



(12) 发明专利申请

(10) 申请公布号 CN 105812281 A

(43) 申请公布日 2016. 07. 27

(21) 申请号 201410851420. 0

(22) 申请日 2014. 12. 31

(71) 申请人 中国电信股份有限公司
地址 100033 北京市西城区金融大街 31 号

(72) 发明人 王勇 陈文华 姚文胜 毛宇
刘汉江 乔宏明 李嫚 梁兔
陈春华

(74) 专利代理机构 中国国际贸易促进委员会专
利商标事务所 11038
代理人 方亮

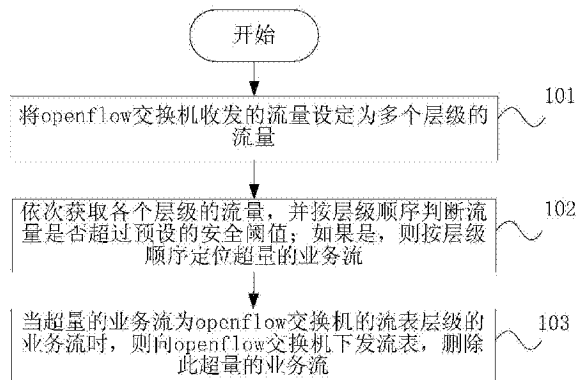
(51) Int. Cl.
H04L 12/857(2013. 01)

权利要求书2页 说明书8页 附图4页

(54) 发明名称
服务质量 QoS 层级控制方法、装置及系统

(57) 摘要

本发明公开了一种服务质量 QoS 层级控制方法、装置及系统,其中的方法包括:将 Openflow 交换机收发的流量设定为多个层级的流量;依次获取各个层级的流量,并按层级顺序判断流量是否超过预设的安全阈值;如果是,则按层级顺序定位超量的业务流;当超量的业务流为 Openflow 交换机的流表层级的业务流时,则向 Openflow 交换机下发流表,删除此超量的业务流。本发明的 QoS 层级控制方法、装置及系统,可以实现多层次多瓶颈点的调度控制,并能按用户的需求定义业务流的优先级,保证业务优先级高的业务流的 QoS;能够减少用户间和应用间带宽相互挤占,同时可最大限度共享带宽资源,还可以保障指定业务 QoS。提高网络服务效率。



1. 一种服务质量 QOS 层级控制方法,其特征在于,包括:
将 Openflow 交换机收发的流量设定为多个层级的流量;
依次获取各个层级的流量,并按层级顺序判断流量是否超过预设的安全阈值;如果是,则按层级顺序定位超量的业务流;
当所述超量的业务流为 Openflow 交换机的流表层级的业务流时,则向 Openflow 交换机下发流表,删除此超量的业务流。
2. 如权利要求 1 所述的方法,其特征在于,所述将 Openflow 交换机收发的流量设定为多个层级流量包括:
将 Openflow 交换机的上连端口流量设定为第一层级的流量;
将 Openflow 交换机的下连端口流量设定为第二层级的流量;
将 Openflow 交换机的流表中与用户 IP 匹配的流量设定为第三层级的流量;
将 Openflow 交换机的流表中与用户 IP 和站点 IP 匹配的流量设定为第四层级的流量。
3. 如权利要求 2 所述的方法,其特征在于,所述按层级顺序判断层级流量是否超过预设的安全阈值包括:
在 Openflow 交换机的入端口获取第一层级的网络总流量 A_z ,判断 A_z 是否超过安全阈值 $A*K$;其中, A 为第一层级网络总容量, K 为安全阈值;
如果超过,则在 Openflow 交换机的出端口获取第二层级的各个通道的总流量 B_z 及第二层级的通道数 N ;
计算第二层级各个通道的平均流量 $B_p = A/N$,判断 B_z 是否超过 B_p ;如果超过,定位该通道通过 Openflow 交换机的端口号;
按 IP 地址分析,获取第三层级各个通道的总体流量 C_z 和通道数 M ;获取各个用户签约的网络业务带宽 C_i ,计算第三层级各个通道的平均流量 $C_p = B / \sum (C_i) * C_i$; B 为第二层级各个通道的网络总容量;
判断 C_z 是否超过 C_p ,如果超过,则进行流量控制。
4. 如权利要求 3 所述的方法,其特征在于:
当判断 C_z 没有超过 C_p 时,则获取第三层级各个用户通道的总流量 C ,判断所述 C_z 是否超过规定的安全阈值流量 $C*K$,如果超过,则进行流量控制。
5. 如权利要求 4 所述的方法,其特征在于:
当判断所述 A_z 没有超过所述 $A*K$ 时,获取第二层级各个通道的网络总流量 B_z 和第二层级各个通道的网络总容量 B ,判断所述 B_z 是否超过该层级的网络安全阈值 $B*K$ 。
6. 如权利要求 4 所述的方法,其特征在于,所述进行流量控制包括:
通过 IP 地址获取用户业务流,按业务流的优先级对该用户的业务流进行排序;
计算出该用户超出带宽量,确定删除的流量,从优先级低的业务流开始建立删除业务流流表,设置该流表过期时间,将所述删除业务流流表下发到 Openflow 交换机。
7. 一种 QOS 层级控制装置,其特征在于,包括:
层级设定单元,用于将 Openflow 交换机收发的流量设定为多个层级的流量;
流量判断单元,用于依次获取各个层级的流量,并按层级顺序判断流量是否超过预设的安全阈值;如果是,则按层级顺序定位超量的业务流;
超量处理单元,用于当所述超量的业务流为 Openflow 交换机的流表层级的业务流时,

则向 Openflow 交换机下发流表,删除此超量的业务流。

8. 如权利要求 7 所述的装置,其特征在于:

所述层级设定单元,用于将 Openflow 交换机的上连端口流量设定为第一层级的流量;将 Openflow 交换机的下连端口流量设定为第二层级的流量;将 Openflow 交换机的流表中与用户 IP 匹配的流量设定为第三层级的流量;将 Openflow 交换机的流表中与用户 IP 和站点 IP 匹配的流量设定为第四层级的流量。

9. 如权利要求 8 所述的装置,其特征在于:

所述流量判断单元,包括:

