Hillstone下一代智能防火墙技术白皮书之增强的智能流量管理(iQoS)篇

关键词：Hillstone T系列、增强的智能流量管理（ iQoS）、管道、两层八级、差分服务、监控、剩余带宽分配。

摘要： 本文介绍Hillstone T系列下一代智能防火墙独创的具有专利技术的增强的智能流量管理（ iQoS）。iQoS是在传统QoS基础上增加了如下功能：两层八级的管道嵌套、管道监控、基于优先级进行差分服务及剩余带宽分配功能。用户通过对这些QoS技术的灵活运用，实现基于用户组织架构的流量控制，保障用户关键业务的顺畅进行并使带宽资源得以充分利用。

概述

随着信息技术的飞速发展，网络所承载的内容变得日益复杂与多元化，新应用类型日益增加、带宽出口瓶颈日益严峻。企事业单位多个分支机构与总部之间的流量也日益增多，面临从上到下的网络管理需求，多层级部门、区域之间超大文件的传输、各种内容的上传/下载等，不仅浪费组织机构宝贵的带宽资源，使关键业务应用访问迟缓，同时无形中增加了组织机构IT维护成本。传统的流控设备由于自身的限制无法满足用户众多需求，主要表现在:

- 无法对流量进行多层级灵活的流量管理，基于企业组织架构，对分公司、分公司下各部门，部门下各种应用，应用下每用户/IP做不同流量控制，这种具有包含关系的多级嵌套完全超出传统流控产品的范围
- 流量的划分不够精细，大部分QoS只能做到基于5元组的流量划分
- 缺乏QoS管理手段，缺少直观可视，简单易用的QoS呈现
- 优先级的处理效果有限，不能很好的保证关键业务优先调度处理
- 剩余带宽不能得到合理有效的利用

Hillstone T系列下一代智能防火墙独创的具有专利技术的增强的智能流量管理（iQoS），可以实现两层八级的管道嵌套以及更细粒度的流量控制，满足不同网络层次部署的需要，能够很好的解决传统QoS无法解决的问题。

Hillstone下一代智能防火墙独创的具有专利技术的增强的智能流量管理（iQoS），可以通过细粒度流量划分和两层八级QoS管道嵌套技术实现基于应用和用户的增强的智能流量管理；配置与呈现的统一，可达到即时的可视化配置调整，实时查看流量控制的效果；凭借基于优先级的分类，优先处理高优先级别的应用，实现灵活的带宽管理，对消耗大量带宽资源的应用，如P2P下载等进行限制，保障用户网络中关键业务的畅通，同时可以更充分的利用现有网络带宽，有效保护客户投资回报。

2.1 两层八级的应用流量控制

Hillstone增强的智能流量管理（iQoS）支持两层流控，每层流控支持四级嵌套，从而可实现两层八级的网络应用控制。

2.1.1 两层流控

当需要控制的流量没有包含关系，无法通过多层级嵌套解决的问题该如何处理呢？Hillstone增强的智能流量管理（iQoS）提供两层流量控制，可以从不同的维度进行流量控制，比如从用户、应用两个维度。举例说明：企业网络中要求限制财务总监流量带宽50Mbps，普通财务员工流量带宽30Mbps，但总的P2P下载带宽限制在30Mbps。

如果只有一层流控，要达到以上目的，一般的配置方法是：限制财务总监带宽50Mbps，再限制其P2P下载带宽到20Mbps； 限制普通员工带宽30Mbps，再限制其P2P下载带宽到10Mbps；最终达到限制总P2P下载带宽30Mbps；这种配置很不灵活，其实是通过分别限制财务总监和普通员工的P2P下载带宽达到限制总P2P下载带宽30Mbps的目的。

iQoS两层流控的做法是：第一层流控基于用户进行控制，即限制财务总监带宽50Mbps、普通财务员工带宽30Mbps，第二层流控基于P2P应用进行控制，即将总的P2P下载速率限制到30Mbps。这种处理很灵活，不需要分别限制财务总监和普通员工的P2P下载带宽，他们各自P2P的下载带宽不用设置成固定的值，经过第二层流控时很自然会将总的P2P下载速率限制到30Mbps。两层流控工作流程如下图：

