ICS 33 040
M 11

YD

中华人民共和国通信行业标准

YD/T 1611.2-2007

IP 网络管理接口技术要求 第 2 部分：支持 IPv6 的设备接口功能与协议

Technical Requirements for Management Interface of IP Network

Part 2: Function and Protocol of IPv6 Equipment Management Interface

2007-04-16 发布　　2007-10-01 实施

中华人民共和国信息产业部　发布

目　　次

前　言

《IP网络管理接口技术要求》分为三个部分：

—第1部分：总则

—第2部分：支持IPv6的设备接口功能与协议

—第3部分：宽带接入服务器（BAS）

本部分为第 2 部分。

本部分参考了以下标准：

ITU-T M.3010（2000）	电信管理网原理
IETF RFC3413	SNMP应用，2002
IETF RFC 1902-1908	SNMP v2c
IETF RFC 3410-3414	SNMP v3
IETF RFC2575	SNMP的基于观点的接入控制模型1999
IETF RFC3164	BSD SYSLOG协议，2001
IETF RFC3917	IPFIX要求，2004
IETF RFC3955	IPFIX候选协议评估，2004

并结合IPv6网络设备管理接口的特性编写而成，与上述国际标准间的关系为非等效。

本部分附录 A 为规范性附录。

附录 B、附录 C 为资料性附录。

本部分由中国通信标准化协会提出并归口。

本部分起草单位：中国移动通信集团公司

京移通信设计院有限公司

华为技术有限公司

中兴通讯股份有限公司

本部分主要起草人：冯瑞军　刘　涛　张　晨　薛　晶　蒋　勇

IP网络管理接口技术要求
第2部分：支持IPv6的设备接口功能与协议

1 范围

本部分规定了对支持IPv6技术的设备进行管理所需的网络管理接口的定义和接口位置，规定了网络管理接口的功能要求、性能要求、管理接口的信息模型和所采用的接口协议。

本部分适用于支持IPv6技术网络的网管接口。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分。然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

ITU-T M.3010（2000）	电信管理网原理
IETF RFC3413	SNMP应用，2002
IETF RFC 1902-1908	SNMP v2c
IETF RFC 3410-3414	SNMP v3
IETF RFC2575	SNMP的基于观点的接入控制模型 1999
IETF RFC3164	BSD SYSLOG协议，2001
IETF RFC3917	IPFIX要求，2004
IETF RFC3955	IPFIX候选协议评估，2004

3 术语、定义和缩略语

下列术语、定义和缩略语适用于本标准。

3.1 术语和定义

3.1.1 IPv6 设备

支持IPv6技术的设备，其范围包括支持IPv6协议栈的设备和同时支持IPv4和IPv6的双栈设备。

3.2 缩略语

下列缩略语适用于本部分。

ASN.1	Abstract Syntax Notation 1	抽象语法表示 1
IETF	Internet Engineering Task Force	互联网工程任务组
IP	Internet Protocol	互联网协议
IPFIX	IP Flow Information Export	IP 流信息输出
NMS	Network Management System	网络管理系统
OMC	Operation & Maitenance Centor	操作维护中心
SNMP	Simple Network Management Protocol	简单网络管理协议
SCTP	Stream Control Transmission Protocol	流控制传输协议

4 IP 网络设备管理概述

IPv6设备构成的网络应提供网络管理接口，以便网络管理系统（NMS）对该网络进行管理。

4.1 网管接口位置

如图1所示，IPv6设备构成的网络的网管接口的物理位置可能有以下两种情况。本部分不对其进行区分，规范的相关内容同时适用于这两种情况。

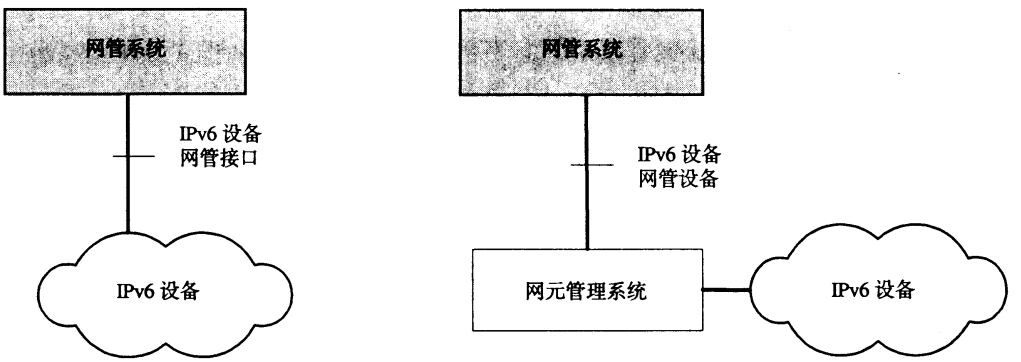


图1 网络管理接口位置

对图1的说明如下：

1）图1（a）所示，本部分定义的网络管理接口的实际物理位置位于网管系统与IPv6设备之间，由设备直接向网管设备提供网管接口；

2）图1（b）所示，本部分定义的网络管理接口的实际物理位置位于网管系统与网元管理系统之间，由网元管理系统向网管系统提供网管接口，网元管理系统与IPv6设备之间的接口定义不在本规范的范围之内。

