ICS 33.040.40
M 32

YD

中华人民共和国通信行业标准

YD/T 3028-2016

IP 网络流量采集分析平台技术要求

Technical requirement of IP network flow sample and analysis device

2016-04-05 发布　　2016-07-01 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本标准编制依据 GB/T 1.1-2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国信息通信研究院、中国联合网络通信集团有限公司、浙江鹏信信息科技股份有限公司。

本标准主要起草人：张宇华、庞　冉、王　健、马　克、刘　佳、祝天鹏。

IP 网络流量采集分析平台技术要求

1 范围

本标准规定了IP网络流量采集分析平台的功能、性能、可靠性、安全、环境等方面的技术要求。

本标准适用于IP网络流量采集分析平台的研发与技术验证。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB2423 电工电子产品基本环境试验规程

GB3483 电子设备雷击试验导则

YD/T 1691-2007 具有内容交换功能的以太网交换机设备技术要求

IETF RFC 1418 在OSI之上的SNMP（SNMP over OSI）

IETF RFC 2578 管理信息结构版本2（Structure of Management Information Version 2）

IETF RFC 2579 SMIv2文本约定（Textual Conventions for SMIv2）

IETF RFC 2580 SMIv2一致性声明（Conformance Statements for SMIv2）

IETF RFC 3413 SNMP应用（Simple Network Management Protocol (SNMP) Applications）

IETF RFC 3414 SNMPv3基于用户的安全模型（User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)）

IETF RFC 3416 SNMPv2协议操作（Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)）

IETF RFC 3417 SNMP传输映射（Transport Mappings for the Simple Network Management Protocol (SNMP)）

IETF RFC 3418 SNMP管理信息库(MIB)（Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)）

IETF RFC 3917 IPFIX需求（Requirements for IP Flow Information Export）

IETF RFC 4789 在IEEE 802网络之上的SNMP（Simple Network Management Protocol (SNMP) over IEEE 802 Networks）

IETF RFC 5470 IPFIX结构（Architecture for IP Flow Information Export）

IETF RFC 7012 IPFIX信息模型（Information Model for IP Flow Information Export）

3 缩略语

下列缩略语适用于本文件。

AS	Acronyms System	自治系统
BGP	Border Gateway Protocol	边界网关协议

HTTP	Hyper Text Transfer Protocol	超文本协议
HTTPS	Hypertext Transfer Protocol Secure	超文本传输安全协议
IP	Internet Protocol	互联网协议
IPFIX	IP Flow Information Export	IP数据流信息输出
IPv4	Internet Protocol Version 4	互联网协议第4版
IPv6	Internet Protocol Version 6	互联网协议第6版
MPLS	Multi-Protocol Label Swithing	多协议标签交换
MTBF	Mean Time Between Failures	平均故障间隔
SNMP	Simple Network Management Protocol	简单网管协议
SSH	Secure Shell	安全外壳
TCP	Transport Control Protocol	传输控制协议
ToS	Type of Service	服务类型
UDP	User Data Protocol	用户数据报协议

4 IP 网络流量采集分析平台概述

随着互联网技术的发展，网络管理者越来越需要对网络流量的分布进行充分的了解。一般的SNMP技术只能做到对单个网元设备上接口级别流量的统计，无法满足网络端到端的流量统计、业务统计，以及一些异常流量发现的需要。根据这些需求，流量采集技术应运而生。

流量采集技术是基于路由器设备上硬件转发方式的革新而产生的。目前的核心路由器、交换机都采用硬件转发的方式，对数据进行逐流转发，需要根据数据流量的特征定义转发的“流”（flow），并建立硬件转发表项，为每条流定义转发策略，当数据流到来时，根据它的特征匹配硬件转发表中不同的“流”来进行转发。通常定义的“流”特征包括入接口、源/目的IP地址、协议类型、源/目的端口号、TOS值等。流量采集技术就是利用了硬件转发中这些流的信息，对不同的“流”信息进行统计，包括时间戳、报文数、字节数等。

随着路由器转发能力的不断提高，如果对转发的每个数据包都进行统计，将浪费大量的计算资源，也会影响路由器的转发能力，因此目前应用的流量采集技术都实现了采样的方式对流量进行统计。但采样所耗费的路由器资源与采样的准确度是一对矛盾的关系，采样比越低，采样准确率越高（当采样比为1:1时准确率为100%），但耗费的路由器计算资源越多；反之，采样比越高，采样准确率越低，消耗的路由器资源则越少。合理地确定采样比，就是在采样准确性与路由器资源消耗之间寻求平衡。一般网络中设置的采样比可以为1000:1或2000:1，即每隔1000个或2000个报文对数据流进行一次采样。