第一层级判断子模块,用于在 Openflow 交换机的入端口获取第一层级的网络总流量 A_z ,判断 A_z 是否超过安全阈值 $A*K$;其中, A 为第一层级网络总容量, K 为安全阈值;

第二层级判断子模块,用于如果超过,则在 Openflow 交换机的出端口获取第二层级的各个通道的总流量 B_z 及第二层级的通道数 N ;计算第二层级各个通道的平均流量 $B_p = A/N$,判断 B_z 是否超过第二层级平均流量 B_p ;如果超过,定位该通道通过 Openflow 交换机的端口号;

第三层级判断单元,用于按 IP 地址分析,获取第三层级各个通道的总体流量 C_z 和通道数 M ;获取各个用户签约的网络业务带宽 C_i ,计算第三层级各个通道的平均流量 $C_p = B/\sum(C_i)*C_i$; B 为第二层级各个通道的网络总容量;判断所述 C_z 是否超过 C_p ;如果超过,则判断此 IP 地址对应的流量超量;

所述超量处理单元进行流量控制。

10. 如权利要求 9 所述的装置,其特征在于:

所述第三层级判断子模块,用于当判断所述 C_z 没有超过 C_p 时,则获取第三层级各个用户通道的总流量 C ,判断所述 C_z 是否超过规定的安全阈值流量 $C*K$,如果超过,则判断与此 IP 地址对应的流量超量;

所述超量处理单元进行流量控制。

11. 如权利要求 10 所述的装置,其特征在于:

所述第二层级判断子模块,用于当判断所述 A_z 没有超过所述 $A*K$ 时,获取第二层级各个通道的网络总流量 B_z 和第二层级各个通道的网络总容量 B ,判断所述 B_z 是否超过该层级的网络安全阈值 $B*K$ 。

12. 如权利要求 10 所述的装置,其特征在于:

所述超量处理单元,包括:

优先级排序子模块,用于通过 IP 地址获取用户业务流,按业务流的优先级对该用户的业务流进行排序;

删除流表建立子模块,用于计算出该用户超出带宽度,确定删除的流量,从优先级低的业务流开始建立删除业务流流表,设置该流表过期时间;

删除流表下发自模块,用于将所述删除业务流流表下发到 Openflow 交换机。

13. 一种 QOS 层级控制系统,其特征在于,包括:

Openflow 交换机、如权利要求 7 至 12 任意一项所述的 QOS 层级控制装置。

服务质量 QOS 层级控制方法、装置及系统

技术领域

[0001] 本发明涉及流量管理技术领域,尤其涉及一种服务质量 QOS 层级控制方法、装置及系统。

背景技术

[0002] 电信运营商宽带接入网络是个树形或者星型逐级汇聚网络,一般存在多个瓶颈点,网络拥塞时处理会非常复杂,并且成本高昂。通常,互联网宽带接入段一般采用星型或者树形结构,一般由以太网交换机实现逐级汇聚,其根部是 BRAS(宽带接入服务点)。由于接入网覆盖和容量有限,用户上网随机行为对网络产生较大的影响,出现拥塞和影响其他用户的情况会经常出现。接入网络设备繁多,能力参差不齐,难以在每个设备上部署统一的 QOS 策略。在网络拥塞时,会随机丢弃数据包,造成网络效率下降,服务质量严重劣化。

[0003] 如图 1 所示,运营商的网络流量通过核心网流向 BRAS,通过 BRAS 下发到各个接入网核心网交换机上,业务流通过接入网交换机下发到各个 DSLAM,由各个 DSLAM 按用户定制的业务分到各个终端用户。在整个过程中,运营商在 BRAS 上部署 QOS 策略,对运营商自营业务进行控制。由于 BRAS 设备厂家种类繁多,造成难以部署统一的 QOS 策略,对业务流控制能力不够灵活。

发明内容

[0004] 有鉴于此,本发明要解决的一个技术问题是提供一种服务质量 QOS 层级控制方法,可以实现层次化的流量调度。

[0005] 一种服务质量 QOS 层级控制方法,包括:将 Openflow 交换机收发的流量设定为多个层级的流量;依次获取各个层级的流量,并按层级顺序判断流量是否超过预设的安全阈值;如果是,则按层级顺序定位超量的业务流;当所述超量的业务流为 Openflow 交换机的流表层级的业务流时,则向 Openflow 交换机下发流表,删除此超量的业务流。

[0006] 根据本发明的一个实施例,进一步的,所述将 Openflow 交换机收发的流量设定为多个层级流量包括:将 Openflow 交换机的上连端口流量设定为第一层级的流量;将 Openflow 交换机的下连端口流量设定为第二层级的流量;将 Openflow 交换机的流表中与用户 IP 匹配的流量设定为第三层级的流量;将 Openflow 交换机的流表中与用户 IP 和站点 IP 匹配的流量设定为第四层级的流量。

[0007] 根据本发明的一个实施例,进一步的,所述按层级顺序判断层级流量是否超过预设的安全阈值包括:在 Openflow 交换机的入端口获取第一层级的网络总流量 A_z ,判断 A_z 是否超过安全阈值 $A*K$;其中, A 为第一层级网络总容量, K 为安全阈值;如果超过,则在 Openflow 交换机的出端口获取第二层级的各个通道的总流量 B_z 及第二层级的通道数 N ;计算第二层级各个通道的平均流量 $B_p = A/N$,判断 B_z 是否超过第二层级平均流量 B_p ;如果超过,定位该通道通过 Openflow 交换机的端口号;按 IP 地址分析,获取第三层级各个通道的总体流量 C_z 和通道数 M ;获取各个用户签约的网络业务带宽 C_i ,计算第三层级各个通道的

平均流量 $C_p = B / \sum (C_i) * C_i$;B 为第二层级各个通道的网络总容量 ;判断所述 C_z 是否超过 C_p , 如果超过, 则进行流量控制。

[0008] 根据本发明的一个实施例, 进一步的, 判断所述 C_z 没有超过 C_p 时, 则获取第三层级各个用户通道的总流量 C , 判断所述 C_z 是否超过规定的安全阈值流量 $C * K$, 如果超过, 则进行流量控制。

[0009] 根据本发明的一个实施例, 进一步的, 当判断所述 A_z 没有超过所述 $A * K$ 时, 获取第二层级各个通道的网络总流量 B_z 和第二层级各个通道的网络总容量 B , 判断所述 B_z 是否超过该层级的网络安全阈值 $B * K$ 。

