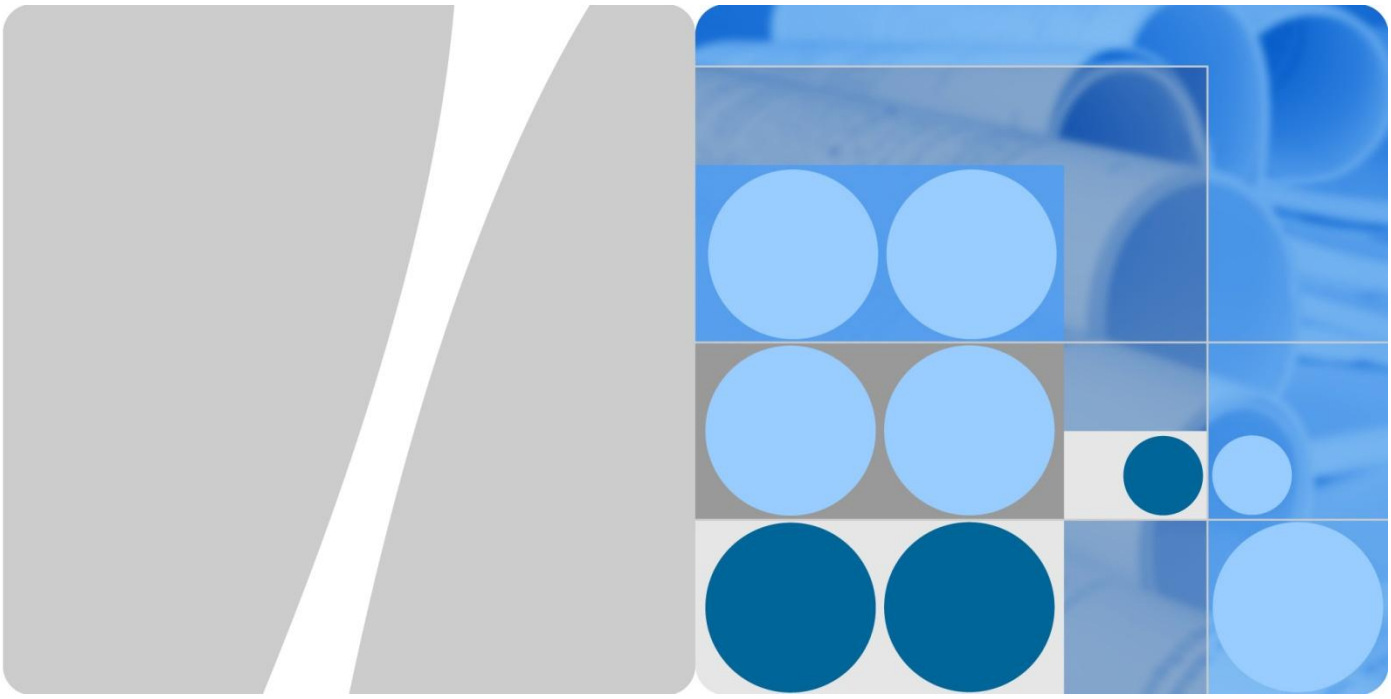


eSight V300R001C10 网流分析特性技术白皮书

文档版本 01

发布日期 2013-12-10

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： http://enterprise.huawei.com

前 言

概述

本文通过对 eSight NTA 网流分析组件的解决方案、基本原理、关键技术、典型应用的描述，帮助用户更好的了解 eSight NTA 网流分析组件的使用方法和使用场景。

读者对象

本文档（本指南）主要适用于以下工程师：

- 技术支持工程师
- 维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	用于警示紧急的危险情形，若不避免，将会导致人员死亡或严重的人身伤害。
警告	用于警示潜在的危险情形，若不避免，可能会导致人员死亡或严重的人身伤害。
小心	用于警示潜在的危险情形，若不避免，可能会导致中度或轻微的人身伤害。
注意	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “注意”不涉及人身伤害。
说明	用于突出重要/关键信息、最佳实践和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修改记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2013-12-10)

第一次正式发布。

目 录

1 执行摘要

eSight NTA 网流分析组件重点是帮助用户实现网络流量可视、故障可查、规划可依的网络透明化管理目标，提供多维度详细的流量分析报表，帮组管理员及时了解网络流量动态，确保网络带宽得到充分合理的使用，保障网络长期稳定高效运行；通过长期报表，为容量规划提供科学的数据依据。

重点功能包括识别消耗最多网络带宽的应用程序、主机、会话信息；基于 DSCP 的流量监控，确保流量优先级策略的有效性；准实时流量监控为预先故障检测、高效故障排除和快速问题解决提供帮助；基于长期的历史数据分析，优化网络设计和规划，实现以最小的网络运营成本达到最佳的网络性能和可靠性。

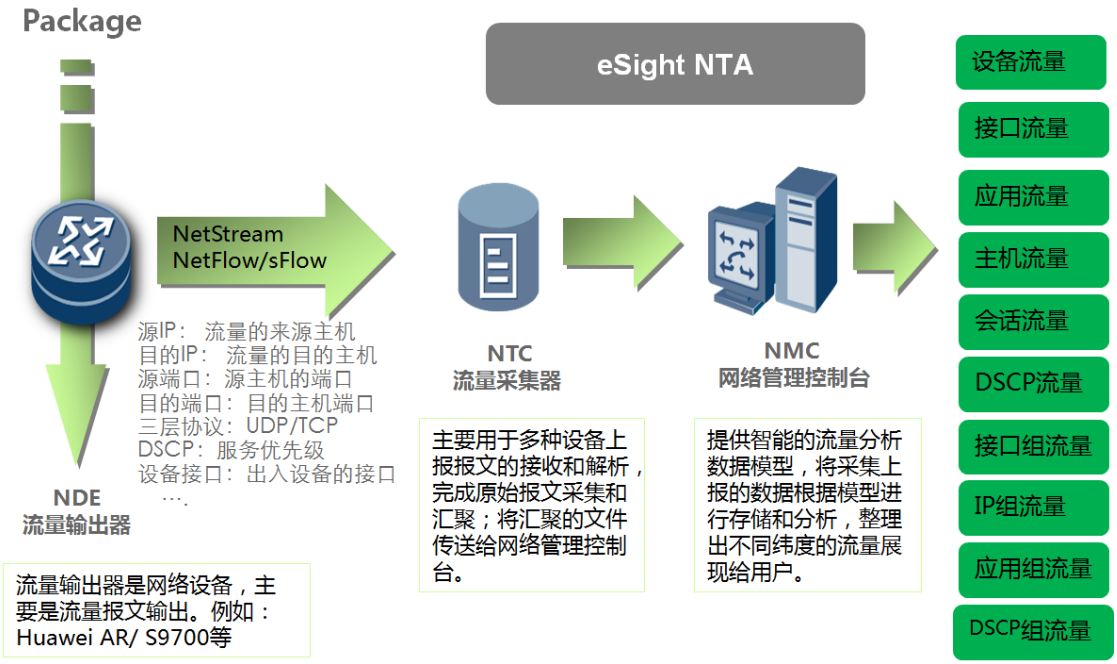
2 简介

eSight NTA 网流分析组件由网流采集器和网络管理控制台构成。网流采集器用于接收设备的 UDP 报文，并将其解析为标准的流结构，同时根据特定的汇聚策略汇聚成文件存储到磁盘，并定时发送给网络管理控制台。网络管理控制台接收采集器的流文件，进行分析，同时根据一定的汇聚策略将文件中数据汇聚到数据库中并提供查询功能。

3 解决方案

3.1 解决方案整体介绍

eSight NTA 网流分析解决方案包括三部分：流量输出器（NDE，Network Data Exporter）、网流采集器（NTC，Network Traffic Collector）和网络管理控制台（NMC，Network Management Console），它们之间的关系如下图所示：



下面详细介绍各组成部分的作用。

流量输出器 NDE

NDE（流量输出器）是支持“流”技术的网络设备，对网络流进行分析处理，提取符合条件的流统计信息，并将统计信息输出给 NTC 设备，输出前也可对数据进行一些处理，比如聚合。eSight NTA 网流分析组件捕获的网络设备流包括 Huawei® NetStream、Cisco® NetFlow 以及 sFlow。

网流采集器 NTC

NTC（网流采集器）是一个应用程序，负责解析 NDE 输出的报文，聚合流量数据、保存原始流量日志，然后通过 https 将数据文件发送到网络管理控制台。NTC 可以采集多个 NetStream 设备输出的数据，对数据进行过滤和聚合。

