

Mocha Network Traffic Analyzer Product

White Paper

摩卡网络流量分析产品白皮书



目 录

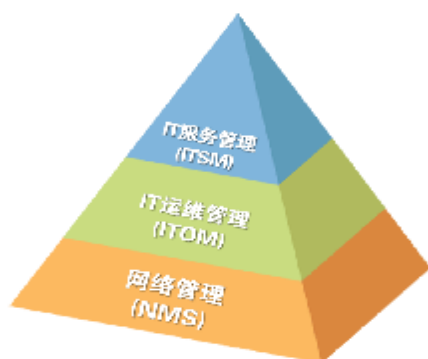
1	Mocha BSM 4+1 介绍	1
1.1	三位一体的产品定位.....	1
1.2	Mocha BSM 4+1, 做得更多.....	1
2	用户面临的挑战	2
3	摩卡网络流量产品概述	2
3.1	产品定位.....	2
3.2	产品架构.....	3
4	系统亮点	3
5	带给客户的价值和收益	4
6	系统运行环境	6
6.1	服务器.....	6
6.2	数据库.....	6
6.3	客户端.....	6
7	联系我们	6

1 Mocha BSM 4+1 介绍

1.1 三位一体的产品定位

摩卡软件是亚太区率先推出三位一体产品定位的软件提供商之一，三个定位包括了：

- n **网络管理 (Network Management System)**— 传统意义上的网络、系统、应用监控，满足了成长中企业的需要；
- n **IT 运维管理(IT Operation Management)**— 把监控上升至管理的层面，帮助企业规划、运维和改进 IT 系统。通过端到端的监控，帮助中大型企业管理 IT 系统；
- n **IT 服务管理(IT Service Management)**— 基于 ITIL 流程框架，带领企业进入流程化，规范化和自动化的时代。



三位一体的解决方案

1.2 Mocha BSM 4+1，做得更多

为了满足三位一体的定位，摩卡软件推出了 Mocha BSM 4+1 产品套装。

Mocha BSM 4+1 涵盖了以下几方面：

- 🔍: **基础架构管理** — 网络拓扑、主机、流量分析、IT 资产；
- 🔍: **应用管理** — 应用服务器、数据库、Web 服务器等；

🔍: **端到端响应时间管理** — 应用响应时间管理，端到端监控；

🔍: **业务服务管理** — 以业务视角看待 IT；

🔍: **IT 运维管理** — 基于 ITIL 流程框架，满足对事故管理、问题管理、性能管理、变更管理、配置管理、发布管理、知识库等需求。



Mocha BSM 解决企业 4+1 方面的问题

整个套装包括了：

- n 以服务的视角看待 IT，提供以服务为导向的监控 — 摩卡业务服务管理 Mocha BSM(Business Service Management)
- n 完整的 IT 资产生命周期 — 摩卡 IT 资产管理 Mocha ITAM(IT Asset Management)
- n 帮助企业找出网络带宽的瓶颈 — 摩卡流量分析 Mocha NTA(Network Traffic Analyzer)
- n 基于 ITIL 流程框架，以服务台为中心，提供流程式管理 — 摩卡 IT 运维管理 Mocha ITOM(IT Operations Management)
- n 提供端到端监控 — 摩卡端到端监控管理(Mocha E2E(End To End)Monitoring)

2 用户面临的挑战

企业的网络规模在扩大，同时企业的业务在激增，企业需要知道整个网络的承载能力已经是否能够支撑现有业务应用系统？经过归纳，企业关心的无非是如下所述的“4W”：

n Who?

到底是谁(用户)或者应用在使用网络带宽？

n What?

什么样的业务和应用占据了企业的大部分带宽？到底是怎样的网络协议在网络中运行？

n When?

在什么样的时段，企业的业务是处于最高峰的？整个网络是否能承载现有的业务？

n Where?

