(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103152279 B
(45)授权公告日 2016.08.03

(21)申请号 201310069573.5

(22)申请日 2008.03.12

(30)优先权数据
11/685164 2007.03.12 US
11/685173 2007.03.12 US

(62)分案原申请数据
200880015802.2 2008.03.12

(73)专利权人 思杰系统有限公司
地址 美国佛罗里达州

(72)发明人 R·普拉蒙东

(74)专利代理机构 北京泛华伟业知识产权代理有限公司 11280
代理人 王勇

(51)Int.Cl.
H04L 12/801(2013.01)
H04L 12/851(2013.01)
H04L 12/855(2013.01)
H04L 12/807(2013.01)

(56)对比文件
CN 1784856 A,2006.06.07,
EP 0782302 A2,1996.11.27,
US 2005/0254420 A1,2005.11.17,
US 7149222 B2,2006.12.12,
KAI-YEUNG SIU ET AL.《Intelligent congestion control for abr service in atm Networks》.《Computer communication review, ACM ,NEW YORK,NY,US》.1994,第89-91页及附图8.

审查员 张小倩

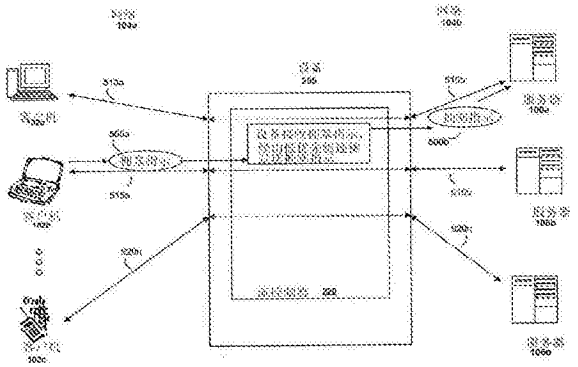
权利要求书3页 说明书45页 附图14页

(54)发明名称

用于在TCP拥塞控制中提供服务质量优先的系统和方法

(57)摘要

本发明描述用于动态控制连接的带宽的系统和方法。在有些实施例中，用于一个或者多个连接的代理可以经由一个或者多个连接分配、分布、或者产生网络拥塞的指示，用于引导连接的发送器降低它们的传输速率。代理可以以这种方式分配、分布或者产生这些指示，使得为一个或者多个连接提供服务质量或者确保多个连接在所接受的带宽限制中传输。在其他实施例中，传输层连接的发送器可以具有用于确定考虑了连接优先权的拥塞指示的响应的方法。在这些实施例中，发送器可以根据连接的优先权来在不同的速率处降低或者提高和传输速率相关的参数。



CN 103152279 B

1.一种动态改变对于一个或者多个传输层连接可用的有效带宽的方法，其通过装置在多个传输层连接之间分布拥塞事件，该方法包括：

(a)通过装置建立多个传输层连接，该一个或者多个传输层连接具有所分配的优先级；

(b)通过该装置经由多个传输层连接的第一传输层连接接收网路拥塞的第一指示；

(c)通过该装置根据所分配的优先级选择所述多个连接的第二传输层连接；并且

(d)通过该装置响应于接收所述第一指示来经由第二传输层连接传输拥塞事件的第二指示。

2.权利要求1的方法，其中，所述装置包括透明代理。

3.权利要求1的方法，还包括通过装置对于多个传输层连接执行加速功能的步骤。

4.权利要求1的方法，其中，步骤(a)包括通过装置建立多个传输控制协议(TCP)连接。

5.权利要求1的方法，其中，步骤(b)包括通过该装置经由多个传输层连接的第一传输层连接接收包括标记的显式拥塞通知(ECN)位的分组。

6.权利要求1的方法，其中，步骤(c)包括通过该装置根据相对于多个传输层连接的每一个的带宽利用数量所确定的优先级来选择所述多个传输层连接的第二传输层连接。

7.权利要求1的方法，其中，步骤(c)包括通过该装置根据所确定的优先级来选择来自所述多个传输层连接的子集的第二传输层连接，其中，所述子集包括符合如下条件的传输层连接:对于至少一个来回行程时间还没有经由其传输拥塞指示。

8.权利要求1的方法，其中，步骤(c)包括通过该装置选择所述多个传输层连接的具有最高带宽利用的传输层连接。

9.权利要求1的方法，其中，步骤(c)包括通过该装置选择所述多个传输层连接的传输超过所分配的带宽的最大数量的传输层连接。

10.权利要求1的方法，其中，步骤(c)包括通过该装置选择所述多个传输层连接的传输超过所分配的带宽最大百分比的数据的传输层连接。

11.权利要求1的方法，其中，步骤(c)包括通过该装置选择所述多个传输层连接的具有最低优先级的传输层连接。

12.权利要求1的方法，其中，步骤(c)包括通过该装置根据所确定的优先级来选择来自所述多个输入连接的子集的传输层连接，其中，所述子集由具有低于给定阈值的优先级的传输层连接组成。

13.权利要求1的方法，其中，步骤(d)包括通过该装置经由第二传输层连接传输拥塞事件的指示，其中该装置没有经由第二传输层连接接收到拥塞事件的指示。

14.权利要求1的方法，其中，步骤(d)包括通过该装置经由第二传输层连接传输分组丢失的指示。

15.权利要求1的方法，其中，步骤(d)包括通过该装置在第二传输层连接中传输包括标记的显式拥塞通知位的分组。

16.权利要求1的方法，其中，还包括如下步骤：

通过该装置根据所分配的优先级来选择多个连接的第三传输层连接；并且

通过该装置响应于接收第一指示经由第三传输层连接来传输拥塞事件的第三指示。

17.一种动态改变对于一个或者多个传输层连接可用的有效带宽的系统，其通过中间设备在多个传输层连接之间分布拥塞事件，所述系统包括：

用作多个传输层连接的中间设备的网络设备，该传输层连接的一个或者多个具有所分配的优先级，所述网络设备包括：

分组处理器，经由多个传输层连接的第一传输层连接接收网路拥塞的第一指示；和

流控制器，根据所分配的优先级选择多个连接的第二传输层连接；并且响应于接收所述第一指示来经由第二传输层连接传输拥塞事件的第二指示。

18.权利要求17的系统，其中，所述网络设备包括透明代理。

19.权利要求17的系统，其中，所述网络设备对于多个传输层连接执行加速功能。

20.权利要求17的系统，其中，所述分组处理器建立多个传输控制协议(TCP)连接。

21.权利要求17的系统，其中，所述分组处理器经由多个传输层连接的第一传输层连接接收包括标记的显式拥塞通知(ECN)位的分组。

22.权利要求17的系统，其中，所述流控制器根据相对于多个传输层连接的每一个的带宽利用数量所确定的优先级来选择所述多个传输层连接的第二传输层连接。

23.权利要求17的系统，其中，所述流控制器根据所确定的优先级来选择来自所述多个传输层连接的子集的第二传输层连接，其中，所述子集由这样的传输层连接组成：对于至少一个来回行程时间还没有经由该传输层连接传输拥塞指示。

24.权利要求17的系统，其中，所述流控制器选择所述多个传输层连接的具有最高带宽利用的传输层连接。

25.权利要求17的系统，其中，所述流控制器选择所述多个传输层连接的传输超过所分配的带宽的最大数量的传输层连接。

26.权利要求17的系统，其中，所述流控制器选择所述多个传输层连接的传输超过所分配的带宽最大百分比的数据的传输层连接。

27.权利要求17的系统，其中，所述流控制器选择所述多个传输层连接的具有最低优先级的传输层连接。

28.权利要求17的系统，其中，所述流控制器根据所确定的优先级来选择所述多个输入连接的子集的输入连接，其中，所述子集由具有低于给定阈值的优先级的传输层连接组成。

29.权利要求17的系统，其中，所述流控制器在所选择的传输层连接传输拥塞事件的指示，其中该网络设备没有经由第二传输层连接接收到拥塞事件的指示。

30.权利要求17的系统，其中，所述流控制器通过该网络设备并经由第二传输层连接传输分组丢失的指示。

31.权利要求17的系统，其中，所述流控制器通过该网络设备并经由第二传输层连接传输包括标记的显式拥塞通知位的分组。

32.一种动态改变对于一个或者多个传输层连接可用的有效带宽的方法，其通过装置在多个传输层连接之间分布拥塞事件，该方法包括：

(a)通过装置建立多个传输层连接；

(b)通过该装置经由多个传输层连接的第一传输层连接接收网路拥塞的第一指示；

(c)通过该装置根据多个传输层连接的每一个的带宽利用来选择所述多个连接的第二传输层连接；并且

(d)通过该装置响应于接收所述第一指示来经由第二传输层连接传输拥塞事件的第二指示。

33.权利要求32的方法，其中步骤(c)包括通过该装置根据所确定的优先级选择来自所述多个传输层连接的子集的第二传输层连接，其中，所述子集由这样的传输层连接组成：对于至少一个来回行程时间还没有经由该传输层连接传输拥塞指示。

34.权利要求32的方法，其中步骤(c)包括通过该装置选择所述多个传输层连接的具有最高带宽利用的传输层连接。

35.权利要求32的方法，其中，步骤(c)包括通过该装置选择所述多个传输层连接的传输超过所分配的带宽的最大数量的传输层连接。

36.权利要求32的方法，其中，步骤(c)包括通过该装置选择所述多个传输层连接的传输超过所分配的带宽最大百分比的数据的传输层连接。

37.一种动态改变对于一个或者多个传输层连接可用的有效带宽的系统，其通过中间设备在多个传输层连接之间分布拥塞事件，所述系统包括：

用作多个传输层连接的中间设备的网络设备，所述网络设备包括：

分组处理器，经由多个传输层连接的第一传输层连接接收网路拥塞的第一指示；和

流控制器，根据多个传输层连接的每一个的带宽利用来选择多个连接的第二传输层连接；并且响应于接收所述第一指示来经由第二传输层连接传输拥塞事件的第二指示。

38.权利要求37的系统，其中，所述流控制器根据所确定的优先级来选择来自所述多个传输层连接的子集的第二传输层连接，其中，所述子集由这样的传输层连接组成：对于至少一个来回行程时间还没有经由该传输层连接传输拥塞指示。

39.权利要求37的系统，其中，所述流控制器选择所述多个传输层连接的具有最高带宽利用的传输层连接。

40.权利要求37的系统，其中，所述流控制器选择所述多个传输层连接的传输超过所分配的带宽的最大数量的传输层连接。

41.权利要求37的系统，其中，所述流控制器选择所述多个传输层连接的传输超过所分配的带宽最大百分比的数据的传输层连接。

用于在TCP拥塞控制中提供服务质量优先的系统和方法

[0001] 本申请为申请号为200880015802.2、申请日为2008年3月12日、发明名称为“用于在TCP拥塞控制中提供服务质量优先的系统和方法”的申请的分案申请。

[0002] 相关申请

[0003] 本申请要求2007年3月12日提交的美国专利申请11/685,173名称为"Systems And Methods For Providing Quality of Service Precedence In TCP Congestion Control"和2007年3月12日提交的美国专利申请11/685,164名称为"Systems And Methods For Providing Virtual Fair Queuing Of Network Traffic"的优先权，其内容通过引用包含于此。

技术领域

[0004] 本发明总的涉及数据通信网络。更具体地，本发明涉及用于通过一个或者多个连接的代理来动态控制带宽的系统和方法。

背景技术

[0005] 在建网过程中，服务质量(QoS)系统可以被用来指定竞争分组流的优先级。在一些情况中，这些流可以是发送器和接收器之间的简单连接。在其他情况中，这些流可以是传递通过一个或者多个代理的发送器和接收器之间的连接，该代理的一些或者全部对于发送器和接收器可以是透明的。标准的QoS信令机制，如TOS(“服务类型”，RFC 1394)和之后的DSCP(“差分服务代码点”，RFC 2474，RFC 2475)位，存在于IP首部中。然而，这些不能以一致的方式布置在网络上，并且它们的存在或者特性是不可依赖的，除非当同一管理员控制整个网络时。当数据经过由第三方拥有的网络时，其可以是广域网(并且特别是因特网)中的情况，在一些情况中，仅可以呈现出最基本的IP功能性，并且瓶颈网关将忽略分组中的任意QoS位。

[0006] QoS通常在带宽瓶颈处实现。这些瓶颈有时发生在网络速度的由快至慢的转变处，例如在桥接LAN和WAN的装置处。如果在装置处存在来自不同流的分组的积压，该装置可以使用QoS做出关于哪个流应该具有下一个被发送的分组的决策。在传统的QoS中，假如其它环境(诸如过多丢失)不禁止连接实现其公平带宽共享，则调整连接之间的带宽可以使用公平排队实现。在公平排队的一些实现方案中，每个连接具有其自己的队列。当排队的总数变得过多时，就会从具有最长队列的连接丢失分组。由于公平排队(其基于循环来输出分组)的性质，具有最长队列的连接是超过最大裕度的其公平带宽共享的连接。从进行得太快的连接丢掉分组而不是随机的丢掉分组，这可以降低连接之间的不公平。不能使用它们的公平带宽共享的连接永远不可以作为目标，而连续超过公平带宽共享的那些连接可预见到更高的丢失率。

[0007] 然而，该QoS方法可以依赖于具有多个流中的分组的积压，这也许不适合用在出于其他考虑而试图最小化积压的情况中。这些QoS机制还不能应用到包括单个流的情况中。因此，需要一种系统和方法允许在存在分组的很小积压或者没有积压的情况中以及关于单个

流的情况中实现QoS。这些系统和方法甚至应该应用到其中流经过网络的部分在第三方控制下的的情况。

[0008] 许多网络业务量使用传输控制协议(TCP)协议，其是IP顶部上的基于连接的层。TCP使用在检测到分组的耗损时降低发送率并且在没有这种耗损时提高发送率的机制。传统的实现(诸如TCP Reno)可以使用网络上的一个来回行程的取样时间(RTT，发送一个分组并且接收来自接收单元的其到达的确认之间的时间)。在没有丢失分组的来回行程中，所传递的数据的数量(拥塞窗)可以增加一个完整尺寸的分组。扩大拥塞窗可以增加连接带宽、网络排队、分组丢失率或者这些的一些组合，这取决于网络状态。实现TCP中拥塞控制的替代方法是使用来回行程时间作为基本控制信号。这通过TCP Vegas和FAST TCP来使用。例如，在FASTTCP中，在这些实现方案中，可以基于最快或者平均来回行程时间与最近的分组来回行程时间的比较来增加或者降低拥塞窗。

[0009] 使用随机丢失来控制连接速度会导致连接之间带宽分配的不公平。假设两个连接，一个仅因为其不凑巧可以接收较少的带宽，其通过具有内部较高丢失率的链路(诸如无线网络)来传递，或者其由于具有比其伙伴更长的路径长度(并且因此具有更长的来回行程时间)而可以接收较少的带宽。由于连接在每个来回行程增速一次，所以具有短行程的连接的斜升率要比具有长行程的更陡峭。此外，TCP关于响应于网络事件的连接带宽的下降和斜升中的连接优先级没有区别。因此，需要一种系统和方法可以补偿基于随机丢失来分配带宽的潜在的不公平，并且允许QoS优先级被考虑到对于分组丢失和其他拥塞事件的响应中。

发明内容

[0010] 本发明涉及用于动态控制连接的带宽的系统和方法。在一些实施例中，用于一个或者多个连接的代理可以分配、分布、或者产生经由一个或者多个连接的网络拥塞的指示，用于引导连接的发送器降低它们的传输速率。代理可以以对一个或者多个连接提供服务质量或者以确保多个连接在所接受的带宽限制中传输的方式来分配、分布或者产生这些指示。在其他实施例中，传输层连接的发送器可以具有用于确定计及连接的优先权的拥塞指示的响应的方法。在这些实施例中，发送器可以根据连接的优先权来降低或者提高和不同的传输速率相关的参数。

[0011] 在第一方面中，本发明涉及通过装置在多个传输层连接之间分布拥塞事件来动态改变对于一个或者多个传输层连接可用的有效带宽的方法。在一个实施例中，该方法包括通过装置建立多个传输层连接，该传输层连接的一个或者多个具有所分配的优先级；并且通过该装置经由多个传输层连接的第一传输层连接接收网络拥塞的第一指示。该装置随后可以根据所分配的优先级选择多个连接的第二传输层连接；并且响应于接收所述第一指示来经由第二传输层连接传输拥塞事件的第二指示。在其他实施例中，该装置可以基于连接的所分配带宽来分配拥塞事件。

[0012] 在第二方面中，本发明涉及通过中间设备在多个传输层连接之间分布拥塞事件来动态改变对于一个或者多个传输层连接可用的有效带宽的系统。在一个实施例中，网络设备用作多个传输层连接的中间设备，该传输层连接的一个或者多个具有所分配的优先级。网络设备可以包括经由多个传输层连接的第一传输层连接接收网络拥塞的第一指示的分组处理器，和根据所分配的优先级选择多个连接的第二传输层连接的流控制器；并且响应

于接收所述第一指示来经由第二传输层连接传输拥塞事件的第二指示。在其他实施例中，该装置可以基于连接的所分配带宽来分配拥塞事件。

[0013] 在第三方面中，本发明涉及用于通过设备使用透明代理对传输层数据通信提供服务质量水平来控制连接带宽的方法。在一个实施例中，该方法包括通过对于发送器和接收器之间的传输层连接用作透明代理的设备来确定经由传输层连接的发送器的传输率不同于预定的传输率；通过该设备响应于该确定来产生包含指示的确认分组以改变传输速率；并且通过设备传输所产生的确认分组到发送器。在此实施例中，即使在没有从接收器接收到确认的情况下也可以产生该确认。该确认可以包括适当增加或者降低发送器的传输率的指示。

[0014] 在第四方面中，本发明涉及用于使用透明代理对传输层数据通信提供服务质量水平来控制连接带宽的计算机实现的系统。在一个实施例中，网络设备对于一个或者多个发送器和一个或者多个接收器之间的传输层连接用作透明代理。网络设备包括确定经由传输层连接的发送器的传输率不同于预定的传输率的流控制模块；并且响应于该确定来产生包含指示的确认以改变传输速率。网络设备还可以包括传输所产生的确认到发送器的分组处理模块。该确认可以包括适当增加或者降低发送器的传输率的指示。

[0015] 在第五方面中，本发明涉及用于由发送器根据分配给一个或者多个传输层连接的优先级来动态控制所述一个或者多个传输层连接的连接带宽的方法。在一个实施例中，该方法包括：通过发送器经由第一传输层连接传输数据，其中，该第一传输层连接在缺乏来自接收器的确认的情况下具有识别由发送器传输的数据数量的第一拥塞窗大小；通过发送器经由第一传输层连接接收经由第一传输层连接的分组丢失的指示；识别缩小因子，所述缩小因子对应于发送器分配给第一传输层连接的优先级；确定第二拥塞窗大小，第二拥塞窗大小包括通过缩小因子降低的第一拥塞窗大小；并且通过发送器根据第二拥塞窗大小经由第一传输层连接来传输数据。在其他实施例中，还可以应用类似的方法，其中连接优先级确定拥塞窗响应于无需接收分组丢失的指示的传递的时间间隔而增加的速率。

[0016] 在第六方面中，本发明涉及用于通过对于一个或者多个连接用作中间设备的网络设备根据分配给一个或者多个传输层连接的优先级来动态控制连接带宽的系统。在一个实施例中，系统包括对发送器和接收器之间的第一传输层连接用作中间设备的网络设备。所述网络设备可以包括分组处理引擎，其经由第一传输层连接传输数据，其中，该第一传输层连接具有对应于被传输的未确认数据的最大数量的第一拥塞窗大小；经由第一传输层连接接收分组丢失的指示；网络设备还可以包括和分组处理引擎通信的流控制模块，其计算缩小因子，所述缩小因子对应于该设备分配给第一传输层连接的优先级；计算第二拥塞窗大小，第二拥塞窗大小包括除以缩小因子的第一拥塞窗大小；通过第一传输层连接根据第二拥塞窗大小来传输数据。在其他实施例中，还可以使用类似的系统，其中连接优先级确定拥塞窗响应于无需接收分组丢失的指示的传递的时间间隔而增加的速率。

[0017] 在下面附图和具体实施方式中提出本发明的多种实施例的细节。

附图说明

[0018] 参考结合附图的以下描述，本发明的前述和其他对象、方面、特征和优势将会更加明显并更好理解，其中：

[0019] 图1A是客户机经由一个或者多个网络优化设备来访问服务器的网络环境的实施例的框图；

[0020] 图1B是客户机经由与其他网络设备结合的一个或者多个网络优化设备来访问服务器的网络环境的另一个实施例的框图；

[0021] 图1C是客户机经由独立布置或者和其他网络设备结合的单个网络优化设备来访问服务器的网络环境的另一个实施例的框图；

[0022] 图1D和1E是计算装置的实施例的框图；

[0023] 图2A是用于处理在客户机和服务器之间的通信的设备的实施例的框图；

[0024] 图2B是布置设备的网络优化特征的客户机和/或服务器的另一个实施例的框图；

[0025] 图3是使用网络优化特征来与服务器进行通信的客户机的实施例的框图；

[0026] 图4是取样TCP分组的框图；

[0027] 图5是用于通过装置在多个传输层连接中分布拥塞事件的系统的框图；

[0028] 图6是用于通过装置在多个传输层连接中分布拥塞事件的方法的流程图；

[0029] 图7是用于使用透明代理对传输连接提供服务质量水平来控制连接带宽的系统的框图；

[0030] 图8是用于使用透明代理对传输连接提供服务质量水平来控制连接带宽的方法的流程图；

[0031] 图9A是用于通过多个传输层连接的发送器根据连接的优先级来动态控制带宽的系统的框图；

[0032] 图9B是用于通过一个或者多个传输层连接的发送器根据被分配给一个或者多个连接的优先级来动态降低连接带宽的方法的流程图；和

[0033] 图9C是用于通过一个或者多个传输层连接的发送器根据被分配给一个或者多个连接的优先级来动态增加连接带宽的方法的流程图。

[0034] 根据以下结合附图提出的详细描述，本发明的特征和优势将变得更加明显，其中相同的参考特征在全文中是指对应的元件。在附图中，相似的附图标记通常指示相同的、功能类似的和/或结构类似的元件。

具体实施方式

[0035] 为了阅读下面的本发明的多个实施例的描述，说明下面的说明书的各部分以及它们相应的内容是有帮助的：

[0036] 部分A描述用于实现本发明的实施例的网络环境和计算环境；

[0037] 部分B描述用于将计算环境加速递送到远程用户的系统和设备架构的实施例；

[0038] 部分C描述用于加速在客户机和服务器之间的通信的客户机代理的实施例；和

[0039] 部分D描述用于有效处理网络拥塞的系统和方法的实施例。

[0040] A.网络和计算环境

[0041] 在讨论设备和/或客户机的系统和方法的实施例的细节之前，讨论可以部署这样的实施例的网络和计算环境是有帮助的。现在参考图1A，描述了网络环境的一个实施例。总的来说，网络环境包括经由一个或多个网络104、104’和104”与一个或多个服务器106a-106n(通常也被称为服务器106或远程机器106)通信的一个或多个客户机102a-102n(通常

也被称为本地机器102或客户机102)。在一些实施例中,客户机102经由一个或者多个网络优化设备200、200'(总的称之为设备200)与服务器106通信。在一个实施例中,网络优化设备200被设计、配置或者调整来优化广域网(WAN)网络业务量。在一些实施例中,第一设备200和第二设备200'相结合或者协同运行来优化网络业务量。例如,第一设备200可以位于分支结构和WAN连接之间而第二设备200'可以位于WAN和公司局域网(LAN)之间。设备200和200'可以一起工作来优化分支机构中的客户机和公司LAN上的服务器之间的WAN相关的网络业务量。

[0042] 虽然图1A示出客户机102和服务器106之间的网络104、网络104'和网络104"(总的称为网络104),但客户机102和服务器106可以在同一个网络104上。网络104、网络104'和网络104"可以是相同类型的网络或不同类型的网络。网络104可以是像公司内联网的局域网(LAN)、城域网(MAN)或者诸如因特网或万维网的广域网(WAN)。网络104、104'和104"可以是专用网或者公用网。在一个实施例中,网络104'或者网络104"可以是专用网而网络104可以是公用网。在一些实施例中,网络104可以是专用网而网络104'和/或网络104"可以是公用网。在另一个实施例中,网络104、网络104'和网络104'可以都是专用网。在一些实施例中,客户机102可以位于企业法人的分支机构,经由网络104上的WAN连接来与位于公司数据中心中的公司LAN上的服务器106进行通信。

[0043] 网络104可以是任意类型和/或形式的网络,并且可以包括下列任意一种网络:点到点网络、广播网、广域网、局域网、远程通信网、数据通信网、计算机网络、ATM(异步传送模式)网络、SONET(同步光学网络)网络、SDH(同步数字系列)网络、无线网络和有线网络。在一些实施例中,网络104可以包括诸如红外信道或卫星频带的无线链路。网络104的拓扑结构可以是总线型、星型或环型网络拓扑结构。网络104以及网络拓扑结构可以是能够支持此处描述的操作的本领域内普通技术人员所知的任一种这样的网络或网络拓扑结构。

[0044] 如图1A所示,在网络104和104'之间示出第一网络优化设备200并且在网络104'和104"之间示出第二网络优化设备200'。在一些实施例中,设备200可以位于网络104上。例如,公司企业可以在所述分支机构处部署设备200。在其它实施例中,设备200可以位于网络104'上。在一些实施例中,设备200'可以位于网络104'或者网络104"上。例如设备200可以位于公司的数据中心。在一个实施例中,设备200和设备200'可以位于相同网络上。在另一个实施例中,设备200和设备200'可以位于不同网络上。