网络管理控制台 NMC

NMC（网络管理控制台）是一个流量分析工具，提供智能的流量分析数据模型，将采集器上报的数据根据不同的模型进行分析和存储，提供多维度的流量分析数据展示给用户。NMC 基于 B/S 架构，通过 Web 浏览器提供直观的、图形化的管理分析界面。

eSight NTA 网流分析组件包括 NTC 和 NMC 两个部分，两个部分可以集成安装在一台服务器上运行。

3.2 关键技术点介绍

3.2.1 NetStream 技术

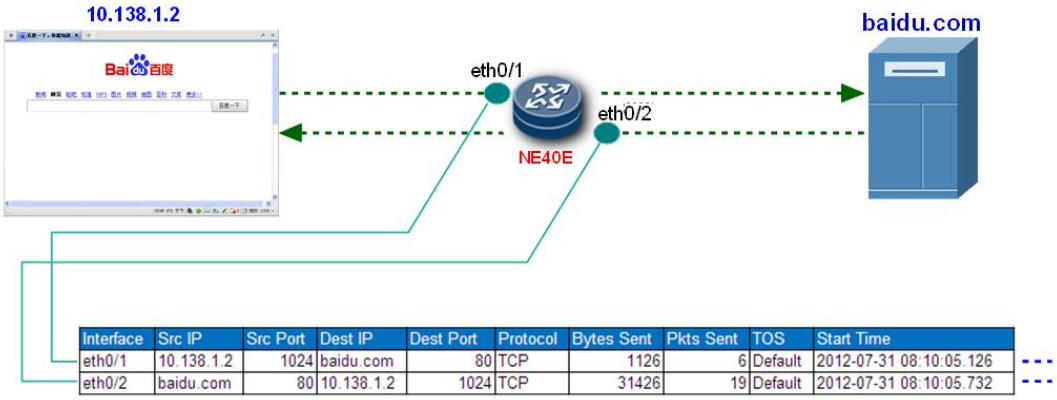
流量统计分析是网络运维和日常管理重要的一部分，传统的流量统计有 SNMP、端口镜像等方式，SNMP 统计仅能统计到设备端口流量的大小，无法统计到流量中发送和接收主机 IP、端口、协议和 DSCP 等信息，无法做到基于应用和主机会话的流量。仅能统计流量大小而无法统计到流量的详细组成和流向信息；端口镜像方式是将流量完全复制一份进行分析，需要有支持逐包分析的探针或者分析系统，这种方式受镜像端口转发能力限制，并且会占用大量的带宽，一般用在分析少量端口和小流量场景，无法做到全网的流量分析。

以 NetFlow 为代表的流技术解决了以上两种流量统计方式的限制，它利用网络中现有的支持流技术的网络设备来完成流量统计，不需要额外的部署探针，只需要在现有设备上做简单配置，即可完成全网流量分析，并提供流量大小、流量详细组成和流量流向的分析报告。

目前主流的流技术包括 Huawei/H3C NetStream，Cisco NetFlow，Juniper J-Flow、IPFIX 以及 sFlow。下面以 NetStream 为例，说明流的含义。

由于 IP 网络的非面向连接特性，网络中不同类型业务的通信可能是任意一台终端设备向另一台终端设备发送的一组 IP 数据包，这组数据包实际上构成了网络中某种业务的一个数据流。绝大部分的数据流量都是短暂、阵发的双向数据流。NetStream 主要根据一个报文的目的 IP 地址、源 IP 地址、目的端口号、源端口号、协议号、ToS（Type of Service）、输入/输出接口组成的 7 元组来区分不同的流，针对这些流做独立的数据统计。

一个流数据示例：



从上图可见，对于接口 eth0/1,用户 10.138.1.2 访问 baidu.com，产生了一条流；对于接口 eth0/2，baidu.com 服务器返回搜索结果给查询用户，产生了一条流。

从上面的描述可以看出，由源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议号、ToS（Type of Service）、输入/输出接口组成 7 元组的一条流信息是单向的、表征 IP 报文流量日志信息，是网络设备流量转发的详细日志记录，将这些重要信息深入分析可知悉网络流量动态。

目前 NetStream 报文输出的格式有 V5、V8、V9 三个版本，V5 采用固定的 7 元组格式进行上报，NDE 设备上不会对数据进行聚合；V8 采用聚合格式上报，NDE 设备会将数据统计后进行聚合，按照 V8 格式上报，上报格式固定；V9 版本是基于模板来进行发送，可以按照 V5 的七元组上报，也可以将数据聚合后上报，还可灵活配置上报的格式。使用较多的是 V5 和 V9 两个版本。各个版本详细比较见下表。

版本	格式说明	优点	缺点
V5	报文格式固定，根据七元组产生的原始流统计记录。	输出的字段丰富，可以把聚合前流记录的所有字段都输出给 NTC；NDE 设备负荷较小；应用广泛，易于对接 NTC。	格式固定且不可扩展；数据量大，对 NTC 设备处理和数据存储性能要求高；NTC 和 NMC 压力大。
V8	NDE 设备聚合后的流信息，报文格式固定，不易扩展。	数据量相对较小。承载内容略为简单，适合特定分析。可以增加新的聚合方式。	格式固定且不可扩展。设备完成聚合工作，负荷较重，只用于将聚合后的流信息输出给 NTC。增加新的聚合方式，需要 NDE 设备和网流采集器升级版本。

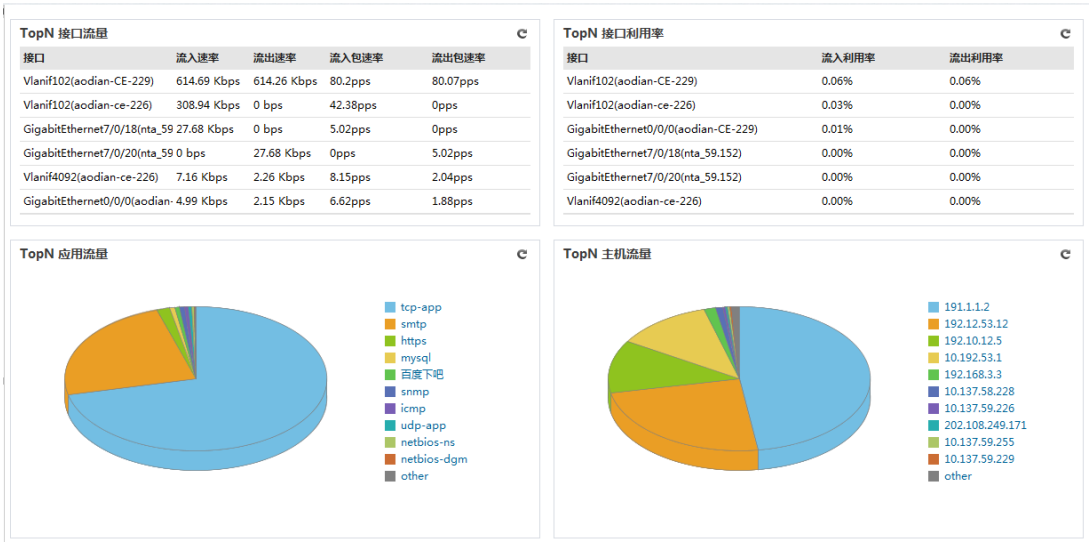
版本	格式说明	优点	缺点
V9	报文格式基于模板，易扩展；可输出两种数据类型，一种是统计数据，第二种是选项数据。	最灵活的输出格式，格式可以变化；可以用来输出聚合前的流记录，也可以输出聚合后的流记录。	需要上层的流量分析系统支持对模板的解析

3.2.2 多层次流量分析

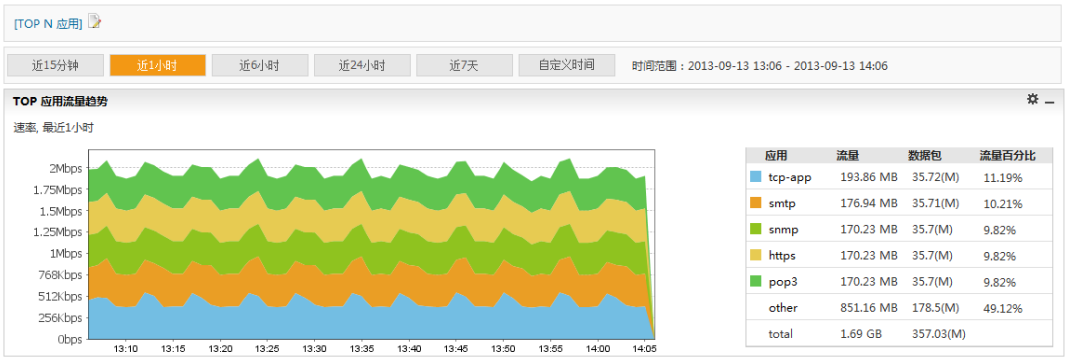
网络管理控制台以图形化的方式提供多维度、多层次的流量分析报表。既可以直观显示全网接口、应用、主机等统计对象的 Top N 排行，又可以针对单个统计对象进行精细化分析，并且能准确查询到原始流量的具体信息，达到流量可视化的目的。