4.2 IPv6 设备范围

本部分规定的需要通过IP6设备网管接口管理的设备包括：

1）IPv6 路由器，包括核心路由器、边缘路由器；

2）IPv6 以太网交换机；

3）IPv4/IPv6 协议转换网关；

4）防火墙。

5 网络管理接口功能要求

IPv6设备应支持网管系统通过网管接口实现对设备的管理，网管接口的功能包括配置管理、性能管理、告警管理、流量管理、日志管理、安全管理和集中操作维护等功能（通用功能）。网管接口功能除满足本系列标准《IP网络管理技术要求 第1部分 总则》中相关规定前提下，应支持以下功能。

5.1 配置管理

应能通过网管接口实现以下配置管理功能：

1）通过网管接口获取或改变设备的详细配置信息，包括设备系统配置信息、设备接口配置信息；

2）管理设备上的协议，配置相关的协议参数：

a） IPv6路由器，包括网络层协议、传输层协议、路由协议和MPLS协议；

b） IPv6以太网交换机，包括网络层协议、传输层协议和路由协议。

3）根据业务的需要，配置业务参数

a）IPv6路由器，包括VPN业务、MPLS业务所需配置和获取的信息。

5.2 告警管理

应能通过网管接口向网管系统实时主动上报设备中定义的告警事件，事件中应至少应包含的内容见5.2.3节。

应能通过网络管理接口实时主动上报经过告警过滤设定的告警事件，告警过滤包括告警时间、告警级别、告警类型、告警原因和告警源等条件。

5.2.1 通用告警管理

网络中的设备可以通过网管接口发送关于系统和链路状态的通用告警。

NMS可以通过网管接口接收来自被管资源的各种告警，所有的被管资源都应支持通用告警类型。各种设备可以通过网管接口发送的关于系统和链路状态的告警类型见表1。

通用通知类型

中文名称	英文名称	说　明
系统冷启动	coldStart	当代理检测到系统冷启动时，向管理站发送 coldStart 告警
系统热启动	warmStart	当代理检测到系统热启动时，向管理站发送 warmStart 告警
连接中断	linkDown	当代理检测到某条链路的 ifOperStatus 将要从其他状态（除 notPresent 外）进入 down 状态，将会触发链路中断 Trap，该其他状态由 ifOperStatus 表示
连接建立	linkUp	当代理检测到某条链路的 ifOperStatus 将要从 down 状态进入其他状态（除 notPresent 外），将会触发链路建立 Trap，该其他状态由 ifOperStatus 表示
认证失败	authenticationFailure	当代理检测到认证失败事件发生时，向管理站发送 authenticationFailure，该陷阱可以由网管系统配置 snmpEnableAuthenTraps 来决定代理是否产生该告警

5.2.2 特定告警管理

IPv6网络中的各设备除了支持网管接口通用告警的上报外，还根据设备的具体性能存在一些特定告警，例如路由器除支持陷阱/通知外还支持特定的协议告警，对于没有指出特定告警类型的暂应支持通用通知类型。

本规范不对特定告警统一规定。

5.2.3 告警数据格式

IPv6网络中的设备通过网管接口向NMS发送的告警中至少应当包含表2所列的信息。

告警格式

中文名称	说　明	数据类型
告警的序列号	告警的序列号	字符串
网元标识名	网元的识别名	字符串
告警原始级别	告警级别，设备上报告警消息中的告警级别：1.严重；2.重要；3.次要；4.一般；5.不确定	字符串
告警原始类型	告警类型，设备上报告警消息中的告警类型，包括通信告警、环境告警、设备告警、处理错误告警、服务质量告警等	字符串
告警原因号	标识告警原因的内部告警号（可选）	整型
告警原因	告警原因（可选）	字符串
告警发生时间	告警发生时间	时间
告警状态	活动状态，表示告警是否被清除还是处于活跃状态	整型
告警标题	告警标题	字符串
告警内容	告警内容	字符串

5.3 性能管理

网管系统可通过网管接口获取设备性能指标数据。

1）通过网管接口，被管设备或网元管理系统可以上报设备的历史性能数据，网管系统可以主动获取设备的历史性能数据。

2）通过网管接口，被管设备或网元管理系统可以周期上报设备的实时性能数据，网管系统可以主动获取设备的实时性能数据。

5.4 流量管理

设备应能通过网管接口向网管系统实时主动上报流量流向统计数据。支持流量管理的设备包括IPv6路由器和IPv6以太网交换机（三层）。

网管系统通过网管接口实现对流量流向统计IPFIX配置参数（如聚合规则、采样率等）的设置和修改。

5.5 安全管理

网络管理接口能够支持以下安全管理功能：

1）支持对通过网管接口访问设备资源的用户进行分角色、分级别的权限管理；

2）设备能通过网管接口向网管系统上报管理操作日志和安全日志。

5.6 日志管理

设备应能通过网管接口主动上报日志，这里特指设备的告警信息通过日志上报到NMS，包括设备部件告警、环境告警和设备功能实体告警等告警信息。

网管系统应能通过设备网管接口对日志进行管理。

5.7 操作维护

设备应能提供本地和远端操作维护接口，以支持网管系统通过该接口以安全有效的方式直接对设备进行操作和维护。

6 网管接口协议要求

6.1 网络管理接口通信协议栈要求

实现IPv6设备网络管理接口通信的协议方式包括两种，一种是单协议栈方式（IPv6协议方式），另一种是双协议栈方式。这两种协议栈方式的主要区别集中在网络层协议的实现上。

