Agent: 首先对报文中携带版本号和团体名进行认证, 认证成功后, SNMP Agent根据请求设置管理变量在管理信息库MIB中对应的节点, 设置成功后向NMS发送响应; 如果设置不成功, Agent会向NMS发送出错响应。

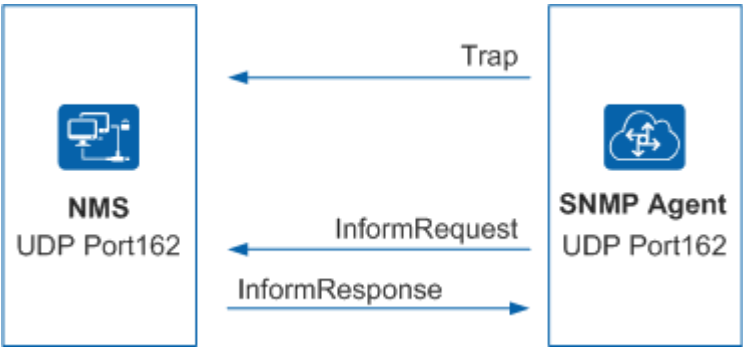


# 5 SNMP Traps

SNMP Traps是指SNMP Agent主动将设备产生的告警或事件上报给NMS，以便网络管理员及时了解设备当前运行的状态。

SNMP Agent上报SNMP Traps有两种方式：Trap和Inform。SNMPv1版本不支持Inform。Trap和Inform的区别在于，SNMP Agent通过Inform向NMS发送告警或事件后，NMS需要回复InformResponse进行确认，如图5-1所示。

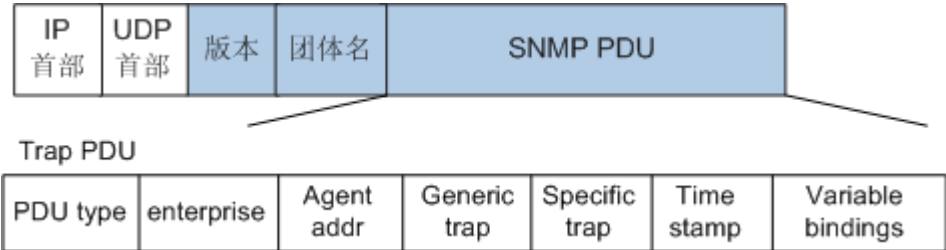
图 5-1 SNMP Traps 操作



## SNMP Traps 报文格式

SNMPv1的Trap操作报文格式如图5-2所示，Trap PDU由PDU type、enterprise、Agent addr、Generic trap、Specific trap、Time stamp和Variable bindings组成。