流量分析维度包含设备维度、接口维度、应用维度、主机维度、DSCP 维度、会话维度、接口组维度、应用组维度、DSCP 组维度和 IP 组维度等 10 种维度，每种维度都是先展现该统计维度下的 Top N 排行，选择一个具体统计对象后，再展现该统计对象的详细流量趋势及各相关流量数据的组成。

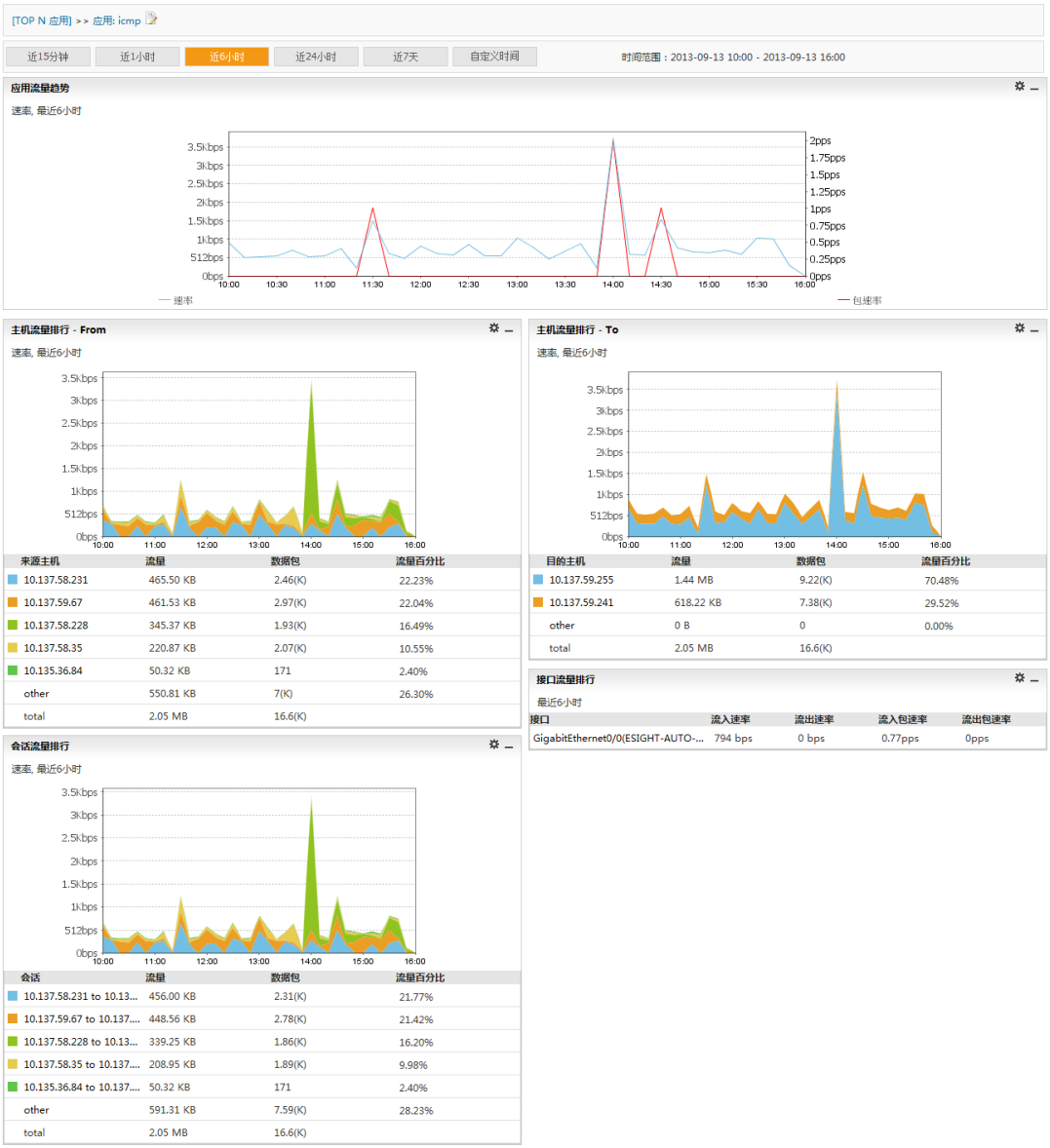
- 首页操控板图形化的显示 Top N 接口利用率/应用/主机，全网流量动态直观显示。



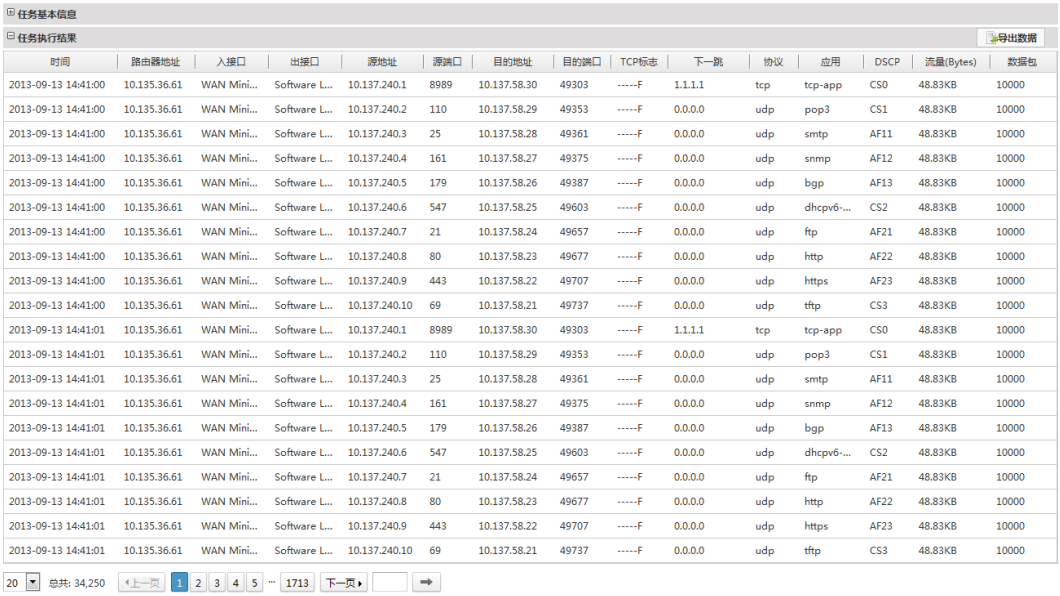
- 单个维度的 Top N 流量排行，从全网角度展现流量、数据包统计信息及流量趋势。