[0045] 在一个实施例中,设备200是用于加速、优化或者以其他方式改善任意类型和形式的网络业务量的性能、操作或服务质量的装置。在一些实施例中,设备200是一个性能强化的代理。在其它实施例中,设备200是任意类型和形式的WAN优化或加速装置,有时也被称为WAN优化控制器。在一个实施例中,设备200是由位于Ft.Lauderdale Florida的Citrix Systems公司出品的被称为WANScaler的产品实施例中的任意一种。在其它实施例中,设备200包括由位于Seattle,Washington的F5 Networks公司出品的被称为BIG-IP链路控制器和WANjet的产品实施例中的任意一种。在另一个实施例中,设备200包括由位于Sunnyvale,California的Juniper NetWorks公司出品的WX和WXC WAN加速装置平台中的任意一种。在一些实施例中,设备200包括由San Francisco,California的Riverbed Technology公司出品的虹鳟(steelhead)系列WAN优化设备中的任意一种。在其它实施例中,设备205包括由位于Roseland,NewJersey的Expand Networks公司出品的WAN相关装置中的任意一种。在一个

实施例中，设备200包括由位于Cupertino，California的Packeteer公司出品的任意一种WAN相关设备，例如由Packeteer提供的PacketShaper、iShared和SkyX产品实施例。在又一个实施例中，设备200包括由位于San Jose，California的Cisco Systems公司出品的任意WAN相关设备和/或软件，例如Cisco广域网应用服务软件和网络模块以及广域网引擎设备。

[0046] 在一些实施例中，设备200提供用于分支机构或远程办公室的应用和数据加速业务。在一个实施例中，设备200包括广域文件服务(WAFS)的优化。在另一个实施例中，设备200加速文件的递送，例如经由公共因特网文件系统(CIFS)协议。在其它实施例中，设备200在存储器和/或存储设备中提供高速缓存来加速应用和数据的递送。在一个实施例中，设备205提供在任意级别的网络堆栈或在任意的协议或网络层的网络业务量的压缩。在另一个实施例中，设备200提供传输层协议优化、流量控制、性能增强或修改和/或管理，以加速WAN连接上的应用和数据的递送。例如，在一个实施例中，设备200提供传输控制协议(TCP)优化。在其它实施例中，设备200提供对于任意会话或应用层协议的优化、流量控制、性能增强或修改和/或管理。在下面B部分中讨论设备200的优化技术、操作和架构的进一步细节。

[0047] 仍旧参考图1A，网络环境可以包括多个、逻辑分组的服务器106。在这些实施例中，服务器的逻辑组可以被称为服务器群组38。在这些实施例中的一些实施例中，服务器106可以是在地理上分散的。有时候，群组38可以被管理为单一的实体。在其它实施例中，服务器群组38包括多个服务器群组38。在一个实施例中，服务器群组代表一个或多个客户机102来执行一个或多个应用。

[0048] 在每个群组38中的服务器106可以是不同种类的。一个或多个服务器106可以根据一种类型的操作系统平台(例如，由位于Redmond，Washington的微软公司出品的WINDOWS NT)来进行操作，而一个或多个其它的服务器106可以根据另一种类型的操作系统平台(例如，Unix或Linux)来进行操作。每个群组38中的服务器106不需要与同一群组38中的另一个服务器106物理上接近。因此，逻辑上被分组为群组38的服务器106的组可以使用广域网(WAN)连接或城域网(MAN)连接来互连。例如，群组38可以包括在物理上位于不同的洲或位于一个洲、国家、州、城市、校园或房间的不同区域的服务器106。如果使用局域网(LAN)连接或一些形式的直接连接来连接服务器106，则可以增加在群组38中的服务器106之间的数据传输速度。

[0049] 服务器106可以是文件服务器、应用服务器、web服务器、代理服务器或网关服务器。在一些实施例中，服务器106可以有能力起到应用服务器或主应用服务器的作用。在一个实施例中，服务器106可以包括活动目录(Active Directory)。客户机102也可以被称为客户机节点或端点。在一些实施例中，客户机102有能力起到寻求访问服务器上的应用的客户机节点以及作为对于其它的客户机102a-102n提供对寄载的应用的访问的应用服务器的作用。

[0050] 在一些实施例中，客户机102与服务器106进行通信。在一个实施例，客户机102直接与群组38中的服务器106的其中一个进行通信。在另一个实施例中，客户机102执行程序邻近应用以与群组38中的服务器106进行通信。在又一个实施例中，服务器106提供主节点的功能。在一些实施例中，客户机102通过网络104与群组38中的服务器106进行通信。例如，通过网络104，客户机102可以请求执行由群组38中的服务器106a-106n寄载的多个应用，并接收应用执行的结果输出用于显示。在一些实施例中，只有主节点提供所要求的识别并提

供与寄载被请求的应用的服务器106'相关的地址信息的功能。

[0051] 在一个实施例中，服务器106提供web服务器的功能。在另一个实施例中，服务器106a接收来自客户机102的请求，将请求转发到第二服务器106b，并使用来自于服务器106b的对请求的响应来对客户机102的请求进行响应。在又一个实施例中，服务器106获得客户机102可用的应用的列举以及与寄载由所述应用的列举所标识的应用的服务器106相关的地址信息。在又一个实施例中，服务器106使用web接口将对请求的响应提供给客户机102。在一个实施例中，客户机102直接与服务器106进行通信以访问所标识的应用。在另一个实施例中，客户机102接收由执行服务器106上的标识的应用所生成的诸如显示数据的应用输出数据。

[0052] 与其他设备一起布置

[0053] 现在参考图1B，描述网络环境的另一个实施例，其中，网络优化设备200和诸如网关、防火墙或者加速设备的一个或者多个其他设备205、205'(总的称为设备205或者第二设备205)布置在一起。例如，在一个实施例中，设备205是防火墙或者安全设备，而设备205'是LAN加速装置。在一些实施例中，客户机102可以经由一个或者多个第一设备200和一个或者多个第二设备205与服务器106相通信。

[0054] 一个或者多个设备200和205可以布置在客户机102和服务器106之间的网络或者网络通信路径中的任一点处。在一些实施例中，第二设备205可以布置在和第一设备200相同的网络104上。在其他实施例中，第二设备205可以布置在和第一设备200不同的网络104上。在又一个实施例中，第一设备200和第二设备205在例如网络104的相同网络上，而第一设备200'和第二设备205'可以位于诸如网络104"的相同网络上。

[0055] 在一个实施例中，第二设备205包括任一类型和形式传输控制协议或者传输后终接装置，诸如网关或者防火墙装置。在一个实施例中，设备205通过建立与客户机的第一传输控制协议连接以及与第二设备或者服务器的第二传输控制连接，来终接传输控制协议。在另一个实施例中，设备205通过改变、管理或者控制客户机和服务器或者第二设备之间的传输控制协议连接的行为，来终接传输控制协议。例如，设备205可以以有效终接传输控制协议连接或者作用为或者模拟为终接连接的方式来改变、排列、转发或者传输网络分组。

[0056] 在一些实施例中，第二设备205是性能强化代理。在一个实施例中，设备205提供虚拟专用网络(VPN)连接。在一些实施例中，设备205提供安全套接字层VPN(SSL VPN)连接。在其他实施例中，设备205提供基于IPsec(互联网协议安全)的VPN连接。在一些实施例中，设备205提供任意一个或者多个以下的功能性：压缩、加速、负载平衡、切换/路由、高速缓存和传输控制协议(TCP)加速。

[0057] 在一个实施例中，设备205是位于Ft.Lauderdale Florida的Citrix Systems公司出品的被称为访问网关、应用防火墙、应用网关或者WANScaler的产品实施例。由此，在一些实施例中，设备205包括任一逻辑、功能、规则或者操作来执行诸如SSL VPN连接、SSL卸载、切换/负载平衡、域名服务解析、LAN加速和应用防火墙的服务或者功能性。

[0058] 在一些实施例中，设备205提供在客户机102和服务器106之间的SSL VPN连接。例如，第一网络104上的客户机102请求建立到第二网络104'上的服务器106的连接。在一些实施例中，第二网络104"是不可从第一网络104路由的。在其它实施例中，客户机102在公用网104上，而服务器106在诸如公司网的专用网104'上。在一个实施例中，客户机代理拦截第一

网络104上的客户机102的通信，加密所述通信，并经由第一传输层连接发送所述通信到设备205。设备205将第一网络104上的第一传输层连接关联到第二网络104上的到服务器106的第二传输层连接。设备205从客户机代理接收被拦截的通信，解密所述通信，并经由第二传输层连接发送所述通信到第二网络104上的服务器106。第二传输层连接可以是池化的传输层连接。在一个实施例中，设备205提供在两个网络104和104'之间用于客户机102的端到端安全传输层连接。

[0059] 在一个实施例中，设备205在虚拟专用网104上寄载客户机102的内联网网际协议或内联网IP地址。客户机102具有诸如第一网络104上的网际协议(IP)地址和/或主机名的本地网络标识符。当经由设备205连接到第二网络104'时，设备205在第二网络104'上为客户机102建立、分配或者以其他方式提供内联网IP，其是诸如IP地址和/或主机名的网络标识符。使用客户机的建立的内联网IP，设备205在第二或专用网104'上监听并接收指向客户机102的任意通信。在一个实施例中，设备205在第二专用网104上充当或代表客户机102。

[0060] 在一些实施例中，设备205具有提供用于操控诸如SSL或者TLS的任意安全相关的协议或者其中涉及的任意功能的处理的逻辑、商业规则、功能或者操作的加密引擎。例如，加密引擎加密和解密经由设备205通信的网络分组或者其中任意部分。加密引擎还可以代表客户机102a-102n、服务器106a-106n或者设备200、205设置或者建立SSL或者TLS连接。由此，加密引擎提供SSL处理的卸载和加速。在一个实施例中，加密引擎使用隧穿协议来在客户机102a-102n和服务器106a-106n之间提供虚拟专用网络。在一些实施例中，加密引擎使用加密处理器。在其他实施例中，加密引擎包括在加密处理器上运行的可执行指令。

[0061] 在一些实施例中，设备205提供下列一个或多个加速技术来在客户机102和服务器106之间进行通信：1)压缩；2)解压缩；3)传输控制协议池；4)传输控制协议多路复用；5)传输控制协议缓冲；以及6)高速缓存。在一个实施例中，设备200通过重复地打开与每个服务器106的一个或多个传输层连接并维持这些连接以允许客户机经由因特网的重复数据访问来减轻服务器106的通过反复打开和关闭到客户机102的传输层连接所造成的大量处理负载。这个技术在这里被称为“连接池(connection pooling)”。

[0062] 在一些实施例中，为了经由池化的传输层连接来无缝拼接从客户机102到服务器106的通信，设备205通过在传输层协议级修改序号和确认号来转换或多路复用通信。这被称为“连接多路复用”。在一些实施例中，不需要应用层协议相互作用。例如，在入站分组(即，接收来自客户机102的分组)的情况中，所述分组的源网络地址被改变为设备205的输出端口的网络地址，而目的网络地址被改变为预期的服务器的网络地址。在出站分组(即，接收来自服务器106的一个分组)的情况中，源网络地址被从服务器106的网络地址改变为设备205的输出端口的网络地址，而目的地址被从设备205的网络地址改变为请求的客户机102的网络地址。所述分组的序号和确认号也被转换为到客户机102的设备205的传输层连接上由客户机102所期待的序号和确认。在一些实施例中，传输层协议的分组校验和被重新计算以计及这些转换。

[0063] 在另一个实施例中，设备205为客户机102和服务器106之间的通信提供切换或负载平衡功能。在一些实施例中，设备205根据层4净荷或应用层请求数据来分配业务量并将客户机请求引向服务器106。在一个实施例中，虽然网络分组的网络层或层2标识了目的地服务器106，但设备205通过作为传输层分组的净荷而携带的应用信息和数据来确定服务器

106以分配网络分组。在一个实施例中，设备205的健康监测程序监控服务器的健康以确定为其分配客户机请求的服务器106。在一些实施例中，如果设备205探测到服务器106不可用或具有超过预定阈值的负载，则设备205可以将客户机请求引向或分配到另一个服务器106。

[0064] 在一些实施例中，设备205充当域名服务(DNS)解析器或者以其他方式提供来自于客户机102的DNS请求的解析。在一些实施例中，设备拦截由客户机102发送的DNS请求。在一个实施例中，设备205响应具有设备205的IP地址或由设备205寄载的IP地址的客户机DNS请求。在该实施例中，客户机102发送用于域名的网络通信到设备200。在另一个实施例中，设备200响应具有第二设备200'的IP地址或由第二设备200'寄载的IP地址的客户机的DNS请求。在一些实施例中，设备205响应具有由设备200确定的服务器106的IP地址的客户机的DNS请求。

[0065] 在又一个实施例中，设备205为客户机102和服务器106之间的通信提供应用防火墙功能。在一个实施例中，策略引擎295'提供用于检测和阻塞非法请求的规则。在一些实施例中，应用防火墙防止拒绝服务(DoS)攻击。在其它实施例中，设备检查被拦截的请求内容以识别和阻塞基于应用程序的攻击。在一些实施例中，规则/策略引擎包括用于提供对多个种类和类型的基于web或因特网的脆弱点的保护的一个或多个应用防火墙或安全控制策略，例如下列的一个或多个：1)缓冲器溢出，2)CGI-BIN参数操纵，3)形式/隐藏字段操纵，4)强制浏览，5)cookie或会话中毒，6)破译的访问控制表(ACLs)或弱的口令，7)跨站点的脚本(XSS)，8)命令注入，9)SQL注入，10)错误触发感测信息泄漏，11)加密技术的不安全使用，12)服务器误配置，13)后门和调试选择，14)web站点毁损，15)平台或操作系统的脆弱点，以及16)零天攻击。在一个实施例中，设备的应用防火墙以检查或分析网络通信是否有下列的一种或多种情况的形式来提供HTML格式字段的保护：1)返回所需的字段，2)不允许附加字段，3)只读和隐藏字段强制(enforcement)，4)下拉列表和单选按钮字段的一致，以及5)格式字段最大长度强制。在一些实施例中，设备205的应用防火墙确保cookies不被修改。在其它实施例中，设备205通过强制实施合法URL来防止强制浏览。

[0066] 还是在又一些实施例中，应用防火墙设备205保护在网络通信中包含的任意机密信息。设备205可以根据策略引擎的规则或策略来检查或分析任意网络通信以识别在网络分组的任意字段中的任意机密信息。在一些实施例中，应用防火墙在网络通信中识别信用卡号、口令、社会保险号、姓名、病人代码、联系信息和年龄的一次或多次出现。网络通信的编码部分可以包括这些出现或机密信息。在一个实施例中，根据这些出现，应用防火墙可以在网络通信上采取策略行动，例如阻止网络通信的传输。在另一个实施例中，应用防火墙可以重写、移除或者以其他方式掩盖这样识别出的出现或机密信息。

[0067] 尽管总的称为网络优化或者第一设备200和第二设备205，但是第一设备200和第二设备205可以是同样类型和形式的设备。在一个实施例中，第二设备205可以执行和第一设备100相同的功能性或者部分，反之亦然。例如，第一设备200和第二设备205可以一起提供加速技术。在一个实施例中，第一设备可以执行LAN加速而第二设备执行WAN加速，或者反之亦然。在另一个例子中，第一设备200还可以是传输控制协议终接装置，如同第二设备205一样。进一步，尽管设备200和205视为网络上的单独设备，但是设备200和/或205可以是任一客户机102或者服务器106的一部分。

[0068] 现在参考图1C，描述用于布置设备200的网络环境的其他实施例。在如图1C的上部所描述的另一个实施例中，设备200可以布置为网络104上的单个设备或者单个代理。例如，设备200可以被设计、构建或者调整来执行此处讨论的WAN优化技术，而不需要第二协作设备200'。在如图1C的下部所描述的其它实施例中，单个设备200可以和一个或者多个第二设备205一起布置。例如，诸如Citrix WANScaler设备的WAN加速第一设备200可以和诸如Citrix NatScaler设备的LAN加速或者应用防火墙第二设备205一起布置。

[0069] 计算装置

[0070] 客户机102、服务器106和设备200和205可以被部署和/或执行在任意类型和形式的计算装置上，例如可以在任意类型和形式的网络上通信并执行此处描述的操作的计算机、网络装置或设备。图1C和1D描述了可用于实施客户机102、服务器106或设备200的实施例的计算装置100的框图。如图1C和1D所示，每个计算装置100包括中央处理单元101和主存储器单元122。如图1C所示，计算装置100可以包括可视显示装置124、键盘126和/或诸如鼠标的定点装置127。每个计算装置100也可以包括附加的可选元件，例如一个或多个输入/输出装置130a-130b(通常使用附图标记130来指示)以及与中央处理单元101通信的高速缓存140。

[0071] 中央处理单元101是响应并处理取自主存储器单元122的指令的任意逻辑电路。在许多实施例中，中央处理单元由微处理器单元提供，例如：由位于Mountain View，California的Intel公司出品的产品；由位于Schaumburg，Illinois的Motorola公司出品的产品；由位于Santa Clara，California的Transmeta公司出品的产品；由位于White Plains，New York的国际商业机器公司出品的RS/6000处理器；或者由位于Sunnyvale，California的Advanced Micro Devices公司出品的产品。计算装置100可以基于任意的这些处理器、或者可以如此处所描述地操作的任意其它处理器。

[0072] 主存储器单元122可以是能够保存数据并允许微处理器101直接访问任意存储位置的一个或多个存储芯片，例如静态随机存取存储器(SRAM)、突发式SRAM或同步突发式SRAM(BSRAM)、动态随机存取存储器(DRAM)、快速页面模式DRAM(FPM DRAM)、增强型DRAM(EDRAM)、扩展数据输出RAM(EDO RAM)、扩展数据输出DRAM(EDO DRAM)、突发式扩展数据输出DRAM(BEDO DRAM)、增强型DRAM(EDRAM)、同步DRAM(SDRAM)、JEDEC SRAM、PC100 SDRAM、双数据速率SDRAM(DDR SDRAM)、增强型SDRAM(ESDRAM)、同步链接DRAM(SLDRAM)、直接Rambus DRAM(DRDRAM)、或铁电RAM(FRAM)。主存储器122可以基于任意一种上面描述的存储芯片、或者可以如此处所描述地操作的任意其它可用的存储芯片。在图1C中所示的实施例中，处理器101通过系统总线150与主存储器122进行通信(在下面进行更详细的描述)。图1C描述了在其中处理器通过存储器端口103直接与主存储器122通信的计算装置100的实施例。例如，在图1D中，主存储器122可以是DRDRAM。

[0073] 图1D描述了在其中主处理器101通过有时被称为背端总线的次级总线来直接与高速缓存140通信的实施例。在其它实施例中，主处理器101使用系统总线150与高速缓存140进行通信。高速缓存140典型地具有比主存储器122更快的响应时间，并且典型地通过SRAM、BSRAM或EDRAM来提供。在图1C中所示的实施例中，处理器101通过本地系统总线150与多个I/O装置130进行通信。多种总线可以用来将中央处理单元101连接到任意一种I/O装置130，所述总线包括VESA VL总线、ISA总线、EISA总线、微通道架构(MCA)总线、PCI总线、PCI-X总

线、PCI-Express总线或NuBus。对于I/O装置是视频显示器124的实施例，处理器101可以使用高级图形端口(AGP)来与显示器124进行通信。图1D描述了在其中主处理器101通过HyperTransport、快速I/O或InfiniBand来直接与I/O装置130通信的计算机100的一个实施例。图1D还描述了混合本地总线和直接通信的一个实施例：处理器101使用本地互连总线与I/O装置130进行通信，同时直接与I/O装置130进行通信。

[0074] 计算装置100可以支持任意适当的安装装置116，例如用于接收像3.5英寸、5.25英寸磁盘或ZIP磁盘这样的软盘的软盘驱动器、CD-ROM驱动器、CD-R/RW驱动器、DVD-ROM驱动器、多种格式的磁带驱动器、USB装置、硬盘驱动器或适于安装像任意客户机代理120或其部分的软件和程序的任意其它装置。计算装置100还可以包括存储装置128，例如一个或多个硬盘驱动器或独立盘的冗余阵列，用于保存操作系统及其它相关软件，以及用于保存诸如与客户机代理120相关的任意程序的应用软件程序。可选地，任意一种安装装置116还可以被用作存储装置128。另外，操作系统和软件可以从可引导介质中运行，所述可引导介质例如像KNOPPIX®的可引导CD，作为来自于knoppix.net可用作GNU/Linux分发的GNU/Linux的可引导CD。

[0075] 进一步地，计算装置100可以包括通过多种连接接口到局域网(LAN)、广域网(WAN)或因特网的网络接口118，所述多种连接包括但不限于标准电话线、LAN或WAN链路(例如，802.11、T1、T3、56kb、X.25)、宽带连接(例如，ISDN、帧中继、ATM)、无线连接或上述任意或所有连接的一些组合。网络接口118可以包括内置网络适配器、网络接口卡、PCMCIA网卡、插件总线网络适配器、无线网络适配器、USB网络适配器、调制解调器或适于将计算装置100接口到可以传达并执行此处所描述的操作的任意类型的网络的任意其它装置。各式各样的I/O装置130a-130n可以存在于计算装置100中。输入装置包括键盘、鼠标、轨迹垫、轨迹球、麦克风以及绘画板。输出装置包括视频显示器、扬声器、喷墨打印机、激光打印机和染料升华打印机。I/O装置130可以由如图1E所示的I/O控制器123控制。I/O控制器可以控制诸如键盘126和例如鼠标或光笔的定点装置127的一个或多个I/O装置。进一步地，I/O装置还可以为计算装置100提供存储装置128和/或安装介质116。还是在其它实施例中，计算装置100可以提供USB连接以接收诸如由位于LosAlamitos,California的Twintech Industry公司出品的USB闪存驱动器系列装置这样的便携USB存储装置。

[0076] 在一些实施例中，计算装置100可以包括或连接到多个显示装置124a-124n，每个显示装置可以是相同或不同的类型和/或形式。因而，任意一种I/O装置130a-130n和/或I/O控制器123可以包括任意类型和/或形式的适当的硬件、软件或硬件和软件的组合，以支持、允许或提供通过计算装置100连接和使用多个显示装置124a-124n。例如，计算装置100可以包括任意类型和/或形式的视频适配器、视频卡、驱动器和/或库，以接口、通信、连接或以其他方式使用显示装置124a-124n。在一个实施例中，视频适配器可以包括多个连接器以接口多个显示装置124a-124n。在其它实施例中，计算装置100可以包括多个视频适配器，每个视频适配器连接到一个或多个显示装置124a-124n。在一些实施例中，计算装置100的操作系统的任意部分可以被配置用于使用多个显示器124a-124n。在其它实施例中，一个或多个显示装置124a-124n可以由一个或多个诸如例如通过网络连接到计算装置100的计算装置100a和100b的其它的计算装置来提供。这些实施例可以包括被设计和构建为将另一个计算机的显示装置用作计算装置100的第二显示装置124a的任意类型的软件。本领域普通技术

人员将认识和理解计算装置100可以被配置为具有多个显示装置124a-124n的多个方法和实施例。

[0077] 在进一步的实施例中，I/O装置130可以是在系统总线150和外部通信总线之间的桥170，所述外部通信总线例如USB总线、Apple Desktop总线、RS-232串行连接、SCSI总线、FireWire总线、FireWire 800总线、以太网总线、AppleTalk总线、吉比特以太网总线、异步传送模式总线、HIPPI总线、超HIPPI总线、SerialPlus总线、SCI/LAMP总线、FibreChannel总线或串行附加小型计算机系统接口总线。

[0078] 图1C和1D中描述类型的计算装置100典型地在控制任务的调度和对系统资源的访问的操作系统的控制下操作。计算装置100可以运行任意操作系统，例如任意一种版本的微软®Windows操作系统、不同版本的Unix和Linux操作系统、用于Macintosh计算机的任意版本的MacOS®、任意的嵌入式操作系统、任意的实时操作系统、任意的开放源操作系统、任意的专用操作系统、用于移动计算装置的任意操作系统、或者可以运行在计算装置上并执行此处所描述的操作的任意其它操作系统。典型的操作系统其中包括：WINDOWS 3.x、WINDOWS 95、WINDOWS 98、WINDOWS 2000、WINDOWS NT 3.51、WINDOWS NT 4.0、WINDOWS CE、WINDOWS 2003、WINDOWS XP和WINDOWS SISTA，所有这些均由位于Redmond，Washington的微软公司出品；由位于Cupertino，California的苹果计算机出品的MacOS和OS X；由位于Armonk，New York的国际商业机器公司出品的OS/2；以及由位于Salt Lake City，Utah的Caldera公司发布的可免费使用的Linux操作系统或者任意类型和/或形式的Unix操作系统(诸如称为Solaris/Sparc，Solaris/x86，AIX IBM，HP UX，和SGI(Silicon Graphics)的Unix的这些版本)，以及其它。

[0079] 在其它实施例中，计算装置100可以具有符合所述装置的不同的处理器、操作系统和输入装置。例如，在一个实施例中，计算机100是由Palm公司出品的Treo180、270、1060、600或650智能电话。在该实施例中，Treo智能电话在PalmOS操作系统的控制下操作，并包括指示笔输入装置以及五向导航装置。在另一个实施例中，计算装置100可以是具有ARM(高级RISC机器)类型的处理器的WinCE或者PchetPC。在一个例子中，计算装置100包括Finland的Nokia出品的Series 80(Nokia 9500或者Nokia 9300)类型的智能电话，其可以运行United Kingdom，London的Symbian软件有限公司出品的Symbian OS或者EPOC移动操作系统。在另一个实施例中，计算装置100可以包括Illimois，Schaumburg的Motorola公司出品的FOMA M100品牌的智能电话，并且操作EPOC或者Symbian OS操作系统。在又一个实施例中，计算装置100包括North Carolina，Research Triangle Park的索尼爱立信通信(USA)公司出品的Sony Ericsson P800、P900或者P910Alpha模型电话(model phone)。此外，计算装置100可以是任意工作站、台式计算机、膝上型或笔记本计算机、服务器、便携计算机、移动电话、智能电话、任意其它计算机、或者可以通信并具有执行此处所描述的操作的足够的处理器能力和存储容量的其它形式的计算或电信装置。