图 5-2 SNMPv1 版本 Trap 操作报文格式

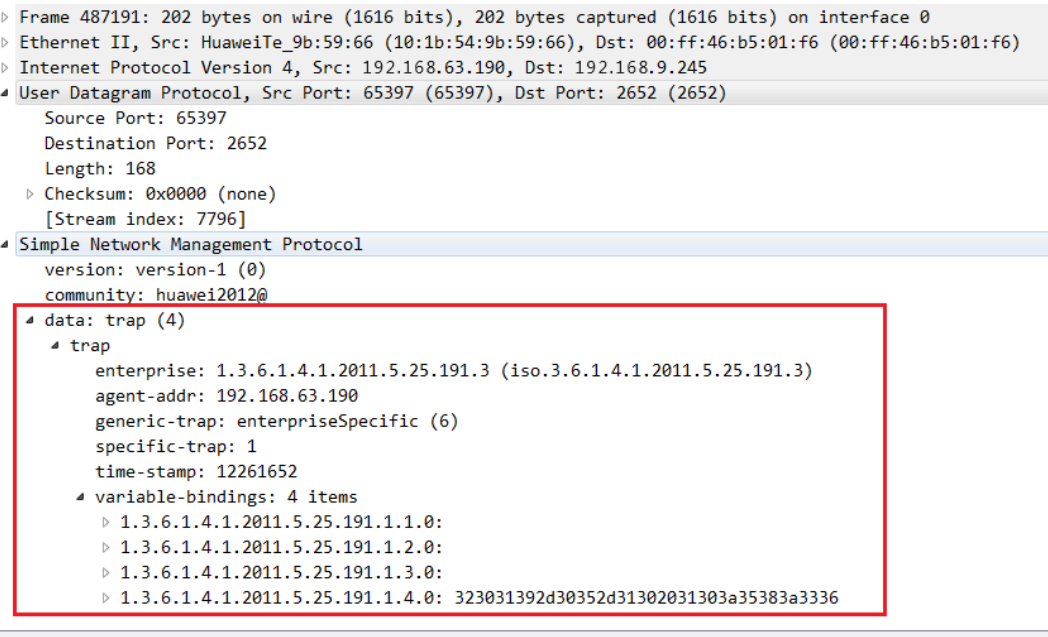


报文中的主要字段定义如下：

- enterprise：Trap源（生成Trap的设备）的类型。
- Agent addr：Trap源的地址。
- Generic trap：通用Trap类型，包括coldStart、warmStart、linkDown、linkUp、authenticationFailure、egpNeighborLoss、enterpriseSpecific。
- Specific trap：企业私有Trap信息。
- Time stamp：上次重新初始化网络实体和产生Trap之间所持续的时间。
- Variable bindings：变量绑定列表，由变量名和变量值对组成。

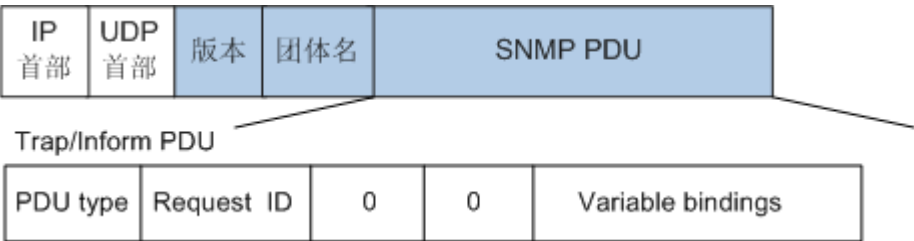
通过捕获报文工具获取设备发送的SNMPv1版本Trap报文如图5-3所示。

图 5-3 SNMPv1 版本 Trap 报文



SNMPv2c的Trap操作的报文格式和Inform操作的报文格式如图5-4所示。一般情况下，SNMPv3的Trap操作或inform操作是经过加密封装在SNMP PDU中，其格式与SNMPv2c的Trap操作或inform操作的报文格式一致。

图 5-4 SNMPv2 版本 Trap/Inform 操作报文格式



报文中的主要字段定义如下：

- Request ID：用于匹配请求和响应，SNMP给每个请求分配全局唯一的ID。
- Variable bindings：变量绑定列表，由变量名和变量值对组成。

通过捕获报文工具获取设备发送的SNMPv2版本Trap报文如图5-5所示，SNMPv2版本Inform报文如图5-6所示。

图 5-5 SNMPv2 版本 Trap 报文

```

> Frame 79294: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits) on interface 0
> Ethernet II, Src: HuaweiTe_9b:59:66 (10:1b:54:9b:59:66), Dst: 00:ff:46:b5:01:f6 (00:ff:46:b5:01:f6)
> Internet Protocol Version 4, Src: 192.168.63.190, Dst: 192.168.9.245
  < User Datagram Protocol, Src Port: 65397 (65397), Dst Port: 2652 (2652)
    Source Port: 65397
    Destination Port: 2652
    Length: 193
    < Checksum: 0x0000 (none)
    [Stream index: 7796]
  < Simple Network Management Protocol
    version: v2c (1)
    community: huawei2012@
    < data: snmpV2-trap (7)
      < snmpV2-trap
        request-id: 31
        error-status: noError (0)
        error-index: 0
        < variable-bindings: 6 items
          > 1.3.6.1.2.1.1.3.0: 10610599
          > 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.4.1.2011.5.25.191.3.1 (iso.3.6.1.4.1.2011.5.25.191.3.1)
          > 1.3.6.1.4.1.2011.5.25.191.1.1.0:
          > 1.3.6.1.4.1.2011.5.25.191.1.2.0:
          > 1.3.6.1.4.1.2011.5.25.191.1.3.0:
          > 1.3.6.1.4.1.2011.5.25.191.1.4.0: 323031392d30352d31302031303a35383a3336