- 单个维度的流量详细统计，包括流量、数据包双坐标趋势图及相关联流量信息排行，直观展现流量的组成。



- 原始流量数据报表，展现完整的流信息，方便定位网络故障。


任务基本信息

任务执行结果 导出数据

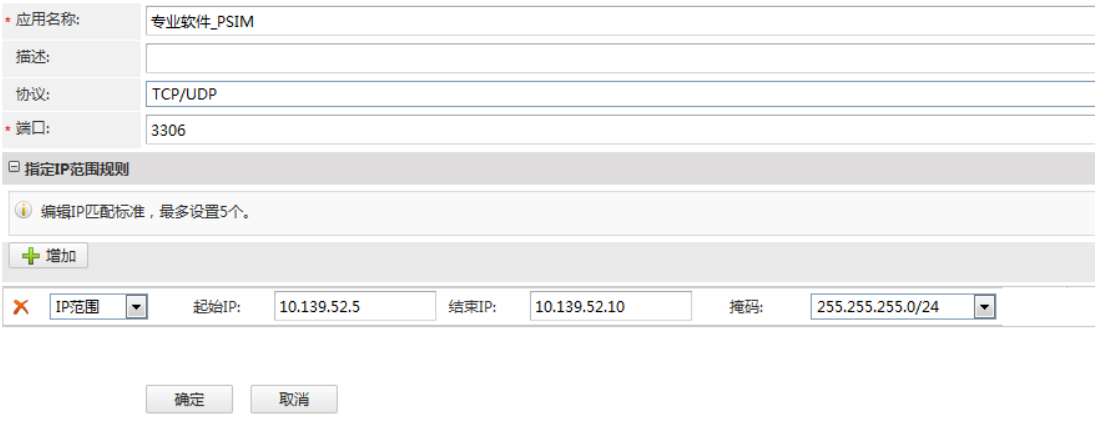
时间	路由器地址	入接口	出接口	源地址	源端口	目的地址	目的端口	TCP标志	下一跳	协议	应用	DSCP	流量(Bytes)	数据包
2013-09-13 14:41:00	10.135.36.61	WAN Mini...	Software L...	10.137.240.1	8989	10.137.58.30	49303	-----F	1.1.1.1	tcp	tcp-app	CS0	48.83KB	10000
2013-09-13 14:41:00	10.135.36.61	WAN Mini...	Software L...	10.137.240.2	110	10.137.58.29	49353	-----F	0.0.0.0	udp	pop3	CS1	48.83KB	10000
2013-09-13 14:41:00	10.135.36.61	WAN Mini...	Software L...	10.137.240.3	25	10.137.58.28	49361	-----F	0.0.0.0	udp	smtp	AF11	48.83KB	10000
2013-09-13 14:41:00	10.135.36.61	WAN Mini...	Software L...	10.137.240.4	161	10.137.58.27	49375	-----F	0.0.0.0	udp	snmp	AF12	48.83KB	10000
2013-09-13 14:41:00	10.135.36.61	WAN Mini...	Software L...	10.137.240.5	179	10.137.58.26	49387	-----F	0.0.0.0	udp	bgp	AF13	48.83KB	10000
2013-09-13 14:41:00	10.135.36.61	WAN Mini...	Software L...	10.137.240.6	547	10.137.58.25	49603	-----F	0.0.0.0	udp	dhcpv6-...	CS2	48.83KB	10000
2013-09-13 14:41:00	10.135.36.61	WAN Mini...	Software L...	10.137.240.7	21	10.137.58.24	49657	-----F	0.0.0.0	udp	ftp	AF21	48.83KB	10000
2013-09-13 14:41:00	10.135.36.61	WAN Mini...	Software L...	10.137.240.8	80	10.137.58.23	49677	-----F	0.0.0.0	udp	http	AF22	48.83KB	10000
2013-09-13 14:41:00	10.135.36.61	WAN Mini...	Software L...	10.137.240.9	443	10.137.58.22	49707	-----F	0.0.0.0	udp	https	AF23	48.83KB	10000
2013-09-13 14:41:00	10.135.36.61	WAN Mini...	Software L...	10.137.240.10	69	10.137.58.21	49737	-----F	0.0.0.0	udp	tftp	CS3	48.83KB	10000
2013-09-13 14:41:01	10.135.36.61	WAN Mini...	Software L...	10.137.240.1	8989	10.137.58.30	49303	-----F	1.1.1.1	tcp	tcp-app	CS0	48.83KB	10000
2013-09-13 14:41:01	10.135.36.61	WAN Mini...	Software L...	10.137.240.2	110	10.137.58.29	49353	-----F	0.0.0.0	udp	pop3	CS1	48.83KB	10000
2013-09-13 14:41:01	10.135.36.61	WAN Mini...	Software L...	10.137.240.3	25	10.137.58.28	49361	-----F	0.0.0.0	udp	smtp	AF11	48.83KB	10000
2013-09-13 14:41:01	10.135.36.61	WAN Mini...	Software L...	10.137.240.4	161	10.137.58.27	49375	-----F	0.0.0.0	udp	snmp	AF12	48.83KB	10000
2013-09-13 14:41:01	10.135.36.61	WAN Mini...	Software L...	10.137.240.5	179	10.137.58.26	49387	-----F	0.0.0.0	udp	bgp	AF13	48.83KB	10000
2013-09-13 14:41:01	10.135.36.61	WAN Mini...	Software L...	10.137.240.6	547	10.137.58.25	49603	-----F	0.0.0.0	udp	dhcpv6-...	CS2	48.83KB	10000
2013-09-13 14:41:01	10.135.36.61	WAN Mini...	Software L...	10.137.240.7	21	10.137.58.24	49657	-----F	0.0.0.0	udp	ftp	AF21	48.83KB	10000
2013-09-13 14:41:01	10.135.36.61	WAN Mini...	Software L...	10.137.240.8	80	10.137.58.23	49677	-----F	0.0.0.0	udp	http	AF22	48.83KB	10000
2013-09-13 14:41:01	10.135.36.61	WAN Mini...	Software L...	10.137.240.9	443	10.137.58.22	49707	-----F	0.0.0.0	udp	https	AF23	48.83KB	10000
2013-09-13 14:41:01	10.135.36.61	WAN Mini...	Software L...	10.137.240.10	69	10.137.58.21	49737	-----F	0.0.0.0	udp	tftp	CS3	48.83KB	10000

20 总共: 34,250 上一页 1 2 3 4 5 ... 1713 下一页

3.2.3 应用识别

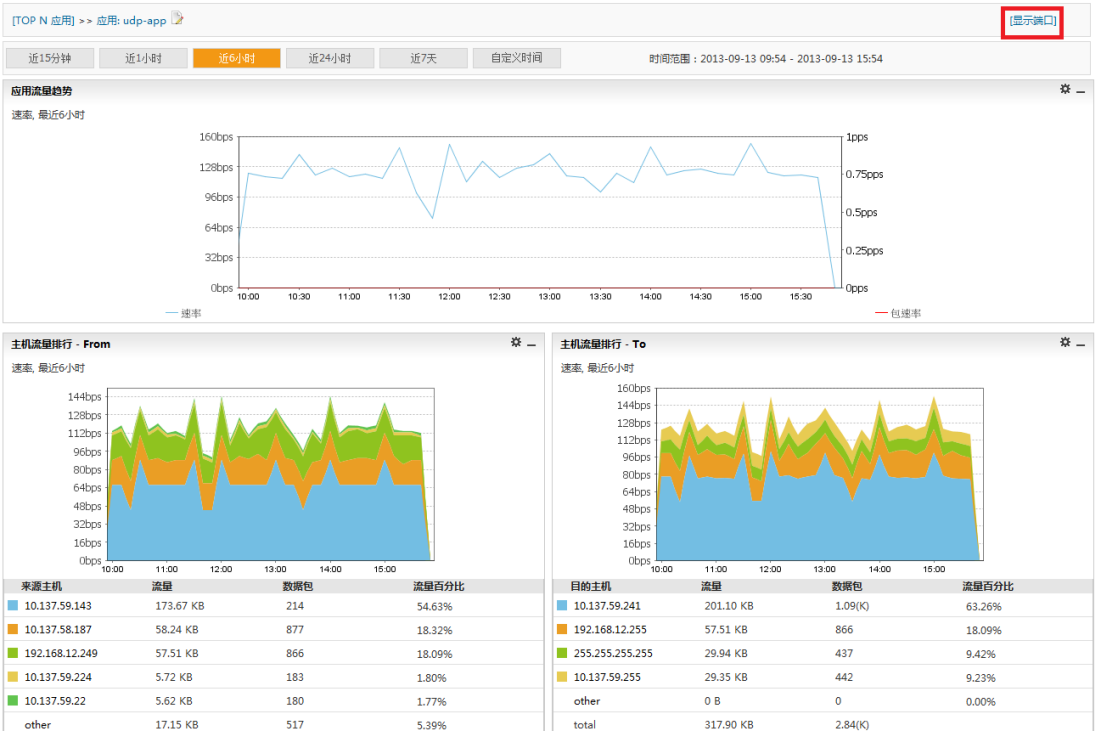
结合我司多年实际运维的经验和 IANA（Internet Assigned Numbers Authority）标准精选了 500 多种系统预定义的应用，包括常用的 SMTP、POP3、SNMP、FTP 等，同时系统提供了用户自定义应用的扩充能力。

管理员可以根据协议、端口和 IP 地址范围定义新的应用，如果出现某个应用使用的端口和 IANA 定义的端口冲突，可以使用 IP 范围来自定义应用，这样可以灵活地适应不同国家、地区和行业软件使用习惯不同的场景。比如某专业软件 XXX 使用 3306 端口，该端口是 MySQL 默认使用的端口。为了避免和 MySQL 冲突，管理员可以定义一个名为 XXX 的应用，同样占用 3306 端口，同时指定该专业软件使用的几个 IP 范围，表示这些 IP 范围内占用了 3306 端口的是 XXX 应用，就能保证系统正确识别该应用。应用定义同样适于异常流量、病毒识别的场景，比如臭名昭著的国产木马“冰河”占用的端口是 7626，管理员可以定义该端口的应用名为“冰河”。这样在应用流量报表中可以快速识别出这些病毒的流量。