6.1.1 单协议栈方式

单协议栈方式是在被管设备上只实现IPv6协议栈，由IPv6协议承载网络管理接口定义的信息交互方式，实现网管系统和IPv6设备之间管理信息的交互，其中管理信息指满足第5节中规定的管理功能所需的信息，如图2所示。

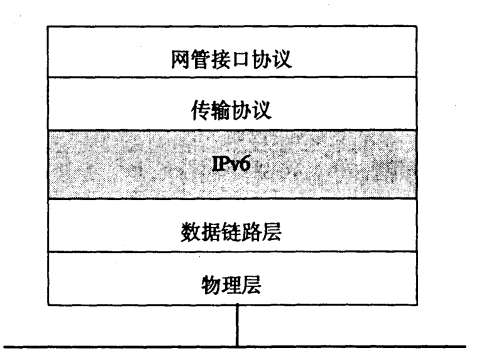


图2 单协议栈方式

6.1.2 双协议栈方式

双协议栈方式是指在被管设备上同时实现了IPv4和IPv6两种协议，网管接口协议可以由两种协议承载，如图3所示。

在网络由IPv4向IPv6的过渡阶段，网管系统可以通过IPv4协议获取IPv6设备的相关管理信息。

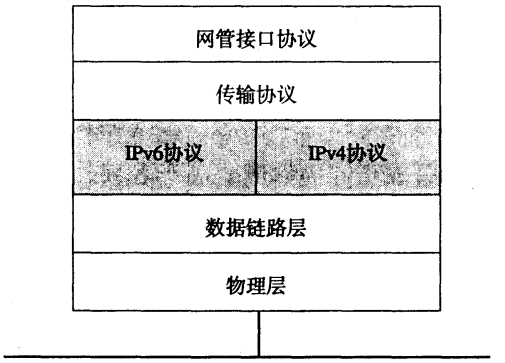


图3 双协议栈方式

IPv6设备应通过SNMP、IPFIX、Syslog、ftp以及telnet等接口协议支持各网管接口功能，且保证这些接口协议可以通过IPv6承载。

6.2 SNMP 管理协议

IPv6设备应该具备SNMP接口以方便提供必要的配置、性能、告警管理等功能，并实现SNMPv2c（RFC 1901-1908）或更高版本。

6.3 IPFIX 管理协议

IPFIX接口应用于网络性能的监测、安全管理和计费管理方面，利用网络设备内部的观测点收集并上报流数据，由网络管理系统统一分类和处理。

6.3.1 信息模型

对于每一个被测量的流，输出过程能够报告流的属性。不同聚合规则的流输出的属性不同，其输出内容应当遵循RFC3954所列出的属性，并至少应该支持以下属性：

- IP 版本号；
- 源 IP 地址；
- 目的 IP 地址；
- IP 传输协议类型（例如：TCP，UDP，ICMP……）；
- 源 TCP / UDP 端口号（如果传输协议是 TCP 或 UDP）；
- 目的 TCP / UDP 端口号（如果传输协议是 TCP 或 UDP）；
- 包计数器（如果包被分片，每一个分片算作一个包）；
- 字节计数器；
- 服务类型（在 IPv4 中）或流类型的类型（在 IPv6 中），根据 RFC2474，这些字节中包含长度为 6 位的 DSCP；
- 流标签（在 IPv6 中）；
- MPLS 标签（在 MPLS 中）；
- 流的第一个包的时间戳；
- 流的最后一个包的时间戳；
- 采样配置（例如采样方式和采样率）；