如图1所示，进行流量采集时一般包括流量采集机及流量分析机两个部分。流量采集机负责对路由器上送的流记录报文进行收集和预处理；流量分析机负责对流量采集机所生成的预处理数据进行分析，根据不同的统计方式生成有意义的统计结果。流量采集/分析一体机是流量采集机和流量分析机的集合，负责流量采集和流量分析的功能。

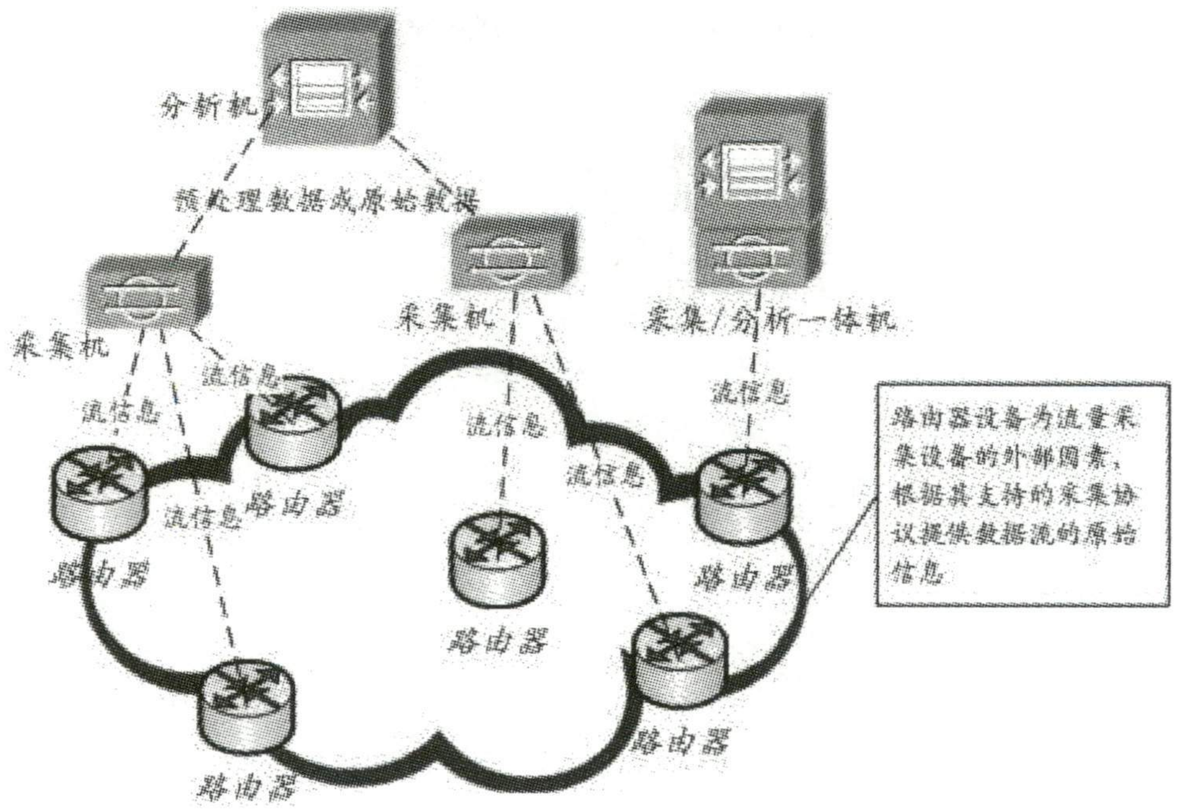


图1 IP 流量采集示意

5 IP 网络流量采集分析平台功能要求-流量采集机

5.1 流量采集协议要求

流量采集机在实现上应不限于某种特定流量采集协议，一般来说，由于现网设备的多样性，流量采集机应兼容各种流量采集协议，包括Netflow（v5，v9）、NetStream（v5，v9）、Cflow、SFlow等，并支持对各种流量采集协议数据进行同时接收处理。