```

图 5-6 SNMPv2 版本 Inform 报文

```

> Frame 239: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits) on interface 0
> Ethernet II, Src: HuaweiTe_9b:59:66 (10:1b:54:9b:59:66), Dst: 00:ff:46:b5:01:f6 (00:ff:46:b5:01:f6)
> Internet Protocol Version 4, Src: 192.168.63.190, Dst: 192.168.8.153
> User Datagram Protocol, Src Port: 65397 (65397), Dst Port: 2652 (2652)
  < Simple Network Management Protocol
    version: v2c (1)
    community: huawei2012
    < data: informRequest (6)
      < informRequest
        request-id: 262
        error-status: noError (0)
        error-index: 0
        < variable-bindings: 6 items
          > 1.3.6.1.2.1.1.3.0: 21913168
          > 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.4.1.2011.5.25.191.3.1 (iso.3.6.1.4.1.2011.5.25.191.3.1)
          > 1.3.6.1.4.1.2011.5.25.191.1.1.0:
          > 1.3.6.1.4.1.2011.5.25.191.1.2.0:
          > 1.3.6.1.4.1.2011.5.25.191.1.3.0:
          > 1.3.6.1.4.1.2011.5.25.191.1.4.0: 323031392d30352d31302031303a35383a3336

```

## SNMP Traps 工作原理

### Trap操作工作原理

Trap不属于NMS对被管理设备的基本操作，它是被管理设备的自发行为。当被管理设备达到告警的触发条件时，会通过SNMP Agent向NMS发送Trap消息，告知设备侧出现的异常情况，便于网络管理人员及时处理。例如被管理设备热启动后，SNMP Agent会向NMS发送warmStart的Trap。

这种Trap信息是受限制的。只有在设备端的模块达到模块预定义的告警触发条件时，SNMP Agent才会向管理进程报告。这种方法的好处是仅在严重事件发生时才发送Trap信息，减少报文交互产生的流量。

### Inform操作工作原理

Inform操作也是被管理设备向NMS主动发送告警。与Trap告警不同的是，被管理设备发送Inform告警后，需要NMS进行接收确认。如果被管理设备没有收到确认信息则：

1. 将告警或事件暂时保存在Inform缓存中。
2. 重复发送该告警或事件，直到NMS确认收到该告警或者发送次数达到最大重传次数。
3. 被管设备上会生成相应的告警或事件日志。

由此可知，使用Inform操作会占用较多的系统资源。

# 6 SNMP 端口号

---

SNMP报文是普通的UDP报文，协议中规定有两个默认端口号：

- 端口号161：NMS发送Get、GetNext、GetBulk和Set操作请求以及SNMP Agent响应这些请求操作时，使用该端口号。  
该端口号支持用户配置，但是需要保证NMS发送请求报文使用的端口号与SNMP Agent响应请求报文使用的端口号要一致。
- 端口号162：SNMP Agent向NMS发送Trap或Inform时，使用该端口号。  
该端口号支持用户配置，但是需要保证SNMP Agent发送Trap或Inform的端口号与NMS监听Trap或Inform的端口号要一致。

# 7 使用 SNMP 的相关信息

---

如果您想了解如何配置或使用SNMP，可参考以下产品文档：

S12700 V200R013C00 配置指南-网络管理与监控中的[SNMP章节](#)

CloudEngine 12800, 12800E V200R005C10 配置指南-网络管理与监控中的[SNMP章节](#)

无线接入控制器(AC和FITAP) V200R010C00 配置指南(命令行)-网络管理与监控配置中的[SNMP章节](#)

HUAWEI USG6000, USG9500, NGFW Module V500R005C00 产品文档-管理员指南-系统中的[SNMP章节](#)

AR100, AR120, AR150, AR160, AR200, AR1200, AR2200, AR3200, AR3600 V200R010 产品文档 配置指南（命令行）-网络管理与监控配置指南中的[SNMP章节](#)

NE20E-S V8R10C10SPC500 产品文档-配置-系统管理中的[SNMP章节](#)

NE40E V8R10C10SPC500 产品文档-配置-系统管理中的[SNMP章节](#)