

文章编号:1006-7329(2000)01-0033-06

基于 SNMP 的 TCP/IP 网络管理

姚家宁

(重庆建筑大学 网络中心, 重庆 400045)

33-38

TF393

摘要:对基于 TCP/IP 互联网的网络管理协议 SNMP 进行了深入的讨论。提出了基于 SNMP 的网络管理系统开发的一些问题。

关键词:网络管理; TCP/IP; SNMP; SMI; MIB

中图分类号:TP393.04

文献标识码:A

1 概述

ISO(国际标准化组织)定义了网络管理的五个功能域:失效管理、配置管理、安全管理、性能管理和计费管理。这些功能的实现的基础是对网络中的设备(路由器、交换机、主机)进行监视和控制。在互联网中,特别是对路由器的监视和控制。

1988年,IAB(Internet Activities Board——互联网活动委员会)建议所有IP和TCP的运行应该都是可网络管理的(network manageable)。提出了采用两个步骤开发基于TCP/IP互联网的网络管理协议:近期内采用SNMP(Simple Network Management Protocol),远期采用OSI网络管理体系。同时产生了与SNMP和OSI网络管理体系都兼容的管理信息结构(SMI)和管理信息库(MIB)。由于SNMP和OSI网络管理体系的要求不同,SMI/MIB与两者的兼容性无法满足。IAB让IETF(Internet Engineering Task Force——互联网工程任务组)在网络管理领域建立两个工作组:一个组负责定义基于TCP/IP的互联网的管理信息结构和标识SMI(RFC1155),基于TCP/IP的互联网的管理信息库MIB(RFC1156);SNMP工作组产生了文件:简单网络管理协议SNMP(RFC1157)。

IAB推荐SNMP(Simple Network Management Protocol)作为基于TCP/IP的互联网网络管理的标准协议。这个协议相当成功,在很短的时间内被众多网络设备制造商所使用。目前,已发展到第二代(SNMPv2),改进了第一代SNMP缺乏安全性和网络监视困难的缺点。

现在,TCP/IP互联网上的各种设备均支持SNMP协议,设备中都配置了SNMP管理代理和管理信息库MIB,这为开发专用或通用的基于SNMP的网络管理系统提供了极大的方便。

2 SNMP 基本工作原理

SNMP协议是通过对监视网关(OSI第三层路由器)的SGMP(网关监视协议)进行改造发展起来的。SNMP使用了按管理信息结构(SMI)规则构造的管理信息库(MIB)所提供的一组最少的,但功能强大的管理信息来监视/控制网络设备。

SNMP采用客户/服务器方式,通过在管理设备中的SNMP客户和被管理设备中的SNMP服务器(Management Agent——管理代理)之间用标准消息通信存/取被管理设备中的管理信息来达到监视/控制的目的。

收稿日期:1999-03-01

作者简介:姚家宁(1945-),男,湖南长沙市人,副教授,主要从事计算机网络技术研究。

被管理设备中有一组按 SMI 规则定义的管理信息和一个 SNMP 管理代理,管理设备中的 SNMP 客户向被管理设备中的管理代理发送 SNMP 消息。SNMP 使用 UDP 作为传输层协议,每一个消息是一个独立的 UDP 包。SNMP 使用五种消息类型:

- 1) Get-Request
- 2) Get-Response
- 3) Get-Next-Request
- 4) Set-Request
- 5) Trap

前四种消息使用 UDP 端口 161,最后一种消息使用 UDP 端口 162。

管理者使用 Get-Request 消息和 Get-Next-Request 消息向管理代理请求读取管理信息。管理代理则用 Get-Response 消息响应管理者的请求,返回相应的管理信息,达到监视网络设置状态的目的。管理者还可使用 Set-Request 消息向管理代理请求设备管理信息,管理代理根据设置管理信息来改变网络设备状态,达到控制的目的。Trap 消息则是在被管理设备发生某些事件时由管理代理主动发送的。

3 管理信息库 MIB

管理信息库 MIB(Management Information Base)使用层次结构化形式,定义了通过网络管理协议可以获得的网络管理信息。RFC1155 描述了基于 TCP/IP 的互联网中的管理信息的结构和标识(SMI)。按照这个规则,RFC1156 给出了用于 TCP/IP 协议簇的第一个 MIB 版本,RFC1158 又给出了用于 TCP/IP 协议簇的第二个 MIB 版本 MIB-II。

被管理设备中必须保存一组管理者可以存/取的管理信息。MIB 定义了这些数据项和对每个数据项可以进行的操作。用于 TCP/IP 的 MIB 把这些数据项分为八类:

- system 包含被管理设备操作系统的信息
- interfaces 包含被管理设备各个网络接口的信息
- addr.trans. 包含地址转换的信息
- ip 包含 IP 协议软件的信息
- icmp 包含 ICMP 协议软件的信息
- tcp 包含 TCP 协议软件的信息
- udp 包含 UDP 协议软件的信息
- egp 包含 EGP 协议软件的信息