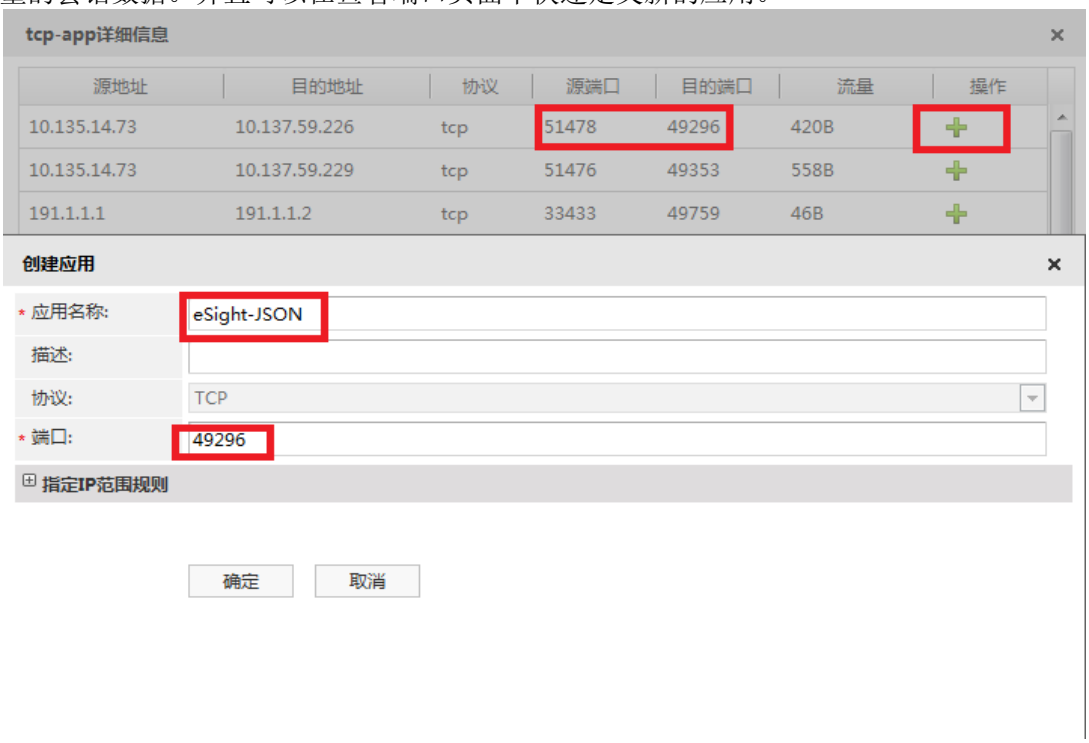


采集器接收到 NetStream 报文后，会根据报文中的协议、端口和 IP 地址等信息，使用哈希表快速匹配应用。系统优先匹配自定义应用，当未匹配到自定义应用时，再匹配预定义应用。如果都匹配失败，系统会按照协议类型将流量统计成 TCP-APP 和 UDP-APP，

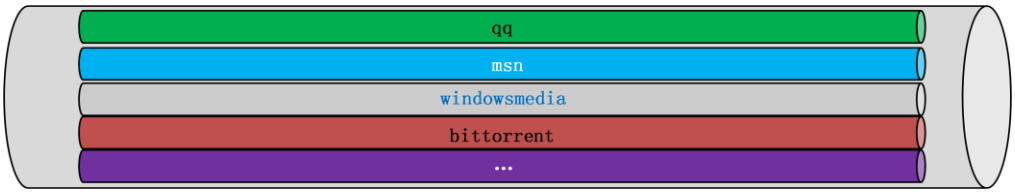
应用流量报表中可以详细显示这两个未知应用的协议、端口、流量等信息。并且支持查看详细的流量数据组成。



系统提供了查看端口的功能，管理员可查看 TCP-APP 中所有的端口以及各个端口上流量的会话数据。并且可以在查看端口页面中快速定义新的应用。



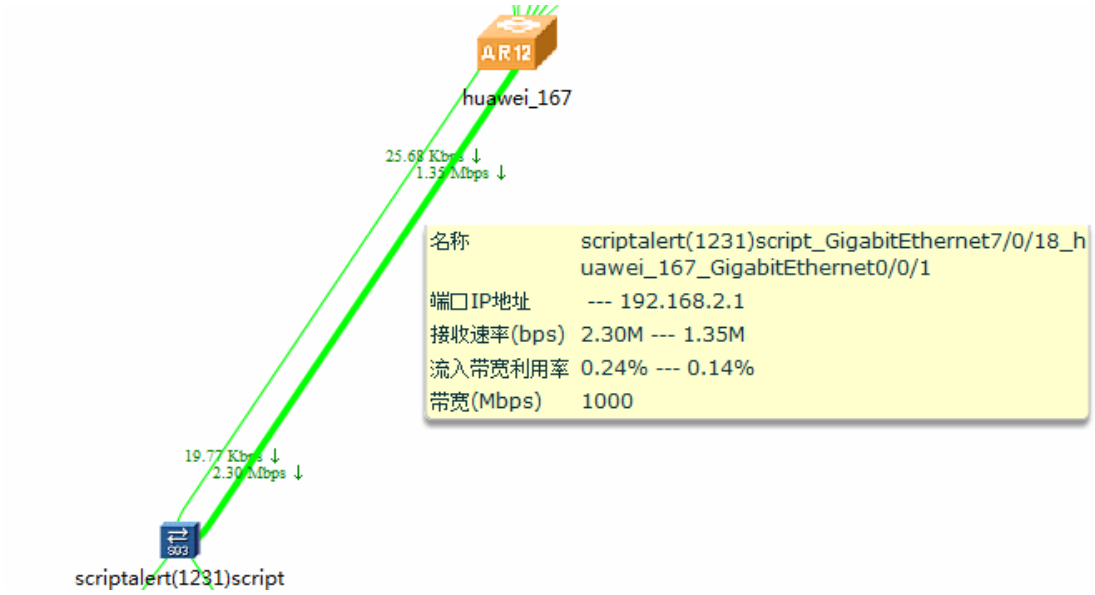
除以上自定义应用的能力， 对于来源目的 IP、端口经常动态变化的网络应用，配合华为 AR 路由器 V2R5 版本的业务感知（SA）能力，eSight 支持超过 60 种七层应用软件的流量，例如 qq、msn、bittorrent、emule、sqlserver、vahoomsg 等。



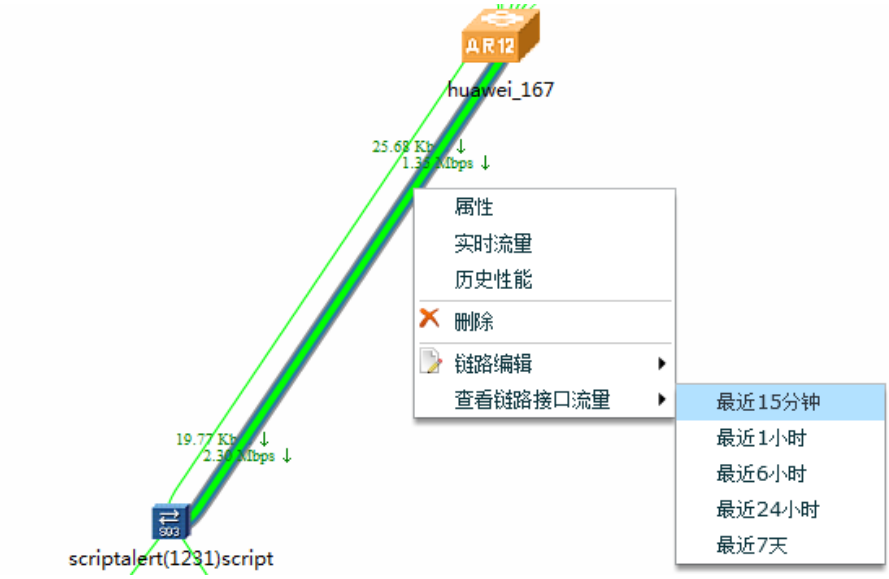
3.2.4 拓扑上查看流量组成

以拓扑图的方式直观显示被管网元及其之间的连接关系和状态，用户可以通过浏览拓扑视图把握全网设备的层次结构和运行状态，拓扑做为运维中心和运维的统一入口，常用的操作可在拓扑上完成。通过性能采集可在拓扑上直观的查看到关键链路流量的大小和带宽利用率，通过流量分析可查看关键链路详细的流量组成和流向，可查看链路上 TOPN 应用、TOPN 会话，以及各个应用正在被哪些主机使用，方便用户在拓扑上完成网络故障的定位。