- 观测点的标识；
- 被聚合的流计数器（如果应用了聚合规则）。

6.3.2 数据模型

使用IPFIX数据模型作为推荐数据模型。

流数据应能够在关键域支持匿名，以防止信息泄密。

6.3.3 IPFIX 管理协议要求

6.3.3.1 流的分类

具有相同流属性的数据包被认为是属于同一种流。一个数据包如果显示多种不同的流属性就可以被认为是属于不同的流。

测量过程必须能够通过配置所有要求的字段或这些字段的子集完成对流的区分。

6.3.3.2 数据输出

以下规定对输出流记录的要求以及对信息模型和数据模型的要求。

6.3.3.2.1 数据输出方式

数据输出方式包括两种：主动模式和被动模式。流数据输出必须支持主动模式。

6.3.3.2.2 流量测量配置

测量过程必须提供配置功能，应支持对以下参数的配置：

- 观测点范围；
- 流的老化设定；
- 报文采样方向、采样方式(计数采样、随机采样)和采样率参数；
- 流的BGP属性（可选）。

6.3.3.2.3 流量输出配置

输出过程必须提供配置功能，应支持对以下参数的配置：

- 输出数据格式；
- 流输出源地址；
- 流输出目的地址。

6.3.4 IPFIX 协议实现要求（可选）

本部分选用 NetFlow v9 作为 IPFIX 的实现协议。

6.3.5 传输承载协议要求

本部分选用 UDP 作为 IPFIX 的承载协议。

应支持通过扩展使用 SCTP 作为承载协议（可选）。

6.3.6 通用要求

6.3.6.1 开放性

这里开放性指测量过程和输出过程配置的可扩展性。数据模型也应具有可扩展性。

6.3.6.2 可伸缩性

收集过程必须支持从大量的输出过程中收集数据。收集过程必须能够区分不同的输出源。

输出过程必须支持输出流信息到多个收集过程。

收集过程应能保证数据的一致性。

6.3.7 包格式与内容

IPFIX的包格式与内容遵循RFC3954的规定，具体内容参见本部分附录B。

6.4 Syslog 接口

Syslog用于记录系统活动的详细情况，所产生的日志用于评估、审查系统的运行环境和各种操作等。

6.4.1 传输承载协议

传输承载协议为UDP。

6.4.2 包格式和内容

Syslog协议的包格式和内容遵循RFC3164的规定，具体内容参见本部分附录C。

6.4.3 输出要求

应能支持同时向多个 Syslog 服务器发送日志信息。

6.5 Telnet 接口

应支持 SSH 2.0 版本。

6.6 FTP 接口

应支持“显示 SSL”（可选）。

7 IPv6 网管接口功能实现的协议支持要求

7.1 配置管理

应支持下述方式的配置数据获取及配置策略执行：

- SNMP方式；
- 命令行方式。

7.2 性能管理

应支持下述方式的性能数据获取：

- SNMP方式；
- 命令行方式；
- 文件方式。

7.3 告警管理

应支持下述方式的告警数据获取：

- SNMP Trap方式；
- Syslog方式。

7.4 流量管理

应支持下述方式的流量统计数据获取：

- SNMP方式；
- IPFIX方式。

7.5 日志管理

应支持下述方式的日志数据获取：

- Syslog方式；
- 文件方式。

7.6 集中操作维护

为了方便网管系统对网络设备的管理，网络设备应支持命令行方式对设备进行操作维护。

7.7 接口安全要求

网管接口应支持以下安全措施：

- telnet/SSH方式；
- SNMPv3；
- FTP/SSL（可选）。

8 网络管理接口性能要求

参见YD/T 1611.1-2007《IP网络管理接口技术要求 第1部分：总则》。

附 录 A
（规范性附录）
数据一致性指标

A.1 标准MIB

A.1.1 IPv6路由器(应支持、可选支持)

- 应支持MIBII RFC1213
- 应支持接口扩展MIB RFC1229
- 应支持BGP4 MIB RFC1657
- 应支持RIPv2 MIB RFC1724
- 应支持OSPF MIB RFC1850
- 应支持IPv6 MIB RFC4293
- 应支持IPv6 TCP MIB RFC4022
- 应支持IPv6 UDP MIB RFC4113
- 可选支持SNMP FRAMEWORK MIB RFC3411*
- 可选支持SNMP MPD MIB RFC3412*
- 可选支持SNMP NOTIFICATION MIB RFC3413*
- 可选支持SNMP TARGET MIB RFC3413*
- 可选支持SNMP USER BASED SM MIB RFC3414*
- 可选支持SNMP VIEW BASED ACM MIB RFC3415*
- 可选支持MIB实体 RFC4133*
- 应支持VRRP MIB RFC2787
- 应支持RMON MIB RFC2819
- 应支持DISMAN PING MIB RFC2925
- 应支持PPP LCP MIB RFC1471
- 应支持PPP IP NCP MIB RFC1473
- 应支持SONET MIB RFC3592
- 应支持EtherLike MIB RFC3635

A.1.2 IPv6以太网交换机

- 应支持MIBII RFC1213中的系统、接口、IP、ICMP和UDP组
- 如果交换机实现TCP，则应支持MIB-II RFC1213中的TCP组
- 应支持接口扩展MIB RFC1229
- 应支持BGP4 MIB RFC1657
- 应支持RIPv2 MIB RFC1724
- 应支持OSPF MIB RFC1850
- 应支持IPv6 MIB RFC4022
- 应支持IPv6 ICMP MIB RFC2466
- 应支持IPv6 TCP MIB RFC2452

- 应支持IPv6 UDP MIB RFC4113
- 可选支持SNMP FRAMEWORK MIB RFC3411*
- 可选支持SNMP MPD MIB RFC3412*
- 可选支持SNMP NOTIFICATION MIB RFC3413*
- 可选支持SNMP TARGET MIB RFC3413*
- 可选支持SNMP USER BASED SM MIB RFC3414*
- 可选支持SNMP VIEW BASED ACM MIB RFC3415*
- 可选支持MIB实体 RFC4133*
- 应支持VRRP MIB RFC2787
- 应支持RMON MIB RFC2819
- 应支持DISMAN PING MIB RFC2925
- 应支持PPP LCP MIB RFC1471
- 应支持PPP IP NCP MIB RFC1473
- 应支持SONET MIB RFC3592
- 应支持EtherLike MIB RFC3635
- 应支持Bridge MIB RFC4188
- 应支持Bridge MIB RFC4363