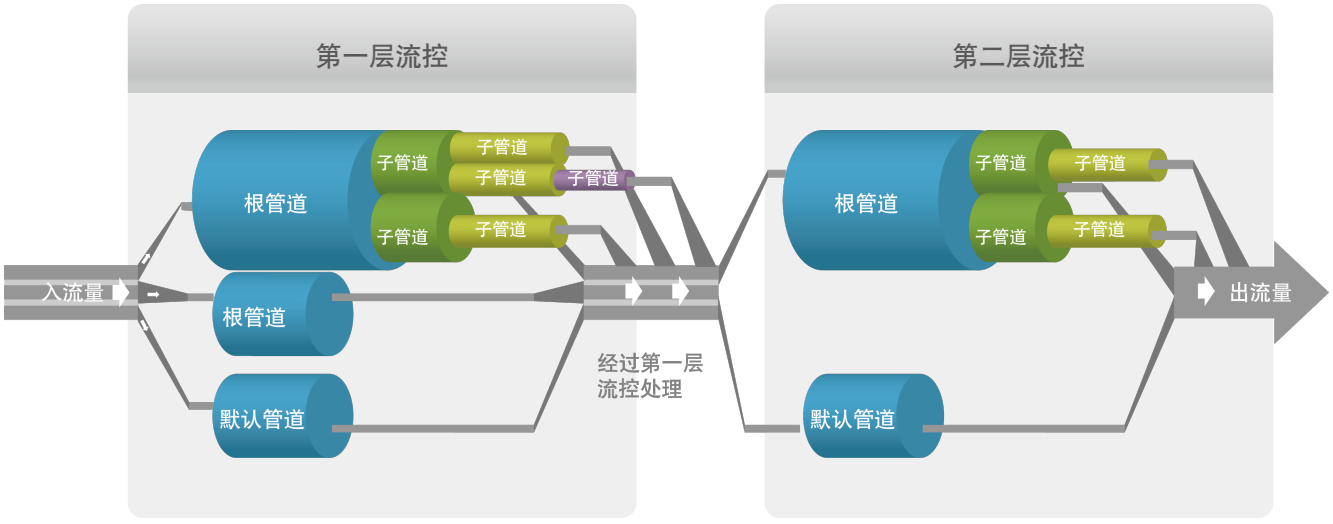

图1 两层流控工作流程示意图

2.1.2 单层四级嵌套

Hillstone增强的智能流量管理（iQoS）在每一层流控中，最多支持四级管道的嵌套。流量会按照匹配条件，逐级匹配管道；未匹配到任何管道的流量，则进入预定义的默认管道。每一级管道都有各自的匹配条件（rule）和流控动作，满足匹配条件的流量按照该管道配置的流控动作进行相应的流量控制。匹配条件（rule）包括源安全域、源接口、源地址条目、目的安全域、目的接口、目的地址条目、用户/用户组、服务/服务组、应用/应用组、TOS、Vlan，可以根据一种条件来划分流量，如根据源地址条目；也可以根据多种条件组合来划分流量，多种条件之间是”与”的关系，如根据源接口、目的地址条目和应用HTTP，即从指定的源接口到具体的目的地址的HTTP流量，这样能够更加精细的划分流量。并且每一级管道可以有多个匹配条件（rule），匹配到多条rule中的任意一条就能按照该管道配置的流控动作进行相应的流量控制。匹配条件（rule）如下图所示:

匹配条件

	源信息			目的信息			用户/用户组	服务/服务组	应用/应用组	VLAN	TOS
	安全域	接口	地址条目	安全域	接口	地址条目					
	-	-	ALL10...	-	-	Any	-	-	HTTP	-	-
	-	-	互联 IP	-	-	Any	-	-	HTTP	-	-