比如，网络管理员接收到设备接口流量超高告警通知邮件，在拓扑上可查看当前链路上流量的大小和带宽利用率。

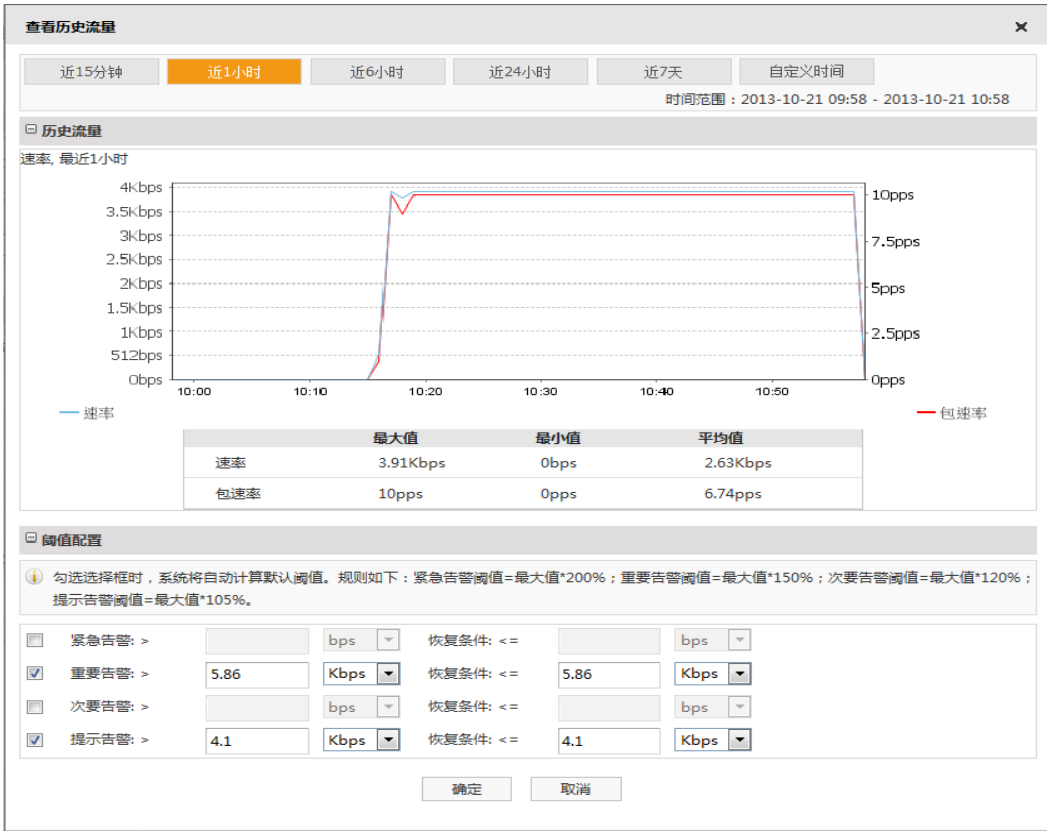


平常流量都在 1M 左右的链路，下行流量达到了 2.3M，可在链路上查看最近 15 分钟、最近 1 小时、最近 6 小时等不同时间段流量的详细组成。查看流量详细信息可参考 3.2.2 对层次流量分析章节。通过对链路流量的详细分析，即可快速定位到造成流量偏高的应用、主机、会话信息。管理员可根据这些信息制定合理的策略来保证链路正常运行。



3.2.5 流量阈值告警

用户可自主选择监控对象设定阈值、定义告警级别，当监控对象的流量超过阈值时将产生告警，并发送邮件或短消息通知用户。配置阈值可参考最近的流量趋势，系统将根据经验公式自动计算推荐的阈值，如紧急告警阈值=最大值*200%，重要告警阈值=最大值*150%，次要告警阈值=最大值*120%，提示告警阈值=最大值*105%。用户也可以自定义阈值的大小。



网络流量告警的产生和清除都遵守一定的规则，以默认的触发告警条件为例：每分钟检测一次流量，最近 10 分钟内 3 次超过阈值则上报告警，计数清零；告警产生后，最近 10 分钟内 3 次满足恢复条件，告警将自动清除。

3.2.6 数据聚合模型

网流采集器需要处理高达上万 Flows/秒的不同协议的数据报文，如何处理原始报文，建立灵活的数据模型，提升流量统计数据准确性，成为本系统面临的关键挑战。下面简要介绍 eSight NTA 网流分析组件数据处理过程。

原始网流报文被网流采集器（NTC）接收之后，将从接口、应用、会话、DSCP 等维度进行原始报文 1 分钟粒度数据聚合处理，然后将聚合结果数据发送到网络管理控制台（NMC），进行多维度多级聚合处理，系统建立 10 分钟、1 小时、6 小时、1 天、1 周等粒度的聚合任务，聚合任务会定时将数据入库保存，不同纬度的数据提供不同的存储策略，同时这些数据还可从数据库中转储成数据文件后永久保存下来。

详细的汇聚规则如下：

汇聚粒度	汇聚执行周期	汇聚基础数据	数据保存时间
分钟数据	每分钟执行	原始数据	1 天
10 分钟数据	每 10 分钟执行	分钟数据	10 天
小时数据	每小时执行	10 分钟数据	1 月
6 小时数据	每 6 小时执行	小时数据	3 月
天数据	每天执行	6 小时数据	1 年
周数据	每周执行	天数据	3 年

3.3 功能约束

3.3.1 适用设备类型约束

网流协议	设备厂商	设备列表
NetStream	Huawei	AR150/AR200/AR1200/AR2200/AR3200 NE80/NE40/NE40E/NE40E-X3 NE20/NE20E-8/NE20E-X6 S7700/S9300/S9700 CE5800/CE6800/CE12800(详细版本参见版本配套表)
NetFlow	Cisco	支持 NetFlow V5、V9 的设备。如：CISCO 6500/7600 系列；
sFlow	HP	支持 sFlow V5 的设备，如 S7500E,S9500E, MSR20 系列；

备注：Netstream/NetFlow 支持 V5、V9 版本，sFlow 支持 V5 版本。

3.3.2 适用场景约束

网流协议	设备厂商	场景约束
NetStream	Huawei	1、 NE40 设备有部分板卡不支持 NetStream，可根据设备版本在 3MS 上查看规格清单； 2、 S7700/S9300/S9700 设备目前 E 系列单板支持随板 NetStream，推荐使用 SPU 板来进行 NetStream 采集。 3、 CE5800/CE6800/CE12800 系列交换机在 V1R2 版本才支持 NetStream。

3.4 典型应用

为了全面了解网络流量的分布以及变化趋势，实现网络流量可视化，管理人员需要解决"4W"(Who/What/When/Where)问题。 eSight NTA 主要协助网络管理员解决如下问题：

哪个主机产生了大量的流量？

哪个应用程序消耗了大部分网络流量？

哪个区域的网络拥塞?

有多少流量是跨越广域网的？

过去一段时间内的 Top N 应用是什么？

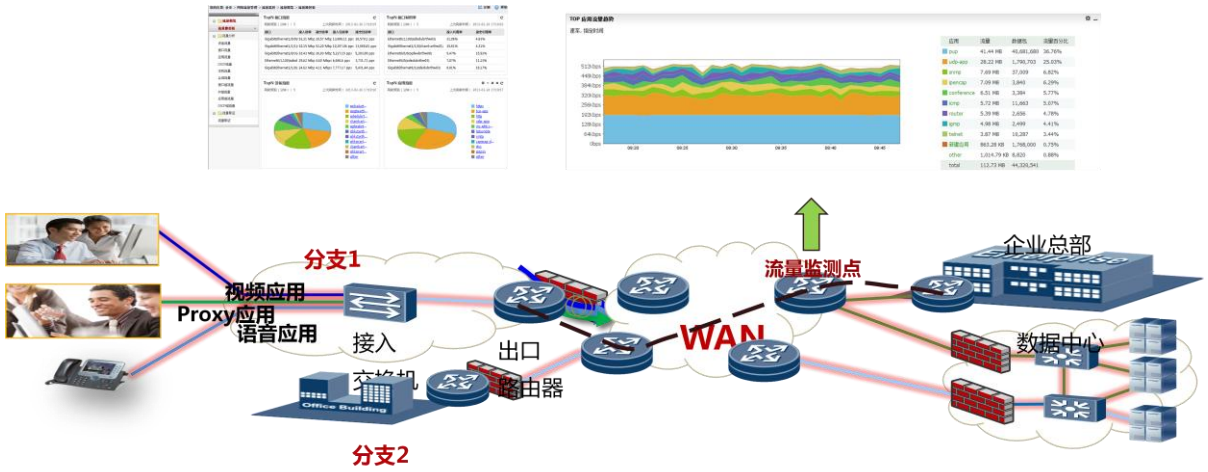
企业的关键业务是否分配了合理的带宽？

分支机构的带宽是否得到了有效的利用？是否需要扩容？

在网络的接入层、汇聚层、核心层的网络设备上，都可以根据不同需求来开启 NetStream 流量统计，完成全网流量的统计分析。

部署位置	应用场景
接入层	应用监控、异常检测
汇聚层	流量分析，应用监控
核心层	流量分析、网络容量规划

3.4.1 广域链路流量分析



对于大部分企业来说，局域网的带宽都是有保证的，网络瓶颈一般都出现在广域网或者连接 Internet 的出口设备上，如上图跨广域、有多个企业分支机构的网络，网络管理员需要解决有限的带宽上如何确保企业众多业务能稳定运行，特别是关键业务需要有足够的带宽保证。从管理员的角度，可以把广域上的流量分为三类：