[0010] 根据本发明的一个实施例, 进一步的, 所述进行流量控制包括 :通过 IP 地址获取用户业务流, 按业务流的优先级对该用户的业务流进行排序 ;计算出该用户超出带宽量, 确定删除的流量, 从优先级低的业务流开始建立删除业务流流表, 设置该流表过期时间, 将所述删除业务流流表下发到 Openflow 交换机。

[0011] 本发明要解决的一个技术问题是提供一种 QOS 层级控制装置, 可以实现层次化的流量调度。

[0012] 一种 QOS 层级控制装置, 包括 :层级设定单元, 用于将 Openflow 交换机收发的流量设定为多个层级的流量 ;流量判断单元, 用于依次获取各个层级的流量, 并按层级顺序判断流量是否超过预设的安全阈值 ;如果是, 则按层级顺序定位超量的业务流 ;超量处理单元, 用于当所述超量的业务流为 Openflow 交换机的流表层级的业务流时, 则向 Openflow 交换机下发流表, 删除此超量的业务流。

[0013] 根据本发明的一个实施例, 进一步的, 所述层级设定单元, 用于将 Openflow 交换机的上连端口流量设定为第一层级的流量 ;将 Openflow 交换机的下连端口流量设定为第二层级的流量 ;将 Openflow 交换机的流表中与用户 IP 匹配的流量设定为第三层级的流量 ;将 Openflow 交换机的流表中与用户 IP 和站点 IP 匹配的流量设定为第四层级的流量。

[0014] 根据本发明的一个实施例, 进一步的, 所述流量判断单元, 包括 :第一层级判断子模块, 用于在 Openflow 交换机的入端口获取第一层级的网络总流量 A_z , 判断 A_z 是否超过安全阈值 $A * K$;其中, A 为第一层级网络总容量, K 为安全阈值 ;第二层级判断子模块, 用于如果超过, 则在 Openflow 交换机的出端口获取第二层级的各个通道的总流量 B_z 及第二层级的通道数 N ;计算第二层级各个通道的平均流量 $B_p = A / N$, 判断 B_z 是否超过第二层级平均流量 B_p ;如果超过, 定位该通道通过 Openflow 交换机的端口号 ;第三层级判断单元, 用于按 IP 地址分析, 获取第三层级各个通道的总体流量 C_z 和通道数 M ;获取各个用户签约的网络业务带宽 C_i , 计算第三层级各个通道的平均流量 $C_p = B / \sum (C_i) * C_i$;B 为第二层级各个通道的网络总容量 ;判断所述 C_z 是否超过 C_p ;如果超过, 则判断此 IP 地址对应的流量超量 ;所述超量处理单元进行流量控制。

[0015] 根据本发明的一个实施例, 进一步的, 所述第三层级判断子模块, 用于当判断所述 C_z 没有超过 C_p 时, 则获取第三层级各个用户通道的总流量 C , 判断所述 C_z 是否超过规定的安全阈值流量 $C * K$, 如果超过, 则判断与此 IP 地址对应的流量超量 ;所述超量处理单元进行流量控制。

[0016] 根据本发明的一个实施例, 进一步的, 所述第二层级判断子模块, 用于当判断所述 A_z 没有超过所述 $A * K$ 时, 获取第二层级各个通道的网络总流量 B_z 和第二层级各个通道

的网络总容量 B , 判断所述 B_z 是否超过该层级的网络安全阈值 $B * K$ 。

[0017] 根据本发明的一个实施例, 进一步的, 所述超量处理单元, 包括: 优先级排序子模块, 用于通过 IP 地址获取用户业务流, 按业务流的优先级对该用户的业务流进行排序; 删除流表建立子模块, 用于计算出该用户超出带宽量, 确定删除的流量, 从优先级低的业务流开始建立删除业务流流表, 设置该流表过期时间; 删除流表下发自模块, 用于将所述删除业务流流表下发到 Openflow 交换机。

[0018] 本发明提供一种 QoS 层级控制系统, 包括: Openflow 交换机、如上所述的 QoS 层级控制装置。

[0019] 本发明的 QoS 层级控制方法、装置及系统, 可以实现层次化 QoS 调度, 实现多层次多瓶颈点的调度控制, 并能按用户的需求定义业务流的优先级, 保证业务优先级高的业务流的 QoS。能够减少用户间和应用间带宽相互挤占, 同时可最大限度共享带宽资源。

附图说明

[0020] 为了更清楚地说明本发明实施例或现有技术中的技术方案, 下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍, 显而易见地, 下面描述中的附图仅仅是本发明的一些实施例, 对于本领域普通技术人员来讲, 在不付出创造性劳动性的前提下, 还可以根据这些附图获得其它的附图。

[0021] 图 1 为现有的运营商网络拓扑图;

[0022] 图 2 为根据本发明的 QoS 层级控制方法的一个实施例的流程图;

[0023] 图 3 为根据本发明的 QoS 层级控制方法的另一个实施例的流程图;

[0024] 图 4 为根据本发明的进行流量控制的流程图;

[0025] 图 5 为具有本发明的 QoS 层级控制装置的网络拓扑图;

[0026] 图 6 为根据本发明的 QoS 层级控制装置的一个实施例的结构框图;

[0027] 图 7 为根据本发明的 QoS 层级控制装置的一个实施例中流量判断单元的结构框图;

[0028] 图 8 为根据本发明的 QoS 层级控制装置的一个实施例中超量处理单元的结构框图。

具体实施方式

[0029] 下面参照附图对本发明进行更全面的描述, 其中说明本发明的示例性实施例。下面将结合本发明实施例中的附图, 对本发明实施例中的技术方案进行清楚、完整地描述, 显然, 所描述的实施例仅仅是本发明一部分实施例, 而不是全部的实施例。基于本发明中的实施例, 本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例, 都属于本发明保护的范围。下面结合各个图和实施例对本发明的技术方案进行多方面的描述。

[0030] 图 2 为根据本发明的 QoS 层级控制方法的一个实施例的流程图, 如图 2 所示:

[0031] 步骤 101, 将 Openflow 交换机收发的流量设定为多个层级的流量。;