每个数据项的标识符包含了类别的代码。如:ipRoutingTable(ip 类)。这些定义仅仅是逻辑定义,它与网络管理协议是无关的,同时与被管理设备中的内部数据结构也可能不同,甚至被管理设备中可以没有相应的常规变量。当查询消息到达被管理设备时,由管理代理负责在 MIB 变量和设备中的内部数据结构之间进行转换,或者用其它常规变量计算出相应的 MIB 变量。

这些管理信息按一组 SMI 规则来识别和组织。SMI 使用一种形式语言——ASN.1(Abstract Syntax Notation 1——抽象语法记法 1)来定义这些信息的命名规则和变量类型以及表格值的结构。

MIB 变量使用的名字来自于层次结构的对象标识符名字空间。对象标识符名字空间可对所有可能的对象命名,它构造的名字在全世界是唯一的。对象标识符名字空间是一棵树,对象是树中的结点,树中每个结点分配了一个字符串和一个小整数作为标号,对象的名字就是从根到对象结点的路径上各个结点的标号的序列,标号之间用点分隔。如:MIB 变量 ipInReceives 的名字为

iso.org.dod.internet.mgmt.mib.ip.ipInReceives

它的数字表示为

1.3.6.1.2.1.4.3

名字的数字表示用于消息报文中表示该变量。所有用于 TCP/IP 协议簇的 MIB 变量的名字都在以结点 `mib` 为根的子树下, 因此, 它们的名字都有前缀

```
iso.org.dod.internet.mgmt.mib(1.3.6.1.2.1)
```

对于含表格值的 MIB 变量, SMI 定义了这些信息的命名规则和变量类型以及表格值的结构。比如, MIB 变量 `ipAddrTable` 的名字为

```
iso.org.dod.internet.mgmt.mib.ip.ipAddrTable
```

它的数字表示为

```
1.3.6.1.2.1.4.20
```

这个变量含有被管理设备中每个网络接口的 IP 地址列表。使用 ASN.1 记法, MIB 变量 `ipAddrTable` 定义为:

```
ipAddrTable ::= SEQUENCE OF ipAddrEntry
```

```
ipAddrEntry ::= SEQUENCE {
    ipAdEntry
        ipAddress,
    ipAdEntindex
        INTEGER,
    ipAdEntNetMask
        ipAddress,
    ipAdEntBcastAddr
        ipAddress,
    ipAdEntReasmMaxSize
        INTEGER(0..65535)
}
```

再为 `ipAddrEntry` 和 `ipAddrEntry` 序列中的每一项指定数值。如:

```
ipAddrEntry{ipAddrTable 1}
ipAdEntNetMask {ipAddrEntry 3}
```

那末, IP 地址表中, 地址为 202.202.69.33 的网络掩码字段的名为:

```
iso.org.dod.internet.mgmt.mib.ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask.202.202.69.33
```

它的数字表示为:

```
1.3.6.1.2.1.4.20.1.3.202.202.69.33
```

4 SNMP 消息报文

SNMP 消息使用 UDP 传输层协议传输。SNMP 消息用 ASN.1 定义为:

```
SNMP - Message ::=
    SEQUENCE {
        version INTEGER{
            version - 1(0)
        },
        community
            OCTET STRING,
        data
```

```

        ANY
    }

```

SNMP 消息分为三个部分:版本号、团体标识和协议数据单元(PDU)。RFC1157 的版本号为 1,团体标识可以作为 SNMP 消息的口令,缺省值为“public”。PDU 则定义为:

```

PDUs ::=
    CHOICE{
        get-request
            Getrequest-PDU
        get-next-request
            GetNextRequest-PDU
        get-response
            Getresponse-PDU
        set-request
            Setrequest-PDU
        trap
            Trap-PDU
    }

```

协议数据单元(PDU)有五种,分别为 Getrequest-PDU、GetNextRequest-PDU、Getresponse-PDU、Setrequest-PDU 和 Trap-PDU。

例如 Getrequest-PDU 定义为:

```

GetRequest-PDU ::= [0]
    IMPLICIT SEQUENCE{
        Request-id
            requestID,
        error-status,
            ErrorStatus,
        error-index,
            ErrorIndex,
        variable-bindings
            VarBildList
    }

```

PDU 则按消息的类型分为二种格式,第一种格式 PDU 用于前四类消息类型,第二类格式 PDU 用于 Trap 消息类型。第一种格式 PDU 分为五部分:PDU 类型、请求 id、错误状态、错误索引和变量表。PDU 类型为 0——Get-Request, 1——Get-Next-Request, 2——Get-Response, 3——Set-Request; 请求 id 是四个字节的整数,用来区分每一个请求,以便使响应消息和请求消息匹配。错误状态是一个字节的整数,用来表示发生错误,取值为 0——NoError, 1——Toobig, 2——NoSuchName, 3——BadValue, 4——ReadOnly, 5——Generr 等。错误索引是一个字节的整数,用来指出变量表中哪一个变量引起了错误。变量表为一系列变量名和相应值组成的序偶的序列。当 PDU 为 GET 时错误状态和错误索引均为 0,变量表中的值部分为 null。第二种格式 PDU 分为七部分:PDU 类型、陷阱对象的类型、陷阱对象的地址、陷阱类型、陷阱性质和变量表。其中,PDU 类型和变量表部分与第一种格式 PDU 相同。