[0080] B、系统和设备架构

[0081] 现在参考图2A，描述了用于递送和/或操作客户机上的计算环境的设备200的系统环境和架构的实施例。在一些实施例中，服务器106包括用于将计算环境或应用和/或数据文件递送给一个或多个客户机102的应用递送系统290。简单概述，客户机102经由网络104和设备200与服务器106通信。例如，客户机102可以驻留在例如分支机构的公司的远程办公

室，而服务器106可以驻留在公司的数据中心。客户机102包括客户机代理120和计算环境215。计算环境215可以执行或操作用来访问、处理或使用数据文件的应用。可以经由设备200和/或服务器106来递送计算环境215、应用和/或数据文件。

[0082] 在一些实施例中，设备200加速将计算环境215或其任意部分递送给客户机102。在一个实施例中，设备200通过应用递送系统290来加速计算环境215的递送。例如，此处描述的实施例可以用来将可由应用处理的流应用和数据文件加速从中央的公司数据中心递送到远程用户的位置，例如公司的分支机构。在另一个实施例中，设备200加速在客户机102和服务器106之间的传输层业务量。在另一个实施例中，设备200控制、管理、或者调整传输层协议来加速递送计算环境。在一些实施例中，设备200使用高速缓存和/或压缩技术来加速递送计算环境。

[0083] 在一些实施例中，应用递送管理系统290根据多个执行方法以及根据经由策略引擎295应用的任意验证和授权策略来提供将计算环境递送到远端或另外的用户的桌面的应用递送技术。使用这些技术，远程用户可以从任意网络连接装置100获取计算环境以及访问服务器存储的应用和数据文件。在一个实施例中，应用递送系统290可以驻留于服务器106或在服务器106上执行。在另一个实施例中，应用递送系统290可以驻留于多个服务器106a-106n上或在多个服务器106a-106n上执行。在一些实施例中，应用递送系统190可以在服务器群组38中执行。在一个实施例中，执行应用递送系统190的服务器106还可以存储或提供应用和数据文件。在另一个实施例中，第一组的一个或多个服务器106可以执行应用递送系统290，而不同的服务器106n可以存储或提供应用和数据文件。在一些实施例中，应用递送系统290、应用和数据文件中的每一个可以驻留或位于不同的服务器上。在又一个实施例中，应用递送系统290的任意部分可以驻留、执行或保存或被分配于设备200或多个设备。

[0084] 客户机102可以包括用于执行使用或处理数据文件的应用的计算环境215。客户机102可以经由网络104、104'和设备200来从服务器106请求应用和数据文件。在一个实施例中，设备200可以将来自于客户机102的请求转发到服务器106。例如，客户机102可以不具有本地存储或可存取的应用和数据文件。响应于请求，应用递送系统290和/或服务器106可以递送应用和数据文件到客户机102。例如，在一个实施例中，服务器106可以以应用流的形式发送该应用，以在客户机102上的计算环境215中进行操作。

[0085] 在一些实施例中，应用递送系统290包括Citrix Systems公司的例如MetaFrame或Citrix表示(Presentation)服务器TM的Citrix访问套件TM的任意部分和/或由微软公司出品的任意一种微软®Windows终端服务。在一个实施例中，应用递送系统290可以通过远程显示协议或以其它方式通过基于远程或基于服务器的计算来递送一个或多个应用到客户机102或用户。在另一个实施例中，应用递送系统290可以通过应用的流式传输来递送一个或多个应用到客户机或用户。

[0086] 在一个实施例中，应用递送系统290包括用于控制和管理应用执行方法的访问、选择以及应用的递送的策略引擎295。在一些实施例中，策略引擎295确定用户或客户机102可以访问的一个或多个应用。在另一个实施例中，策略引擎295确定应用应该如何被递送给用户或客户机102，例如执行方法。在一些实施例中，应用递送系统290提供从中选择应用执行方法的多个递送技术，例如基于服务器的计算、本地流式传输或递送应用给客户机120以用于本地执行。

[0087] 在一个实施例中，客户机102请求执行应用程序而包括服务器106的应用递送系统290选择执行应用程序的方法。在一些实施例中，服务器106从客户机102接收证书。在另一个实施例中，服务器106从客户机102接收可用应用的列举的请求。在一个实施例中，响应于所述请求或收到的证书，应用递送系统290列举客户机102可用的多个应用程序。应用递送系统290接收请求以执行所列举的应用。应用递送系统290选择预定数目的方法中的一个来执行列举的应用，例如响应于策略引擎的策略。应用递送系统290可以选择一个执行应用的方法，使得客户机102可以接收通过在服务器106上执行应用程序而生成的应用输出数据。应用递送系统290可以选择执行应用的方法，使得本地机器102可以在检索包括应用的多个应用文件之后本地执行所述应用程序。在又一个实施例中，应用递送系统290可以选择执行应用的方法以经由网络104将应用流式传输到客户机102。

[0088] 客户机102可以执行、操作或以其他方式提供应用，所述应用可以是任意类型和/或形式的软件、程序或可执行指令，例如任意类型和/或形式的web浏览器、基于web的客户机、客户机-服务器应用、瘦-客户机的计算客户机、ActiveX控件、或Java小程序、或可以在客户机102上执行的任意其它类型和/或形式的可执行指令。在一些实施例中，应用可以是代表客户机102在服务器106上执行的基于服务器或基于远程的应用。在一个实施例中，服务器106可以使用任意瘦-客户机或远程显示协议来显示输出到客户机102，所述远程显示协议例如由位于Ft.Lauderdale,Florida的Citrix Systems公司出品的独立计算架构(ICA)协议或由位于Redmond,Washington的微软公司出品的远程桌面协议(RDP)。应用可以使用任意类型的协议，并且它可以是例如HTTP客户机、FTP客户机、Oscar客户机或Telnet客户机。在其它实施例中，应用包括与VoIP通信相关的任意类型的软件，例如软IP电话。在进一步的实施例中，应用包括与实时数据通信相关的任意应用，例如用于流式传输视频和/或音频的应用。

[0089] 在一些实施例中，服务器106或服务器群组38可以运行一个或多个应用，例如提供瘦-客户机计算的应用或远程显示表示应用的应用。在一个实施例中，服务器106或服务器群组38作为应用而执行Citrix Systems公司的例如MetaFrame或Citrix表示服务器TM的Citrix访问套件TM的任意部分和/或由微软公司出品的任意一种微软®Windows终端服务。在一个实施例中，应用是由位于Fort Lauderdale,Florida的Citrix Systems公司开发的ICA客户机。在其它实施例中，应用包括由位于Redmond,Washington的微软公司开发的远程桌面(RDP)客户机。此外，服务器106可以运行应用，例如，所述服务器106可以是提供例如由位于Redmond,Washington的微软公司出品的微软Exchange的电子邮件服务的应用服务器、web或网络服务器、或桌面共享服务器、或协作服务器。在一些实施例中，任意一种应用可以包括任意类型的寄载服务或产品，例如由Santa Barbara,California的Citrix Online部门提供的GoToMeetingTM、由位于Santa Clara,California的WebEx公司提供的WebExTM、或由位于Redmond,Washington的微软公司提供的微软Office Live Meeting。

[0090] 示例设备架构

[0091] 图2A还示出设备200的示例实施例。仅通过示例来提供图2A中的设备200的架构并且不意于以任一方式受限。设备200可以包括任一类型和形式的计算装置100，诸如结合上面图1D和1E所描述的任一元件或者部分。总的来说，设备200具有一个或者多个网络端口266A-266N和一个或者多个网络堆栈267A-267N用于经由网络104接收和/或传输通信。设备

200还局域网络优化引擎250，用于优化、加速或者以其他方式改进通过设备200的任一网络业务量或者通信的性能、操作或者质量。

[0092] 设备200包括操作系统或者受操作系统的控制。设备200的操作系统可以是任一类型和/或形式的Unix操作系统，但是本发明不受这样的限制。由此，设备200可以运行任意操作系统，诸如任意一种版本的微软®Windows操作系统、不同版本的Unix和Linux操作系统、用于Macintosh计算机的任意版本的Mac OS®、任意的嵌入式操作系统、任意的网络操作系统、任意的实时操作系统、任意的开放源操作系统、任意的专用操作系统、用于移动计算装置或者网络装置的任意操作系统、或者可以运行在设备200上并执行此处所描述的操作的任意其它操作系统。

[0093] 设备200的操作系统将可用的系统存储器分配、管理或者以其他方式分离成内核或者系统空间和用户或者应用空间。内核空间典型地被保留用于运行内核，所述内核包括任一设备驱动程序、内核扩展或其它内核相关软件。如本领域技术人员所知，内核是操作系统的核心，并提供对设备200的资源和硬件相关的元件的访问、控制和管理。根据设备200的实施例，内核空间还包括和网络优化引擎250或其部分一起工作的多个网络服务或进程。另外，内核的实施例将依赖于由装置200所安装、配置或者以其他方式使用的操作系统的实施例。与内核空间不同，用户空间是由用户模式应用或者以其他方式运行于用户模式的程序所使用的存储器区域或部分操作系统。用户模式应用不可以直接访问内核空间而使用服务调用以访问内核服务。操作系统使用用户或者应用空间用于执行或者运行应用和提供用户级程序、服务、过程和/或任务。

[0094] 设备200具有一个或者多个网络端口266用于通过网络104传输和接收数据。网络端口266提供计算装置和网络104或者另一个装置100之间的物理和/或逻辑接口用于传输和接收网络通信。网络端口266的类型和形式依赖于网络的类型和形式以及用于连接到网络的介质的类型。进一步，提供用于网络端口266和网络堆栈267或者由其使用的任一软件可以运行在内核空间或者用户空间中。

[0095] 在一个实施例中，设备200包括诸如基于TCP/IP的堆栈的一个网络堆栈267，用于在网络105上与客户机102和/或服务器106进行通信。在一个实施例中，网络堆栈267用于与诸如网络104的第一网络以及第二网络104'进行通信。在另一个实施例中，装置200可以包括两个或多个网络堆栈，例如第一网络堆栈267A和第二网络堆栈267N。第一网络堆栈267A可以用于和第一端口266A相结合在第一网络104上通信。第二网络堆栈267N可以用于和第二端口266N相结合在第二网络104'上通信。在一个实施例中，网络堆栈267包括一个或多个缓冲器用于对一个或多个网络分组排队以便被设备200发送。

[0096] 网络堆栈267包括任意类型和形式的软件或硬件或其任意组合，用于提供到网络的连通性以及与网络的通信。在一个实施例中，网络堆栈267包括用于网络协议套件的软件实现。网络堆栈267可以包括一个或多个网络层，例如如本领域技术人员所认识和理解的开放系统互连(OSI)通信模型的任意网络层。因而，网络堆栈267可以包括用于下列OSI模型的任意一层的任意类型和形式的协议：1)物理链路层，2)数据链路层，3)网络层，4)传输层，5)会话层，6)表示层以及7)应用层。在一个实施例中，网络堆栈267包括在网际协议(IP)的网络层协议上的传输控制协议(TCP)，通常被称为TCP/IP。在一些实施例中，可以在以太网协议上携带TCP/IP协议，所述以太网协议可以包括诸如由IEEE802.3所覆盖的那些协议的

IEEE广域网(WAN)或局域网(LAN)协议的任意族。在一些实施例中，网络堆栈267包括诸如IEEE 802.11和/或移动网际协议的任意类型和形式的无线协议。

[0097] 考虑到基于TCP/IP的网络，可以使用任意基于TCP/IP的协议，包括消息应用编程接口(MAPI)(电子邮件)、文件传送协议(FTP)、超文本传送协议(HTTP)、公共因特网文件系统(CIFS)协议(文件传送)、独立计算架构(ICA)协议、远程桌面协议(RDP)、无线应用协议(WAP)、移动IP协议和IP上语音(VoIP)协议。在另一个实施例中，网络堆栈267包括诸如修改的传输控制协议的任意类型和形式的传输控制协议，例如事务TCP(T/TCP)、具有选择确认的TCP(TCP-SACK)、具有大窗口的TCP(TCP-LW)、诸如TCP-Vegas协议的拥塞预测协议以及TCP欺骗协议。在其它实施例中，网络堆栈267可以使用诸如IP上UDP的任意类型和形式的用户数据报协议(UDP)，例如用于音频通信或实时数据通信。

[0098] 进一步，网络堆栈267可以包括诸如TCP驱动程序或网络层驱动程序的支持一个或多个层的一个或多个网络驱动程序。网络驱动程序可以被包括作为计算装置100的操作系统的一部分或作为计算装置100的任意网络接口卡或其它网络访问部件的一部分。在一些实施例中，网络堆栈267的任意一种网络驱动程序可以被定制、修改或改变以提供支持此处描述的任意技术的网络堆栈267的定制或修改部分。

[0099] 在一个实施例中，设备200使用单个网络堆栈267提供或者维持客户机102和服务器106之间的传输层连接。在一些实施例中，设备200通过改变、管理或者控制客户机和服务器之间的传输控制协议连接的行为来有效终接传输层连接。在这些实施例中，设备200可以使用单个网络堆栈267。在其他实施例中，设备200终接诸如客户机102的TCP连接的第一传输层连接，并且建立代表客户机102或者由客户机102使用的到服务器106的第二传输层连接，例如第二传输层连接在设备200和服务器106处终接。第一和第二传输层连接可以经由单个网络堆栈267建立。在其他实施例中，设备200使用多个网络堆栈，例如267A和267B。在这些实施例中，第一传输层连接可以在一个网络堆栈267A处建立或者终接，而第二传输层连接可以在第二网络堆栈267N处建立或者终接。例如，一个网络堆栈可以用于在第一网络上接收和发送网络分组，并且另一个网络堆栈用于在第二网络上接收和发送网络分组。

[0100] 如图2A中所示，网络优化引擎250包括一个或者多个以下的元件、部件或者模块：网络分组处理引擎240、LAN/WAN探测器210、流控制器220、Qos引擎236、协议加速器234、压缩引擎238、高速缓存管理器232和策略引擎295'。网络优化引擎250或其一部分可以包括软件、硬件或者软件和硬件的任意组合。此外，网络优化引擎250所提供的或者使用的任一软件可以运行在内核空间或者用户空间。例如，在一个实施例中，网络优化引擎250可以运行在内核空间中。在另一个实施例中，网络优化引擎250可以运行在用户空间中。在又一个实施例中，网络优化引擎250的第一部分运行在内核空间中，而网络优化引擎250的第二部分运行在用户空间中。

[0101] 网络分组处理引擎

[0102] 通常也被称为分组处理引擎或分组引擎的网络分组引擎240，负责管理由设备200经由网络端口266和网络堆栈267接收和发送的分组的处理。网络分组引擎240可以操作在网络堆栈267的任一层。在一个实施例中，网络分组引擎240操作在网络堆栈267的层2或者层3。在一些实施例中，分组引擎240在在诸如TCP/IP实施例中的IP层的网络层处拦截或者以其他方式接收分组。在另一个实施例中，分组引擎240在网络堆栈267的层4处操作。例如，

在一些实施例中，分组引擎240在传输层处拦截或者以其他方式接收分组，诸如在TCP/IP实施例中的TCP层处拦截分组。在其他实施例中，分组引擎240在层4之上的任一会话或者应用层处操作。例如，在一个实施例中，分组引擎240在传输层之上的协议层拦截或者以其他方式接收网络分组，诸如TCP实施例中的TCP分组的净荷。

[0103] 分组引擎240可以包括用于在例如接收网络分组或发送网络分组的处理期间排队一个或多个网络分组的缓冲器。另外，分组引擎240与一个或多个网络堆栈267通信以经由网络端口266发送和接收网络分组。分组引擎240可以包括分组处理定时器。在一个实施例中，分组处理定时器提供一个或多个时间间隔以触发输入(即，接收)或输出(即，发送)的网络分组的处理。在一些实施例中，分组引擎240响应于定时器来处理网络分组。分组处理定时器提供任意类型和形式的信号给分组引擎240，以通知、触发或通信时间相关的事件、间隔或发生。在许多实施例中，分组处理定时器以例如像100毫秒、50毫秒、25毫秒、10毫秒、5毫秒或者1毫秒的这样的毫秒级来进行操作。

[0104] 在操作期间，分组引擎240可以与诸如LAN/WAN探测器210、流控制器220、Qos引擎236、协议加速器234、压缩引擎238、高速缓存管理器232和/或策略引擎295'的网络优化引擎250的任一部分接口、集成或通信。因而，可以响应于分组处理定时器和/或分组引擎240来执行LAN/WAN探测器210、流控制器220、Qos引擎236、协议加速器234、压缩引擎238、高速缓存管理器232和策略引擎295'的任意逻辑、功能或操作。在一些实施例中，可以以例如小于或等于10毫秒的时间间隔的、通过分组处理定时器提供的时间间隔的粒度来执行加密引擎234、高速缓存管理器232、策略引擎236和多协议压缩逻辑238的任意逻辑、功能或操作。例如，在一个实施例中，高速缓存管理器232可以响应于集成的分组引擎240和/或分组处理定时器242来执行任意高速缓存的对象的终止。在另一个实施例中，可以将高速缓存的对象的满期或终止时间设置为与分组处理定时器的时间间隔相同的粒度级，例如每10毫秒。

[0105] 高速缓存管理器

[0106] 高速缓存管理器232可以包括软件、硬件或软件和硬件的任意组合，以将数据、信息和对象保存到存储器或者存储装置的高速缓存中，提供高速缓存访问，并且控制和管理高速缓存。由高速缓存管理器232处理和保存的数据、对象或内容可以包括诸如标记语言的或者通过任意协议通信的任意类型的数据。在一些实施例中，高速缓存管理器232复制存储在别处的原始数据或者以前计算、生成或发送的数据，其中原始数据也许需要相对于读取高速缓存存储器或者存储元件来说更长的访问时间以取出、计算或者以其他方式获取。一旦数据被保存在高速缓存中，未来的使用可以通过访问高速缓存的拷贝而不是重新取回或再计算原始数据来进行，从而减少访问时间。在一些实施例中，高速缓存可以包括设备200的存储器中的数据对象。在另一个实施例中，高速缓存可以包括诸如硬盘的一部分的设备200的任意类型和形式的存储元件。在一些实施例中，装置的处理单元可以提供由高速缓存管理器232使用的高速缓存存储器。在又一个进一步的实施例中，高速缓存管理器232可以使用存储器、存储装置或处理单元的任意部分和组合，以用于高速缓存数据、对象及其它内容。

[0107] 进一步地，高速缓存管理器232包括任意逻辑、功能、规则或操作，以执行设备200的任意高速缓存技术。在一些实施例中，高速缓存管理器232可以作为应用、库、程序、服务、进程、线程或任务来操作。在一些实施例中，高速缓存管理器232可以包括任意类型的通用

处理器(GPP)或者诸如现场可编程门阵列(FPGA)、可编程逻辑器件(PLD)或专用集成电路(ASIC)的任意其它类型的集成电路。

[0108] 策略引擎

[0109] 策略引擎295'包括任意逻辑、功能或者操作，用于提供和应用一个或者多个策略或者规则到设备200的任一部分的功能、操作或者配置。策略引擎295'可以包括例如智能统计引擎或者其他可编程应用。在一个实施例中，策略引擎295提供配置机制来允许用户识别、指定、限定或者配置用于网络优化引擎250或者其任一部分的策略。例如，策略引擎295可以提供策略，用于高速缓存哪些数据、何时高速缓存数据、高速缓存数据用于谁、何时终止高速缓存中的对象或者刷新高速缓存。在其它实施例中，策略引擎236可以包括任意逻辑、规则、功能或操作，以便确定和提供由设备200高速缓存的对象、数据或内容的访问、控制和管理以及由设备200执行的安全、网络业务量、网络访问、压缩或任意其它功能或操作的访问、控制和管理之外。

[0110] 在一些实施例中，策略引擎295'基于以下的任意一个或者多个来提供和应用一个或者多个策略：用户、客户机的标识、服务器的标识、连接的类型、连接的时间、网络的类型或者网络业务量的内容。在一个实施例中，策略引擎295'基于网络分组的任意协议层处的任一字段或者首部来提供和应用策略。在另一个实施例中，策略引擎295'基于网络分组的任一净荷来提供和应用策略。例如在一个实施例中，策略引擎295'基于将所运载的应用层协议的内容的特定部分识别为传输层分组的净荷来应用策略。在另一个实施例中，策略引擎295'基于客户机、服务器或者用户证书所识别的任一信息来应用策略。在又一个实施例中，策略引擎295'基于关于客户机所获取的任意属性或者特征来应用策略，诸如经由任一类型和形式的端点检测(参见示例以下讨论的客户机代理的收集代理)。

[0111] 在一个实施例中，策略引擎295'和应用递送系统290的策略引擎295结合或者协同运行。在一些实施例中，策略引擎295'是应用递送系统290的策略引擎295的分布的部分。在另一个实施例中，应用递送系统290的策略引擎295被部署在或者执行在设备200上。在一些实施例中，策略引擎295和295'都在设备200上操作。在又一个实施例中，设备200的策略引擎295'或其一部分在服务器106上操作。

[0112] 多协议和多层压缩引擎

[0113] 压缩引擎238包括用于压缩诸如由装置200的网络堆栈267使用的任意一种协议的网络堆栈的一个或多个协议的网络分组的任意逻辑、商业规则、功能或操作。压缩引擎238也可以被称为多协议压缩引擎238，这是由于其可以被设计、构建或者能够压缩多个协议。在一个实施例中，压缩引擎238应用上下文不敏感的压缩，其是应用到数据而不需要知道数据类型的压缩。在另一个实施例中，压缩引擎238应用上下文敏感的压缩。在此实施例中，压缩引擎238利用知道数据类型来从一组合适算法中选择特定压缩算法。在一些实施例中，特定协议的知识被用来执行上下文敏感的压缩。在一个实施例中，设备200或者压缩引擎238可以使用端口号(例如，公知端口)以及来自自身连接的数据来确定要使用的适当的压缩算法。一些协议仅使用单个类型的数据，仅要求在连接建立时可以被选择的单个压缩算法。其他协议在不同时间包括不同类型的数据。例如，引入有其他协议数据的随意类型的POP、IMAP、SMTP和HTTP所有移动文件。

[0114] 在一个实施例中，压缩引擎238使用德尔塔类型的压缩算法。在另一个实施例中，

压缩引擎238使用第一位置压缩以及在高速缓存、存储器或者盘中保存的数据上搜索重复的模式。在一些实施例中，压缩引擎238使用无损压缩算法。在其他实施例中，压缩引擎使用有损压缩算法。在一些情况中，知道数据类型和有时来自用户的许可被要求使用有损压缩算法。在一些实施例中，压缩不限于协议的净荷。协议自身的控制字段可以被压缩。在一些实施例中，与对于净荷的使用不同，压缩引擎238对于控制字段使用不同的算法。

[0115] 在一些实施例中，压缩引擎238在网络堆栈267的一个或者多个层处压缩。在一个实施例中，压缩引擎238在传输层协议处压缩。在另一个实施例中，压缩引擎238在应用层协议处压缩。在一些实施例中，压缩引擎238在层2-4协议处压缩。在其他实施例中，压缩引擎238在层5-7处压缩。在又一个实施例中，压缩引擎238压缩传输层协议和应用层协议。在一些实施例中，压缩引擎238压缩层2-4协议和层5-7协议。

[0116] 在一些实施例中，压缩引擎238使用基于存储器压缩、基于高速缓存压缩或者基于盘压缩，或者其任一组合。由此，压缩引擎238可以被称为多层压缩引擎。在一个实施例中，压缩引擎238使用保存在诸如RAM的存储器中的数据的历史。在另一个实施例中，压缩引擎238使用保存在诸如处理器的L2高速缓存的高速缓存中的数据的历史。在其他实施例中，压缩引擎238使用保存到盘或者存储位置的数据的历史。在一些实施例中，压缩引擎238使用分层的基于高速缓存、基于存储器和基于盘的数据历史。压缩引擎238可以首先使用基于高速缓存的数据来确定一个或者多个数据匹配用于压缩，并且随后可以检查基于存储器的数据来确定一个或者多个数据匹配用于压缩。在另一个情况中，压缩引擎238在检查基于高速缓存和/或基于存储器的数据历史之后可以检查盘存储用于数据匹配来压缩。

[0117] 在一个实施例中，多协议压缩引擎238双向地在客户机102a-102n和服务器106a-106n之间压缩任意的基于TCP/IP的协议，包括消息应用编程接口(MAPI)(电子邮件)、文件传送协议(FTP)、超文本传送协议(HTTP)、公共因特网文件系统(CIFS)协议(文件传送)、独立计算架构(ICA)协议、远程桌面协议(RDP)、无线应用协议(WAP)、移动IP协议和IP上语音(VoIP)协议。在其它实施例中，多协议压缩引擎238提供基于超文本标记语言(HTML)的协议的压缩，并且在一些实施例中提供诸如可扩展标记语言(XML)的任意标记语言的压缩。在一个实施例中，多协议压缩引擎238提供诸如为设备200设计用于设备200通信的的任意协议的任意高性能协议的压缩。在另一个实施例中，多协议压缩引擎238使用修改的传输控制协议来压缩任意通信的任意净荷或任意通信，所述修改的传输控制协议诸如事务TCP(T/TCP)、具有选择确认的TCP(TCP-SACK)、具有大窗口的TCP(TCP-LW)、诸如TCP-Vegas协议的拥塞预测协议以及TCP欺骗协议。

[0118] 因而，多协议压缩引擎238为经由桌面客户机以及甚至移动客户机访问应用的用户加速性能，所述桌面客户机例如微软Outlook以及诸如由诸如Oracle、SAP和Siebel的通用的企业应用所启动的任意客户机的非web瘦客户机，所述移动客户机例如掌上电脑。在一些实施例中，通过与访问网络堆栈267的分组处理引擎240结合在一起，多协议压缩引擎238可以压缩由传输层协议所携带的任意一种协议，诸如任意应用层协议。