如果网络出现问题，到底是哪里出现了问题？什么样的业务受到的危害最大？

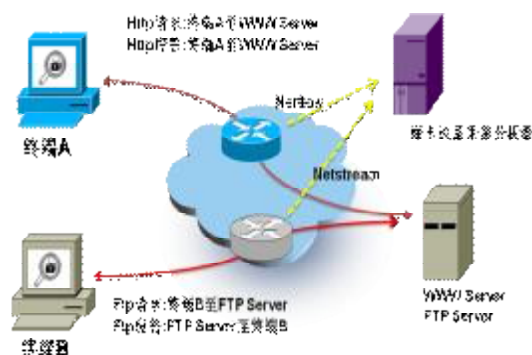
摩卡网络流量分析针对以上“4W”问题，为企业分析网络承载力和业务应用的复杂关系，提供依据和分析结果。

3 摩卡网络流量产品概述

3.1 产品定位

为了满足企业的业务需求，网络接口带宽速率经历了十兆、百兆、千兆和万兆的过程，如果仅靠传统的手段，对流经网络设备的海量数据都进行统计，已成为不可能，通过何种手段才能监控企业的网络流量，并加以分析，才能达到优化网络，优化业务的效果呢？

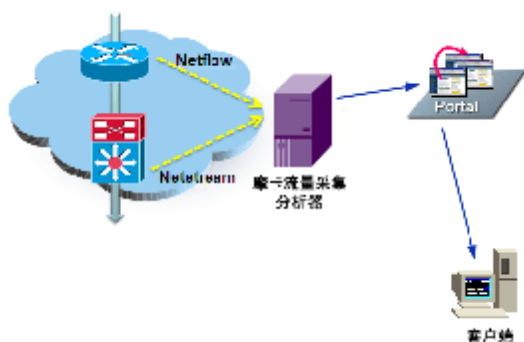
如下图所示，摩卡网络流量分析(Mocha Network Traffic Analyzer)产品，它是摩卡软件有限公司(Mocha Software Co., Ltd.)针对各行业企业的网络系统，通过支持各种厂家的流量统计协议，并获取核心网络设备流量分析协议包，分析和统计网络的真实流量，以及对网络流量中的协议进行分析，来达到监控网络流量的目的。



图表 1：摩卡网络流量分析说明

如今市面上各种厂家的网络设备层出不穷，而各个厂家所支持的流量分析协议也各不相同。摩卡网络流量分析产品通过长期积累，是少数支持所有主流厂家网络流量分析协议，并且满足企业不同网络流量分析管理需要的管理软件。

3.2 产品架构



图表 2: 摩卡网络流量分析产品架构图

从上图，我们可以看到流量分析管理软件的架构非常易于部署，只需要在企业内部网络中部署一台摩卡流量采集分析器，然后将所有网络设备的流量分析包发送到摩卡流量采集分析器即可。摩卡流量采集分析器既可以和 Mocha BSM (Business Service Management) 在一台物理机器上，也可以分别部署在两台不同的物理机器上。最终网络管理人员可以通过任何一台终端，由浏览器访问到流量分析结果。快速发现网络中的流量异常，并加以处理。

4 系统亮点

n 低廉的全网流量监控成本，并持多层次的流量监控

不需要增加任何特有的流量分析监控板卡，或开启端口镜像功能，将所有真实流量复制到流量分析板上，不需要改变网络拓扑的情况下就能实现网络流量统计，只需要部署一台网络流量分析器，通过与不同层次网络设备的配合，支持对广域网核心层、广域网出口、局域网核心层、局域网汇聚层网络流量的监控与分析，实现整网流量多点的可视性。是一种低成本、高性价比、部署灵活的流量分析方案，同时不会给网络自身和流量分析服务器造成太大压力。

n 少数兼容所有主流网络设备

支持各种不同网络流量采集协议，包括 **Netflow**、**Netstream**、**Sflow**、**Cflow**、**IPFIX** 等各厂家协议标准；无论是哪种 Flow 格式，都定义了数据交互的标准格式，摩卡能够通过这些格式规范支持业内几乎所有的主流网络设备，如 Cisco、Foundry、Extreme、Juniper、华为、H3C 等，保证了对采集目标设备流量良好的兼容性。企业用户不必再担心为了不同厂家的设备，分别购买不同厂家的流量分析模块。

n 对各种应用的广泛支持

基于三层协议号、端口号，可识别上千种已知应用（比如：HTTP 应用、FTP 应用、MAIL 应用、P2P 等等），并提供应用自定义功能，当网内出现新应用的时候，很容易进行新应用的识别，方便管理人员从业务的角度对网络流量进行分析。