[0032] 步骤 102, 依次获取各个层级的流量, 并按层级顺序判断流量是否超过预设的安全阈值; 如果是, 则按层级顺序定位超量的业务流。

[0033] 步骤 103, 当超量的业务流为 Openflow 交换机的流表层级的业务流时, 则向

Openflow 交换机下发流表,删除此超量的业务流。

[0034] 上述实施例中的本发明的 QoS 层级控制方法,可以设置 Openflow 交换机,实现全局优化的层次化 QoS 调度,实现多层次多瓶颈点的调度控制,并能按用户的需求定义业务流的优先级,保证业务优先级高的业务流的 QoS。

[0035] 软件定义网络 SDN(Software Defined Network) 是 Emulex 网络一种新型网络创新架构,其核心技术 OpenFlow 通过将网络设备控制面与数据面分离开来,从而实现了网络流量的灵活控制。OpenFlow 是 SDN 架构中定义的一个控制器与转发器之间的通信接口标准。OpenFlow 允许控制器直接访问和操作网络设备的转发平面,这些网络设备可能是物理上的,也可能是虚拟的路由器或者交换机。

[0036] Openflow 交换机是整个 OpenFlow 网络的核心部件,主要管理数据层的转发。Openflow 交换机接收到数据包后,首先在本地的流表上查找转发目标端口,如果没有匹配,则把数据包转发给 Controller,由控制层决定转发端口。Openflow 交换机由流表、安全通道和 OpenFlow 协议三部分组成。安全通道是连接 Openflow 交换机到控制器的接口。控制器通过这个接口控制和管理交换机,同时控制器接收来自交换机的事件并向交换机发送数据包。

[0037] 将 Openflow 交换机的上连端口流量设定为第一层级的流量。将 Openflow 交换机的下连端口流量设定为第二层级的流量。将 Openflow 交换机的流表中与用户 IP 匹配的流量设定为第三层级的流量。将 Openflow 交换机的流表中与用户 IP 和站点 IP 匹配的流量设定为第四层级的流量。

[0038] 例如, Openflow 交换机的上连端口流量为第一层流量,例如 BRAS 用户侧端口, Openflow 交换机的下连端口流量为第二层级流量,例如 DSLAM 中继端口, Openflow 交换机流表(源或目的)匹配用户 IP 为第三层级流量,例如用户线路, Openflow 交换机流表(源与目的)匹配用户 IP 和站点 IP(或增加四层端口)为第四层级流量,例如用户应用。

[0039] 对各层级流量判断是否超过安全阈值,如果没有超过,进入下一层级判断。如果超过则逐级定位超量群组,直至用户应用级流量,进行精准的丢弃控制。

[0040] 在一个实施例中,在 Openflow 交换机的入端口获取第一层级的网络总流量 A_z ,判断 A_z 是否超过安全阈值 $A * K$ 。其中, A 为第一层级网络总容量, K 为安全阈值。

[0041] 如果超过,则在 Openflow 交换机的出端口获取第二层级的各个通道的总流量 B_z 及第二层级的通道数 N 。计算第二层级各个通道的平均流量 $B_p = A / N$,判断 B_z 是否超过第二层级平均流量 B_p 。

[0042] 如果超过,定位该通道通过 Openflow 交换机的端口号。按 IP 地址分析,获取第三层级各个通道的总体流量 C_z 和通道数 M 。

[0043] 获取各个用户签约的网络业务带宽 C_i ,计算第三层级各个通道的平均流量 $C_p = B / \sum (C_i) * C_i$ 。 B 为第二层级各个通道的网络总容量。

[0044] 判断 C_z 是否超过 C_p ,如果超过,则进行流量控制。

[0045] 当判断 C_z 没有超过 C_p 时,则获取第三层级各个用户通道的总流量 C ,判断 C_z 是否超过规定的安全阈值流量 $C * K$,如果超过,则进行流量控制。

[0046] 当判断 A_z 没有超过 $A * K$ 时,获取第二层级各个通道的网络总流量 B_z 和第二层级各个通道的网络总容量 B ,判断 B_z 是否超过该层级的网络安全阈值 $B * K$ 。

[0047] 图 3 为根据本发明的 QoS 层级控制方法的另一个实施例的流程图。如图 3 所示：其中，A 为第一层级网络总容量，Az 为第一层级网络总流量，B 为第二层级各个通道网络总容量，Bz 为第二层级各个通道网络总流量，N 为第二层级网络通道数，Bp 为第二层级各个通道网络平均流量，C 为第三层级各个通道网络总容量，Cz 为第三层级各个通道网络总流量，M 为第三层级网络通道数，Ci 为第三层级网络业务带宽，Cp 为第三层级各个通道网络平均流量。

[0048] 步骤 200, 首先要设置安全阈值 K。安全阈值指的是整个网络管道流量占整体网络容量的百分比，例如设置安全阈值 $K = 90\%$ 。

[0049] 步骤 200, 第一层级网络总容量（核心网到接入网总容量）为 A, 通过 Openflow 交换机 INPUT 端口获取第一层级网络总流量 Az。

[0050] 步骤 201, 判断 Az 是否超过规定的安全阈值 $A*K$ 。

[0051] 步骤 202, 如果超过规定的第一层级的安全阈值 $A*K$, 通过接入网核心 Openflow 交换机的 OUTPUT 端口获取第二层级各个通道的总体流量 Bz 及第二层级的通道数 N。计算出第二层级各个通道的平均流量 $Bp = A/N$ 。

[0052] 步骤 203, 挨个判断第二层级各个通道的总流量 Bz 是否超过第二层级平均流量 Bp。

[0053] 步骤 204, 如果超过, 定位该通道通过接入网 OF 核心交换机的端口号, 通过控制装置按 IP 地址分析, 获取第三层级各个通道的总体流量 Cz 和通道数 M。

[0054] 获取各个用户签约的网络业务带宽 Ci, 计算第三层级各个通道的平均流量 $Cp = B / \sum (Ci) * Ci$ 。第二层级各个通道的网络总容量为 B。