图2 管道匹配条件示意图

下面以某企业的应用场景为例说明如何嵌套多级管道，如下图所示：可以按照公司组织架构来划分管道，管理员可以先创建一个根管道，限制该企业北京分公司的流量，在该根管道下创建一个子管道，限制其研发部门的流量；然后再创建子管道对研发部的不同用户/IP进行不同的流量控制；最后为某用户/IP设置子管道，限制该用户/IP的不同应用带宽流量，管道逻辑关系如下图所示:

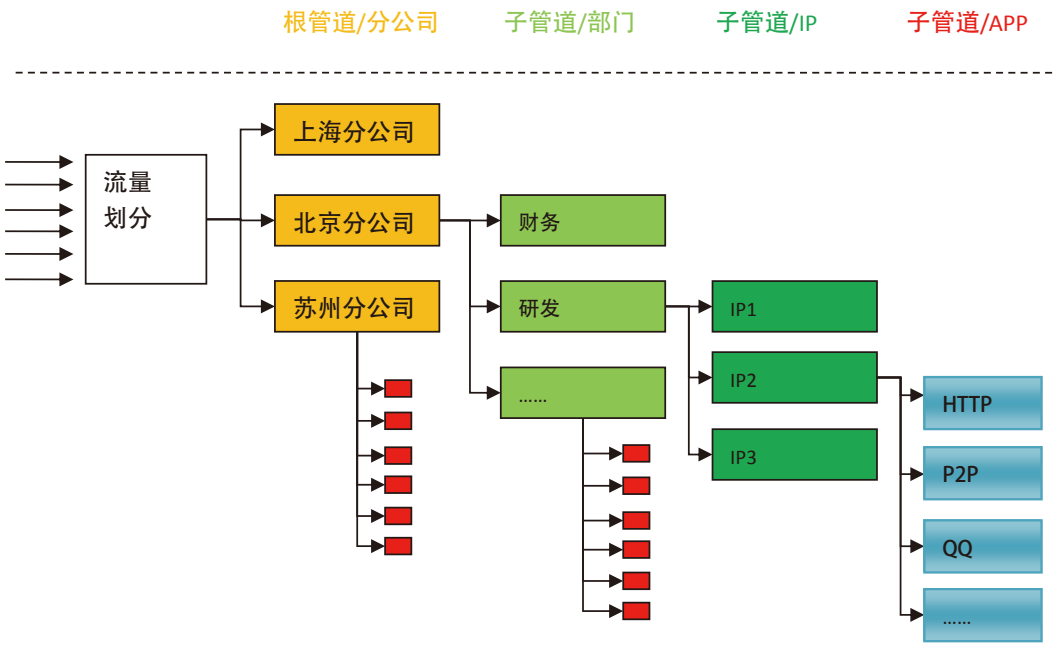

图3 管道逻辑关系示意图

2.1.3 流控动作

Hillstone 增强的智能流量管理（iQoS）能实现带宽限制、带宽保证等一系列流量控制动作:

- 最小带宽保证：为某些特定的应用或用户指定最小带宽保证
- 最大带宽限制：为某些特定的应用或用户指定最大带宽，限制非关键应用，保证关键应用的服务质量
- 支持正向、反向或双向的带宽管理与控制
- 到不同目的地址的流量采取不同的流量管理策略
- 针对P2P等特殊应用，可根据时段提供不同的带宽服务

2.2 管道监控

Hillstone T系列下一代智能防火墙除了能够提供基于应用与用户等传统的监控外，还能提供专门针对管道的监控，管道的配置与管道监控统一。管道监控提供第一层流控和第二层流控中各级管道的流量排名及百分比，且可通过管道状态、管道流量方向、时间粒度、排名个数，图表显示方式等过滤条件来查看各级管道的流量排名；还可进行各个管道流量及其丢弃流量的正、反向流量对比；此外，管道详细信息页面通过某管道的流量历史趋势及其丢弃流量历史趋势，呈现出该管道的相关用户、应用的流量排名情况。如下图:

某公司对不同分公司进行不同流量控制，管道配置如下:

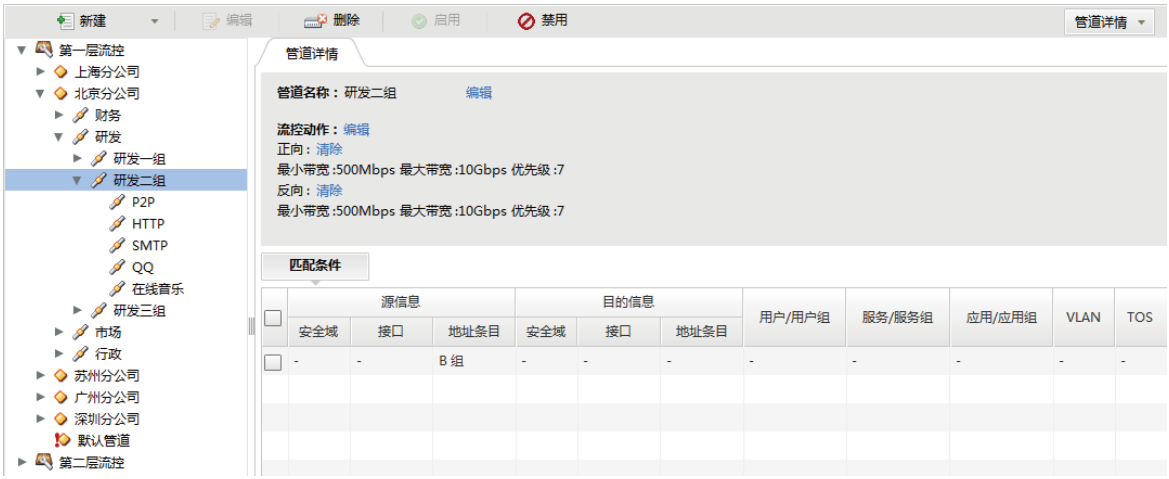

图4 iQoS 管道配置图

根管道各个分公司的流量控制呈现:

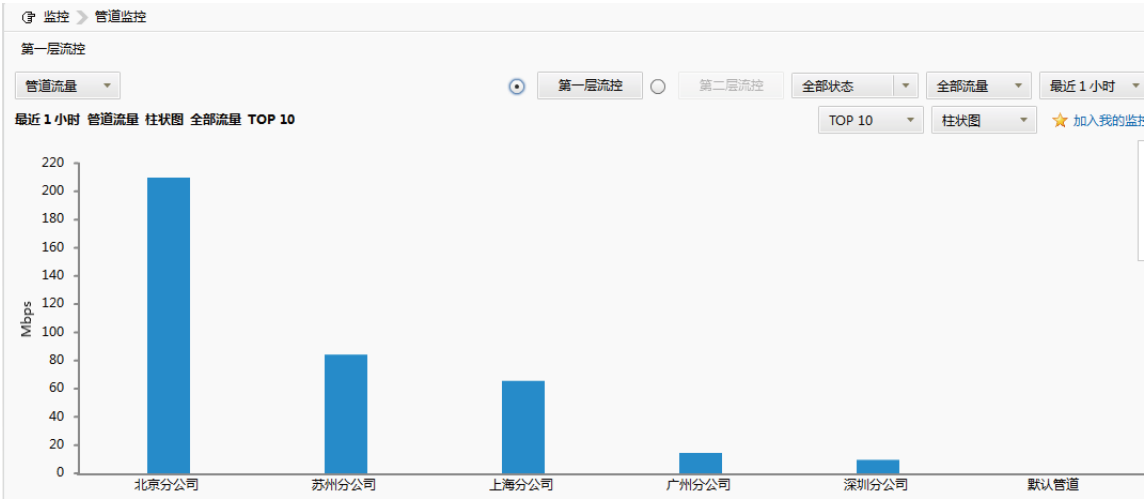

图5 第一层流控第一级管道流量监控图

北京分公司各个部门的流量控制呈现:

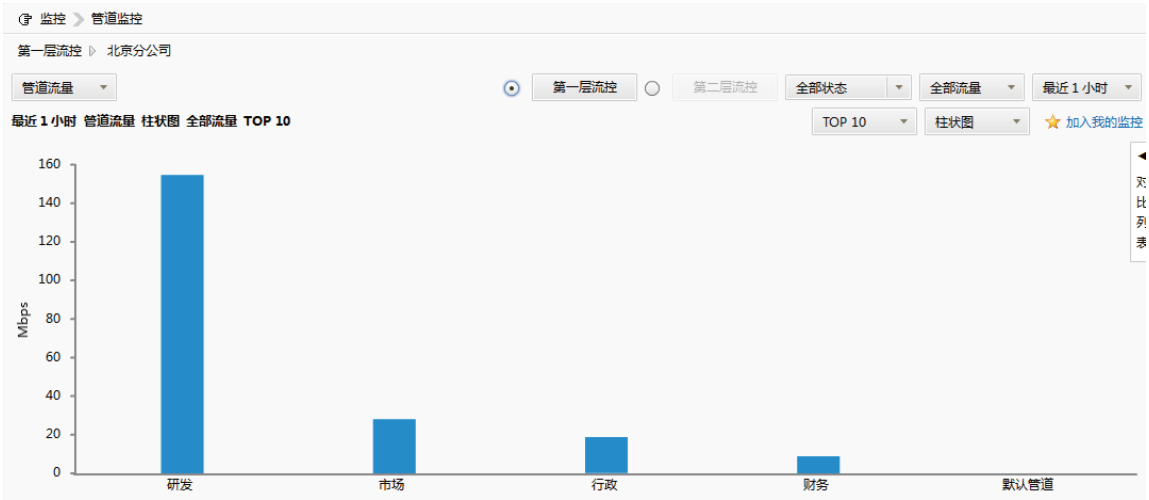

图6 第一层流控第二级管道流量监控图

研发部门下各研发小组的流量控制呈现:

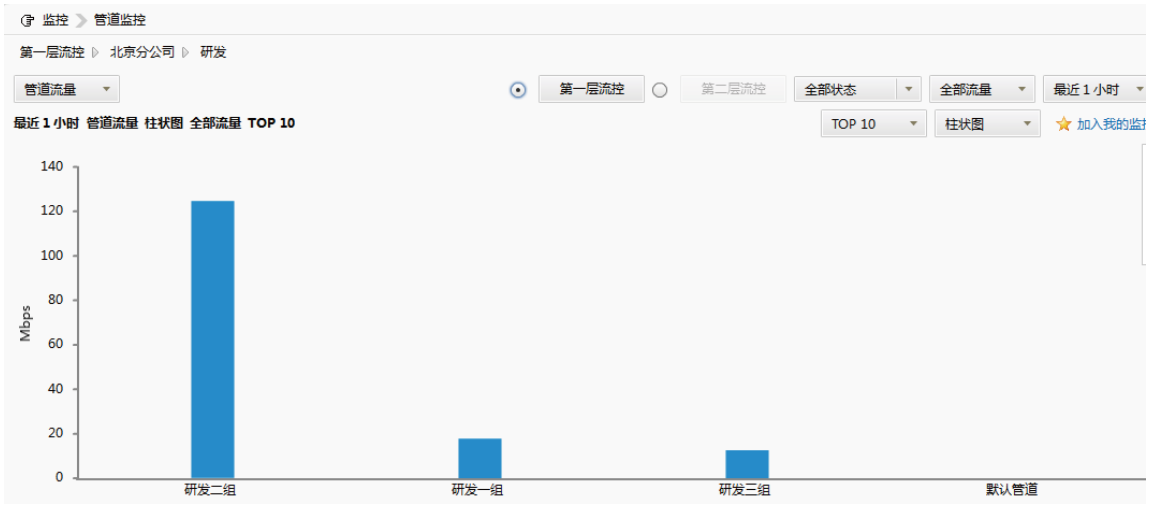

图7 第一层流控第三级管道流量监控图

研发二组下每种应用的流量控制呈现:

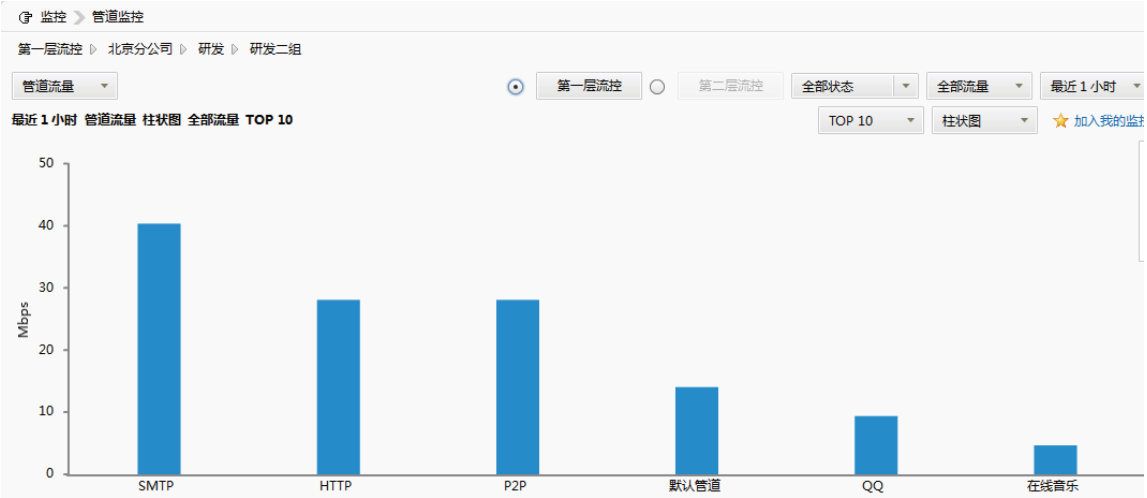

图8 第一层流控第四级管道流量监控图

2.3 差分服务

目前网络中存在着日益复杂多变的应用类型，传统的流量控制设备无法区分如此复杂的应用类型，即使有能力识别所有应用，但也无法对P2P、多线程下载等非关键应用的带宽资源占用情况进行评估，因此很多企业只能不断增加带宽。

Hillstone增强的智能流量管理（iQoS）能够通过设置优先级（0-7级）进行差分服务。用户通过应用识别功能识别出网络中的应用类型，并根据管道监控分析出:

1） 哪些应用需要优先保证

2） 哪些应用需要低优先级控制

3） 哪些应用需要禁止

当我们非常清楚的了解网络上每种应用类型的带宽分布，可以建立一套基于应用级别差异化服务的可行性策略，为关键应用分配更高优先级，并对其进行高优先级的调度控制。

2.4 剩余带宽分配机制

Hillstone　T系列下一代智能防火墙通过配置管道来实现流量控制。当每一级管道有剩余带宽时，可以借给子管道使用，使带宽能够充分利用。当管道下有多个子管道，并且每个子管道的优先级相同，则以抢占的方式抢占上一级管道的剩余带宽；当管道下多个子管道的优先级不同，则按照优先级比例借父管道的剩余带宽，高优先级的应用能够获得更多的剩余带宽。从而保证带宽得到更合理、高效的利用。

总结

Hillstone增强的智能流量管理（iQoS）与传统的流控设备相比，具有明显的优势:

- 两层八级管道嵌套，带宽资源灵活管理
- 细粒度流量划分，网络流量精细化控制
- 配置与呈现统一，方便用户管理设置优先级实现差分服务，保证关键业务畅通
- 剩余带宽分配机制，充分利用剩余带宽

文档编号：EX-09.01-SG0000-5.0R3-0613-Ch-01