A.1.3 防火墙

（待定）

A.1.4 协议转换网关

（待定）

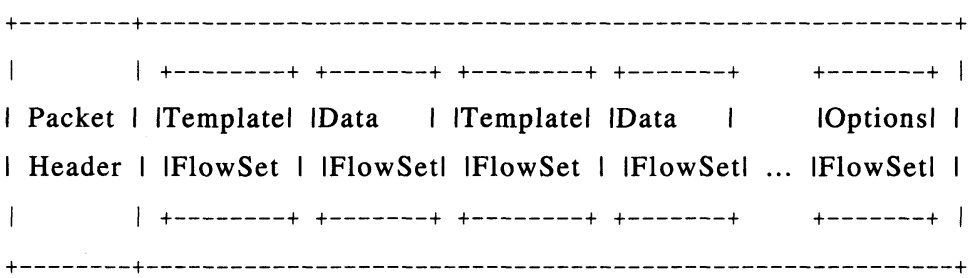
A.2 厂商特定的MIB

互联网标准和根据试验的MIB不能完全覆盖网络单元统计、状态、配置和控制信息。路由器厂商可以自己开发覆盖上述信息的MIB扩展，这些MIB扩展成为厂商特定的MIB。

这些扩展必须符合RFC1155中的相关规定，并且必须以RFC1212指定的方式描述。

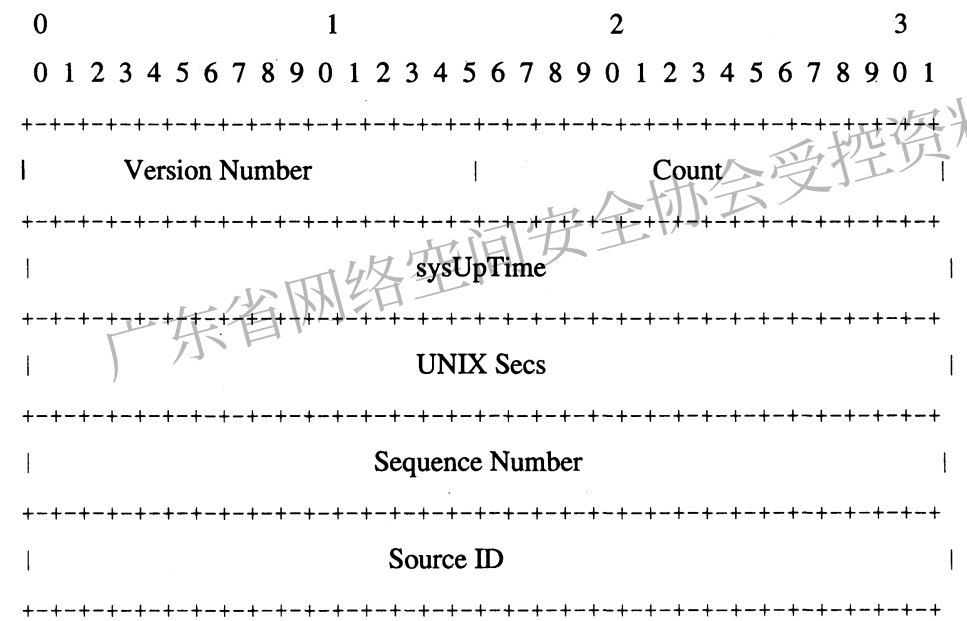
附 录 B
（资料性附录）
IPFIX 协议的包格式与内容

B.1 包的结构



流集（FlowSet）：报文内部划分了多个数据块，一个流集相当于一个数据块，每个报文可以混杂不同的流集。使用TLV方式定义模板，充分体现可扩展性、协议无关性。

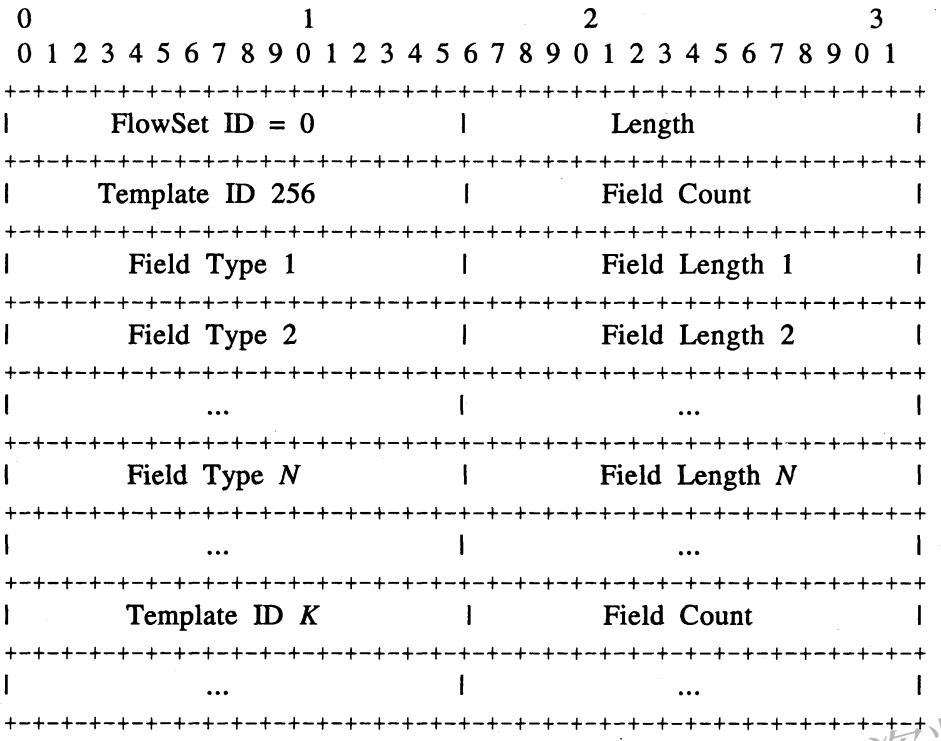
B.1.1 报文头格式



报文头中的字段描述：

- Version Number　　报文中记录的版本号
- Count　　报文中流集数量
- sysUpTime　　系统启动时间（ms）
- UNIX Secs　　自1970年的秒数
- Sequence Number　　基于设备的递增序号，可以用于检测丢包情况
- Source ID　　标识输出数据的设备接口，网流采集器应使用源IP地址加上Source ID来惟一标识一个网流输出设备