[0055] 步骤 206, 判断第三层级各个通道的总体流量 Cz 是否超过第三层级的平均流量 Cp。

[0056] 步骤 207, 如果超过, 进行流量控制流程, 回到层次化调度流程开始。

[0057] 步骤 209, 如果没有超过, 获取第三层级各个用户通道的总流量 C, 判断第三层级用户总流量 Cz 是否超过规定的安全阈值流量 $C*K$ 。

[0058] 步骤 210, 如果超过, 进行流量控制流程, 回到层次化调度流程开始。

[0059] 如果没有超过, 直接回到层次化调度流程开始。

[0060] 步骤 205, 如果第二层级的总流量 Bz 没有超过该层级的平均流量 Bp, 通过控制平台按 IP 地址分析, 获取第三层级各个通道的总体流量 Cz 和第三层级的网络带宽总容量 C。

[0061] 步骤 208, 判断第三层级总流量 Cz 是否超过安全阈值流量 $C*K$ 。

[0062] 如果没有超过, 回到层次化调度流程开始。

[0063] 步骤 211, 如果超过, 进入流量控制流程。

[0064] 步骤 212, 如果第一层级的网络总流量 Az 没有超过该层级的安全阈值流量 $A*K$, 获取第二层级各个通道的网络总流量 Bz 和第二层级各个通道的网络总容量 B。

[0065] 步骤 213, 判断第二层级总流量 Bz 是否超过该层级的网络安全阈值 $B*K$ 。

[0066] 步骤 214, 如果超过, 通过控制平台按 IP 地址分析, 获取第三层级各个通道的总体流量 Cz 和通道数 M。获取各个用户签约的网络业务带宽 Ci, 计算第三层级各个通道的平均流量 $Cp = B / \sum (Ci) * Ci$ 。

[0067] 步骤 216, 判断各个通道第三层级总流量 Cz 是否超过该层级的平均流量 Cp。

[0068] 步骤 219, 如果超过, 进入流量控制流程, 回到层次化调度流程开始。

[0069] 步骤 217, 如果没有超过, 获取第三层级网络总容量 C , 判断该层级的网络总流量 C_z 是否超过该层级的网络安全阈值 $C * K$ 。

[0070] 步骤 220, 如果第三层级网络总流量 C_z 超过该层级网络安全阈值 $C * K$, 进入流量控制流程, 回到层次化调度流程开始。反之, 直接返回到层次化调度流程开始。

[0071] 步骤 215, 如果第二层级网络总流量 B_z 没有超过规定的该层级的网络安全阈值 $B * K$, 获取第三层级各个网络通道总流量 C_z 。

[0072] 步骤 218, 判断第三层级网络总流量是否超过该层级的网络安全阈值 $C * K$ 。

[0073] 步骤 221, 如果超过进入流量控制流程, 回到层次化调度流程开始。

[0074] 如果没有超过, 直接回到层次化调度流程开始。

[0075] 在一个实施例中, 通过 IP 地址获取用户业务流, 按业务流的优先级对该用户的业务流进行排序。计算出该用户超出带宽量, 确定删除的流量, 从优先级低的业务流开始建立删除业务流流表, 设置该流表过期时间, 将删除业务流流表下发到 Openflow 交换机。

[0076] 图 4 为根据本发明的进行流量控制的流程图, 如图 4 所示:

[0077] 步骤 301, 流量控制流程开始。

[0078] 步骤 302, 通过控制平台通过用户 IP 地址获取通过用户的业务流。

[0079] 步骤 303, 按业务流的优先级对该用户的业务流进行排序。

[0080] 步骤 304, 计算出该用户超出带宽量, 确定该用户应该删除多少流量。

[0081] 步骤 305, 从优先级低的业务流开始建立删除业务流流表。

[0082] 步骤 306, 设置该流表过期时间。

[0083] 步骤 306, 通过 SDN 控制装置或平台把流表下发到 Openflow 交换机上, 删除业务流, 流量控制流程结束。

[0084] 上述实施例中的 QOS 层级控制方法, 减少用户间和应用间带宽相互挤占, 同时可最大限度共享带宽资源, 还可以保障指定业务 QOS。提高网络服务效率。采用 SDN 技术, 软硬件分离方案, 软件可以根据业务需求灵活定制。可以根据业务需要灵活部署全网统一的 QOS 策略, 不会受到接入网 BRAS 或者其他硬件设备不同厂家的影响。

[0085] 采用支持 OPENFLOW 协议的交换及替代现有的接入网核心交换机, 在 Openflow 交换机外侧部署控制装置或平台, 如图 5 所示, 并开发层次化调度应用。在控制装置上分析用户业务流, 定位超量用户, 由控制器向 Openflow 交换机下发流表, 删除用户优先级低的业务流。

[0086] 如图 6 所示, 本发明提供一种 QOS 层级控制装置 4。层级设定单元 41 将 Openflow 交换机收发的流量设定为多个层级的流量。流量判断单元 42 依次获取各个层级的流量, 并按层级顺序判断流量是否超过预设的安全阈值。如果是, 则按层级顺序定位超量的业务流。

[0087] 当超量的业务流为 Openflow 交换机的流表层级的业务流时, 超量处理单元 43 则向 Openflow 交换机下发流表, 删除此超量的业务流。

[0088] 层级设定单元 41 将 Openflow 交换机的上连端口流量设定为第一层级的流量。将 Openflow 交换机的下连端口流量设定为第二层级的流量。将 Openflow 交换机的流表中与用户 IP 匹配的流量设定为第三层级的流量。将 Openflow 交换机的流表中与用户 IP 和站点 IP 匹配的流量设定为第四层级的流量。

[0089] 如图 7 所示, 第一层级判断子模块 421 在 Openflow 交换机的入端口获取第一层级的网络总流量 A_z , 判断 A_z 是否超过安全阈值 $A * K$ 。其中, A 为第一层级网络总容量, K 为安全阈值。如果超过, 则第二层级判断子模块 422 在 Openflow 交换机的出端口获取第二层级的各个通道的总流量 B_z 及第二层级的通道数 N 。

[0090] 第二层级判断子模块 422 计算第二层级各个通道的平均流量 $B_p = A/N$, 判断 B_z 是否超过第二层级平均流量 B_p 。如果超过, 定位该通道通过 Openflow 交换机的端口号。