流量采集机应能够识别流量采集协议报文中的流量信息，这些流量信息包括：

a） 入/出接口号

b） 流字节数

c） 流总包数

d） 协议类型

e） TOS 值

f） TCP flag

g） IPv4/IPv6 源、目的地址/端口号

h） IPv4/IPv6 源、目的地址掩码

i） IPv6 流标签

j） IPv4/IPv6 下一跳

k） 源、目的 AS

l） BGP 下一跳

m） MPLS 标签

n） 采样间隔

流量采集机应支持对采集流输出设备的 IP 地址，流量数据接收端口号等进行设定。

5.2 流量采集数据的预处理与转发

流量采集机应对接收到的流记录进行预处理，生成预处理数据，并定期发送至流量分析机。流量采集机应支持对流数据的采样功能。

流量采集机应支持对接收到的流记录进行转发，将原始流记录转发（或按一定抽样比例）至流量分析机或其他流量采集机。

5.3 流量监测

由于在不同路由器上可能设置不同的采样率，流量采集机应该能够根据每台路由设备不同的采样率对从该设备采集的数据进行还原，以得到正确的统计结果。

5.4 对网管协议的支持

流量采集机应支持被网管系统管理，通过网管系统对其故障、性能、日志、告警、安全等各个方面进行监测。

流量采集机应支持IETF RFC2578/IETF RFC2579/IETF RFC2580/IETF RFC3416/IETF RFC3417/IETF RFC3418中规定的SNMPv2，可选支持IETF RFC3413、IETF RFC3414中规定的SNMPv3。

SNMP必须使用UDP/IP作为传输层/网络层协议，也可以使用其它协议（例如IETF RFC1418和IETF RFC4789）。

6 IP 网络流量采集分析平台功能要求-流量分析机

6.1 流量分析功能要求

流量分析机应可以依据流量来源和目的AS号、IP地址段、应用协议、网络设备接口和Community等监控参数来设定监控范围。

根据流量采集机提供的数据，流量分析机应实现以下流量分析功能：

（1）网络流量流向分析

根据流量的源、目的IP地址，以及源、目的AS号，结合流量统计数据，实现对网络中某个设备，以及全网的流量、流向（网络内部流量、出网流量、穿越流量、骨干流量等）的统计。

（2）网络业务流量分析

根据流量的端口号，对常见网络业务流量、流向进行分析。如统计HTTP、SNMP、TELNET、FTP等常用协议的流量以及占总流量的比例。

（3）基于用户的流量分析

以某一地址/多个地址、某一端口/多个端口、某一Community/多个Community或某一自治域号（AS）/多个自治域号（AS组）为分析对象，分析该地址组、端口组、Community组或AS组代表的客户的流量行为状况，如链路带宽占用情况，该用户访问其它地址/AS的情况，访问该用户的地址/AS分布情况，该用户流量的协议、业务分布状况等。

（4）异常流量分析

流量分析机应能够根据设定的条件（如病毒或网络攻击的流量特征）对流量进行实时监测，当出现异常流量时，对病毒或攻击的来源、目的、攻击的类型、攻击的规模、持续的时间等进行分析呈现，并支持多种方式告警。

6.2 原始数据的过滤功能

流量分析机应可以根据需要依据设定的条件对接收到的原始数据进行过滤处理。如利用OR、NOT、AND等逻辑运算或其组合对原始数据进行过滤或二次处理，并根据结果形成各种报表或表格。

6.3 实时监测

流量分析机应可以实时的呈现所设定的网络范围内瞬间的流量状况并生成相应的报表，其实时性依赖于设备对流数据的发送参数以及流量采集机对原始数据的发送参数设置，对基于物理端口的实时监测的最小时间粒度应不大于5秒，即支持基于物理端口每*n*秒（*n*≤5）采样一个基于端口的实时流入、流出流量数据（bit/s），并存储数据、生成相应报表。

流量分析机应支持存储连续24小时的实时流量检测结果，并生成相应的报表。

流量分析机应支持基于所设定的网络范围内实时流量监测数据的15分钟流量峰值统计功能，即第一个*n*秒(*n*≤5)采样一个流量数据,后续每*n*秒采样一个数据,并与前面的数据进行比对，保留秒级采样的最大值和最小值，每隔15分钟，在15分钟性能数据中存储15分钟内的秒级流量最大值和最小值，并对统计结果的最大值、最小值、平均值形成相应报表。

流量分析机应支持存储不小于连续24小时的15分钟流量峰值统计数据,应支持不小于连续1个月的15分钟流量峰值统计，并生成相应的报表。

6.4 基于 BGP 路由对流量分析

流量分析机可选支持BGP协议。通过与骨干路由器（或路由反射器）建立BGP邻居关系，流量分析机可以接收和分析BGP路由，并从路由表中获得BGP Community、AS_Path、BGP NextHop等信息，从而更加精确地分析流量的属性。