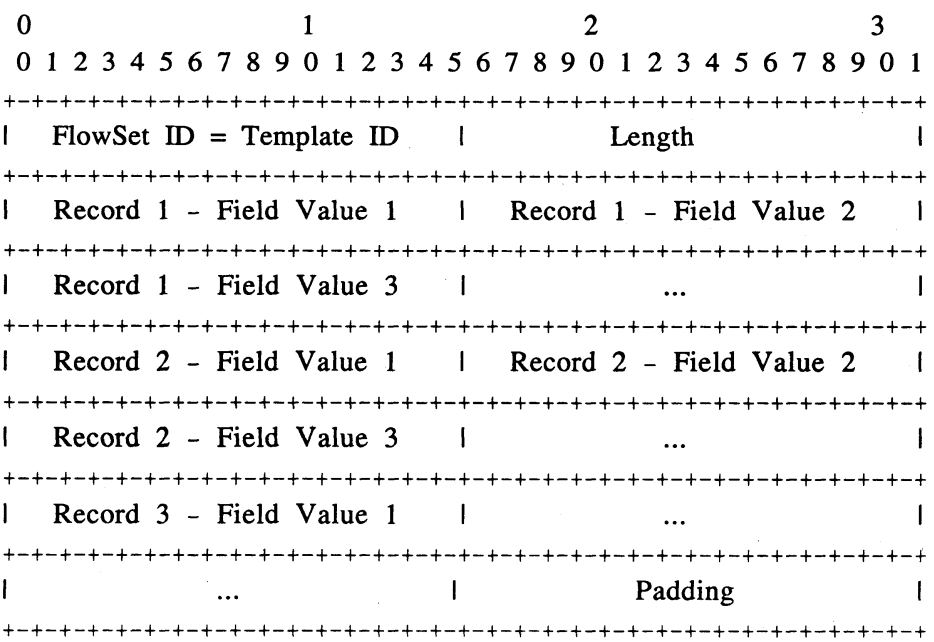
B.1.2 模板流集格式



模板流集的字段描述：

- FlowSet ID　　流集编号，0为模板流集编号
- Length　　流集长度，包括FlowSet ID、Length和所有模板记录
- Template ID　　模板编号，通常模板编号是256~65535
- Field Count　　模板记录中的字段数
- Field Type　　字段类型（有定义）
- Field Length　　字段长度（字节数）

B.1.3 数据流集格式



数据流集的字段描述：

- FlowSet ID = Template ID　流集编号，网流收集器使用FlowSet ID找到相应的模板记录
- Length　流集长度，包括FlowSet ID、Length、所有流记录和Padding
- Record N - Field Value M　记录*N*的字段*M*的值（有多个字段，各个字段的类型、长度在模板中已经定义）
- Padding　填充字节

B.1.4 字段类型定义

字段类型	取　值	长　度	描　述
IN_BYTES	1	*N*	入接口流量字节数
IN_PKTS	2	*N*	入接口流量包数
FLOWS	3	N	流数
PROTOCOL	4	1	IP 协议类型
SRC_TOS	5	1	入接口服务类型
TCP_FLAGS	6	1	TCP 标志
L4_SRC_PORT	7	2	源端口号
IPV4_SRC_ADDR	8	4	IPv4 源地址
SRC_MASK	9	1	IPv4 源地址掩码
INPUT_SNMP	10	*N*	入接口索引
L4_DST_PORT	11	2	目的端口号
IPV4_DST_ADDR	12	4	IPv4 目的地址
DST_MASK	13	1	IPv4 目的地址掩码
OUTPUT_SNMP	14	*N*	出接口索引
IPV4_NEXT_HOP	15	4	IPv4 下一跳地址
SRC_AS	16	*N*	源自治域号
DST_AS	17	*N*	目的自治域号
BGP_IPV4_NEXT_HOP	18	4	IPv4 BGP 下一跳地址
MUL_DST_PKTS	19	*N*	出接口组播包数
MUL_DST_BYTES	20	*N*	出接口组播字节数
SWITCHED	21	4	流持续时间（s）
FIRST_SWITCHED	22	4	流生成时间
OUT_PKTS	23	*N*	出接口流量包数
OUT_BYTES	24	*N*	出接口流量字节数
IPV6_SRC_ADDR	27	16	IPv6 源地址
IPV6_DST_ADDR	28	16	IPv6 目的地址
IPV6_SRC_MASK	29	1	IPv6 源地址掩码
IPV6_DST_MASK	30	1	IPv6 目的地址掩码
IPV6_FLOW_LABEL	31	3	IPv6 流标签
ICMP_TYPE	32	2	ICMP 报文类型
MUL_IGMP_TYPE	33	1	IGMP 组播报文类型
SAMPLING_INTERVAL	34	4	流采样频率
SAMPLING_ALGORITHM	35	1	采样规则
FLOW_ACTIVE_TIMEOUT	36	2	流活动的老化时间
FLOW_INACTIVE_TIMEOUT	37	2	流不活动的老化时间