[0091] 第三层级判断单元 423 按 IP 地址分析, 获取第三层级各个通道的总体流量 C_z 和通道数 M 。获取各个用户签约的网络业务带宽 C_i , 计算第三层级各个通道的平均流量 $C_p = B / \sum (C_i) * C_i$ 。 B 为第二层级各个通道的网络总容量。判断 C_z 是否超过 C_p 。如果超过, 则判断此 IP 地址对应的流量超量。超量处理单元进行流量控制。

[0092] 当判断 C_z 没有超过 C_p 时, 则第三层级判断子模块 423 获取第三层级各个用户通道的总流量 C , 判断 C_z 是否超过规定的安全阈值流量 $C * K$, 如果超过, 则判断与此 IP 地址对应的流量超量。超量处理单元进行流量控制。

[0093] 当判断 A_z 没有超过 $A * K$ 时, 第二层级判断子模块 422 获取第二层级各个通道的网络总流量 B_z 和第二层级各个通道的网络总容量 B , 判断 B_z 是否超过该层级的网络安全阈值 $B * K$ 。

[0094] 如图 8 所示, 优先级排序子模块 431 通过 IP 地址获取用户业务流, 按业务流的优先级对该用户的业务流进行排序。删除流表建立子模块 432 计算出该用户超出带宽量, 确定删除的流量, 从优先级低的业务流开始建立删除业务流流表, 设置该流表过期时间。删除流表下发自模块 433 将删除业务流流表下发到 Openflow 交换机。

[0095] 本发明提供一种 QOS 层级控制系统, 包括: Openflow 交换机、如上的 QOS 层级控制装置。

[0096] 上述实施例中的本发明的 QOS 层级控制方法、装置及系统, 可以实现全局优化的层次化 QoS 调度, 实现多层次多瓶颈点的调度控制, 并能按用户的需求定义业务流的优先级, 保证业务优先级高的业务流的 QOS。能够减少用户间和应用间带宽相互挤占, 同时可最大限度共享带宽资源, 还可以保障指定业务 QOS。提高网络服务效率。采用 SDN 技术, 软、硬件分离方案, 软件可以根据业务需求灵活定制。可以根据业务需要灵活部署全网统一的 QOS 策略, 不会受到接入网 BRAS 或者其他硬件设备不同厂家的影响。

[0097] 上述实施例中的本发明的 QOS 层级控制方法、装置及系统, 可以部署在宽带接入网, 提高网络运行效率, 也可以用于大客户多级嵌套业务的接入, 提高大客户业务服务质量。

[0098] 可能以许多方式来实现本发明的方法和系统。例如, 可通过软件、硬件、固件或者软件、硬件、固件的任何组合来实现本发明的方法和系统。用于方法的步骤的上述顺序仅是为了进行说明, 本发明的方法的步骤不限于以上具体描述的顺序, 除非以其它方式特别说明。此外, 在一些实施例中, 还可将本发明实施为记录在记录介质中的程序, 这些程序包括用于实现根据本发明的方法的机器可读指令。因而, 本发明还覆盖存储用于执行根据本发明的方法的程序的记录介质。

[0099] 本发明的描述是为了示例和描述起见而给出的, 而并不是无遗漏的或者将本发明限于所公开的形式。很多修改和变化对于本领域的普通技术人员而言是显然的。选择和描