6.5 全网关联性流量分析

流量分析机应能够将通过不同的采集机采集的多条链路上的同类流量数据进行合并汇总，从而实现对全网多节点关联的业务流量分析，实现多出口整体状况的关联性分析。如对全部出入口流量进行统一汇总和分析；对网内某些热点资源与其他网络间的流量进行统计分析等。

流量分析机应能够将所有采集设备采集的数据进行统一的汇总、处理和关联分析，并将汇总的结果通过统一的界面展现给用户。

7 IP 网络流量采集分析平台功能要求-流量采集/分析一体机

流量采集/分析一体机是流量采集机和流量分析机的集合，属于同一台物理实体设备，且应具备单一流量采集机和流量分析机所有的功能。

8 管理功能

8.1 性能监测

IP网络流量采集分析平台应提供对自身性能的实时监测。性能监测包括：设备使用状态，CPU使用率，内存使用率，数据库使用率等。

8.2 用户及权限管理

IP网络流量采集分析平台应能够支持分级分权管理功能，支持用户根据需要进行自定义的授权，开放相应的权限与功能。IP网络流量采集分析平台管理权限应与用户管理权限分离。

8.3 数据管理

流量分析机应能够实现历史分析结果的在线保存，保存期限可由用户设定，同时支持过期数据自动删除功能。

流量采集机和分析机应支持设备配置的备份和读取。

8.4 数据呈现

IP网络流量采集分析平台应能够通过图、表等方式对实时和历史数据进行呈现，并提供天/周/月/年的分析结果统计报表，并支持以XML/EXCEL等可再编辑处理的通用格式对分析结果进行输出存储，并能够提供报表的定制功能。

9 IP 网络流量采集分析平台性能及可靠性要求

IP网络流量采集分析平台的性能根据每秒可同时处理的流（flow）数来进行统计，在正常处理能力下，设备平均CPU和内存负荷应低于65%。

IP网络流量采集分析平台平均无故障运行时间(MTBF)应大于100000h。

10 IP 网络流量采集分析平台安全要求

IP网络流量采集分析平台的远程接入应通过HTTPS和SSH实现，支持通过带IP访问控制的HTTPS来确保远程web接入的安全性。系统还应该支持客户自定义HTTPS的访问端口。

IP网络流量采集分析平台具备安全日志功能，可完整地记录用户的重要操作和访问信息。

IP网络流量采集分析平台应提供数据备份手段，定期对各种重要数据进行备份，并具备恢复能力。

11 IP 网络流量采集分析平台环境及供电要求

11.1 环境要求

IP网络流量采集分析平台正常工作的温度、湿度条件应符合GB2423的规定。

IP网络流量采集分析平台工作环境的防尘要求应符合GB2423的规定。

IP网络流量采集分析平台产生的电磁干扰应符合GB2423的规定。

IP网络流量采集分析平台的抗电磁干扰能力应符合GB2423的规定。

IP网络流量采集分析平台防雷击能力应符合GB3483。

11.2 电源与接地

11.2.1 电源

IP网络流量采集分析平台电源要求应符合YD/T 1691-2007中13.1节相关要求。

12.2.2 接地要求

IP网络流量采集分析平台接地要求应符合YD/T 1691-2007中13.2节相关要求。

附 录 A
（资料性附录）
IP 流量采集协议

最初的流量采集技术是1996年由思科公司发明的，并申请了专利。随着路由器设备设计水平的整体进步，以及网络管理者对流量统计的需求越来越迫切，其他厂家也开始发展流量采集技术，目前思科、Juniper、华为等厂家都拥有自己的流量采集技术。由于专利限制，这些采集技术虽然实现方式大同小异，但在数据格式等细节方面各有不同。

IPFIX

由于各厂商的流量采集技术相互之间不能兼容，无法满足大规模异构网络中应用的需要，因此需要对流量采集技术从协议层面上进行统一。出于这一考虑，IETF成立了IPFIX工作组，并基于思科公司的Netflow v9制定了IPFIX协议，目前已经发布了“IPFIX需求”（参见IETF RFC 3917）、“IPFIX信息模型”（参见IETF RFC 7012）、“IPFIX结构”（参见IETF RFC 5470）等多个RFC。