[0119] LAN/WAN检测器

[0120] LAN/WAN检测器238包括用于自动检测慢侧连接(例如诸如内联网的广域网(WAN)连接)和相关端口267以及快侧连接(例如局域网(LAN)连接)和相关端口267的任一逻辑、商业规则、功能或者操作。在一些实施例中，LAN/WAN检测器238监控设备200的网络端口267上

的网络业务量来检测同步分组，有时称之为“标记”网络分组。该同步分组识别网络分组的类型或者速度。在一个实施例中，同步分组识别WAN速度或者WAN类型的连接。LAN/WAN检测器238还识别对标记的同步分组的确认分组的接收以及其在哪个端口上被接收。设备200随后配置其自身来操作标记的同步分组到达的所识别的端口，使得该端口上的速度被设置为与该端口连接的网络相关联的速度。其它端口随后被设置为和该端口连接的网络相关联的速度。

[0121] 此处为了讨论方便，“慢”侧可以参考关于与诸如因特网的广域网(WAN)的连接，并且操作在WAN的网络速度。同样，“快”侧可以参考关于与局域网(LAN)的连接并且操作在LAN的网络速度。然而，注意到网络中“快”和“慢”侧可以根据每个连接而改变并且是针对网络连接的速度或网络拓扑的类型的相对术语。这样的配置可以用在复杂网络拓扑中，其中网络仅在和相邻网络比较时是“快”或“慢”的并且在某种意义上不是绝对的。

[0122] 在一个实施例中，LAN/WAN检测器238可以被用来允许设备自动发现其连接的网络。在另一个实施例中，LAN/WAN检测器238可以被用来检测部署在网络104中的第二设备200’的存在或者缺失。例如，根据图1A的操作中的自动发现机制起到以下作用：设备200和200’被置于和联接客户机102和服务器106的连接相一致。设备200和200’处于连接两个LAN的诸如内联网的低速链路的端点。在一个示例实施例中，设备200和200’的每一个包括两个端口，一个连接到“较低”速链路并且另一个连接到诸如LAN的“较高”速链路。到达一个端口的任一分组被复制到其它端口。因此，设备200和200’每一个被配置为起到两个网络104之间的桥接器的作用。

[0123] 当诸如客户机102的端点节点开启与诸如服务器106的另一个端点节点的新的TCP连接，则客户机102将具有同步(SYN)首部位集或者SYN分组的TCP分组发送到服务器106。在本例中，客户机102打开到服务器106的传输层连接。当SYN分组传递通过设备200时，设备200将特征TCP首部选项插入、附加或者以其他方式提供给分组，以告知其存在。如果分组传递通过第二设备，则在此示例设备200’中，第二设备记录SYN分组上的首部选项。服务器106响应于具有同步确认(SYN-ACK)分组的SYN分组。当SYN-ACK分组传递通过设备200’时，TCP首部选项被标记(例如附加、插入或者增加)到SYN-ACK分组来将设备200’的存在告知设备200。当设备200接收到此分组，则两个设备200和200’此时互相察觉并且该连接可以被适当加速。

[0124] 进一步到LAN/WAN检测器238的操作，描述用于使用SYN分组来检测网络的“快”和“慢”侧的方法或者过程。在客户机102和服务器106之间的传输层连接建立期间，设备200经由LAN/WAN检测器238确定SYN分组是否用确认(ACK)来被标记。如果其被标记，则设备200将接收标记的SYN分组(SYN-ACK)的端口识别或者配置为“慢”侧。在一个实施例中，设备200可选地在将分组复制到其它端口之前将ACK标记从分组移除。如果LAN/WAN检测器238确定分组未被标记，则设备200将接收未标记的SYN分组的端口识别或者配置为“快”侧。设备200随后用ACK来标记SYN分组并且将分组复制到其它端口。

[0125] 在其他实施例中，LAN/WAN检测器238使用SYN-ACK分组来检测网络的快和慢侧。设备200经由LAN/WAN检测器238确定是否用确认(ACK)标记了SYN-ACK分组。如果其被标记，则设备200将接收标记的SYN分组(SYN-ACK)的端口识别或者配置为“慢”侧。在一个实施例中，设备200可选地在将分组复制到其它端口之前将ACK标记从分组移除。如果LAN/WAN检测器

238确定分组未被标记，则设备200将接收未标记的分组的端口识别或者配置为“快”侧。LAN/WAN检测器238确定SYN分组是否被标记。如果SYN分组未被标记，则设备200将分组复制到其它端口。如果SYN分组被标记，则设备在将SYN-ACK分组复制到其它端口之前标记该SYN-ACK端口。

[0126] 设备200、200’可以增加、插入、修改、附加或者以其他方式提供TCP选项中的任意信息或者数据来提供关于网络连接、网络业务流或者设备200的配置或者操作的任意信息、数据或者特征。以此方式，设备200不仅将其存在通知给另一个设备200’或者标记较高或者较低的速度连接，设备200还经由TCP选项首部来提供关于设备或者连接的附加信息和数据。TCP选项首部信息可以用于或者被设备用于控制、管理、优化、加速或者改进通过设备200的网络业务流，或者以其他方式配置其自身或者网络端口的操作。

[0127] 尽管总的结合检测网络连接的速度或者设备的存在来描述，但是LAN/WAN检测器238还可以被用于将设备200的任意类型的功能、逻辑或者操作应用到网络业务量的端口、连接或者流。更具体地，无论装置在何时在不同端口上执行不同的功能，都可以发生端口的自动分配，其中，在单元操作期间可以做出对任务的端口分配，和/或由设备200可以发现每一端口上的网络段的性质。

[0128] 流控制

[0129] 流控制器220包括用于优化、加速或者以其他方式改进网络分组的传输层通信的性能、操作或者服务质量或者传输层处的分组的递送的任意逻辑、商业规则、功能或者操作。流控制器有时也称之为流控制模块，其调节、管理和控制数据传输率。在一些实施例中，该流控制器220被部署在网络104中的带宽瓶颈处或与其连接。在一个实施例中，该流控制器220有效地调节、管理和控制带宽使用或者利用。在其他实施例中，流控制模块还可以部署在等待时间转变(低等待时间到高等待时间)的网络上和具有介质损失的链路(诸如无线或者卫星链路)上的点处。

[0130] 在一些实施例中，流控制器220可以包括用于控制网络传输量的接收率的接收器侧流控制模块和用于控制网络分组的传输率的发送器侧流控制模块。在其他实施例中，第一流控制器220包括接收器侧流控制模块并且第二流控制器220’包括发送器侧流控制模块。在一些实施例中，第一流控制器220部署在第一设备200上并且第二流控制器220’部署在第二设备200’上。同样，在一些实施例中，第一设备200控制接收器侧上的数据流，并且第二设备200’控制来自发送器侧的数据流。在又一个实施例中，单个设备200包括用于传播通过设备200的网络通信的接收器侧和发送器侧的流控制。

[0131] 在一个实施例中，流控制模块220被配置为允许瓶颈处的带宽更充分利用，并且在一些实施例中，不能过度利用。在一些实施例中，流控制模块220透明地缓冲(或者重新缓冲由例如发送器已经缓冲的数据)在具有相关联的流控制模块220的节点之间传递的网络会话。当会话传递通过两个或者多个流控制模块220，则一个或者多个流控制模块控制会话的速率。

[0132] 在一个实施例中，流控制模块200被配置具有涉及瓶颈带宽的预定数据。在另一个实施例中，流控制模块220可以被配置为检测瓶颈带宽或者其关联数据。接收器侧流控制模块220可以控制数据传输率。接收器侧流控制模块220通过将传输率限制转发到发送器侧流控制模块220来控制发送器侧流控制模块220，例如数据传输率。在一个实施例中，接收器侧

流控制模块220到在由例如服务器106的接收器发送到诸如客户机102的发送器的确认(ACK)分组(或者信号)上捎带(piggyback)这些传输率限制。接收器侧流控制模块220响应于发送器侧流控制模块220'发送的速率控制请求来做这一工作。来自发送器侧流控制模块220'的请求可以在发送器106发送的数据分组上被"捎带"。

[0133] 在一些实施例中,流控制器220掌控、调整、模拟、改变、改进或者以其他方式调节传输层协议的行为来提供传输层的递送、数据率和/或带宽利用的改进的性能或者操作。流控制器220可以在传输层实现多个数据流控制技术,包括但不限于1)预确认,2)窗口虚拟化,3)重新拥塞技术,3)本地重传输技术,4)波前检测和消除二义性。5)传输控制协议选择性确认,6)事务边界检测技术和7)重新分包。

[0134] 尽管发送器总的在此处描述为客户机102以及接收器为服务器106,但是发送器也可以是诸如网络104上服务器106或者任一计算装置100的任一端点。同样,接收器也可以是网络104上客户机102或者任意其它计算装置。

[0135] 预确认

[0136] 对于预确认流控制技术总的来说,在一些实施例中,流控制器220处理发送器的确认和重新传输,有效终接发送器与网络连接的下游部分的连接。参考图1B,描述用来实现该特征的将设备200布置到网络架构中的一个可能的部署。在此示例实施例中,发送计算机或者客户机102在网络104上例如经由转换器发送数据,其确定该数据发往VPN设备205。由于所选择的网络拓扑,发往VPN设备205的所有数据传播通过设备200,使得设备200可以将任一必要的算法应用到该数据。

[0137] 进一步在该例中,客户机102发送由设备200接收的分组。当设备200接收从客户机102经由VPN设备205发送到接收者的分组时,设备200保留分组的备份并且将分组向下游转发到VPN设备205。设备200随后产生确认分组(ACK)并且将ACK分组发送回客户机102或者发送端点。该ACK即预确认使得发送器102相信分组已经被成功递送,释放发送器的资源用于随后的处理。在请求分组重新传输的事件中,设备200保留分组数据的备份,使得发送器102不必处理数据的重新传输。这个确认的早期产生可以称为"预确认"。

[0138] 如果需要分组的重新传输,设备200将分组重新传输到发送器。设备200可以确定当发送器处于传统系统中时是否需要重新发送,例如,在预定时间之后对于该分组如果没有接收到确认信息则确定分组丢失。对此,设备200监控例如服务器106(或者任意其它下游网络实体)的接收端点产生的确认,使得其可以确认是否分组已经成功递送或者需要重新传输。如果设备200确定分组已经成功发送,则设备200能够自由丢弃所保存的分组数据。设备200还可以禁止将已经由发送端点接收的分组的确认进行转发。

[0139] 在上述实施例中,设备200经由流控制器220通过预确认(也称之为"预告知")的递送来控制发送器102,如同设备200是接收端点本身一样。由于设备200不是端点并且实际上不消耗数据,所以设备200包括用于对发送端点提供过流控制的机制。无需过流控制,因为设备200保存已经预确认到发送端点但还没有确认为由接收端点接收的分组,所以设备200能够用完存储器。在发送器102发送分组到设备200快于设备向下游转发分组的情况中,设备200中可用于保存未确认分组数据的存储器可以快速填充。用于过流控制的机制允许设备200控制来自发送器102的分组的传输以避免该问题。

[0140] 在一个实施例中,设备200或者流控制器包括固有的"自同步"(self-clocking)过

流控制机制。该自同步归因于这样的顺序：设备200可以被设计为将分组发送到下游并且将ACK发送到发送器102或者106。在一些实施例中，设备200并不预确认分组，直到其向下游发送分组为止。以此方式，发送器102以设备200能够发送分组而不是设备200能够从发送器100接收分组的速率接收ACK。这有助于调节来自发送器102的分组的传输。

[0141] 窗口虚拟化

[0142] 设备200可以实现的另一个过流控制机制是使用TCP窗大小参数，其告知发送器接收器允许发送器填满多少缓冲器。预确认中的非零窗大小(例如至少一个最大段大小(MSS)的大小)允许发送端点继续将数据递送到设备，而零窗大小禁止进一步的数据传输。相应地，设备200可以例如当设备200的缓冲器变满时通过适当地设置每一预确认中的TCP窗大小来调节来自发送器的分组的流量。

[0143] 另一项用来降低该附加开销的技术是应用滞后作用(hysteresis)。当设备200将数据递送到较慢侧时，设备200中的过流控制机制可以在发送非零窗公布到发送器之前要求可用的最小数量的空间。在一个实施例中，设备200在发送非零窗分组之前等待直到存在最小的预定数量的分组(诸如四个分组)的可用空间，，非零窗分组诸如是指示四个分组的窗大小的分组。对于四个数据分组的每个组由于仅两个ACK分组被发送，而不是对于四个数据分组要发送八个ACK分组，这可以将开销大概降低到原来的四分之一。

[0144] 设备200或者流控制器220可以用于过流控制的另一个技术是TCP延迟ACK机制，其跳过ACK来降低网络业务量。TCP延迟ACK自动延迟ACK的发送，直到接收到两个分组或者直到发生固定的超时为止。该机制单独导致开销减半，此外，通过增加分组的数量高于两个，实现附加的开销降低。但是仅延迟ACK本身不足以控制过流，并且设备200还可以使用ACK上公布的窗机制来控制发送器。当这样操作时，在一个实施例中，设备200通过延迟ACK很长时间来避免触发发送器的超时机制。

[0145] 在一个实施例中，流控制220不对一组分组的最后一个分组进行预确认。通过不对最后一个分组或者该组的分组的至少一个预确认，设备避免对一组分组的错误确认。例如，如果设备将发送最后一个分组的预确认并且该分组随后丢失，则发送器在分组没有被递送时已经被欺骗认为其被递送。考虑到分组已经递送，则发送器丢弃该数据。如果设备还损失该分组，则不能重新传输该分组到接收者。通过不对一组分组的最后一个分组预确认，则发送器直到该分组被递送时才将其丢弃。

[0146] 在另一个实施例中，流控制器220可以使用窗虚拟化技术来控制流速或者网络连接的带宽利用。虽然根据检查诸如RFC 1323的传统文献其可能不是直接明显的，但是存在用于诸如TCP的传输层协议的发送窗。发送窗由于消耗缓冲器空间(尽管在发送器上)，所以和接收窗相同。发送器的发送窗包括接收器还没有确认的应用发送的所有数据。在要求重传输的情况中该数据必须保留在存储器中。由于存储器是共享资源，所以一些TCP堆栈实现限制了该数据的大小。当发送窗满时，应用程序尝试发送更多的数据导致阻断应用程序，直到空间可用为止。随后的确认接收将释放发送窗存储器并且不阻断应用程序。该窗大小公知为一些TCP实现中的套接字缓冲器大小。

[0147] 在一个实施例中，流控制模块220被配置为提供对增加的窗(或者缓冲器)大小的访问。该配置还可以称为窗虚拟化。在包含作为传输层协议的TCP的实施例中，TCP首部可以包括对应窗范围的位字符串。在一个实施例中，“窗”可以在发送、接收或者二者的上下文中

提及。

[0148] 窗虚拟化的一个实施例是将预确认设备200插入到TCP会话中。参考图1A或1B的任意一个环境，建立例如客户机102(为讨论方便，现在称为源节点102)的源节点和例如服务器106(为讨论方便，现在称之为目标节点106)的目标节点之间数据通信会话的初始化。对于TCP通信，源节点102最初将同步信号(“SYN”)通过其局域网104传输到第一流控制模块220。第一流控制模块220将配置标识符插入到TCP首部选项区域中。该配置标识符将数据路径中的该点识别为流控制模块。

[0149] 设备200经由流控制模块220提供窗(或者缓冲器)来允许会话内的增加的数据缓冲能力，尽管具有例如16k字节的小缓冲器大小的端节点。然而，RFC 1323要求窗缩放大于64k字节的任何缓冲器大小，其必须在会话初始化(SYN、SYN-ACK信号)时设置。此外，窗的缩放对应于数据路径中的最小公分母(common denominator)，经常是具有小的缓冲器大小的端节点。该窗比例(window scale)通常是0或者1的比例，其对应于直到64k或者128k字节的缓冲器大小。注意到，由于窗大小被限定为随窗比例改变的每一分组中的窗字段，则窗比例建立用于该缓冲期的上限，但并不保证该缓冲器实际上就那么大。每个分组指示窗字段中接收器处当前可用的缓冲器空间。

[0150] 在使用窗的虚拟技术缩放的实施例中，在当第一流控制模块220从源节点102接收SYN信号(或者分组)的连接建立(即，会话初始化)期间，流控制模块220将源节点102(其是之前的节点)的窗比例或者如果之前的节点的比例丢失则为窗比例保存0值。第一流控制模块220还在SYN-FCM信号中修改比例，例如将比例从0或者1增加到4。当第二流控制模块220接收SYN信号时，其将来自第一流控制信号的增加的比例保存并且将SYN信号中的比例重置为源节点103的比例值以用于传输到目标节点106。当第二流控制器220接收到来自目标节点106的SYN-ACK信号时，其将来自目标节点106比例(例如，0或者1)的比例保存并且将其修改为与SYN-ACK-FCM信号一起发送的增加的比例。第一流控制节点220接收并且记录所接收的窗比例并且将发送返回源节点102的窗比例修订为下降到例如0或者1的初始比例。基于上面连接建立期间的窗变化会话，会话的例如TCP分组的每一个随后的分组中的窗字段必须根据窗变化转换而改变。

[0151] 如上所述，窗比例表示出大于64k的缓冲器大小，并且可以不需要窗虚拟化。因此，窗比例的变化可以用于表示每一个流控制模块220中的增加的缓冲器容量。该缓冲器容量的增加可以被称为窗(或者缓冲器)虚拟化。该缓冲器大小的增加允许更大的分组从各自的端节点102和106进出。注意到，TCP中的缓冲器大小典型地以字节表示，但是为了讨论方便由于“分组”和虚拟化相关，在此处描述中可以使用“分组”。

[0152] 通过示例，描述流控制器220执行的窗(或者缓冲器)虚拟化。在此例中，源节点102和目标节点106配置为与具有受限的16k字节的缓冲器容量的传统端节点相同，其大约等于10个数据分组。典型地，端节点102、106在下一组分组能够传输之前必须等到该分组被传输并且收到确认。在一个实施例中，使用流控制模块220中的增加的缓冲器容量，当源节点103发送其数据分组时，第一流控制模块220接收该分组，将该分组保存在其例如512个分组容量的较大容量的缓冲器中，并且立即发送指示分组接收(“REC-ACK”)的确认信号回到源节点102。源节点102可以随后“清除”其当前缓冲器，将10个新的数据分组载入缓冲器，并且将这些传输到第一流控制模块220上。在此，第一流控制模块220发送REC-ACK信号回到源节

点，并且源节点102清除其缓冲器并且对其载入10个更新的分组用于传输。

[0153] 当第一流控制模块220接收到来自源节点的数据分组时，其相应地将该数据分组载入到缓冲器中。当其准备好时，第一流控制模块220可以开始将数据分组传送到第二流控制模块230，其还具有增加的缓冲器大小例如来接收512个分组。第二流控制模块220'接收数据分组并且开始每次传输10个分组到目标节点106。在第二流控制节点220处接收的来自目标节点106的每一个REC-ACK导致10个更多分组传输到目标节点106，直到所有的数据分组被传送。因此，本发明能够通过利用装置之间的流控制模块220、220'的较大的缓冲器来增加源节点(发送器)102和目标节点(接收器)106之间的传输量。

[0154] 注意到通过之前描述的数据的"预确认"传输，发送器(或者源节点102)被允许传输超过不需要预确认的可能的更多的数据，因此造成更大的窗大小。例如，在一个实施例中，该技术有效地用在流控制模块220、220'处于缺乏大窗的节点(例如，源节点102或者目标节点106)附近的时候。

[0155] 重新拥塞

[0156] 流控制器220的另一个技术或者算法称之为重新拥塞。标准的TCP拥塞避免算法在面对特定网络条件时公知地表现差，包括：大的RTT(往返时间)、高分组损失率以及其它。当设备200检测到诸如长的往返时间或者高的分组损失的拥塞条件时，设备200插入、代入更好地适合特定网络条件的替代的拥塞避免算法。在一个实施例中，该重新拥塞算法使用分组来有效终接发送器和接收器之间的连接。设备200随后使用不同的拥塞避免算法从自身重新发送分组到接收器。重新拥塞算法可以依赖于TCP连接的特性。设备200监控每一个TCP连接，在特征在于关于不同的维度，选择适合用于当前特征的重新拥塞算法。

[0157] 在一个实施例中，当检测到通过往返时间(RTT)限制的TCP连接时，作为多个TCP连接运行的重新拥塞算法被应用。每个TCP连接操作在其自身性能限度内，但是集合的带宽实现了更高的性能水平。该机制中的一个参数是所应用的并行连接的数量(N)。N和连接束的值过大实现超过其合理共享的带宽。N和连接束的值过小实现低于其合理共享的带宽。建立"N"的一个方法依赖于监控分组损失率、RTT和实际连接的分组大小的设备200。这些数字插入TCP响应曲线方程来提供本配置中单个TCP连接的性能的上限。如果连接束中每个连接正获得与计算到上限的基本相同的性能，则应用附加的并行连接。如果当前束正获得低于上限的性能，则降低并行连接的数量。以此方式，由于单独的连接束包含不超过其所需的并行，则维持系统的总的共享，来消除协议自身强加的限制。进一步，每个单独的连接保留TCP兼容性。

[0158] 建立"N"的另一个方法是使用诸如TCP"Vegas"算法或者TCP"稳定Vegas"算法的并行流控制算法。在此方法中，和连接束中的连接相关的网络信息(例如，RTT、损失率、平均分组大小等等)被集合并且应用到替代流控制算法。该算法的结果相应被分布到控制他们数量(即，N)的束的连接之间。可选地，束中的每个连接仍旧使用标准TCP拥塞避免算法。

[0159] 在另一个实施例中，并行束中的单独连接被虚拟化，即实际上不建立单独的TCP连接。事实上拥塞避免算法仍被修改为好像存在N个并行连接来运行。该方法的优点呈现为如同单个连接一样传输网络节点。因此，通过重新拥塞算法而不会影响这些节点的QOS、安全性和其他监控方法。在又一个实施例中，并行束中的单独连接是真实存在的，即独立的。TCP连接被建立用于束中的并行连接的每一个。不必修改用于每一个TCP连接的拥塞避免算法。

[0160] 重新传输

[0161] 在一些实施例中，流控制器220可以应用本地重传输技术。用于实现预确认的一个原因是准备发送到高损链路(例如无线)。在这些实施例中，预确认设备200或者流控制模块220最有益地位于无线链路“之前”。这允许要进行的重传输更接近于高损链路，将重传输负荷从网络的剩余部分移除。设备200可以提供本地重传输，在此情况中，由于链路失败而丢失的分组由设备200直接重传输。由于这消除了诸如服务器106的端节点上的重传输负担和任一网络104的基础结构，所以这是有益的。利用设备200提供本地重传输，丢失的分组可以被重传输通过高损链路而不需要必须由端节点重传输并且来自端节点的数据传输率对应下降。

[0162] 用于实现预确认的另一个原因是避免接收超时(RTO)惩罚。在标准TCP中，存在多种情况导致RTO，即使是成功接收传输中的较大百分比的分组。使用标准TCP算法，RTT窗中丢失多于一个分组有可能会导致超时。此外，如果重传输分组丢失，则大部分TCP连接经历超时。在具有高带宽延迟产品的网络中，甚至相对小的分组损失率也会导致频繁的重传输超时(RTO)。在一个实施例中，设备200使用重传输和超时算法来避免早期的RTO。设备200或者流控制器220基于每一分组来维持重传输的计数。每当重传输分组时，计数加一并且设备200继续传输分组。在一些实施例中，仅有当一个分组已经被重传输预定次数后后才被宣告为RTO。

[0163] 波前检测和消除二义性

[0164] 在一些实施例中，设备200或者流控制器220在管理和控制网络业务量的流时使用波前检测和消除二义性技术。在此技术中，流控制器220使用传输标识符或者号码来确定是否需要重传输特定数据分组。通过示例，发送器在网络上传输数据分组，其中所传输的数据分组的每一个实例和传输号码相关联。可以理解，由于序列号索引分组中的数据而传输号码索引该数据的传输的实例，分组的传输号码与分组的序列号不相同。传输号码可以是对于该目的可用的任意信息，包括和分组相关联的时间戳或者简单地增加的号码(类似于序列号或者分组号)。由于数据段可以被重传输，则不同的传输号码可以和特定序列号相关联。

[0165] 由于发送器传输数据分组，所以发送器保持数据分组传输的所确认的实例的数据结构。数据分组传输的每个实例由其序列号和传输号码索引。通过保持对于每个分组的传输号码，发送器保留数据分组的传输的顺序。当发送器接收到ACK或者SACk时，发送器确定和所指示的接收器(在所接收的确认中)已经接收的分组相关联的最高传输号码。具有最低传输号码的任一未完成的未确认分组被假设丢失。

[0166] 在一些实施例中，当到达分组已经被重传输时，发送器呈现出不明确的状态：标准的ACK/SACK没有包含足够的信息来允许发送器确定到达分组的传输已经触发该确认。从而接收到不明确确认之后，发送器将确认消除二义性来将其和传输号码相关联。在不同的实施例中，多个技术的其中之一或者组合可以被用来解决该不确定性。

[0167] 在一个实施例中，发送器包括具有所传输的数据分组的标识符，并且接收器返回该标识符或者其中具有确认的函数。标识符可以是时间戳(例如在RFC 1323中描述的TCP时间戳)、序列号、可以被用来在分组传输的两个或者多个实例之间解析的任一其他信息。在TCP时间戳选项被用来消除确认的二义性的实施例中，每一分组使用高达32位唯一的信息

来标记。接收到数据分组时，接收器将此唯一信息回送到具有该确认的发送器。发送器确保最初发送的分组和其重传输的一个或者多个版本包含对于时间戳选项的不同值，允许明确地消除ACK不确定性。发送器可以将该唯一信息保存在例如用来保存所发送数据分组的状态的数据结构中。由于该技术与工业标准相兼容并且因此不会遇到或者遇到很少互操作性的问题，所以该技术是有益的。然而，该技术在一些实现中可以要求十个字节的TCP首部空间，降低了网络上的有效吞吐率并且减少了可用于其它TCP选项的空间。