n 简单易用的专家级分析报表：

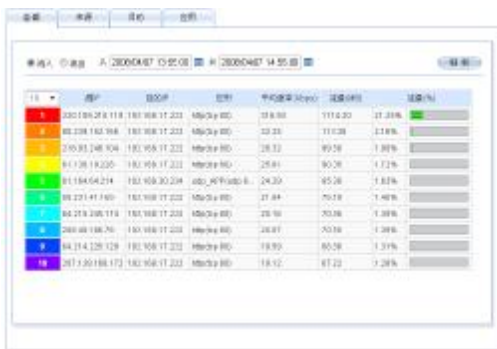
提供业界最流行的报表展示形式，如叠加图、二维饼图、三维饼图等，报表界面简单易用，并从多个分析的角度将分析内容进行了整合，使用户更快速的得到所需要的分析结果。从会话报表中点击协议，可以直接跳转至应用报表。而从应用报表点击源地址或者目的地址，也可以直接跳转至会话报表，方便管理人员进行流量分析。

5 带给客户的价值和收益

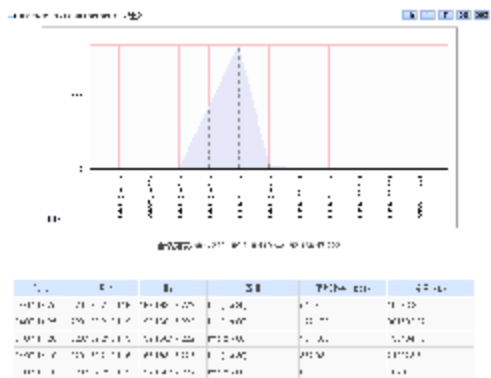
我们帮助企业彻底解决‘4W’问题，将网络流量彻底透明化,管理人员能够随时了解到谁在使用网络(Who)? 什么样的应用和协议在网络中传输(What)? 什么时候网络处于最忙的时候(When)? 到底哪里网络存在问题, 问题在什么地方(Where)? 在了解了企业网络流量的‘4W’问题, 企业 IT 管理者才能够更好的对网络和业务进行优化。下面将详细说明我们带给客户的价值和收益:

n 谁正在使用网络(Who)?

通过流量分析帮助管理人员了解到网络中哪个用户正在大量的下载或者上传数据, 或者网络的 HTTP 服务器正在被大量的用户访问? 如下图所示, 通过监控某个网络设备的端口会话情况, 我们可以很清楚的看到, 到底谁正在用何种方式访问网络?



图表 3: 分析网络内的某个端口的所有会话的流量
同时再点击某个会话后, 我们还可以看到该会话在不同时段的数据流量情况。



图表 4: 分析网络内的某个端口的某个会话的具体流量情况

n 什么样的应用和协议在网络中传输(What)?

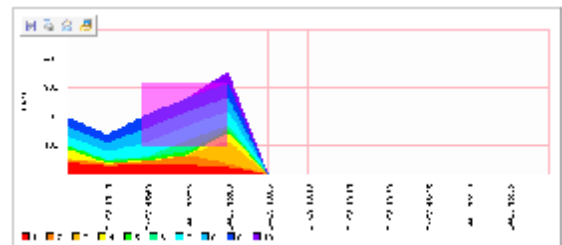
通过流量分析管理, 可以使网络管理人员快速掌握网络负载状况, 网内应用及不同业务使用情况, 在 5 分钟内即可发现网络结构的不合理, 或是网络性能瓶颈, 尽快制定网络优化方案, 使网络带宽分配最优化, 为用户提供高品质的网络服务, 并且避免了网络带宽和服务器瓶颈问题。同时有助于网络管理员跟踪和预测网络链路流量的增长, 从而能有效的规划网络升级(例如, 增加路由设备、端口或使用更高带宽的接口)。



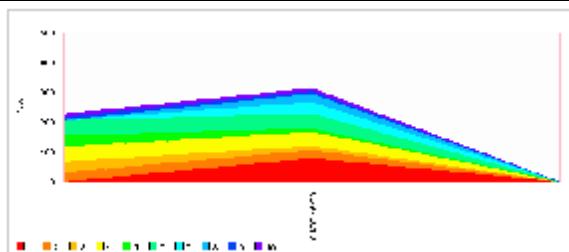
图表 5: 分析网络内的各种应用所占的带宽比率

n 什么时候网络处于最忙的时候(When)?