- 合理流量：企业正常业务流量，比如企业内部的数据中心访问，ERP 系统使用，正常的会议电话等，这部分业务需要有足够的带宽保证；
- 垃圾流量：管理员不希望看到的流量，比如在线视频、游戏、炒股、访问娱乐网站等，这部分流量需要识别出那些人在使用，尽量通过 ACL、QOS 进行限制。
- 不合理流量：合理的流量出现不合适的时间、不合适的网络状况下。比如企业的一些备份业务出现在会议高峰时间，识别这部分流量可以提示用户避开高峰时间进行备份，同时可对这部分进行限速。

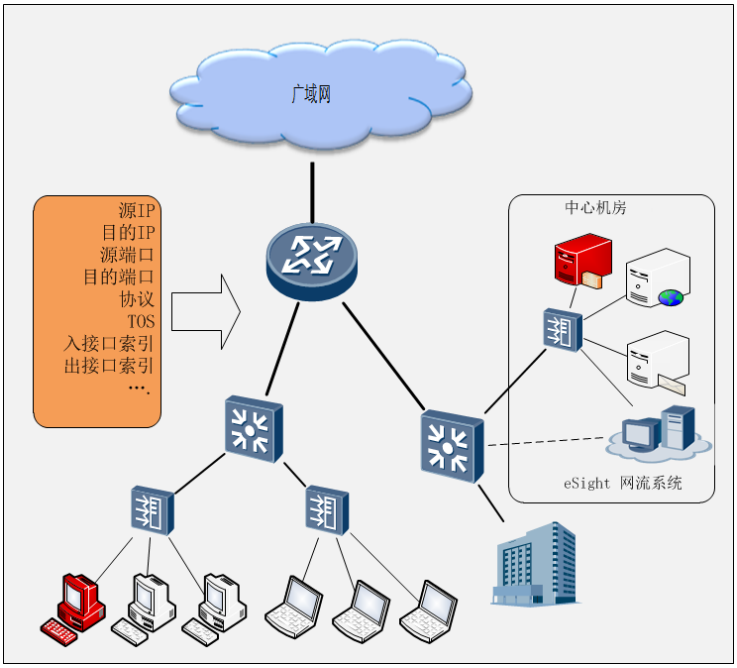
流量监控可部署在广域出口路由器上，通过监控广域链路，eSight NTA 提供详细的流量报表，提供各类业务流量分布和流向，及时全面了解各类业务流量的分布，识别出垃圾流量和不合理流量，确保合理流量有足够的带宽保证，充分利用宝贵的广域带宽资源。

eSight 上操作如下：

1. 自定义应用（协议+端口+IP 范围），可以创建一个应用组存放所有垃圾应用。

2. 打开设备/接口流量分析界面，查看应用流量，是否有垃圾应用占用带宽，分析限制策略
3. 查看垃圾应用的主机排行，整理对应主机 IP，能够发现哪些 IP 地址在访问垃圾应用。

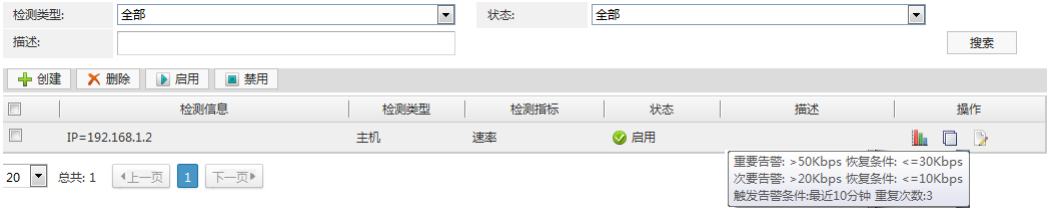
3.4.2 应用流量异常分析



在企业的日常运维中，关键应用的正常访问是企业运维的基本要求。通过查看各个应用服务器的流量详细分布，有助于提前发现网络风险，保障业务系统稳定运行。

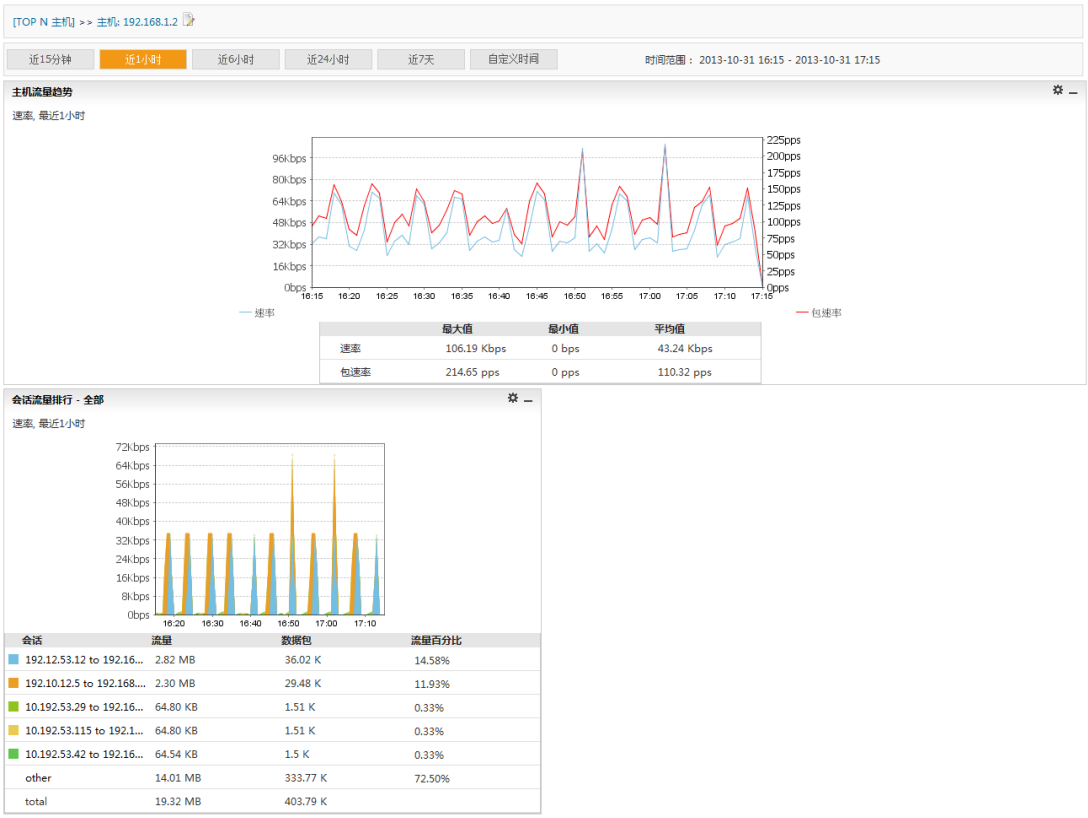
如上图所示，在连接中心机房的网络设备上启用 NetStream，监控分析所有进出中心机房的流量。通过 eSight NTA，可检测到发生故障的服务器，并协助用户定位造成故障的原因。

1、 将应用服务器的IP地址作为检测对象创建阈值告警配置，并设定告警级别和阈值。



2、若流量发生异常，在当前告警中可查看到该主机上报的网络流量告警。

3、通过告警中提供的流量分析链接，可查看该主机的详细流量组成，主要的流量集中在几个会话之间。



4、查看会话的详细数据，如果每条记录流量和包数都相同，可能存在异常攻击，创建流量取证任务，查看详细原始流信息，根据端口和 tcp_flag 信息判断是否存在典型病毒或者 TCP Flood 攻击。