[0168] 在另一个实施例中，分组中的另一个字段，诸如IP ID字段，被用来以与上述TCP时间戳选项类似的方式来消除二义性。发送器安排该分组的最初的和重传输形式的的ID字段值，以使在IP首部中具有不同的ID字段。在接收器或者其中代理装置接收到数据分组时，接收器将ACK分组的ID字段设置为触发ACK的分组的ID字段的函数。由于该方法不需要附加的数据发送，保持网络和TCP首部空间的有效性，所以该方法是有益的。所选择的功能应该提供消除二义性的高度可能性。在优选实施例中，发送器选择具有最高有效位设置为0的IP ID值。当接收器响应时，IP ID值被设置为具有最高有效位设为1的同样的IP ID值。

[0169] 在另一个实施例中，和非模糊性确认相关联的传输号码被用来消除不确定确认的二义性。该技术基于的原理是由于该两个分组在时间上更接近地传输，则对于两个分组的确认将倾向于时间上更接近地接收。由于对于这样的分组所接收的确认不能轻易地与传输号码相关联，所以没有重传输的分组不会导致不确定性。因此，对于在时间上接近于已知确认的多接收的不确定确认，比较这些已知的传输号码和可能的传输号码。发送器将不确定确认的传输号码和最近已知的所接收的传输号码相比较，选择对于已知的所接收的传输号码最接近的一个。例如，如果接收到数据分组1的确认并且最后所接收的确认是用于数据分组5，发送器通过假设数据分组1的第三实例所导致的确认来解析该不确定性。

[0170] 选择性确认

[0171] 设备200或者流控制器220的另一个技术是实现传输控制协议选择性确认或者TCP SACK的实施例来确定哪些分组已经接收到或者没有接收到。该技术允许发送器明确确定已经由接收器接收的一分组列表以及没有接收到的一精确分组列表。可以通过修改发送器和/或接收器或者通过将发送器和接收器侧流控制模块220插入到发送器和接收器之间的网络路径中来实现该功能。参考图1A或者图1B，例如客户机102的发送器被配置为通过网络104将数据分组传输到例如服务器106的接收器。作为响应，接收器将称之为SACK分组的TCP选择性确认选项返回给发送器。在一个实施例中，尽管此处为了简便仅讨论一个方向的通信，但是该通信是双向的。接收器保持一个列表或者其它适合的数据结构，包含用于接收器已经实际接收到的数据分组的序列号的一组范围。在一些实施例中，该列表根据序列号以升序或者降序排列。接收器还保持放弃(left-off)的指针，其包括对列表的引用并且指示从之前产生的SACK分组的放弃点。

[0172] 当接收到数据分组时，接收器产生SACK分组并将其传输回到发送器。在一些实施例中，SACK分组包括多个字段，每个字段可以保持序列号的范围来指示一组已接收的数据分组。接收器使用包括触发SACK分组的登陆(landing)分组的序列号的范围来填充SACK分组的该第一字段。剩余可用的SACK字段使用来自所接收分组的列表的序列号的范围填充。由于列表中的范围多于可以被载入SACK分组的，则接收器使用放弃指针来确定哪个范围被载入SACK分组。接收器从分类的列表连续插入SACK范围，从指针索引的范围开始并且在列

表持续向下，直到消耗完SACK分组的TCP首部中的可用SACK范围空间。如果到达末端，则接收器环绕到列表的开始。在一些实施例中，两个或者三个附加的SACK范围可以被增加到SACK范围信息。

[0173] 一旦接收器产生SACK分组，则接收器将确认发送回发送器。接收器随后在列表中将放弃指针前进一个或者多个SACK范围项。例如，如果接收器插入四个SACK范围，则放弃指针可以在列表中被推进两个SACK范围。当所推进的放弃指针达到列表的末端，则指针被重置为列表的开始，有效地围绕已知所接收范围的列表。将该列表围绕使得系统可以执行得好，甚至在SACK分组大的损失的情况下，这是由于一旦列表被围绕，则由于丢失的SACK分组导致的未被通信的SACK信息最终被通信。

[0174] 因此可以理解，SACK分组可以通信关于接收器的情况的多个细节。第一，SACK分组指示在SACK分组产生时接收器已经接收该SACK信息的第一字段中的数据分组。其次，SACK信息的第二和随后的字段指示接收器已经接收这些范围中的数据分组。SACK信息还暗示接收器在SACK分组的产生时没有接收落入SACK信息的第二和随后的字段之间的任意一个数据分组。本质上，SACk信息中的第二和随后的范围之间的范围是所接收数据中的“孔”，其中已知的未被递送的数据。从而，使用该方法，当SACK分组具有足够空间来包括多于两个的SACK范围，接收器可以向发送器指示还没有由接收器接收的数据分组的范围。

[0175] 在另一个实施例中，发送器使用之上描述的SACK分组结合上述重传输技术来假设数据分组已经被递送到接收器。例如，当重传输算法(使用传输号码)宣告分组丢失，则发送器认为该分组仅是条件性丢失，有可能识别该分组接收的SACK分组丢失，而不是数据分组本身丢失。发送器因此将该分组增加到潜在丢失的分组的列表，称之为假定丢失的列表。每当SACK分组到达，来SACK分组的数据的已知丢失范围和假定丢失列表中的分组相比较。包括已知丢失的数据的分组被宣告实际丢失并且被随后重传输。以此方式，组合这两个方案来给予发送器关于分组已经丢失并且需要重传输的更好的信息。

[0176] 事务边界检测

[0177] 在一些实施例中，设备200或者流控制器220应用称之为事务边界检测的技术。在一个实施例中，该技术适合于乒乓(ping-pong)表现的连接。在TCP层，乒乓行为是当一个通信器例如发送器发送数据并且随后等待来自另一个通信器例如接收器的响应。乒乓行为的例子包括远程程序调用、HTTP和其他。以上描述的算法使用重传输超时来恢复和事务相关的最后的分组的丢失。由于在一些实施例中TCP RTO机制极端粗略，例如在所有情况中要求最小一秒的值，差的应用行为在这些情况中可以看到。

[0178] 在一个实施例中，数据的发送器或者耦合到发送器的流控制模块220检测所发送数据中的事务边界。在检测到事务边界时，发送器或者流控制模块220发送附加的分组，其接收产生来自于接收器的附加的ACK或者SACK响应。附加分组的插入优选地限制到改进的应用响应时间和网络能力利用之间的平衡。所插入的附加分组的数量可以根据和该连接相关的当前损失率来选择，对于越高损失率的连接选择更多的分组。

[0179] 检测事务边界的一个方法是基于时间的。如果发送器已经发送数据并且停止，则在一段时间之后发送器或者流控制模块200宣告事务边界。这可以和其他技术相组合。例如，通过发送器在TCP首部中设置PSH(TCP进栈)位可以指示事务边界。随之，将基于时间的方法和这些附加的试探方法相组合可以提供对于事务边界的更精确的检测。在另一个技术

中，如果发送器或者流控制模块220理解应用协议，其可以解析协议数据流并且直接确定事务边界。在一些实施例中，可以独立于任一基于时间的机制使用此最后的行为。

[0180] 响应于检测事务边界，发送器或者流控制模块220将附加的数据分组传输到接收器来从其引发确认。从而附加数据分组应该使得接收器将响应于接收数据分组来至少产生ACK或者SACK。在一个实施例中，简单地重传输事务的最后一个或者多个分组。相比于仅发送哑元数据分组，如果最后一个或者多个分组已经丢失，这就具有重传输所需数据的增加的益处。在另一个实施例中，发送最后一个或者多个分组的片段，允许发送器来消除来自于他们最初分组的这些分组到来的二义性。允许接收器来避免错误的搞乱任一重新排序自适应算法。在另一个实施例中，任意数量的公知的前向纠错技术可被用来产生附加的数据用于插入的分组，允许重新构造接收器处丢失的或者以其他方式失败的数据。

[0181] 在一些实施例中，当事务中的最后一个分组的确认丢失时，此处描述的边界检测技术有助于避免超时。当发送器或者流控制模块220接收用于这些附加数据分组的确认时，发送器可以从这些附加确认来确定是否最后一个分组已经接收或者需要重发送，从而避免超时。在一个实施例中，如果最后的分组已经接收到但是它们的确认丢失，则流控制模块220产生用于该数据分组的确认，并且将确认发送给发送器，从而告知发送器数据分组已经递送。在另一个实施例中，如果最后的数据分组还没有接收到，则流控制模块220发送一个分组给发送器来引发发送来重发送丢失的数据分组。

[0182] 重新分包

[0183] 在又一个实施例中，设备200或者流控制器220应用重新分组技术来改进传输层网络业务量的流。在一些实施例中，TCP的性能和分组大小成比例。因此增加分组大小能改进性能，除非其引发实质的增加的分组损失率或者其他的非线性效应，例如IP分片(fragmentation)。通常，有线介质(诸如铜缆或者光纤)具有极低的误码率，低到可以忽略不计。对于这些介质，在分片发生之前，最大化分组大小可以是有益的(通过基本传输介质的协议来限制最大化分组大小)。但是对于具有较高损失率的传输介质(例如，诸如WiFi等的无线技术或者诸如配电线网络等的高损环境)，由于介质引发的错误导致整个分组丢失(即，介质引发的错误超过对于该介质的标准纠错码的能力)，增加了分组丢失率，从而增加分组大小可以导致较低传输率。分组损失率中的显著大的增加实际上否定了增加的分组大小的任一性能益处。在一些情况中，对于TCP端点来选择最优的分组大小可能是困难的。例如，最优的分组大小根据每个链路的性质在通过传输路径时改变。

[0184] 通过将设备200或者流控制模块220插入到传输路径中，流控制器220监控链路的特征并且根据所确定的链路特征重新分组。在一个实施例中，设备200或者流控制器220将具有连续数据的分组重新分组为较小数量的较大的分组。在另一个实施例中，设备200或者流控制器220通过一列大的分组的部分分为大量的较小的分组而将分组重新分组。在其他实施例中，设备200或者流控制器220监控链路特征并且通过重新组合来调整分组大小以改进吞吐量。

[0185] QoS

[0186] 仍旧参考图2A，在一些实施例中，流控制器220可以包括QoS引擎236，也称为QoS控制器。在另一个实施例中，例如设备200和/或网络优化引擎250包括单独的但与流控制器220通信的QoS引擎236。QoS引擎236包括用于执行一个或者多个服务质量(QoS)技术改进任

一网络连接的性能、操作或者服务质量的任意逻辑、商业规则、功能或者操作。在一些实施例中，QoS引擎236包括为不同用户、应用、数据流或者连接提供不同特性的网络业务量控制和管理机制。在其他实施例中，QoS引擎236为用户、应用、数据流或者连接控制、维持或者确保特定水平的性能。在一个实施例中，QoS引擎236为用户、应用、数据流或者连接控制、维持或者确保特定部分的带宽或者网络容量。在一些实施例中，QoS引擎236监控性能的实现水平或者对应于用户、应用、数据流或者连接的服务质量，例如数据率和延迟。响应于监控，QoS引擎236动态地控制或者调整网络分组的调度特性来实现期望水平的性能或者服务质量。

[0187] 在一些实施例中，QoS引擎236根据一个或者多个服务的等级或者水平来优先排序、调度和传输网络分组。在一些实施例中，服务的等级或者水平可以包括：1)最好的努力，2)控制的负载，3)担保或者4)性质。对于服务的最好结果等级，设备200作出合理的努力来递送分组(标准服务水平)。对于服务的控制的负载等级，设备200或者QoS引擎236逼近传输介质的标准的分组错误损失或者逼近小负载网络条件中的最好努力的服务的行为。对于服务的担保等级，设备200或者QoS引擎236保证该能力来在连接期间以确定速率传输数据。对于服务的性质等级，设备200或者QoS引擎236使用性质服务等级用于请求或者期望优先排序的业务量但不能保证资源需求或者服务水平的应用、用户、数据流或者连接。在这些情况中，设备200或者QoS引擎236基于QoS引擎236的任意逻辑或者配置或者基于商业规则或者策略来确定服务等级或者优先级。例如，在一个实施例中，QoS引擎236根据策略引擎295、295'执行的一个或者多个策略来优先排序、调度和传输网络分组。

[0188] 协议加速

[0189] 协议加速器234包括用于优化、加速或者以其他方式改进一个或者多个协议的性能、操作或者服务质量的任意逻辑、商业规则、功能或者操作。在一个实施例中，协议加速器234在网络堆栈的层5-7处加速任意应用层协议。在其他实施例中，协议加速器234加速传输层或者层4协议。在一个实施例中，协议加速器234加速层2或者层3的协议。协议加速器234被配置、构建或者设计来根据数据类型、协议的特征和/或行为来优化或者加速一个或者多个协议的每一个。在另一个实施例中，协议加速器234被配置、构建或者设计来改进用户体验、响应时间、网络或者计算机负载和/或关于协议的网络或者带宽利用。

[0190] 在一个实施例中，协议加速器234被配置、构建或者设计来最小化文件系统访问上的WAN等待时间的效应。在一些实施例中，协议加速器234优化或者加速CIFS(公共因特网文件系统)协议的使用来改进文件系统访问时间或者对数据和文件的访问时间。在一些实施例中，协议加速器234优化或者加速NFS(网络文件系统)协议的使用。在另一个实施例中，协议加速器234优化或者加速文件传输协议(FTP)的使用。

[0191] 在一个实施例中，协议加速器234被配置、构建或者设计来优化或者加速承载净荷或者使用任一类型和形式标记语言的协议。在其他实施例中，协议加速器234被配置、构建或者设计为优化或者加速超文本传输协议(HTTP)。在另一个实施例中，协议加速器234被配置、构建或者设计为来优化或者加速承载净荷或者以其他方式使用XML(可扩展标记语言)的协议。

[0192] 透明并且多点布置配置

[0193] 在一些实施例中，设备200和/或网络优化引擎250对于通过诸如WAN链路的网络连

接或链路的任意数据流是透明的。在一个实施例中，设备200和/或网络设备250以此方式操作：通过WAN的数据流是由任意网络监控、QoS管理或者网络分析工具可识别的。在一些实施例中，设备200和/或网络优化引擎250不产生任意隧道或者流用于传输可以隐藏、混淆或者以其他方式是网络业务量不透明的数据。在其他实施例中，设备200透明操作，其中设备不改变网络分组的任一源和/或目标地址信息或者端口信息，诸如互联网协议地址或者端口号。在其他实施例中，设备200和/或网络优化引擎250被认为对于网络架构中的网络、应用、客户机、服务器或者其他设备或者计算装置透明地操作或者运转。也就是在一些实施例中，设备是透明的，其中网络上的任意装置或者设备的网络相关配置不必修改来支持设备200。

[0194] 设备200可以以下面的布置配置方式来布置：1)串行业务量，2)代理模式，3)虚拟串行模式。在一些实施例中，设备200可以与以下的一个或者多个串行布置：路由器、客户机、服务器或者另一个网络装置或者设备。在其他实施例中，设备200可以与以下的一个或者多个并行布置：路由器、客户机、服务器或者另一个网络装置或者设备。在并行布置中，客户机、服务器、路由器或者其它网络设备可以被配置为转发、传送或者传输到设备200或者经由设备200。

[0195] 在串行的实施例中，设备200与路由器的WAN链路串行布置。以此方式，来自WAN的所有业务量在到达LAN的目标之前传递通过设备。

[0196] 在代理模式的实施例中，设备200被布置为客户机和服务器之间的代理装置。在一些实施例中，设备200允许客户机做出到网络上的资源的间接连接。例如，客户机经由设备200连接到资源，并且设备通过连接到资源、不同的资源、或者通过从高速缓存服务该资源来提供资源。在一些情况中，设备可以对于不同的目的来改变客户机请求或者服务器响应，诸如对于此处讨论的任一优化技术。在一个实施例中，客户机102发送寻址到代理的请求。在一个情况中，代理响应于客户机来代替或者充当服务器106。在其他实施例中，设备200通过将请求和响应拦截并透明地转发到客户机和/或服务器，用作为透明代理。不使用客户机侧配置，设备200可以将客户机请求重定向到不同的服务器或者网络。在一些实施例中，设备200可以在穿越设备的任一网络业务量上执行任一类型和形式的网络地址转换，称之为NAT。

[0197] 在一些实施例中，设备200以虚拟串行模式配置来布置。在此实施例中，具有路由或者转换功能的路由器或者网络装置被配置为转发、路由或者去以其他方式提供发往网络或者设备200的网络分组。设备200随后在网络分组上执行任一期望的处理，诸如此处讨论的任一WAN优化技术。当完成处理时，设备200将处理的网络分组阻转发到路由器以发送到网络上的目的地。以此方式，设备200可以并行耦合到路由器，但是仍旧如同设备200串行一样操作。因为分组经由设备通过网络处理和传输，则该布置模式还透明地提供所保持的源和目标地址以及端口信息。

[0198] 端点节点布置

[0199] 尽管网络优化引擎250以上总的结合设备200描述，但是网络优化引擎250或者其任意部分可以被布置、分布或者以其他方式操作在诸如客户机102和/或服务器106的任一端节点上。由此，客户机或者服务器可以提供此处描述的结合一个或更多设备200或者不结合设备200的网络优化引擎250的任一系统和方法。

[0200] 现在参考图2B，描述布置在一个或者多个端节点的网络优化引擎250的示例实施

例。总的来说，客户机102可以包括第一网络优化引擎250'并且服务器106可以包括第二网络优化引擎250"。客户机102和服务器106可以建立传输层连接并且交换穿越或者不穿越设备200的通信。

[0201] 在一个实施例中，客户机102的网络优化引擎250'执行此处描述的技术来优化、加速或者以其他方式改进与服务器106通信的网络业务量的性能、操作或者服务质量。在另一个实施例中，服务器106的网络优化引擎250"执行此处描述的技术来优化、加速或者以其他方式改进与客户机102通信的网络业务量的性能、操作或者服务质量。在一些实施例中，客户机102的网络优化引擎250'和服务器106的网络优化引擎250"执行此处描述的技术来优化、加速或者以其他方式改进在客户机102与服务器106之间通信的网络业务量的性能、操作或者服务质量。在又一个实施例中，客户机102的网络优化引擎250'结合设备200执行此处描述的技术来优化、加速或者以其他方式改进与客户机102通信的网络业务量的性能、操作或者服务质量。仍在另一个实施例中，服务器106的网络优化引擎250"结合设备200执行此处描述的技术来优化、加速或者以其他方式改进与服务器106通信的网络业务量的性能、操作或者服务质量。

[0202] C.客户机代理

[0203] 如图2A和2B所示，部署在系统中或者具有设备200或者205的客户机可以包括客户机代理120。在一个实施例中，客户机代理120被用来促进与一个或者多个设备200或者205的通信。在一些实施例中，此处描述的设备200或者205的任意系统和方法可以经由客户机代理120部署、实施或者包含在客户机中。在其他实施例中，客户机代理120可以包括提供诸如端点检测和验证、虚拟专用网络连接和应用流式传输的附加功能性的应用、程序或者代理。在讨论设备200的系统和方法的其它实施例之前，将描述客户机代理120的实施例。

[0204] 现在参考图3，描述了客户机代理120的一个实施例。客户机102包括用于经由网络104与设备200、设备205和/或服务器106建立、交换、管理或者控制通信的客户机代理120。在一些实施例中，也被称为WAN代理的客户机代理120加速WAN网络通信和/或被用来经由网络上的设备200进行通信。简单概述，客户机102在计算装置100上操作，所述计算装置100具有带有内核模式302和用户模式303的操作系统以及带有一个或多个层310a-310b的网络堆栈267。客户机102已经安装和/或执行一个或多个应用。在一些实施例中，一个或多个应用可以经由网络堆栈267通信到网络104。诸如web浏览器的一个应用还可以包括第一程序322。例如，第一程序322可以被用于在一些实施例中安装和/或执行客户机代理120或者其任意部分。客户机代理120包括用于从一个或多个应用中拦截来自于网络堆栈267的网络通信的拦截机制或拦截器350。

[0205] 如同设备200一样，客户机具有包括任意类型和形式的软件、硬件或者其任一组合的网络堆栈267来提供与网络104的连接性以及与网络104的通信。客户机102的网络堆栈267包括以上结合设备200描述的任一网络堆栈实施例。在一些实施例中，客户机代理120或者其任一部分被设计和构建为和网络堆栈267一起操作或者结合工作，网络堆栈267是由客户机102的操作系统安装或者以其他方式提供的。

[0206] 在进一步的细节中，客户机102或者设备200(或者205)的网络堆栈267可以包括用于接收、获取、提供或者以其他方式访问与客户机102的网络通信相关联的任意信息和数据的任意类型和形式的接口。在一个实施例中，到网络堆栈267的接口包括应用编程接口

(API)。该接口还可以包括任意函数调用、挂钩或过滤机制、事件或回叫机制、或任意类型的连接技术。网络堆栈267经由接口可以接收或提供诸如对象的与网络堆栈267的功能或操作相关的任意类型和形式的数据结构。例如，数据结构可以包括与网络分组相关的信息和数据或者一个或多个网络分组。在一些实施例中，数据结构包括、参考或者识别诸如传输层的网络分组的在网络堆栈267的协议层处理的网络分组的一部分。在一些实施例中，数据结构325是内核级数据结构，而在其它实施例中，数据结构325是用户模式数据结构。内核级数据结构可以包括获得的或与在内核模式302中操作的网络堆栈267的一部分相关的数据结构、或者运行在内核模式302中的网络驱动程序或其它软件、或者由运行或操作在操作系统的内核模式中的服务、进程、任务、线程或其它可执行指令获得或收到的任意数据结构。

[0207] 另外，例如数据链路或网络层的网络堆栈267的一些部分可以在内核模式302中执行或操作，而诸如网络堆栈267的应用层的其它部分执行或操作在用户模式303中。例如，网络堆栈的第一部分310a可以给应用提供对网络堆栈267的用户模式访问，而网络堆栈267的第二部分310a提供对网络的访问。在一些实施例中，网络堆栈的第一部分310a可以包括诸如层5-7中的任意一个的网络堆栈267的一个或多个较上的层。在其它实施例中，网络堆栈267的第二部分310b包括诸如层1-4中的任意一个这样的一个或多个较低的层。网络堆栈267的第一部分310a和第二部分310b中的每一个可以在任意一个或多个网络层处、在用户模式203、内核模式202或其组合中、或者在网络层的任意部分或网络层的接口点或用户模式302和内核模式203的任意部分或接口点处，包括网络堆栈267的任意部分。

[0208] 拦截器350可以包括软件、硬件或软件和硬件的任意组合。在一个实施例中，拦截器350在网络堆栈267中的任一点拦截或者以其他方式接收网络通信，并且将所述网络通信重定向或发送到被拦截器350或客户机代理120所期望、管理或控制的目的地。例如，拦截器350可以拦截第一网络的网络堆栈267的网络通信并发送该网络通信给设备200以用于在第二网络104上的传输。在一些实施例中，拦截器350包括或者是驱动器，诸如被构造和设计为与网络堆栈267接口和工作的网络驱动器。在一些实施例中，客户机代理120和/或拦截器350在诸如传输层处的网络堆栈267的一个或多个层处操作。在一个实施例中，拦截器350包括过滤器驱动程序、挂钩机制或任意格式和类型的适当的网络驱动程序接口，所述接口例如经由传输驱动程序接口(TDI)来接口于网络堆栈的传输层。在一些实施例中，拦截器350接口到诸如传输层的第一协议层以及诸如传输协议层之上的任意层的例如应用协议层的另一个协议层。在一个实施例中，拦截器350可以包括遵照网络驱动程序接口规范(NDIS)的驱动程序或NDIS驱动程序。在另一个实施例中，拦截器350可以是小过滤器(min-filter)或迷你端口(mini-port)驱动程序。在一个实施例中，拦截器350或者其一部分操作于内核模式202中。在另一个实施例中，拦截器350或者其一部分操作于用户模式203中。在一些实施例中，拦截器350的一部分操作于内核模式202中，而拦截器350的另一部分操作于用户模式203中。在其它实施例中，客户机代理120操作于用户模式203中，但经由拦截器350连接到内核模式驱动程序、进程、服务、任务或一部分操作系统，以便获得内核级数据结构225。在进一步的实施例中，拦截器350是诸如应用的用户模式应用或程序。

[0209] 在一个实施例中，拦截器350拦截或者接收任意的传输层连接请求。在这些实施例中，拦截器350执行传输层应用编程接口(API)调用以对于该位置设置目的地信息，诸如所期望的位置的目的地IP地址和/或端口。以此方式，拦截器350拦截并重定向传输层连接到

由拦截器350或客户机代理120控制或管理的IP地址和端口。在一个实施例中，拦截器350为到客户机102的本地IP地址和端口的连接设置目的地信息，客户机代理120在客户机102的本地IP地址和端口上进行监听。例如，客户机代理120可以包括在用于重定向的传输层通信的本地IP地址和端口上监听的代理服务。在一些实施例中，客户机代理120随后传达重定向的传输层通信到设备200。

[0210] 在一些实施例中，拦截器350拦截域名服务(DNS)请求。在一个实施例中，客户机代理120和/或拦截器350解析DNS请求。在另一实施例中，拦截器发送被拦截的DNS请求到设备200以用于DNS解析。在一个实施例中，设备200解析DNS请求并通信DNS响应给客户机代理120。在一些实施例中，设备200解析经由另一设备200'或DNS服务器106的DNS请求。

[0211] 在又一个实施例中，客户机代理120可以包括两个代理120和120'。在一个实施例中，第一代理120可以包括操作于网络堆栈267的网络层的拦截器350。在一些实施例中，第一代理120拦截诸如因特网控制消息协议(ICMP)请求(例如，查验和跟踪路由)的网络层请求。在其它实施例中，第二代理120'可以在传输层操作并拦截传输层通信。在一些实施例中，第一代理120拦截在网络堆栈210的一层处的通信，并与第二代理120'连接或通信被拦截的通信到第二代理120'。