表（续）

字段类型	取　值	长　度	描　述
ENGINE_TYPE	38	1	设备类型
ENGINE_ID	39	1	设备索引
TOTAL_BYTES_EXP	40	*N*	总的字节数
TOTAL_EXP_PKTS_SENT	41	*N*	总的包数
TOTAL_FLOWS_EXP	42	*N*	总的流数
MPLS_TOP_LABEL_TYPE	46	1	MPLS 顶层标签
MPLS_TOP_LABEL_IP_ADDR	47	4	MPLS 顶层标签的 IP 地址
FLOW_SAMPLER_ID	48	1	流采样标志
FLOW_SAMPLER_MODE	49	1	流采样方式
FLOW_SAMPLER_RANDOM_INTERVAL	50	4	随机流采样间隔
DST_TOS	55	1	出接口服务类型
SRC_MAC	56	6	源 MAC 地址
DST_MAC	57	6	目的 MAC 地址
SRC_VLAN	58	2	VLAN 入接口
DST_VLAN	59	2	VLAN 出接口
IP_PROTOCOL_VERSION	60	1	IP 协议版本
DIRECTION	61	1	流向（指流入或流出）
IPV6_NEXT_HOP	62	16	IPv6 下一跳地址
BPG_IPV6_NEXT_HOP	63	16	IPv6 BGP 下一跳地址
IPV6_OPTION_HEADERS	64	4	IPv6 可选报文头
MPLS_LABEL_1	70	3	MPLS 1层标签
MPLS_LABEL_2	71	3	MPLS 2层标签
MPLS_LABEL_3	72	3	MPLS 3层标签
MPLS_LABEL_4	73	3	MPLS 4层标签
MPLS_LABEL_5	74	3	MPLS 5层标签
MPLS_LABEL_6	75	3	MPLS 6层标签
MPLS_LABEL_7	76	3	MPLS 7层标签
MPLS_LABEL_8	77	3	MPLS 8层标签
MPLS_LABEL_9	78	3	MPLS 9层标签
MPLS_LABEL_10	79	3	MPLS 10层标签
保留字段	25，26，43~45，51~54，65~69		

B.2　内容

IPFIX接口至少应支持标识流的内容和流统计内容。

B.2.1　标识流的内容

IPv6源地址、源端口、IPv6目的地址、目的端口、服务类型（TOS）、传输层协议和出/入接口索引。

B.2.2　流统计内容

流开始时间、流结束时间、报文数和字节数。

B.2.3　可选的流属性

IPv6源地址掩码、IPv6目的地址掩码、IPv6下一跳地址、IPv6 BGP下一跳地址、IPv6 流标签、源自治域号和目的自治域号等。

附 录 C
（资料性附录）
Syslog 协议的包格式与内容

对于任何一个IP包的净荷，如果是一条目的端口号为514的UDP消息，该净荷就必须视作Syslog消息。传送的初始Syslog消息与经过中继的Syslog消息的格式可能会有所不同。如果中继能够识别出符合格式的消息，它必须不做任何修改而转发这条消息。但是，如果中继收到一条（Syslog）消息但无法识别为正确的消息格式，中继必须在转发消息以前，修改它的格式以符合要求。第1节将描述Syslog消息的规定格式。第2节将描述对被传输的初始消息的要求。第3节将描述对经过中继的消息的要求。

C.1 Syslog消息的组成

格式完整的Syslog消息由三个可识别的部分组成：第一个部分称为PRI；第二个部分称为HEADER；第三个部分称为MSG。包的总长度必须不能超过1024byte。这里不对Syslog消息的最小长度作出限制。

C.1.1 PRI部分

PRI部分必须由3、4或5个字符组成且起止字符必为尖括号。PRI部分开头为小于号“<”，接下来是一个数字，最后以大于号“>”结束。使用的字符集必须是由7位ASCII码组成的八位字段（具体参见RFC2234）。在一对尖括号内的数字被认为是优先级，同时代表着功能实体（Facility）和严重性（Severity）（具体描述见下文）。优先级由1位、2位或3位十进制数组成。

消息中的功能实体与严重性由十进制数字表示。一些操作系统的后台程序和进程已经指定了功能实体的值。还没有被指定明确的功能实体值的进程和后台程序可以使用属性为“本地使用（local use）”的功能实体的值或是使用属性为“用户级（user-level）”的功能实体的值。那些已经指定了具体值的功能实体的名称和编码值详见表C.1。

表C.1 Syslog的功能实体

编码值	功能实体（Facility）
0	内核消息
1	用户级消息
2	邮件系统
3	系统后台进程
4	安全／认证消息（注1）
5	由 Syslog 内部发起的消息
6	行式打印机子系统
7	网络消息子系统
8	UUCP 子系统
9	时钟进程（注2）
10	安全／认证消息（注1）
11	FTP 进程
12	NTP 子系统
13	日志检查（注1）
14	日志告警（注1）
15	时钟后台进程（注2）