述实施例是为了更好说明本发明的原理和实际应用,并且使本领域的普通技术人员能够理解本发明从而设计适于特定用途的带有各种修改的各种实施例。

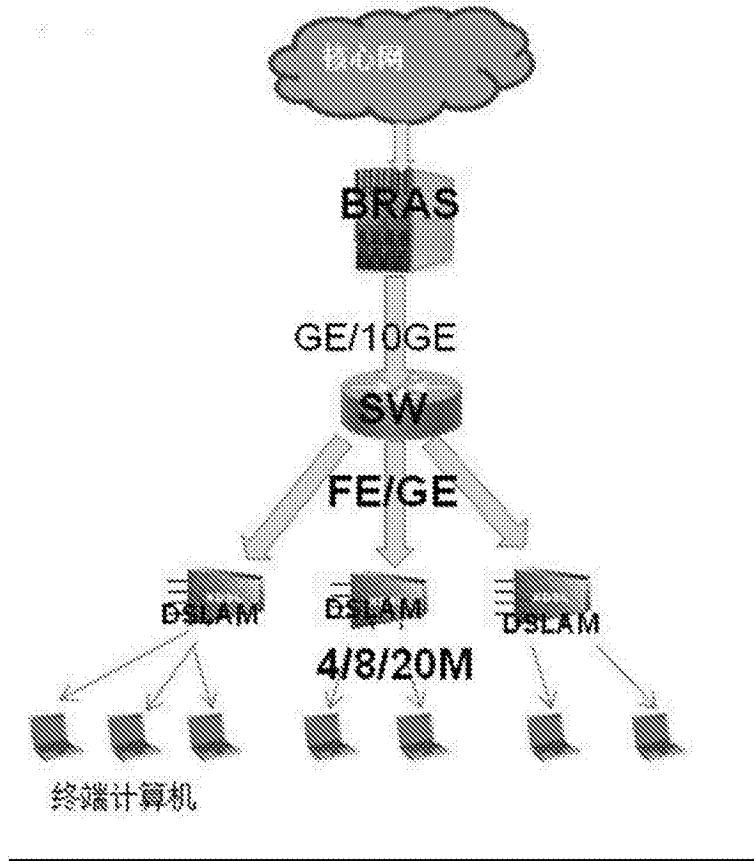


图 1

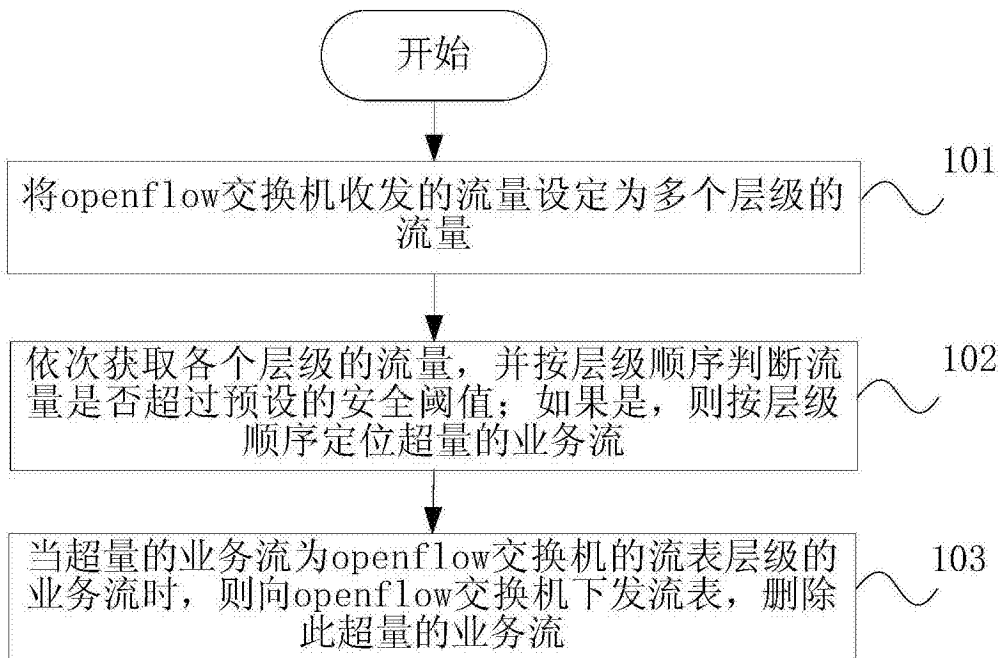


图 2

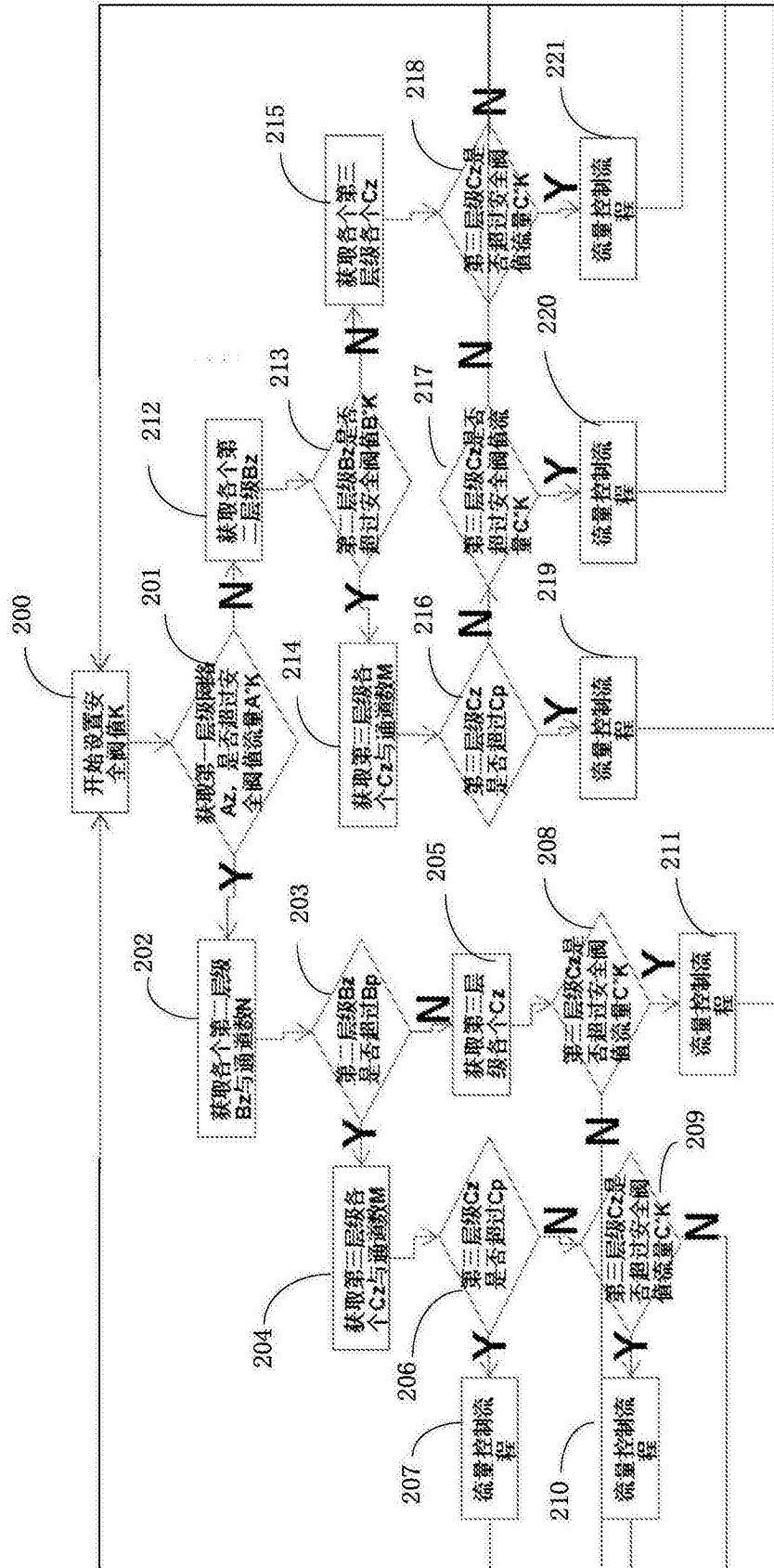


图 3