5 SNMP 消息的 ASN.1 编码格式

SNMP 消息是用 ASN.1 编码格式编码的。例如：用于 MIB 变量 sysDescr(数字表示为 1.3.6.1.2.1.1.1) 的 Get-Request 消息的 ASN.1 编码为：

```

    30          29          02          01          00
SEQUENCE      len = 41    INTEGER      len = 1    vers = 0
    40          06          70          75          62          6C          69          63
    string      len = 6    p          u          b          l          i          c
    A0          IC          02          04          05          AE          56          02
getrequest    len = 28    INTEGER      len = 4    —request ID—
    02          01          00          02          01          00
INTEGER      len = 1    status      INTEGER      len = 1    error index
    30          0E          30          0C          06          08
SEQUENCE      len = 14    SEQUENCE      len = 12    objectid    len = 8
    2B          06          01          02          01          01          01          00          05          00
    1.3 . 6 . 1 . 2 . 1 . 1 . 1 . 0    null len = 0
  
```

6 SNMP 消息的传输和接收的过程

SNMP 消息的传输过程：首先构造 PDU，把这个 PDU 和源、目的地址、团体标识传递给一个认证服务，认证服务进行所需要的格式转换（比如加密），但认证服务并不是必需的，然后构造一个消息，使用基本的编码规则编码，传递给传输服务。

SNMP 消息的接收过程：首先对消息进行句法分析，如果没有通过就放弃这个消息，再检查版本号，如果匹配错误也放弃这个消息，然后将源、目的地址、团体标识传递给一个认证服务，认证服务则返回一个信号，它将产生一个陷阱 (TRAP) 并放弃这个消息，认证成功则返回一个 PDU，最后，对该 PDU 进行句法分析，分析失败，放弃这个消息，否则按合适的访问策略进行相应的处理，同样，认证服务是不必需的。

7 结 论

SNMP 是一种简单的网络管理协议，它简单、灵活、功能强大、易于实现和调试。目前，几乎所有的网络设备都支持 SNMP，因此，基于 SNMP 的网络管理系统的开发是非常需要的。基于 SNMP 的网络管理系统的开发关键在 SNMP 客户软件的开发。在开发 SNMP 客户软件时要注意下列问题：

- 1) 在开发 SNMP 客户软件之前，要核实被管理设备是否支持 SNMP，即被管理设备中是否有 SNMP 管理代理和管理信息库 MIB。另外，还必须确认被管理设备中的团体标识 (community)。
- 2) SNMP 客户软件的传输层协议要使用 UDP，Getrequest 消息、GetNextRequest 消息和 Setrequest 消息发送到对方 UDP 端口 161，Getresponse 消息使用 UDP 端口 161 接收，Trap 消息使用 UDP 端口 162 接收。
- 3) 由于 UDP 协议是无连接的，因此 SNMP 客户软件必需设置定时器和超时重发机制，以保证可靠性。在收到响应消息后还必需对消息中的请求 id 和请求消息中的请求 id 相比较，以验证该响应消息是对请求消息的响应。
- 4) 消息是按 ASN.1 编码格式编码的，SNMP 客户软件必需对 ASN.1 编码格式和内部表示形式

之间进行转换。在发送请求消息时,按 ASN.1 编码格式编码。在响应消息到达时,先按 ASN.1 编码格式分析该响应消息,再将 ASN.1 编码格式转换为内部表示形式。

参考文献:

- [1] Case, J., M. Fedor, M. Schoffstall, and J. Davin, "A Simple Network Management Protocol(SNMP)", RFC 1157, Performance Systems International and Hughes LAN Systems, [EB/OL] May 1990
- [2] Rose, M., and K. McCloghrie, "Structure and Identification of Management Information for TOP/IP - based Internets", RFC 1155, Performance Systems International and Hughes LAN Systems, [EB/OL] May 1990
- [3] McCloghrie, K., and M. Rose, "Management Information Base for Network Management of TCP/IP - based Internets", RFC1156, Hughes LAN Systems and Performance Systems International, [EB/OL] May 1990
- [4] Information processing system - Open Systems Interconnection, "Specification of Abstract Syntax Notation One(ASN.1)", International Organization for Standardization, International Standard 8824, [EB/OL] December 1987
- [5] Information processing system - Open Systems Interconnection, "Specification of Basic Encoding Rules for Abstract Syntax Notation One(ASN.1)", International Organization for Standardization, International Standard 8825, [EB/OL] December 1987
- [6] Postel, J., "User Datagram Protocol", RFC 768, USC/Information Sciences Institute, [EB/OL] November 1980

Network Management of TCP/IP - based SNMP

YAO Jia-ning

(Network Center, Chongqing Jianzhu University, Chongqing 400045, China)

Abstract: This paper discusses thoroughly SNMP for TCP/IP - based Internet and the problems of developing the network management system.

Keywords: network management; TCP/IP; SNMP; SMI; MIB