[0212] 客户机代理120和/或拦截器350可以以相对于网络堆栈267的任意其它协议层透明的方式操作于协议层处或与协议层连接。例如，在一个实施例中，拦截器350以相对于诸如网络层的传输层之下的任意协议层以及诸如会话、表示或应用层协议的传输层之上的任意协议层透明地来操作网络堆栈267的传输层或与其连接。这允许网络堆栈267的其它协议层按意愿地操作而不用修改来使用拦截器350。因而，客户机代理120和/或拦截器350可以与传输层交互或者在其上操作以保护、优化、加速、路由或负载平衡经由诸如TCP/IP之上的任意应用层协议的通过传输层携带的任意协议提供的任意通信。

[0213] 进一步地，客户机代理120和/或拦截器350可以以相对于任意应用、客户机102的用户以及诸如与客户机102通信的服务器的任意其它计算装置100透明的方式来操作于网络堆栈267处或与网络堆栈267连接。客户机代理120或者其任一部分可以以一定方式安装和/或执行于客户机102上而不修改应用。客户机代理120或者其任一部分可以以对于客户机102、设备200、205或者服务器106的任意网络配置透明的方式安装和/或执行。客户机代理120或者其任一部分可以以一定方式安装和/或执行而不修改客户机102、设备200、205或者服务器106的任意网络配置。在一个实施例中，客户机102或与客户机102通信的计算装置的用户不知道客户机代理120或其任一部分的存在、执行或操作。因而，在一些实施例中，相对于应用、客户机102的用户、客户机102、诸如服务器或者设备200、205的另一个计算装置、或者在由拦截器350联接的协议层之上和/或之下的任意协议层透明地来安装、执行和/或操作客户机代理120和/或拦截器350。

[0214] 客户机代理120包括流客户机306、收集代理304、SSL VPN代理308、网络优化引擎250和/加速程序302。在一个实施例中，客户机代理120是由位于Fort Lauderdale,Florida的Citrix Syestems公司开发的独立计算架构(ICA)客户机或者其任意部分，并且还被称为ICA客户机。在一些实施例中，客户机120包括用于将应用从服务器106流式传输到客户机102的应用流客户机306。在另一个实施例中，客户机代理120包括用于执行端点检测/扫描以及为设备200和/或服务器106收集端点信息的收集代理304。在一些实施例中，客户机代

理120包括诸如网络优化引擎250和加速程序302的一个或者多个网络加速或者优化程序或者代理。在一个实施例中，加速程序302加速经由设备205'的客户机102和服务器106之间的通信。在一些实施例中，网络优化引擎250提供此处讨论的WAN优化技术。

[0215] 流客户机306是用于接收和执行来自于服务器106的流式传输的应用的应用、程序、进程、服务、任务或可执行指令集。服务器106可以将一个或多个应用数据文件流式传输到流客户机306，以用于在客户机102上播放、执行所述应用或者以其他方式使所述应用被执行。在一些实施例中，服务器106发送一组压缩的或封装的应用数据文件到流客户机306。在一些实施例中，多个应用文件在文件服务器上被压缩和存储在诸如CAB、ZIP、SIT、TAR、JAR或其它档案(archive)的档案文件中。在一个实施例中，服务器106解压缩、解封装或解档(unarchives)应用文件，并发送所述文件到客户机102。在另一个实施例中，客户机102解压缩、解封装或解档应用文件。流客户机306动态地安装应用或其中的一部分，并执行应用。在一个实施例中，流客户机306可以是可执行程序。在一些实施例中，流客户机306可以启用另一个可执行程序。

[0216] 收集代理304是用于识别、获得和/或收集关于客户机102的信息的应用、程序、进程、服务、任务或可执行指令集。在一些实施例中，设备200发送收集代理304到客户机102或客户机代理120。可以根据设备的策略引擎236的一个或多个策略来配置收集代理304。在其它实施例中，收集代理304发送收集的有关客户机102的信息给设备200。在一个实施例中，设备200的策略引擎236使用收集的信息来确定并提供对客户机到网络104的连接的访问、验证和授权控制。

[0217] 在一个实施例中，收集代理304是端点检测和扫描程序，其识别和确定客户机的一个或多个属性或特性。例如，收集代理304可以识别和确定任意一个或多个以下的客户机侧属性：1)操作系统和/或操作系统的版本，2)操作系统的服务包，3)运行的服务，4)运行的进程，和5)文件。收集代理304还可以识别和确定客户机上的任意一个或多个下列软件的存在或版本：1)防病毒软件，2)个人防火墙软件，3)反垃圾邮件软件，和4)因特网安全软件。策略引擎236可以具有根据客户机或客户机侧属性的任意一个或多个属性或特性的一个或多个策略。

[0218] SSL VPN代理308是用于建立从第一网络104到第二网络104'、104"的安全套接字层(SSL)虚拟专用网络(VPN)连接或者从客户机102到服务器106的SSL VPN连接的应用、程序、进程、服务、任务或者可执行指令集。在一个实施例中，SSL VPN代理308建立从公共网络104到专用网络104'或者104"的SSL VPN连接。在一些实施例中，SSL VPN代理308结合设备205一起工作来提供SSL VPN连接。在一个实施例中，SSL VPN代理308建立与设备205的第一传输层连接。在一些实施例中，设备205建立与服务器106的第二传输层连接。在另一个实施例中，SSLVPN代理308建立与客户机上的应用的第一传输层连接，和与设备205的第二传输层连接。在其他实施例中，SSL VPN代理308和WAN优化设备200结合工作来提供SSL VPN连接。

[0219] 在一些实施例中，加速程序302是用于执行一个或多个加速技术的客户机侧加速程序，以加速、增强或者以其他方式改善客户机与服务器106的通信和/或对服务器106的访问，诸如访问由服务器106提供的应用。加速程序302的可执行指令的逻辑、功能和/或操作可以执行一个或多个的下列加速技术：1)多协议压缩，2)传输控制协议池，3)传输控制协议

多路复用,4)传输控制协议缓冲,以及5)经由高速缓存管理器的高速缓存。另外,加速程序302可以执行对由客户机102接收和/或发送的任意通信的加密和/或解密。在一些实施例中,加速程序302以集成的方法或方式来执行一个或多个加速技术。另外,加速程序302可以在被携带为传输层协议的网络分组的净荷的任意协议或多个协议上执行压缩。

[0220] 在一个实施例中,加速程序302被设计、构建或者配置为和设备205一起工作来提供LAN侧加速或者提供经由设备205提供的加速技术。例如,在Citrix System公司出品的NetScaler设备205的一个实施例中,加速程序302包括NetScaler客户机。在一些实施例中,加速程序302提供在诸如分支结构中的远程装置中独立的NetScaler加速技术。在其他实施例中,加速程序和一个或者多个NetScaler设备205一起工作。在一个实施例中,加速程序302提供网络业务量的LAN侧或者基于LAN的加速或者优化。

[0221] 在一些实施例中,网络优化引擎250可以被设计、构建或者配置为和WAN优化设备200一起工作。在其他实施例中,网络优化设备250可以被设计、构建或者配置为提供设备200的WAN优化技术,需要或者不需要设备200。例如,在Citrix System公司出品的NeNScaler设备205的一个实施例中,网络优化设备250包括NeNScaler客户机。在一些实施例中,网络优化引擎250提供在诸如分支结构中的远程位置中独立的NeNScaler加速技术。在其他实施例中,网络优化引擎250和一个或者多个NeNScaler设备200一起工作。

[0222] 在另一个实施例中,网络优化引擎250包括加速程序302,或者加速程序302的功能、操作和逻辑。在一些实施例中,加速程序302包括网络优化引擎250,或者网络优化引擎250的功能、操作和逻辑。在又一个实施例中,网络优化引擎250被提供或者安装为来自加速程序302的单独的程序或者可执行指令集。在其他实施例中,网络优化引擎250和加速程序302包括在相同的程序中或者同一个可执行指令集中。

[0223] 在一些实施例中以及仍然参考图3,可以使用第一程序322来自动地、静默地、透明地或以其他方式地安装和/或执行客户机代理120或者其一部分。在一个实施例中,第一程序322是诸如被加载应用并由应用执行的ActiveX控件或Java控件或脚本的插件部件。例如,第一程序包括由web浏览器应用加载并运行在例如应用的存储空间或上下文中的ActiveX控件。在另一个实施例中,第一程序322包括由诸如浏览器的应用加载并运行的一组可执行指令。在一个实施例中,第一程序322被设计和构造来安装客户机代理120。在一些实施例中,第一程序322通过网络来从另一个计算装置获得、下载或接收客户机代理120。在另一个实施例中,第一程序322是客户机102的操作系统上的诸如网络驱动程序和客户机代理120或其任意部分的安装程序或用于安装程序的即插即用管理器。

[0224] 在一些实施例中,客户机代理120、流客户机306、收集代理304、SSL VPN代理308、网络优化引擎250、加速程序302、拦截器350的每一个或者其中任意部分可以被安装、执行、配置或者操作为单独的应用、程序、进程、服务、任务或者可执行指令集。在其他实施例中,客户机120的每一个或者任意部分可以被一起安装、执行、配置或者操作为单独的客户机代理120。

[0225] D、用于处理网络拥塞的系统和方法

[0226] 现在参考图4,示出取样TCP分组。总的来说,TCP分组包括首部410和有效载荷490。首部410包括可以被用来指示和数据通信和网络拥塞相关的传输事件的多个标识,包括ACK号460、显式拥塞通知回应(ECE标志)、ACK标志440和进栈(PSH)标志420。

[0227] 仍旧参考图4，所示取样TCP分组图形示出可包括在TCP分组中的一些信息。尽管所示取样反映了TCP分组的特定实施例，但是本领域内普通技术人员可以认识到TCP和其他网络协议的许多实现方案和变化可以应用到此处描述的系统和方法中，包括RFC 793、RFC 1122中指定的TCP实现方案，并且特别是涉及拥塞控制和避免的RFC 2581和RFC 3168。在其中一些实现方案和其他实现方案中，ECE标记可以被用来通知分组接收器发生了网络拥塞。分组接收器随后可以选择降低它们的传输率或者调整任一其它拥塞控制或者避免策略。该ECE标记还被用来和其他信令位相结合，其和接收器协商是否支持显式拥塞通知(ECN)。显式拥塞的协商或者信令中使用的任一协议中的任一位可以称之为ECN位。

[0228] 现在参考图5，示出通过装置在多个传输层连接之间分布拥塞事件的系统。总的来说，多个客户机102a、102b、102n经由设备200和多个服务器106a、106b、106n相通信。当设备接收到网络拥塞500a的指示时，设备中操作的流控制器可以拦截指示500a，并且经由不同的连接传输第二拥塞指示500b。以此方式，设备可以在多个连接之间分配拥塞指示来控制每一连接所使用的带宽。在一些实施例中，拥塞指示的分配可以被用来协助提供关于一个或者多个连接的服务质量(QoS)保证。

[0229] 仍旧参考图5，更详细地说多个客户机102经由设备200和多个服务器106相通信。客户机102可以通过包括LAN、WAN、MAN或者任意其它网络或者网络的组合的任意方式来连接到设备200。在一些情况中，客户机102每一个可以经由一个或者多个其他设备连接到设备200。例如，客户机102每一个可以驻留在分支机构，而设备200和服务器106位于中央办公室。客户机106可以经由位于分支机构的第二设备200'连接到设备200。尽管图中描述多个客户机，但是所描述的系统和方法还可以应用到单个客户机102通过多个连接和一个或者多个服务器通信的情况。

[0230] 服务器106可以通过包括LAN、WAN、MAN或者任意其它网络或者网络的组合的任意方式来连接到设备200。所描述的系统和方法还可以应用到单个服务器106通过多个连接和一个或者多个客户机通信的情况。

[0231] 在一些实施例中，设备200可以用作对于连接510、515、520的代理。在其他实施例中，设备200可以用作该连接的透明代理。设备200可以提供关于该连接的高速缓存、加速或者任意其它网络服务。

[0232] 设备200经由连接515a接收拥塞指示500a。拥塞指示可以包括显式传达网络拥塞或者允许做出潜在的网络拥塞论断的任一通知。拥塞指示500可以包括但不限于丢失的分组的指示、延迟的分组的指示、受损的分组的指示和显式拥塞指示。拥塞指示500的特定例子可以包括但不限于包括复制确认(ACK)的TCP分组和包括一个或者多个标记的ENC位的TCP分组。拥塞指示500还可以被称为拥塞事件的指示。拥塞事件可以是可能由网络拥塞引发的任一网络或者装置事件。

[0233] 设备200可以随后产生经由一个连接传输的拥塞指示500b，该连接不同于对应于在其上接收拥塞指示500a的连接的连接。设备可以经由任一装置产生拥塞指示，并且可以产生和传输任一类型的拥塞指示。在一些实施例中，设备200可以以透明的方式产生拥塞指示500b，使得其向服务器106a呈现出该拥塞指示源自客户机102a。

[0234] 现在参考图6，示出通过装置在多个传输层连接中分布拥塞事件的方法的一个实施例。总的来说，该方法包括通过装置建立多个传输层连接，该传输层连接的一个或者多个

具有所分配的优先级(步骤601)。该装置经由第一传输层连接接收网络拥塞的第一指示(步骤603)。该装置随后根据所分配的优先级选择第二传输层连接(步骤605),并且经由所选择的第二传输层连接传输拥塞事件的第二指示(步骤609)。在一些实施例中,该方法还可以包括根据所分配的优先级来选择第三传输层连接(步骤611)并且经由第三传输层连接传输第三拥塞指示(步骤613)。

[0235] 仍旧参考图6,更详细地说可以期望在一些网络环境中具有用于指派拥塞事件的装置。如果网络104变得拥塞,则其不能期望所有经由网络104通信的连接受到该拥塞相同的影响。当视频质量和响应时间遭受损害时,传输实时视频会议数据的连接的降速对于连接的接收器可以导致严重的后果。相反,大的文件传送可以承担显著的拥塞延迟,而不会对于用户产生严重的负面结果。然而,如果多个连接在同一网络104上操作,则不能保证遭受诸如丢失分组的拥塞事件的第一连接将是最低优先级的连接。在这些情形中,也许重新分布拥塞事件对设备来说是有利的,使得较低优先级连接接收拥塞事件并相应降低其带宽,而允许较高优先级连接继续以较高速率传输。在其它情形中,重新分布拥塞事件可以被用来确保即便其中拥塞事件没有在所有连接中均匀地出现,多个连接继续以相同的速率传输。依然在其它实施例中,装置可以根据事务大小来分布拥塞事件。

[0236] 在所示实施例中,装置可以建立多个传输层连接,该传输层连接的一个或者多个具有所分配的优先级(步骤601)。装置可与一个或者多个计算装置建立多个连接,计算装置可以包括客户机102、服务器106和其他设备200。在一些实施例中,装置可以在对于传输层连接用作中间设备过程中建立传输层连接。在这些实施例中,多个传输层连接的两个或者多个可以包括类似于图5中的连接510a和510b的对应的传输层连接。该装置可以包括设备200、客户机代理或者服务器代理。在一个实施例中,传输层连接可以包括TCP连接。在其他实施例中,传输层连接可以包括任一其它协议。在一个实施例中,装置可以将具有相同的源和目标的分组序列处理为单个连接,甚至在该分组未使用明确使用连接的协议发送时。

[0237] 该装置可以以任一方式分配优先级给一个或者多个所建立的连接。在一些实施例中,装置可以为多个连接的每一个分配唯一的优先级。在其他实施例中,装置可以为多个连接的一些或者全部连接分配单个优先级。在一些实施例中,该装置可以在连接建立时为连接分配优先级。在其他实施例中,该装置可以只有在拥塞事件或者其他事件已经发生之后为连接分配优先级。在一些实施例中,分配给给定连接的优先级可以保持不变。在其他实施例中,分配给给定连接的优先级可以响应于连接的特性和装置或者网络中的条件而随时间改变。例如,装置可以分配更高的优先级给当前相对低的带宽使用的连接,分配较低的优先级给使用更多当前带宽的连接。

[0238] 在一个实施例中,该装置可以基于连接的一个或多个协议来分配优先级。例如,装置可以相对于TCP业务量分配较高的优先级给UDP业务量。或者例如,装置可以相对于FTP业务量分配更高的优先级给HTTP业务量。在另一个实施例中,装置可以基于经由连接承载的业务量的一个或者多个特性来分配优先级。例如,设备可以给突发连接分配相比于具有相对稳定带宽的连接更高的优先权。在一些实施例中,通过装置的管理员或者通过连接自身中包含的消息可以明确配置优先级。

[0239] 在一些实施例中,所分配的优先级可以直接关联到连接所分配的带宽。例如,设备可以分配10Mb/sec的最大带宽给多个连接的每一个。或者设备可以分配5Mb/sec的目标带

宽给多个连接的其中一个，而分配10Mb/sec的目标带宽给多个连接的第二个。

[0240] 在其他实施例中，所分配的优先级可以对应于连接的服务质量水平。服务质量水平可以以任意方式指定。在一些实施例中，设备可以识别和/或利用在连接中的TCP相关或者IP相关的协议中使用的任一服务质量指示。例如，RFC1394、RFC2474和RFC2475详细描述了这些方法，通过这些方法，TCP和IP连接可以通知涉及服务质量和类型的信息。

[0241] 仍在其他实施例中，所分配的优先级可以对应于连接的当前或者平均事务大小。在这些实施例中，装置可以分配更高的优先级给承载更短事务的连接。这些连接更可能载有诸如VoIP或者远程程序调用的时间敏感的业务量，其更容易受到拥塞事件的负面影响。

[0242] 该装置可以以任一方式经由第一传输层连接接收网络拥塞的第一指示(步骤603)。该网络拥塞的指示可以包括此处描述的任一拥塞指示500。在一些实施例中，该装置可以接收多个拥塞指示。在这些实施例中，可以经由多个连接的一个或者多个来接收多个拥塞指示。

[0243] 该装置随后可以根据所分配的优先级选择多个连接的第二传输层连接(步骤605)。在一些实施例中，该装置可以选择具有最低分配的优先级的传输层连接。在其他实施例中，装置可以选择具有最低分配的优先级的连接，该连接还通过接收到拥塞事件的同一网络来传输数据。在此实施例中，该设备可以选择通过接收到拥塞事件的同一网络间接传输数据的连接。例如，在图5中，即使连接510b不能在连接515b使用的网络上直接通信时，设备还选择连接510b。然而，通过连接510b发送的数据随后通过连接510a发送，其可以使用与连接515a相同的网络，并且因此选择连接510b可以产生降低网络104a上业务量的期望结果。

[0244] 在一个实施例中，装置可以选择相对于当前带宽利用具有最低分配的优先级的连接(步骤605)。在此实施例中，目标可以是识别消耗大量带宽的低优先级连接，并且可能是所接收的拥塞事件的部分原因。例如，装置可以选择具有低于给定阈值的优先级但传输超过第二给定阈值的连接。在此例中，装置可以选择具有低于临界阈值的优先级的连接，其传输超过2Mb/sec的阈值。或者该装置选择传输超过给定带宽阈值的最低优先级连接。仍在其他实施例中，装置可以选择使用最大量带宽的连接。

[0245] 在一些实施例中，该装置可以选择传输超过分配带宽最多的连接。例如，如果三个连接每个分配给4Mb/sec并且经由第一连接接收到拥塞事件，则装置可以选择传输超过4Mb/sec阈值最多的连接来传输拥塞指示。该装置可以选择传输超过每秒绝对位或者按百分比最多的连接。例如，如果三个连接分配给1Mb/sec、2Mb/sec和10Mb/sec的带宽，则装置可以选择超过其分配带宽最高百分比的连接。

[0246] 在一些实施例中，装置还可以考虑在选择连接来接收随后的拥塞指示过程中连接是否接收了另一个最近的拥塞指示。在其中一个实施例中，设备可以从考虑事项中移除已经接收到最后的来回行程时间(RTT)中的拥塞指示的任一连接，该拥塞指示通过装置产生或者来自另一个源。在此实施例中，装置可以选择传输超过其分配带宽最多、在最后的RRT中没有接收到拥塞指示的连接。在一些实施例中，装置可以维持列表、队列或者其它数据结构来记录在连接之间接收的或者指派的拥塞指示。在其中一些实施例中，装置可以使用循环或者其它算法来在连接中分布拥塞指示。

[0247] 在选择连接(步骤605)之后，装置可以以任一方式经由所选择的连接传输网络拥

塞的指示。在一些实施例中，装置可以传输分组已经丢失的指示。在其他实施例中，装置可以传输具有标记的ECN位的一个或多个分组。

[0248] 装置可以抑制、丢弃、忽视、重写或者以其他方式处理所接收的拥塞指示用来隐藏来自目的接收器的指示。例如，如果所接收的拥塞指示是具有标记的ECN位的分组，则装置可以在将分组转发给接收器之前取消ECN位标记。或者例如，如果所接收的拥塞指示是丢失分组的指示，则装置可以重传丢失的分组，而无需通知分组的最初的发送器。

[0249] 在一些实施例中，装置可以响应于单个所接收的拥塞指示传输多个拥塞指示。在这些实施例中，装置可以使用用来选择第二连接的任一标准来选择三个连接来接收拥塞事件。例如，如果拥塞指示经由高优先级连接接收，装置可以经由两个较低优先级连接来传输拥塞指示，以产生足以减轻网络拥塞的较低优先级连接的之后带宽利用的下降。该例子适合用在两个较低的优先级连接在相对于较高的优先级连接的较低的速率传输的情况中。

[0250] 现在参见图7，示出用于使用透明代理对传输连接提供服务质量水平来控制连接带宽的系统。在一些实施例中，该系统类似于图5的系统，因为设备使用拥塞指示来控制多个连接中的带宽利用。然而，在图7中，设备没必要在发送拥塞事件之前等待输入的拥塞指示的到来。而是，一旦设备检测到连接超过所分配的带宽时，设备就可以传输拥塞指示。

[0251] 仍旧参考图7，更详细地说多个客户机102经由设备200和多个服务器106相通信。客户机102可以通过包括LAN、WAN、MAN或者任意其它网络或者网络的组合的任意方式来连接到设备200。在一些情况中，客户机102每一个可以经由一个或者多个其他设备连接到设备200。例如，客户机102每一个可以驻留在分支机构，而设备200和服务器106位于中央办公室。在另一实施例中，设备200可以位于具有客户机的分支机构。客户机106可以经由位于分支机构的第二设备200'连接到设备200。尽管图中描述多个客户机，但是所描述的系统和方法还可以应用到单个客户机102通过多个连接和一个或者多个服务器通信的情况。

[0252] 服务器106可以通过包括LAN、WAN、MAN或者任意其它网络或者网络的组合的任意方式来连接到设备200。所描述的系统和方法还可以应用到单个服务器106通过多个连接和一个或者多个客户机通信的情况。

[0253] 在一些实施例中，设备200可以用作对于连接510、520的代理。在其他实施例中，设备200可以用作该连接的透明代理。设备200可以提供关于该连接的高速缓存、加速或者任意其它网络服务。在一个实施例中，该连接可以包括TCP连接。在其他实施例中，该连接可以包括任一其它传输层协议。

[0254] 在所示系统中，设备包括确定连接何时超过所分配的带宽的流控制器。流控制器随后在期望导致连接的发送器降低它们的带宽时引发连接中的拥塞事件。该过程将结合图8更详细地进行描述。

[0255] 现在参考图8，示出用于使用透明代理对传输连接提供服务质量水平来控制连接带宽的方法。总的来说，该方法包括通过用作对于发送器和接收器之间的传输层连接的透明代理的设备确定经由传输层连接的发送器的传输率不同于预定的传输率(步骤801)。该设备可以随后响应于该确定来产生包含以改变传输速率的指示的确认分组(步骤803)；并且传输所产生的确认(步骤805)。

[0256] 仍旧参考图8，更详细地说用作对于发送器和接收器之间的传输层连接的透明代理的设备可以以任一方式确定经由传输层连接的发送器的传输率不同于预定的传输率(步

骤801)。传输率可以使用任意规格并且通过任意时间间隔来测量。在一个实施例中,设备可以确定连接已经超过在给定时间间隔上传输的所允许的最大数量的字节。时间间隔可以包括任一持续时间,包括但不限于.1秒、.5秒、1秒、2秒、3秒、5秒、和10秒。在一个实施例中,设备可以确定连接低于在给定时间间隔上传输的所允许的最大数量的字节。

[0257] 在一些实施例中,多个连接每一个可以被分配给相同的预定传输率。在其他实施例中,不同的连接可以被分配给不同的预定传输率。可以以任一方式为连接分配传输率,包括但不限于基于优先级、之前带宽消耗、协议、源地址、目标地址、和连接突发性(connection burstiness)。在一些实施例中,多个连接可以分配给总的公知可用带宽的相对的一部分。例如,如果设备用作对于具有公知或者近似公知容量的WAN上的多个连接的透明代理,则通过WAN上的每个连接可以指派给总容量的一部分。在此例中,如果四个连接通过具有公知10Mb/sec带宽的WAN,则每个连接可以被分配给2.5Mb/sec的预定传输率。可替代地,一个优先级连接可以被分配给6Mb/sec的速率,而其他三个连接可以被分配给2Mb/sec的速率。在此例和其它例子中,随着新的连接建立或者停止已有的连接,可以改变预定的传输率。

[0258] 在一些实施例中,预定的传输率可以对应于对于连接的服务质量水平。可以以任一方式指定服务质量水平。在一个实施例中,设备可以识别和/或利用在TCP相关或者IP相关的协议中使用的任一服务质量指示。在其他实施例中,预定的传输率可以对应于给定连接在WAN或者LAN上传输的确定。

[0259] 仍在其他实施例中,设备可以给多个连接的每一个分配优先级,并且随后基于分配的优先级来分配预定的传输率。优先级可以使用任意方式来分配,包括上面结合图5和6描述的那些内容。