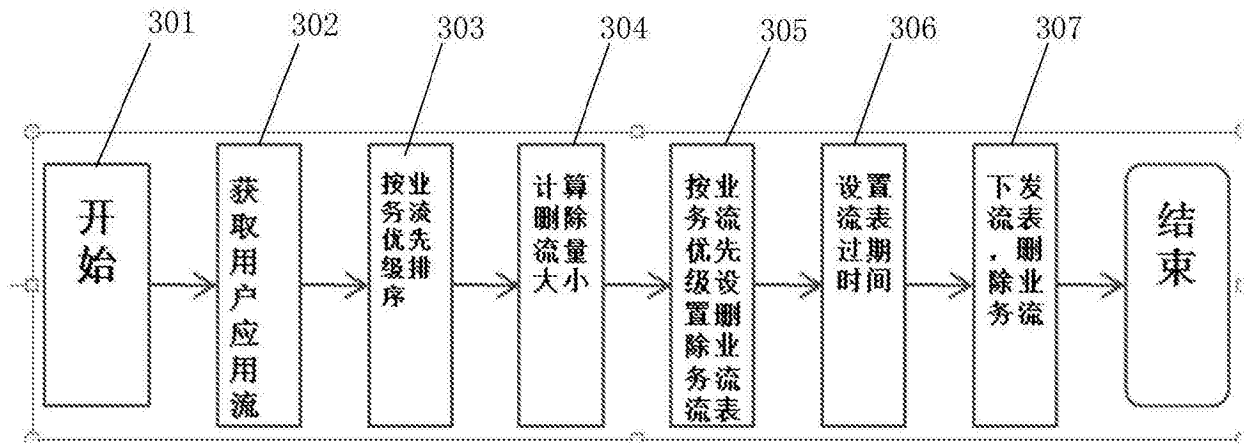


图 4

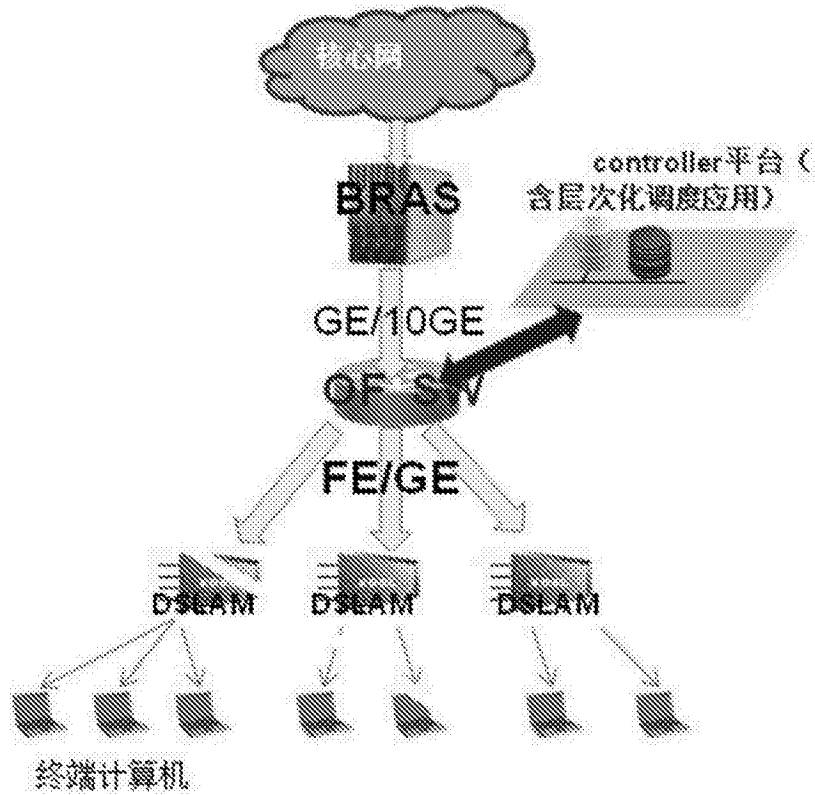


图 5

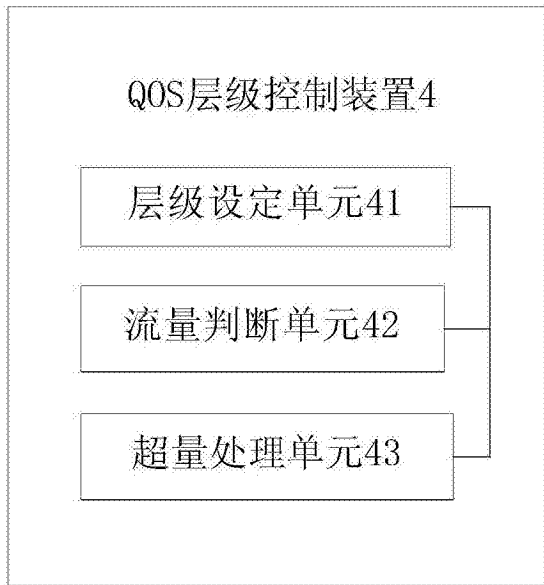


图6

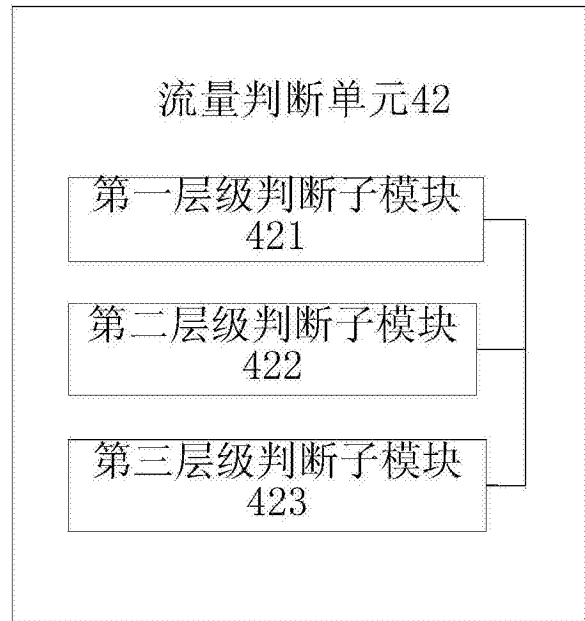


图7

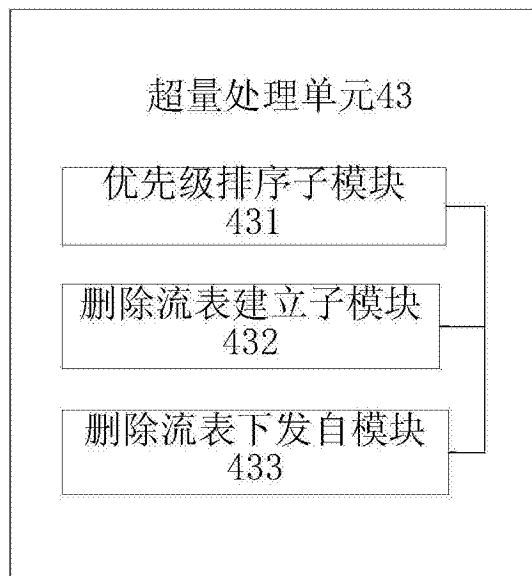


图8