表C.1（续）

编码值	功能实体（Facility）
16	本地用户 0
17	本地用户 1
18	本地用户 2
19	本地用户 3
20	本地用户 4
21	本地用户 5
22	本地用户 6
23	本地用户 7

注1：存在有不同的操作系统同时使用功能实体值4、10、13和14来表示安全／认证、检查和告警消息，因为这几种消息看起来比较相似。

2：存在有不同的操作系统同时使用功能实体值9和15来表示时钟消息。

每一条消息的优先级也包含了一个十进制的严重性指示位。它们的具体取值详见表C.2。

表C.2 Syslog消息的严重性

编码值	严重性（severity）
0	紧急：系统不可用
1	告警：必须立刻采取行动
2	危险的条件
3	错误的条件
4	警告：警告的条件
5	注意：正常但是显著性条件
6	报告：报告型消息
7	调试：调试级消息

优先级的计算是首先将功能实体的值乘以8，然后加上严重性的值。

C.1.2 HEADER部分

HEADER部分包含一个时间标记和一个主机名的标识或是设备的IP地址。Syslog包的HEADER部分必须包含可视的（可打印的）字符。和PRI部分一样，使用的编码集必须是由7位ASCII码组成的八位字段。在这个编码集中，可以使用的字符只有ABNF VCHAR（值为%d33~126）和空格（值为%d32）。

HEADER包含的两个字段称为TIMESTAMP和HOSTNAME。TIMESTAMP将紧跟在大于号“>”的后边。单个的空格符必须跟在每一个TIMESTAMP和HOSTNAME字段的后面。如果知道自己的主机名，在HOSTNAME就应当把它包含进去，如果没有主机名，就包含进去它自己的IP地址。如果一台设备有多个IP地址，通常会使用发送该消息使用的IP地址。对于这种情况还有一种可行的方法。设备可以被配置为使用同一个IP地址发送所有的消息而不管消息是从哪一个接口送出的。

TIMESTAMP字段的值为当地时间，格式为“Mmm dd hh:mm:ss”（不包含引号），具体含义如下：

Mmm是一年中某一月份的英文缩写，第一个字母大写，另外两个字母均为小写。以下是各月份惟一可以接受的缩写方式：

Jan，Feb，Mar，Apr，May，Jun，Jul，Aug，Sep，Oct，Nov，Dec。

dd是一个月中的某一天。如果某月这一天的取值小于10，那么dd必须表示为一个空格和一个数字的形式。例如，八月的第7天将会表示为“Aug 7”，在“g”和“7”之间有两个空格。

hh:mm:ss是当地时间。小时（hh）采用24小时格式。正确的取值在00到23之间（包含00和23）。分钟（mm）和秒（ss）的取值在00~59之间（包含00和59）。

TIMESTAMP字段后必须跟一个空格。

HOSTNAME字段只能包含消息发起者的一个主机名、一个IPv4地址或者一个IPv6地址。首选值是主机名。如果使用的是主机名，HOSTNAME字段必须遵照STD 13（RFC1034）的规定包含设备的主机名。需要注意的是HOSTNAME字段内部不能有空格。域名不能写进HOSTNAME字段。如果使用的是IPv4地址，必须使用STD 13中规定使用的分段十进制格式。如果使用的是IPv6地址，任何在RFC 2373中规定的正确的表达形式都可以。HOSTNAME字段后面必须跟一个空格。

C.1.3 MSG部分

MSG部分必须包含TAG字段和CONTENT字段。TAG字段的值是产生消息的程序或进程的名称。CONTENT字段包含消息的细节。TAG是一串ABNF alphanumeric字符，但不能超过32个字符。任何一个非alphanumeric字符表示TAG字段已经终止，并且将作为CONTENT字段的第一个字符。作为能够终止TAG字段而成为CONTENT字段的起始字符的，最为常见的有左方括号（“[”）、引号（“:”）或者是空格。

C.1.4 CONTENT字段的内容

Syslog接口主要提供设备的运行日志信息，包括执行命令信息、各类告警信息等。具体信息可能包括但不限于：

- LOG类，包括用户登录登出日志、用户配置操作日志等；
- TRAP类，包括电源告警、风扇告警、环境告警（指温度、湿度、门磁告警）、设备重启告警、CPU和内存告警、端口Up/Down告警、协议告警、错误提示告警等。

C.2 设备产生的Syslog包

任何一个IP包的净荷如果其目的地址为UDP的514号端口，那么该净荷必须被视为一条正确的Syslog消息。但是，必须在Syslog包中包含上节中描述的所有部分——PRI、HEADER和MSG。

Syslog消息的组织应当遵守以下的规定：

- 如果最初形成的消息在HEADER部分有TIMESTAMP，那么它应当是设备所在时区的当地时间；
- 如果最初形成的消息有HOSTNAME字段，只要消息知道自己的主机名，就会将该主机名写入HOSTNAME字段。否则就会写它自己的IP地址；
- 如果最初形成的消息有TAG值，该值应当是生成消息的程序或是进程的名称。

中华人民共和国
通信行业标准
IP网络管理接口技术要求
第2部分：支持IPv6的设备接口功能与协议
YD/T 1611.2-2007

*

人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码：100061
北京新瑞铭印刷有限公司

*

本书如有印装质量问题，请与本社联系　电话：(010)67114922