[0260] 设备可以响应于步骤801的确定来产生包括改变传输率的指示的确认分组。该设备可以以任一方式产生确认分组。在一些实施例中,设备可以在确定之后立刻产生确认分组。在其他实施例中,设备可以在产生确认之前等待预定的时间间隔。即使没有来自该连接的接收器的确认,设备可以产生确认。设备可以使用任一技术来产生对于连接的发送器和接收器透明的确认,包括匹配源地址、目标地址、序列号和/或确认号。

[0261] 在一些实施例中,确认分组可以包含降低发送器传输率的任一指示。在一个实施例中,降低传输率的指示可以包括包含分组丢失的指示的确认。在另一个实施例中,降低传输率的指示可以包括包含标记的ECN位的确认。仍在另一个实施例中,降低传输率的指示可以包括具有用于发送器减小连接的窗大小的指示的确认。在此例中,所减小的窗大小可以不同于连接的接收器所通告的窗大小。

[0262] 在其他实施例中,确认分组可以包含增加发送器的传输率的任一指示。在一个实施例中,该增加传输率的指示可以包括具有用于发送器增加连接的窗大小的指示的确认。在此例中,所增加的窗大小可以不同于连接的接收器通告的窗大小。

[0263] 在一些实施例中,设备可以响应于单个确定来传输多个指示。例如,如果连接显著超过所分配的带宽,则设备可以产生并传输包括分组丢失的指示和对于发送器减小窗的指示的确认。在一些实施例中,设备可以传输指示到连接的两个端点。这可以适合用在连接双方正相对等量传输的情况中。

[0264] 在上述所有实施例中,设备可以继续传输包含改变传输率的指示的确认,直到连

接开始在预定的传输率范围内传输。例如，设备可以继续向发送器传输降低窗大小的指示，直到指示具有发送器足以降低它们的传输率的期望的效果。

[0265] 现在参考图9A，示出用于通过多个传输层连接的发送器根据连接的优先级来动态控制带宽的系统。总的来说，客户机102经由客户机代理120发送数据给多个服务器106。当客户机代理120经由其中一个连接接收到拥塞事件的指示时，流控制器220根据分配给连接的优先级来减低连接的拥塞窗。以此方式，较高优先级的连接可以对拥塞事件更不容易敏感，而较低优先级的连接可以对拥塞事件响应更快速。尽管所示系统描写了客户机代理120上的流控制器220，但在其他实施例中，流控制器220可以驻留在设备200、服务器106或者服务器代理上。

[0266] 仍旧参考图9A，更详细地说诸如TCP的多个协议提供用于在检测到潜在网络拥塞时降低数据传输的机制。关于TCP，这些机制可以包括修改拥塞窗，其规定所允许的最大数量的传输的未确认数据。例如，每当接收到分组已经被丢失的指示时，TCP Reno和FAST-TCP可以将拥塞窗分成两半。这可以导致在接收到分组丢失指示时显著降低传输的数据。其他协议可以提供其他方案以用来确定给定的分组丢失事件的未确认数据的最大数量。然而，在许多情况中，期望调整用于基于连接的优先级来响应拥塞事件的方案。例如，如果多个连接在具有固定容量的链路上传输，则可以响应于拥塞事件期望更高优先级的连接来将它们的拥塞窗下降的相比于较低优先级的连接更慢。这可以允许较高优先级的连接以相对较高的速率持续传输，而通过较低优先级的连接来吸收大批的带宽下降。这还可以允许诸如实时应用的得益于相对稳定带宽的连接来避免拥塞窗快速下降所引起的性能中的不期望的峰值。

[0267] 现在参考图9B，示出用于通过一个或者多个传输层连接的发送器根据分配给一个或者多个连接的优先级来动态控制连接带宽的方法。总的来说，该方法包括：发送器经由第一传输层连接传输数据，该连接具有识别在缺乏来自接收器的确认的情况下传输的数据数量的第一拥塞窗大小(步骤901)。发送器可以经由连接接收分组丢失的指示(步骤903)，并且识别对应于连接的缩小因子(步骤905)。发送器随后可以确定第二拥塞窗大小，第二拥塞窗大小包括根据缩小因子降低的第一拥塞窗大小(步骤907)。发送器可以随后根据第二拥塞窗大小来传输数据(步骤909)。发送器可以包括任意计算装置和/或软件，包括但不限于客户机、服务器、客户机代理、服务器代理和设备。

[0268] 仍旧参考图9B，更详细地说装置经由具有第一拥塞窗大小的传输层连接传输数据(步骤901)。拥塞窗大小可以包括“传送(in flight)”的未确认数据的数量上的任一上限、约束、或者其他限制。例如，一旦未确认数据数量等于或者超过拥塞窗大小时，发送器可以停止传输新的数据。在一个实施例中，第一拥塞窗大小可以是TCP拥塞窗大小。在一些实施例中，装置可以经由多个连接传输数据，每个连接具有拥塞窗大小。

[0269] 发送器可以随后经由第一连接接收分组丢失的指示(步骤903)。发送器可以经由任意一个或者多个协议接收该指示。在一些实施例中，分组丢失指示可以包括一个或者多个TCP连接中的复制的确认。在其他实施例中，分组丢失指示可以包括超时或者指示由发送器传输的分组没有接收到的一些可能性的任意其它指示。仍在其他实施例中，发送器可以如上所述接收拥塞的指示。

[0270] 发送器可以以任一方式识别对应于传输层连接的优先级的缩小因子(步骤905)。

发送器可以使用任一方法分配优先级给传输层连接，包括此处描述的任一方法。在一些实施例中，相对于较低优先级的连接，较高优先级的连接可以被标识以更低的缩小因子。缩小因子可以包括用来降低拥塞窗大小的任一数量。例如，在许多TCP实现中，标准的缩小因子缩小因子可以是2，指定每次发生丢失事件时拥塞窗被分为两半。关于所示方法，缩小因子可以是任一数量。在一个实施例中，缩小因子可以是1。在此实施例中，如果发生拥塞事件，拥塞窗大小可以完全不下降。在其他例子中，下降因素可以包括1.1、1.2、1.3、1.4、1.5、1.6、1.7、1.8、1.9或者2，或者此范围内的任一数量。在一些实施例中，低于2的缩小因子可以关于较高优先级的连接来使用。仍在其他实施例中，缩小因子可以包括2.1、2.5、3、3.5、4、4.5、5、5.5、或者6或者此范围内的任一数量。在一些实施例中，大于2的缩小因子可以关于较低优先级的连接来使用。

[0271] 发送器随后确定第二拥塞窗大小，第二拥塞窗大小包括通过缩小因子降低的第一拥塞窗大小(步骤907)。发送器可以以任一方式通过缩小因子来降低拥塞窗大小。在一些实施例中，发送器可以将第一拥塞窗大小除以缩小因子。在其他实施例中，发送器可以从第一拥塞窗大小减去缩小因子。仍在其他实施例中，发送器可以从拥塞窗大小减去被乘以缩小因子的常数。例如，发送器可以从拥塞窗大小中减去缩小因子与最大片段大小的乘积。此时应该认识到缩小因子可以包括到响应丢失事件来改变拥塞窗大小的任意方法中，包括TCP的任一变量。

[0272] 为了给出详细的例子，在一个实施例中，发送器可以将第一拥塞窗大小除以缩小因子来确定新的拥塞窗大小。在此例中，发送器可以分配4的缩小因子给低优先级的连接，分配2的缩小因子给正常优先级的连接，并且分配1.33的缩小因子给高优先级的连接。

[0273] 发送器可以随后经由该连接并根据第二拥塞窗大小来传输数据。在一些实施例中，发送器可以继续使用所示方法，使得拥塞窗在新的分组丢失指示到来时继续改变。

[0274] 现在参考图9C，示出用于通过一个或者多个传输层连接的发送器根据分配给一个或者多个该连接的优先级来动态控制连接带宽的第二方法。广义而言，该方法将图9A和9B的系统和方法的概念应用到拥塞窗应该增加而不是减小的状况中。总的来说，所述方法包括：发送器经由第一传输层连接传输数据，在缺乏来自接收器的确认的情况下该连接具有识别传输的数据数量的第一拥塞窗大小(步骤901)。发送器可以随后在给定时间间隔期间不接收分组丢失的指示(步骤903)，并且识别对应于连接的扩大因子(步骤905)。发送器随后可以计算第二拥塞窗大小，基于第一拥塞窗大小和扩大因子来计算第二拥塞窗大小(步骤907)。发送器可以随后根据第二拥塞窗大小来传输数据(步骤909)。发送器可以包括任意计算装置和/或软件，包括但不限于客户机、服务器、客户机代理、服务器代理和设备。

[0275] 仍旧参考图9C，更详细地说装置经由具有第一拥塞窗大小的传输层连接传输数据(步骤931)。在一些实施例中，装置可以经由多个连接传输数据，每个连接具有拥塞窗大小。在一个实施例中，传输层连接可以包括TCP连接。

[0276] 发送器可以随后在时间间隔期间不接收经由第一连接的分组丢失的指示(步骤933)。时间间隔可以包括任一时间间隔。在一个实施例中，时间间隔可以包括固定数量的时间，包括但不限于.05秒、.1秒、.2秒、.4秒、.5秒、1秒或者2秒。在其他实施例中，时间间隔可以对应于连接的特性。在一个实施例中，时间间隔可以对应于连接的来回行程时间。在另一个实施例中，时间间隔可以对应于连接的平均来回行程时间。仍在其他实施例中，时间间隔

可以对应于多个来回行程时间或者平均来回行程时间。

[0277] 发送器可以以任一方式识别对应于传输层连接的优先级的扩大因子(步骤935)。发送器可以使用任一方法分配优先级给传输层连接,包括此处描述的任一方法。在一些实施例中,相对于较低优先级的连接,较高优先级的连接可以被识别为具有更高的扩大因子。扩大因子可以包括用来增加拥塞窗大小的任一数量。例如,在一些TCP实现中,扩大因子可以是对于连接的最大分组大小,指定每次没有丢失事件通过的时间间隔(来回行程时间)时将拥塞窗增加最大分组大小。在其他TCP实现中,扩大因子可以包括将最小来回行程时间除以最近来回行程时间。关于所示方法,扩大因子可以是任意数量。在一个实施例中,扩大因子可以是0。在此实施例中,如果发生拥塞事件,拥塞窗大小可以完全不增加。在其他例子中,扩大因子可以包括0.1、.5、.75、.9、1、1.1、1.2、1.3、1.4、1.5、1.6、1.7、1.8、1.9或者2,或者此范围内的任一数量。仍在其他实施例中,缩小因子可以包括2.1、2.5、3、3.5、4、4.5、5、5.5、或者6或者此范围内的任一数量。在一些实施例中,小于1的扩大因子可以关于较低优先级的连接来使用。在一些实施例中,大于1的扩大因子可以关于较高优先级的连接来使用。

[0278] 发送器随后确定第二拥塞窗大小,第二拥塞窗大小基于第一拥塞窗大小和扩大因子来计算(步骤937)。发送器可以以任一方式使用扩大因子来计算第二拥塞窗大小。在一些实施例中,发送器可以将第一拥塞窗大小乘以扩大因子。在其他实施例中,发送器可以将扩大因子加到第一拥塞窗大小。仍在其他实施例中,发送器可以将被乘以扩大因子的常数加到拥塞窗大小。例如,发送器可以将扩大因子与最大片段大小的乘积加到拥塞窗大小。在其他实施例中,发送器还可以将一个或者多个来回行程时间计算合并到计算结果中。例如,发送器可以设置第二拥塞窗大小等于EF(MPS)+CWND_OLD*MIN_RTT/LAST_RTT,其中,EF是扩大因子,MSS是最大分组大小,CWND_OLD是之前的拥塞窗大小,并且MIN_RTT和LAST_RTT分别是连接的最小和最后的来回行程时间。

[0279] 此时应该认识到扩大因子可以被合并到响应丢失事件来改变拥塞窗大小的任意方法中,包括TCP的任一变量。在一些实施例中,上述方法可以被应用来改变TCP慢启动方法的行为。例如,在慢启动阶段分配给连接的初始拥塞窗可以关于连接的优先级来确定。在此例中,低优先级的连接可以用1的初始拥塞窗启动,而高优先级的连接可以用4的拥塞窗启动。

[0280] 为了给出详细的例子,在一个实施例中,发送器可以将最大分组大小乘以扩大因子的乘积加到之前的拥塞窗大小。在此例中,发送器可以分配.5的扩大因子给低优先级的连接,分配1的扩大因子给正常优先级的连接,并且分配2的扩大因子给高优先级的连接。

[0281] 发送器可以随后通过连接并根据第二拥塞窗大小来传输数据。在一些实施例中,发送器可以继续使用所示方法,使得拥塞窗在新的分组丢失指示到来时继续改变。

[0282] 在有些实施例中,图9B和9C中描述的方法可以结合一个或者多个连接来使用。为了给出一个例子,用作对于多个连接的透明代理的WAN优化设备可以为每一个连接和对应的扩大与缩小因子分配优先级。在此例中,优先级和扩大与缩小因子可以关于每一连接的等待时间来选择。由于典型的TCP连接在等待时间增加时需要较长的时间来增速,所以设备可以通过分配较高的扩大因子给较高的等待时间连接来对此计数。按照这些方法,设备可以检测多个连接的哪一个在WAN上传播并且相应地增加那些连接的扩大因子。设备还可以

分配较小的缩小因子给高的等待时间连接，因为它们将比较缓慢地从拥塞窗大小的任一突然下降中恢复。这些较小的缩小因子还可以反映出这样一个事实：对于高的等待时间连接越有可能瞬时拥塞已经过去了丢失的分组的任一指示到达的时间。该装置因此可以使用扩大和缩小因子来平衡具有不同等待时间的连接的各自带宽。

[0283] 虽然本发明参考特定的优选实施例具体描述和示出，但是本领域内的普通技术人员应该理解在不脱离由下面的权利要求书限定的本发明的精神和保护范围的情况下，可以在形式和细节上作出多种变化。

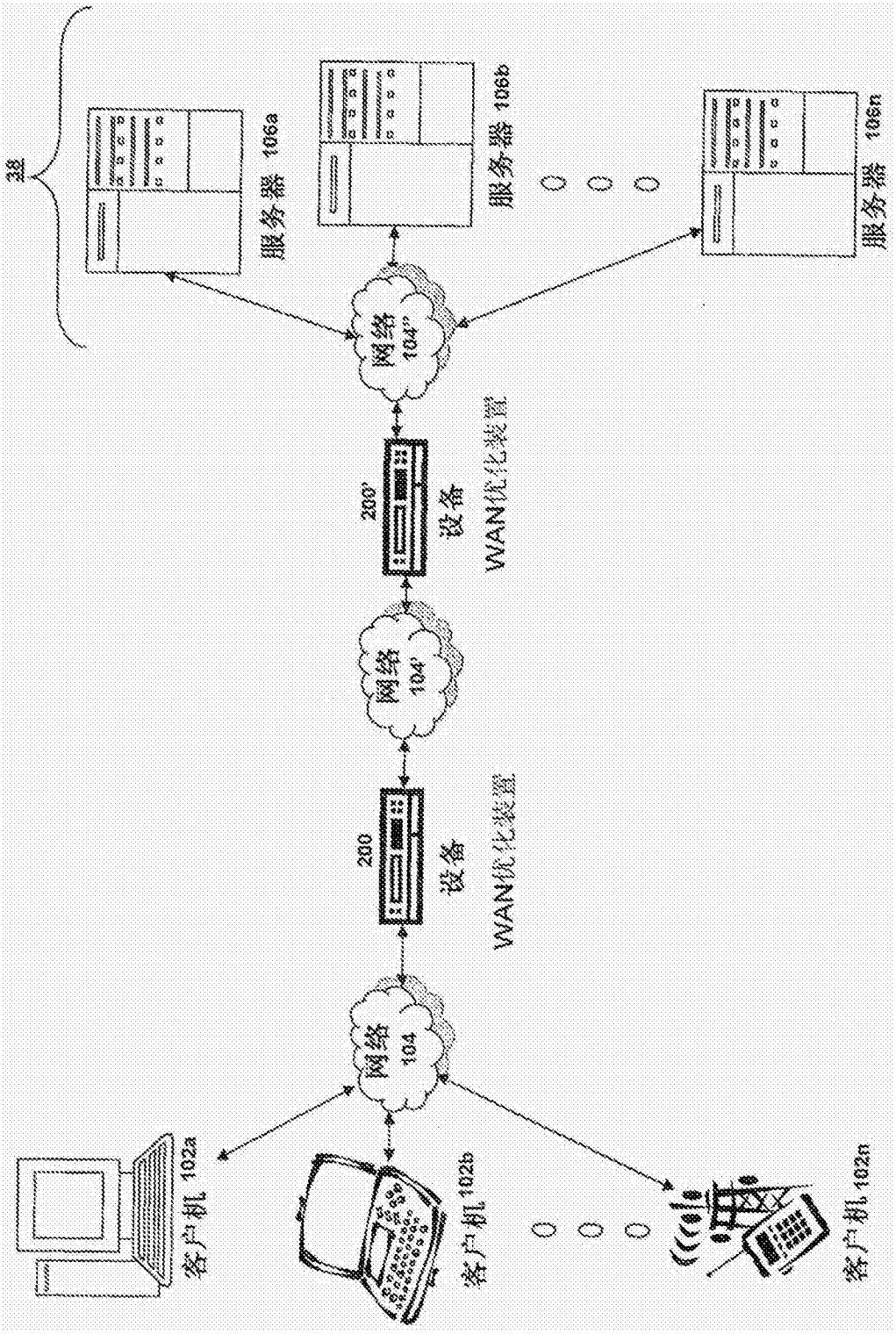

客户机 102a
客户机 102b
客户机 102n
网络 104
设备 200
WAN优化装置
网络 104'
设备 200'
WAN优化装置
网络 104''
服务器 106a
服务器 106b
服务器 106n
多

图1A

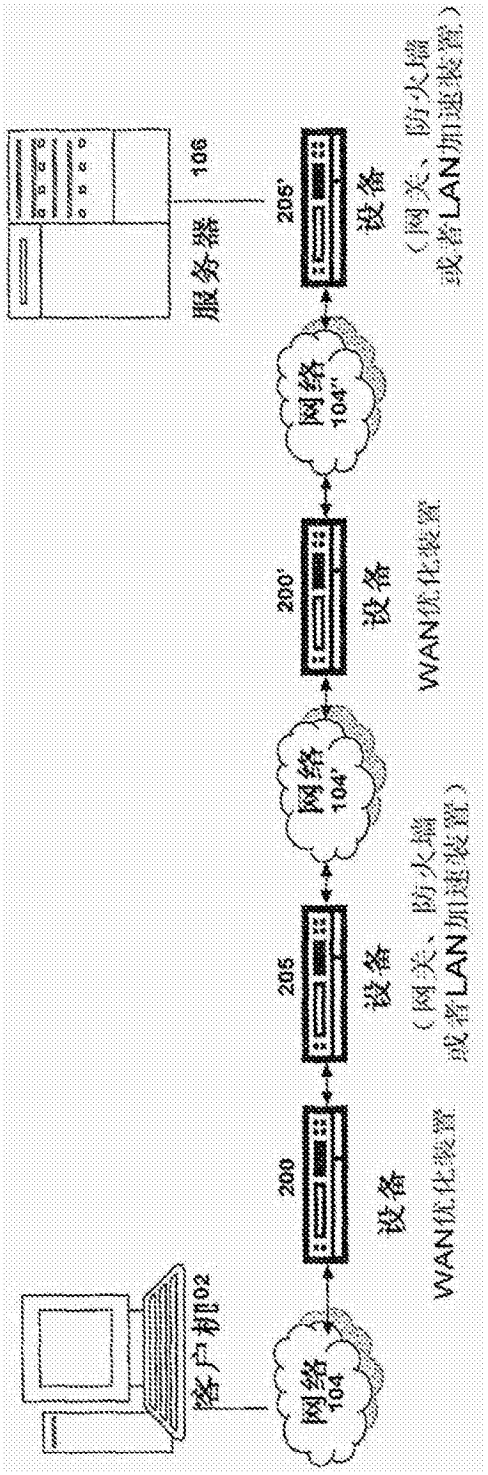

客户机 102
网络 104
200
设备
WAN优化装置
205
设备
（网关、防火墙
或者LAN加速装置）
网络 104'
200'
设备
WAN优化装置
205'
设备
（网关、防火墙
或者LAN加速装置）
网络 104''
服务器 106

图1B

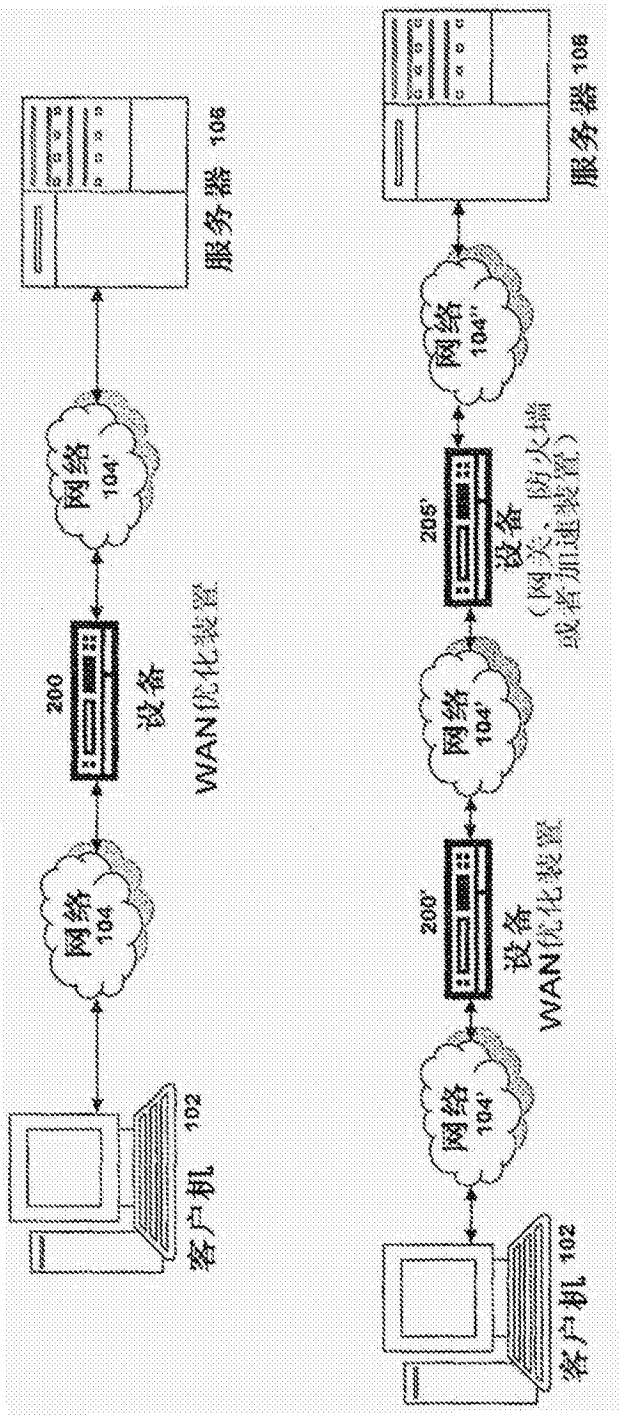

客户机 102
网络 104
200
设备
WAN优化装置
网络 104'
205'
设备
（网关、防火墙
或者加速装置）
网络 104''
服务器 106

图1C

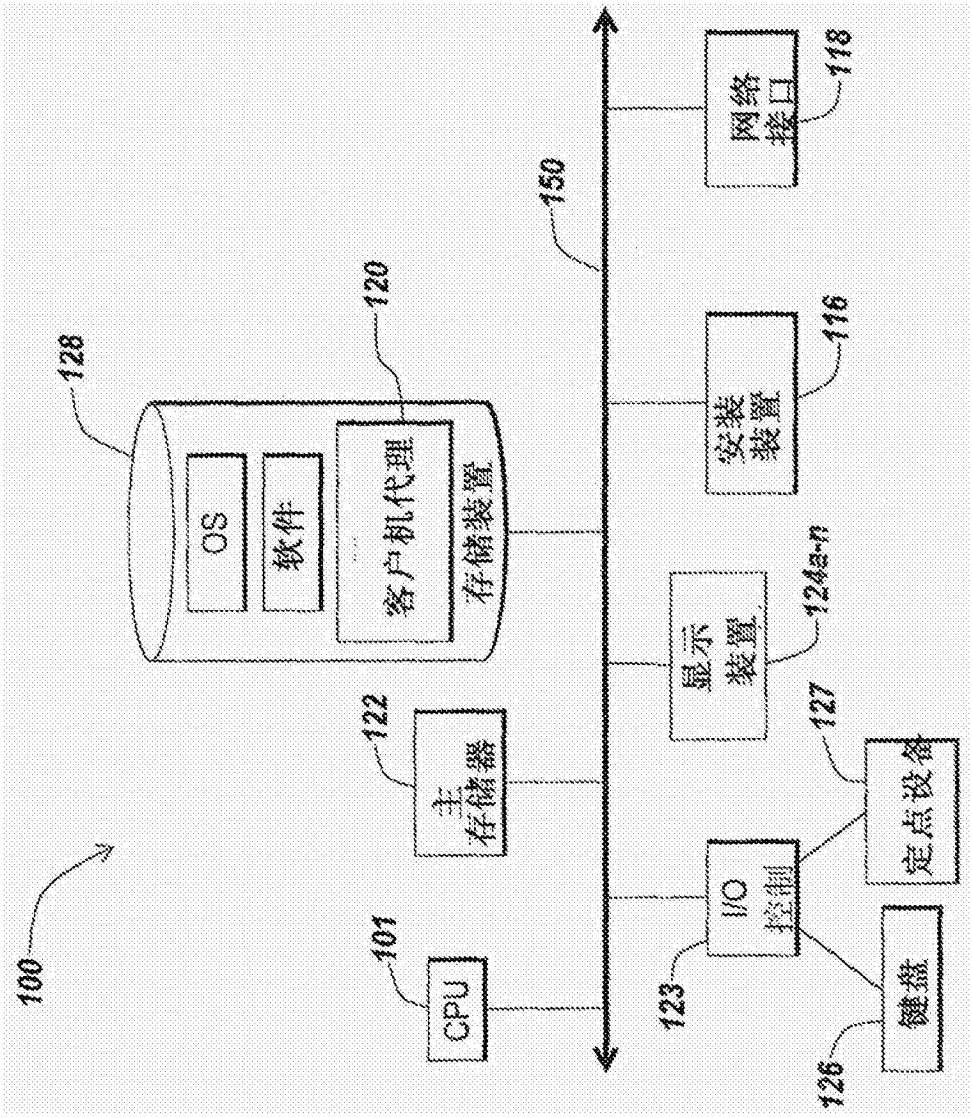

100
101
CPU
122
主存储器
128
OS
软件
客户机代理
存储装置
120
150
网络接口
118
安装装置
116
显示装置
124a-n
I/O 控制
123
127
定点设备
键盘
126