通过流量分析管理, 可以使网络管理人员快速掌握网络负载状况, 网内应用及不同业务使用情况, 在 5 分钟内即可发现网络结构的不合理。管理人员通过手工拖选时间段, 快速展示某个时间段内的流量概况, 帮助管理人员分析网络流量异常:



图表 6: 在数据流量分析图表中直接用鼠标选中一段时间轴



最主要的带宽。

应用名称	平均速率 (Kbps)	流量占比	流量 (M)
http	68.85	52.35%	52.35%
ftp_app	19.41	14.87%	14.87%
ftp	12.30	9.38%	9.38%
telnet	7.68	5.86%	5.86%
smtp	5.91	4.51%	4.51%
ftp_app	3.81	2.90%	2.90%
ftp_app	0.37	0.28%	0.28%
smtp	0.24	0.18%	0.18%
ssh	0.11	0.08%	0.08%
ssh	0.08	0.06%	0.06%

应用名称	平均速率 (Kbps)	流量占比	流量 (M)
http	68.85	52.35%	52.35%
ftp_app	19.41	14.87%	14.87%
ftp	12.30	9.38%	9.38%
telnet	7.68	5.86%	5.86%
smtp	5.91	4.51%	4.51%
ftp_app	3.81	2.90%	2.90%
ftp_app	0.37	0.28%	0.28%
smtp	0.24	0.18%	0.18%
ssh	0.11	0.08%	0.08%
ssh	0.08	0.06%	0.06%

图表 7: 展示选定时间段内的会话和应用所占流量

上图为在用户选定的时间轴内，网络管理人员可以通过查看会话，了解到在该时段内，网内或者网外哪些 IP 所占的流量最高；也可以通过查看应用，快速得知该时间段内，哪些业务和应用占用了大量的带宽。做到真正帮助管理员快速发现问题，分析网络流量异常数据。

n 到底哪里的网络存在问题，问题在什么地方 (Where)?

对于一个企业来说，网络环境非常复杂，企业有广域网、局域网、Internet 出口等，尤其是广域网和 Internet 出口的带宽通常是有限的，一旦有异常数据产生，将会对企业的网络产生非常严重的影响。如下图所示，我们可以通过应用排行，分析出 HTTP 应用占据了某企业的 Internet 出口的主要带宽；

应用名称	平均速率 (Kbps)	流量占比	流量 (M)
http	1992.04	547.71%	54.38%
ftp_app	38.15	10.22%	2.32%
smtp	28.51	7.81%	1.68%
telnet	13.28	3.61%	0.78%
ftp_app	3.92	1.06%	0.23%
ftp_app	3.88	1.05%	0.23%
ssh	0.78	0.21%	0.05%
pop3	0.68	0.18%	0.04%
ssh	0.28	0.07%	0.01%
ssh	0.18	0.05%	0.01%

我们通过点击该应用后，弹出的分析框，可以很清楚的的分析出，到底哪一点到哪一点的访问占据了网络中

因此，我们帮助企业能掌握网络中流量的特征，制定相应的策略(比如QoS和针对源或目的IP地址作流限制)，就能使广域网、Internet出口的带宽得到最合理最充分的使用，避免进行不必要的升级投资，而摩卡网络流量分析所提供的分析结果能够使网络管理员洞察广域网链路的流量特征、承载的应用、用户使用状况，从而针对是否应投资升级带宽，而快速的做出决断！

6 系统运行环境

6.1 服务器

- n 服务器:PC Intel PIII600 以上服务器
- n 内存:1GB 以上
- n 磁盘空间:10GB 以上
- n 操作系统支持:
 - n Windows 2000\2003\NT4.0
 - n Sun Solaris V8\9
 - n IBM AIX 5.0 以上版本, iSeries 模式
 - n Linux (Redhat AS3\4)
 - n HP-UX 11i

6.2 数据库

- n Oracle, Versions 8i, 9i, 9i Release 2 and 10g
- n Mysql 4, 5

6.3 客户端

- n PIII 以上计算机, 128MB 内存
- n IE 5.5 或更高版本

7 联系我们

摩卡软件有限公司

地址: 北京西城区宣武门西大街 127 号大成大厦 15 层

联系电话: 400 611 5522

传真: (8622)87341661

网址: <http://www.mochabsm.com>

电子邮件: Marketing@mochasoft.com.cn