时间	路由器地址	入接口	出接口	源地址	源端口	目的地址	目的端口	TCP标志	下一跳	协议	应用	DSCP	流量(Bytes)	数据包
2013-08-29 19:27:04	10.137.59.167	GigabitEthernet0/0/0	GigabitEthernet0/0/1	192.12.53.12	3306	192.168.3.3	3306	------	0.0.0.0	tcp	mysql	CS3	590.32KB	773
2013-08-29 19:27:32	10.137.59.167	GigabitEthernet0/0/1	GigabitEthernet0/0/0	192.12.53.12	3	192.168.1.2	3	-A--S-	192.168.1.1	tcp	tcp-app	CS3	696.24KB	1225
2013-08-29 19:28:06	10.137.59.167	GigabitEthernet0/0/0	GigabitEthernet0/0/1	192.12.53.12	3306	192.168.3.3	3306	------	0.0.0.0	tcp	mysql	CS3	591.08KB	774
2013-08-29 19:28:33	10.137.59.167	GigabitEthernet0/0/1	GigabitEthernet0/0/0	192.12.53.12	3	192.168.1.2	3	-A--S-	192.168.1.1	tcp	tcp-app	CS3	696.81KB	1226
2013-08-29 19:29:07	10.137.59.167	GigabitEthernet0/0/0	GigabitEthernet0/0/1	192.12.53.12	3306	192.168.3.3	3306	------	0.0.0.0	tcp	mysql	CS3	590.32KB	773
2013-08-29 19:29:34	10.137.59.167	GigabitEthernet0/0/1	GigabitEthernet0/0/0	192.12.53.12	3	192.168.1.2	3	-A--S-	192.168.1.1	tcp	tcp-app	CS3	696.24KB	1225
2013-08-29 19:30:08	10.137.59.167	GigabitEthernet0/0/0	GigabitEthernet0/0/1	192.12.53.12	3306	192.168.3.3	3306	------	0.0.0.0	tcp	mysql	CS3	591.08KB	774
2013-08-29 19:30:36	10.137.59.167	GigabitEthernet0/0/1	GigabitEthernet0/0/0	192.12.53.12	3	192.168.1.2	3	-A--S-	192.168.1.1	tcp	tcp-app	CS3	696.81KB	1226
2013-08-29 19:31:10	10.137.59.167	GigabitEthernet0/0/0	GigabitEthernet0/0/1	192.12.53.12	3306	192.168.3.3	3306	------	0.0.0.0	tcp	mysql	CS3	590.32KB	773
2013-08-29 19:31:37	10.137.59.167	GigabitEthernet0/0/1	GigabitEthernet0/0/0	192.12.53.12	3	192.168.1.2	3	-A--S-	192.168.1.1	tcp	tcp-app	CS3	696.24KB	1225
2013-08-29 19:32:11	10.137.59.167	GigabitEthernet0/0/0	GigabitEthernet0/0/1	192.12.53.12	3306	192.168.3.3	3306	------	0.0.0.0	tcp	mysql	CS3	591.08KB	774
2013-08-29 19:32:38	10.137.59.167	GigabitEthernet0/0/1	GigabitEthernet0/0/0	192.12.53.12	3	192.168.1.2	3	-A--S-	192.168.1.1	tcp	tcp-app	CS3	696.81KB	1226
2013-08-29 19:33:12	10.137.59.167	GigabitEthernet0/0/0	GigabitEthernet0/0/1	192.12.53.12	3306	192.168.3.3	3306	------	0.0.0.0	tcp	mysql	CS3	590.32KB	773
2013-08-29 19:33:39	10.137.59.167	GigabitEthernet0/0/1	GigabitEthernet0/0/0	192.12.53.12	3	192.168.1.2	3	-A--S-	192.168.1.1	tcp	tcp-app	CS3	696.24KB	1225
2013-08-29 19:34:13	10.137.59.167	GigabitEthernet0/0/0	GigabitEthernet0/0/1	192.12.53.12	3306	192.168.3.3	3306	------	0.0.0.0	tcp	mysql	CS3	590.32KB	773
2013-08-29 19:34:41	10.137.59.167	GigabitEthernet0/0/1	GigabitEthernet0/0/0	192.12.53.12	3	192.168.1.2	3	-A--S-	192.168.1.1	tcp	tcp-app	CS3	696.81KB	1226

如果原始报文中存在大量的 TCP_SYN 标志，并且数据包和流量大小都是固定的，说明该服务器极有可能是遭受了 TCP_SYN 的攻击

3.4.3 网络容量规划

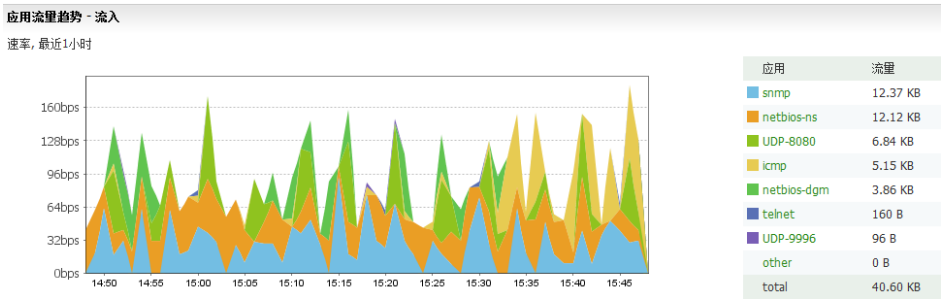
随着企业规模的不断壮大，企业应用的不断丰富，网络扩容成为 IT 工程师无法绕开的话题，但是盲目的扩容可能无法从根本上解决问题，昂贵的带宽扩容后还是无法满足日益增长的带宽需求。

网络扩容重点关注以下两个方面：一方面需要了解现有的网络规划配置是否合理，各个业务带宽分配是否合理，在不增加带宽的情况下是否可以完成优化；另一方面需要关注过去各个业务变化的趋势，比如，某条链路每个月增加的幅度，某个应用过去每个月增长的趋势。掌握了以上两方面的信息，网络管理员可合理的完成容量规划。

在 eSight NTA 上可以通过报表来查看长期的流量数据，可以查看每个月关键链路的上各个业务流量的分布，查看关键业务所分配的带宽是否合理，是否有非关键业务占用大量带宽，根据各个应用流量分布重新分配各个业务的带宽。

也可创建周期报表来观测每个周期内应用流量的增长情况，在带宽分配合理的情况下，链路的带宽利用率持续升高，就需要根据流量增长的趋势进行带宽扩容，可选择查看链路、应用、DSCP 等维度的流量定义报表，通过每个周期报表数据的对比可看出流量增长的趋势和幅度。

查看应用流量分布



4 结论

eSight NTA 网流分析组件主要特点：

- 全面支持 NetStream/NetFlow/sFlow 主流协议，全面的设备支持，保护客户投资。
- 网络流量概览，使得网络状态一览无余：基于 Portal 规范的操控板。
- 自定义应用以及多种分组，方便网络管理人员获得更多量身定做的流量统计结果。
- 全方位的网络流量分析，简化网络管理员进行网流监控的操作。
- 可定制的流量报表：五步法定制报表，可指定过滤规则、报表类型以及报表布局等。
- 流量取证：根据给定时间段和过滤条件，提取原始数据流，深入故障定位。

综上可见，eSight NTA 网流分析组件可以帮助客户实现流量可视、异常可查和规划可依，为企业网络的长期健康高效运行保驾护航，是企业网络的真正守护者。

5 缩略语表

缩略语	英文全名	中文解释
NetStream	NetStream	Huawei 公司开发的流协议，提供报文统计功能，它根据七元组：目的 IP 地址、源 IP 地址、目的端口号、源端口号、协议号、ToS、输入/输出接口来区分流，并针对不同的流进行独立的数据统计。
NetFlow	NetFlow	NetFlow 是由思科公司开发的一种专有技术，它被应用在思科的互联网操作系统（IOS）中，基于七元组来统计通过交换机的交通流量。
sFlow	Sampled Flow	采样流,是一种基于报文采样的网络流量监控技术，主要用于对网络流量进行统计分析。
NTA	Network Traffic Analyzer	网络流量分析组件
NDE	Network Data Exporter	网络流量输出器
NTC	Network Traffic Collector	网络流量采集器
NMC	Network Management Console	网络管理控制台
DSCP	Differentiate Services Code Point	差分服务代码点