IPFIX 要达到以下目标：

定义“标准 IP 流”的概念。类似的定义在实践中已经广为应用，IPFIX 所要做的就是把它们标准化。

在分组采样的基础上考虑 IP 流信息的概念。

考虑影响到流数据的安全和隐私问题，为输出的流数据选择安全的传送。

规定将 IP 流信息在传输层上的传送方式。

保证流输出系统的可靠性。

附 录 B
（资料性附录）
IP 流量采集技术

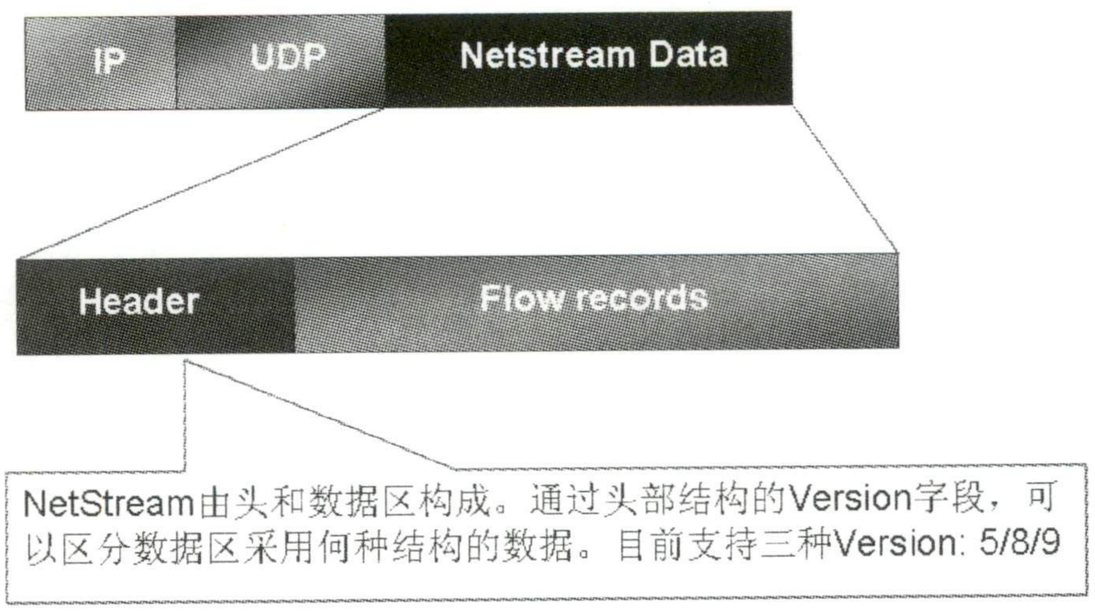
Netflow

Netflow是思科公司的专利技术，也是最早出现的流量采集技术。目前主要使用的有v5、v9两个版本，图B.1是Netflow v9版本的数据记录格式，其中包含了数据流的出/入接口、QoS位、协议类型、源/目的IP地址、源/目的端口号等基本信息，还包括了下一跳地址、源/目的AS号等路由信息。

图A.1 Netflow v9 数据记录格式

Netflow v9的数据输出格式与v5有较大区别，主要是因为Netflow v9采用了基于模板式的数据输出方式。网络设备在进行Netflow v9格式的数据输出时会向采集机分别发送数据包模板和数据流纪录。数据包模板确定了后续发送的数据流纪录数据包的格式和长度，便于采集机对后续数据包的处理。同时为避免传输过程中出现丢包或错误，网络设备会定期重复发送数据包模板给采集机。

NetStream



图A.2 NetStream 的报文格式

NetStream是华为公司推出的流量采集技术，其基本功能与Netflow类似，目前华为设备通常支持的NetStream版本为v5、v8和v9。Netstream支持二层报文、IP报文（TCP、UDP、ICMP报文）和MPLS报文的统计。

sFlow

sFlow（RFC3176）主要在阿尔卡特、惠普、网捷（Foundry，现已被博科收购）等交换机设备中使用，是由硬件实现的数据采集协议，可以实现对数据包二层至七层各种信息的记录。

Cflow

Cflow 协议主要由 Juniper、阿尔卡特等公司设备支持，其原理和机制与 Netflow 基本一致。

中华人民共和国
通信行业标准
IP网络流量采集分析平台技术要求
YD/T 3028-2016
*
人民邮电出版社出版发行
北京市丰台区成寿寺路11号邮电出版大厦
邮政编码：100164
北京康利胶印厂印刷

*
开本：880×1230　1/16　　2016年6月第1版
印张：1　　2016年6月北京第1次印刷
字数：23千字
15115·993
定价：10元
本书如有印装质量问题，请与本社联系　电话：(010)81055492