图1D

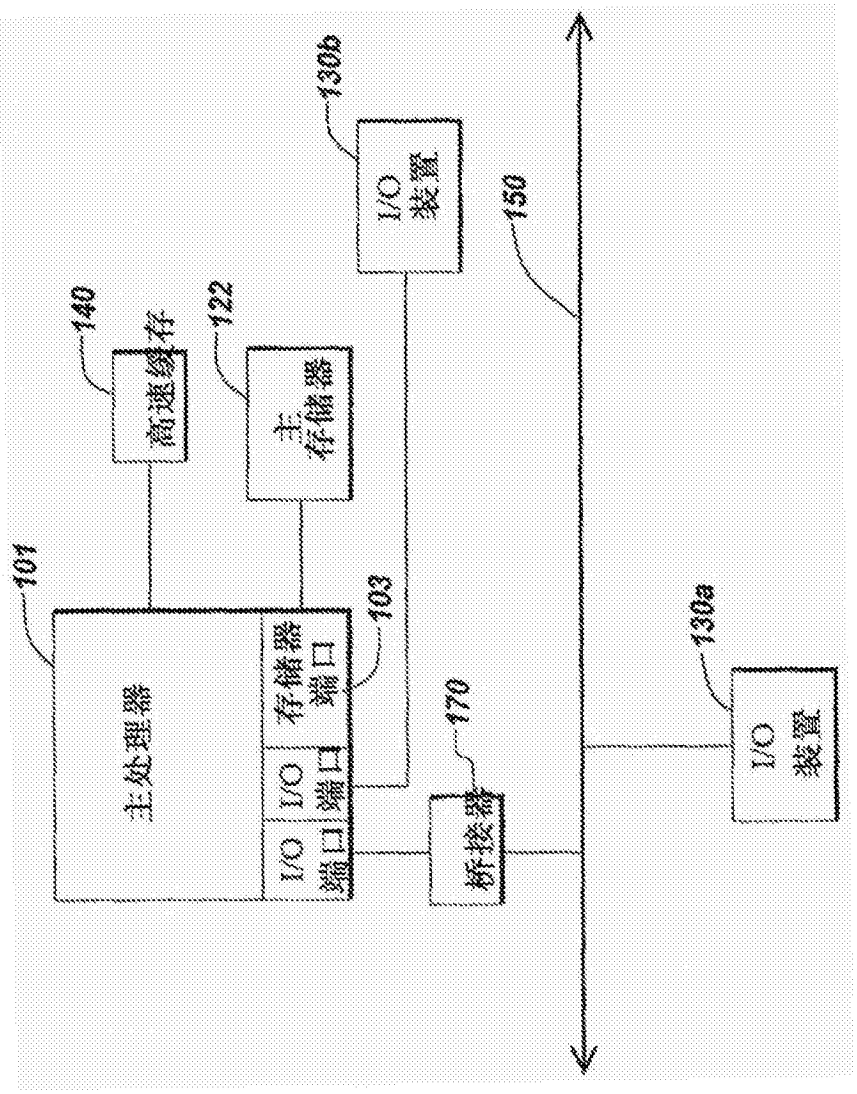

130b
I/O 装置
150
140
高速缓存
122
主存储器
101
103
主处理器
存储器端口
I/O 端口
I/O 端口
170
桥接器
130a
I/O 装置

图1E

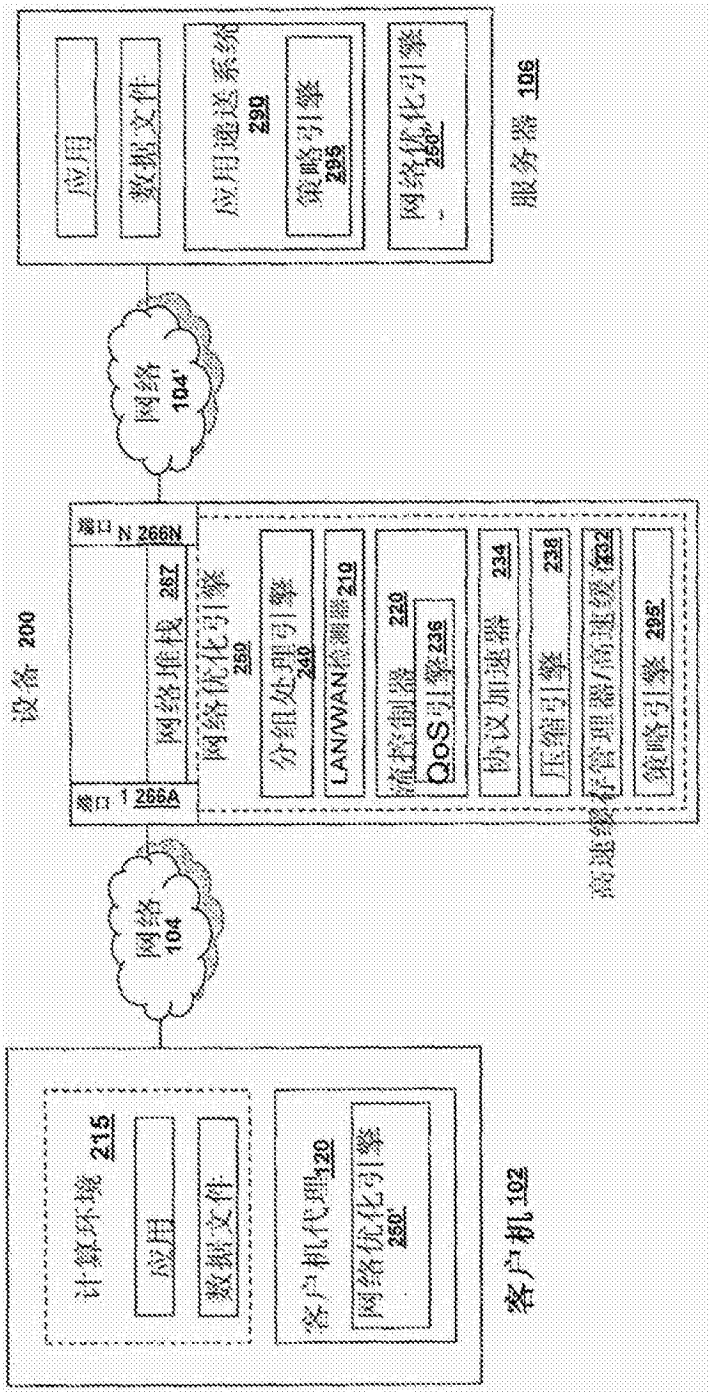

客户机 102
计算环境 215
应用
数据文件
客户机代理 120
网络优化引擎 250'
网络 104
设备 200
端口 1 266A
端口 N 266N
网络堆栈 267
网络优化引擎 250
分组处理引擎 240
LANWAN检测器 219
缓存管理器 220
QoS引擎 236
协议加速器 234
压缩引擎 238
缓存管理器/加速缓存 262
策略引擎 252
高速缓存
网络 104'
服务器 106
应用
数据文件
应用递送系统 290
策略引擎 295
网络优化引擎 250'

图2A

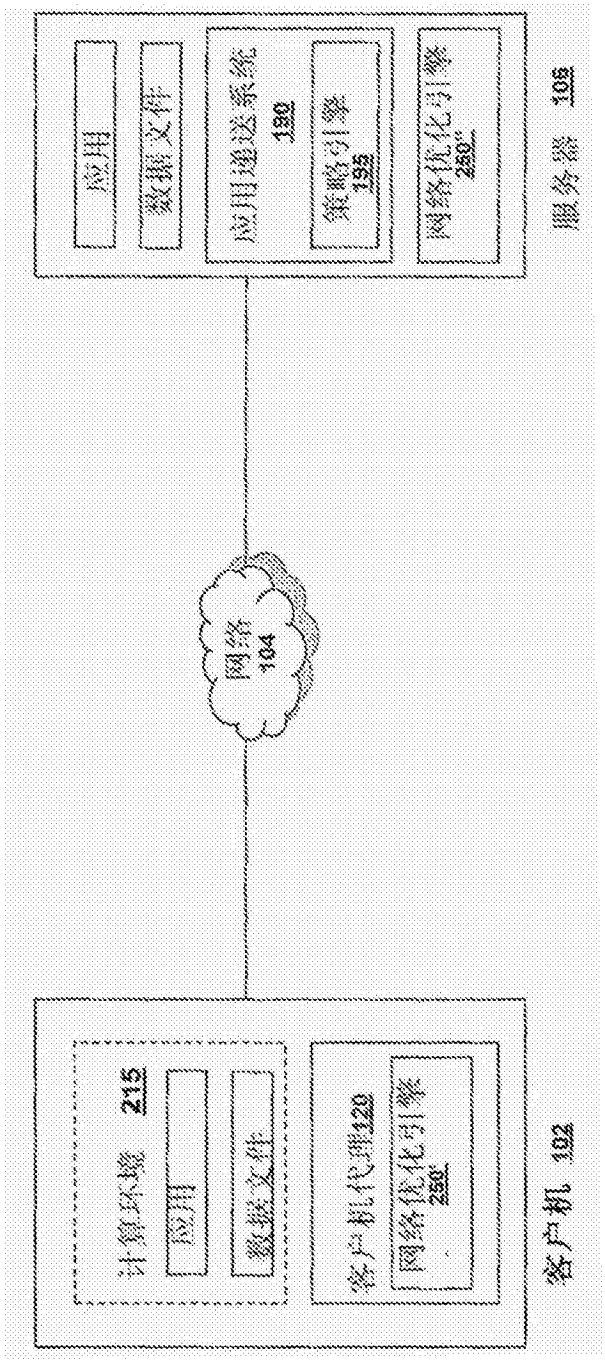

应用
数据文件
应用递送系统
190
策略引擎
195
网络优化引擎
250"
服务器 106
网络
104
计算环境 215
应用
数据文件
客户机代理120
网络优化引擎
250'
客户机 102

图2B

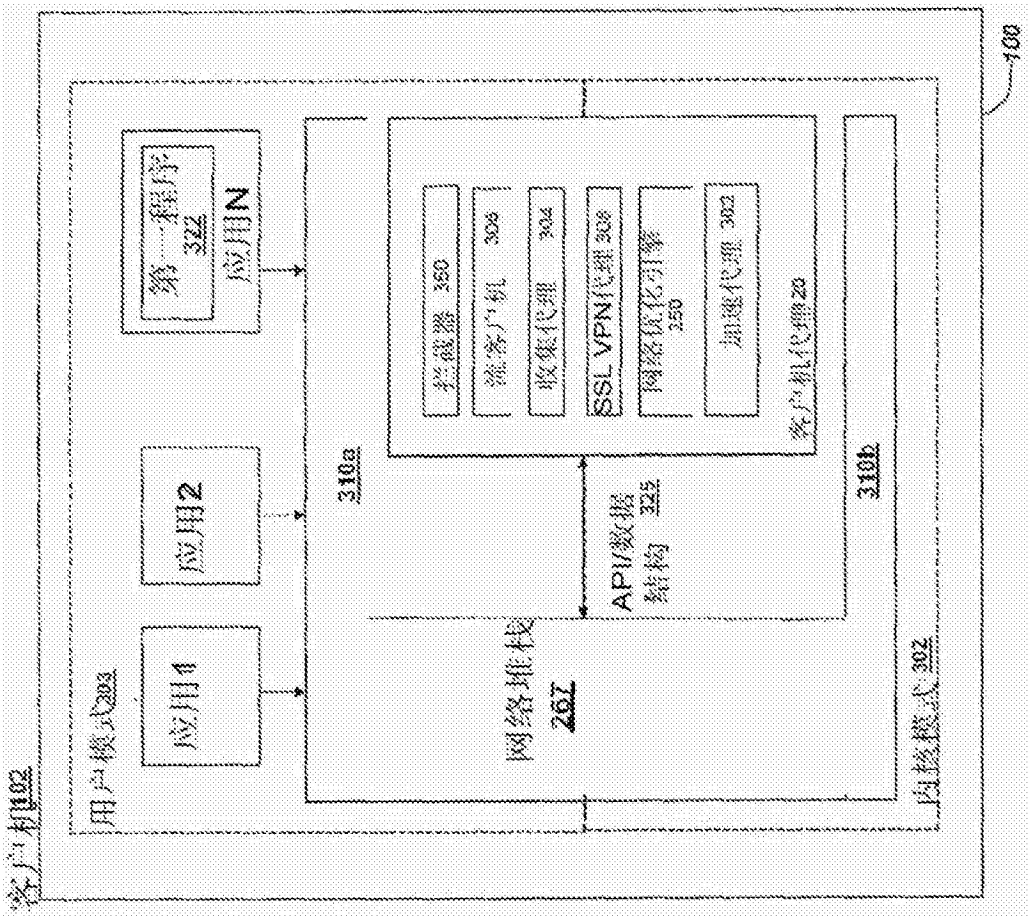

100
客户机102
用户模式203
应用1
应用2
第一程序 322
应用N
网络堆栈 267
310a
API/数据结构 325
310b
内核模式 302
客户机代理 220
拦截器 360
流客户机 306
收集代理 304
SSL VPN代理 308
网络优化引擎 250
加速代理 302

图3

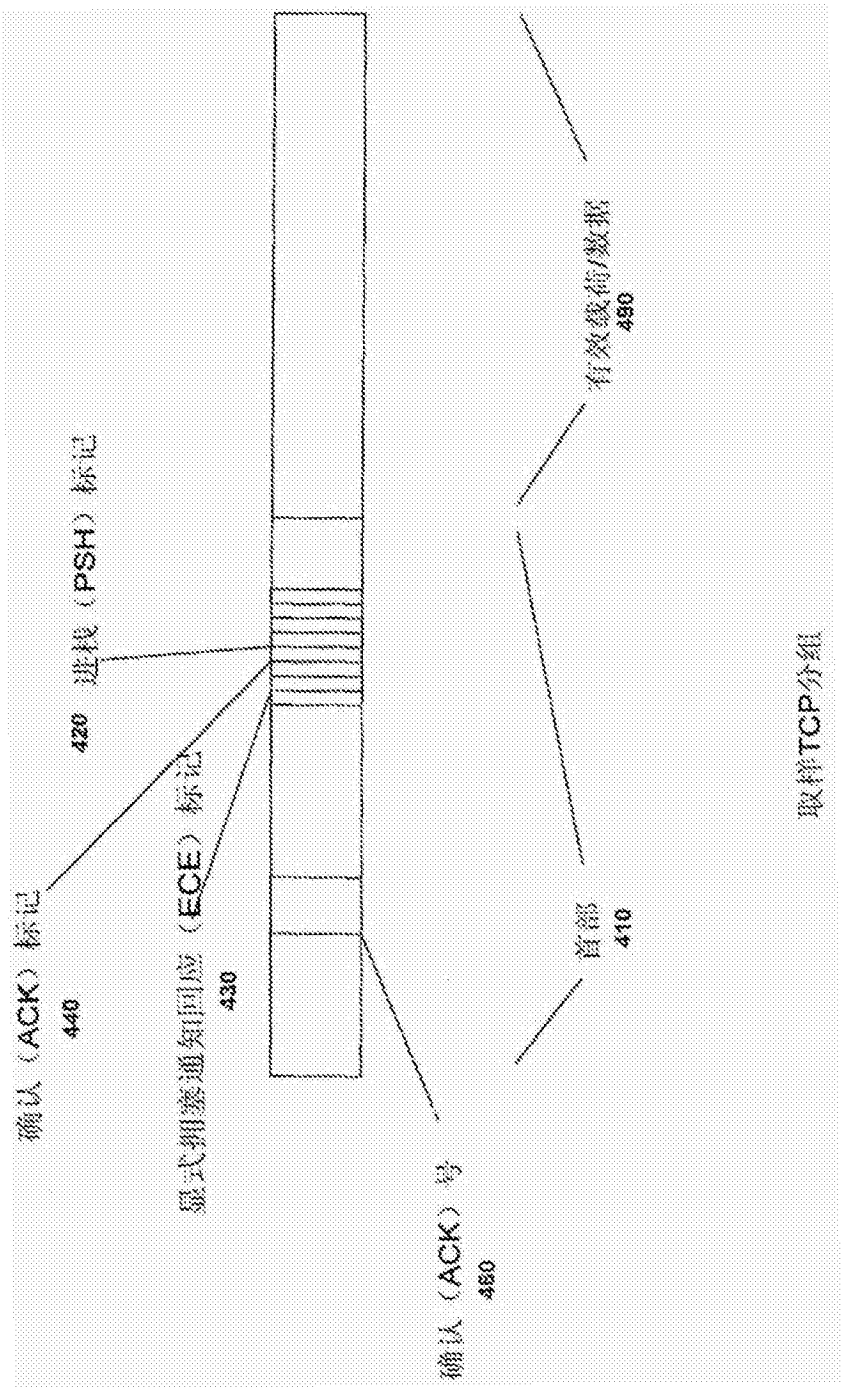

取样TCP分组
首部
410
有效载荷/数据
480
确认（ACK）号
460
显式拥塞通知回应（ECE）标记
430
进栈（PSH）标记
420
确认（ACK）标记
440

图4

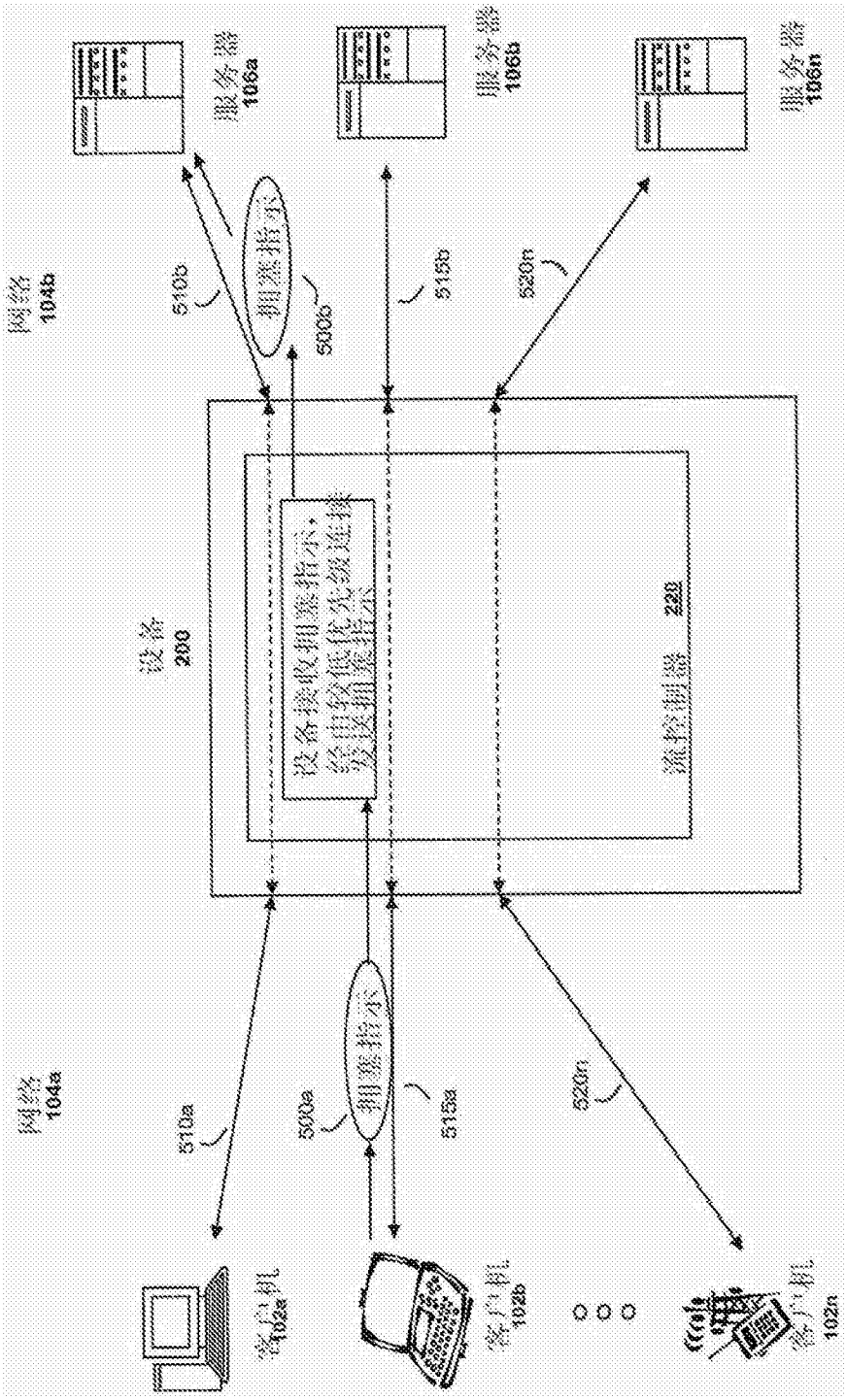

服务器
106a
服务器
106b
服务器
106n
网络
104b
510b
拥塞指示
500b
515b
520n
设备
200
设备接收拥塞指示，
经由较低优先级连接
发送拥塞指示
流控制器
230
网络
104a
510a
500a
拥塞指示
515a
520n
客户机
102a
客户机
102b
客户机
102n

图5

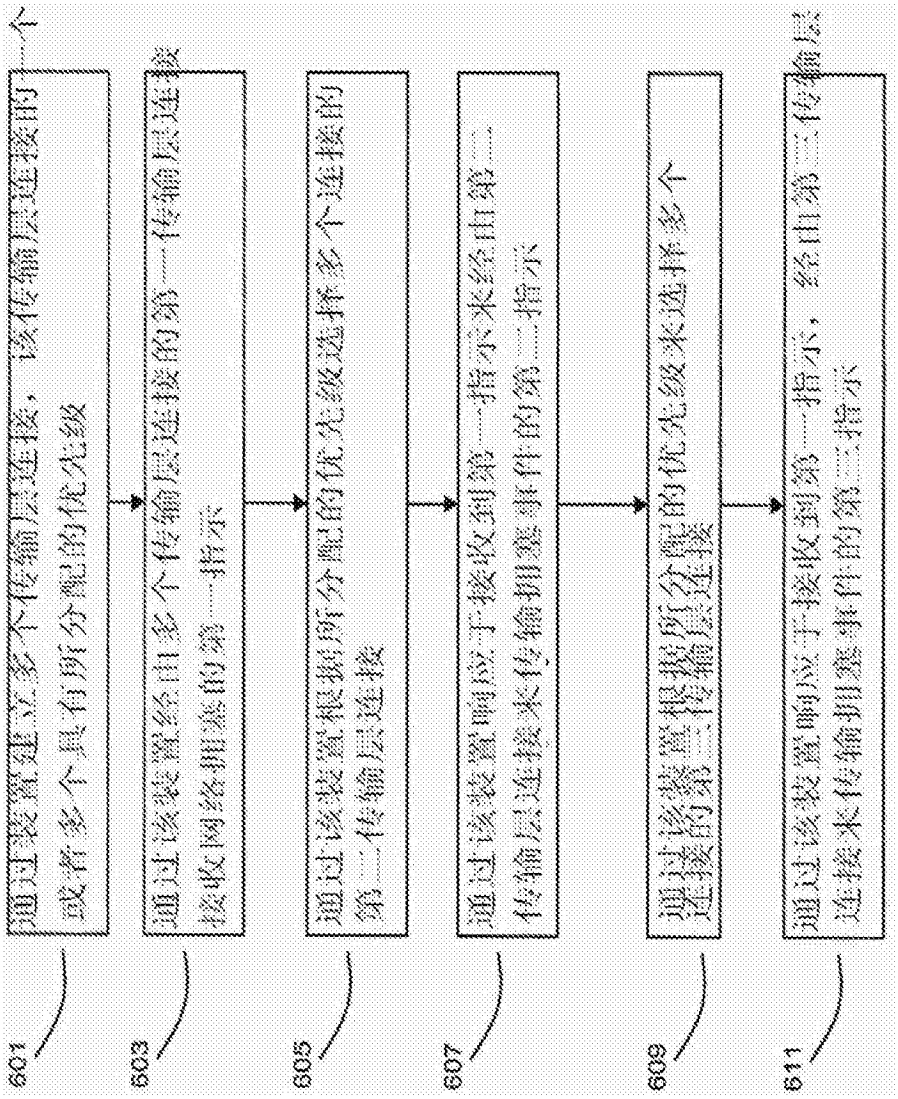

通过装置建立多个传输层连接，该传输层连接的一个或者多个具有所分配的优先级
601
通过该装置经由多个传输层连接的第一传输层连接接收网络拥塞的第一指示
603
通过该装置根据所分配的优先级选择多个连接的第二传输层连接
605
通过该装置响应于接收到第一指示来经由第二传输层连接来传输拥塞事件的第二指示
607
选择的第二传输层连接
609
通过该装置响应于接收到第一指示，经由第三传输层连接来传输拥塞事件的第三指示
611

图6

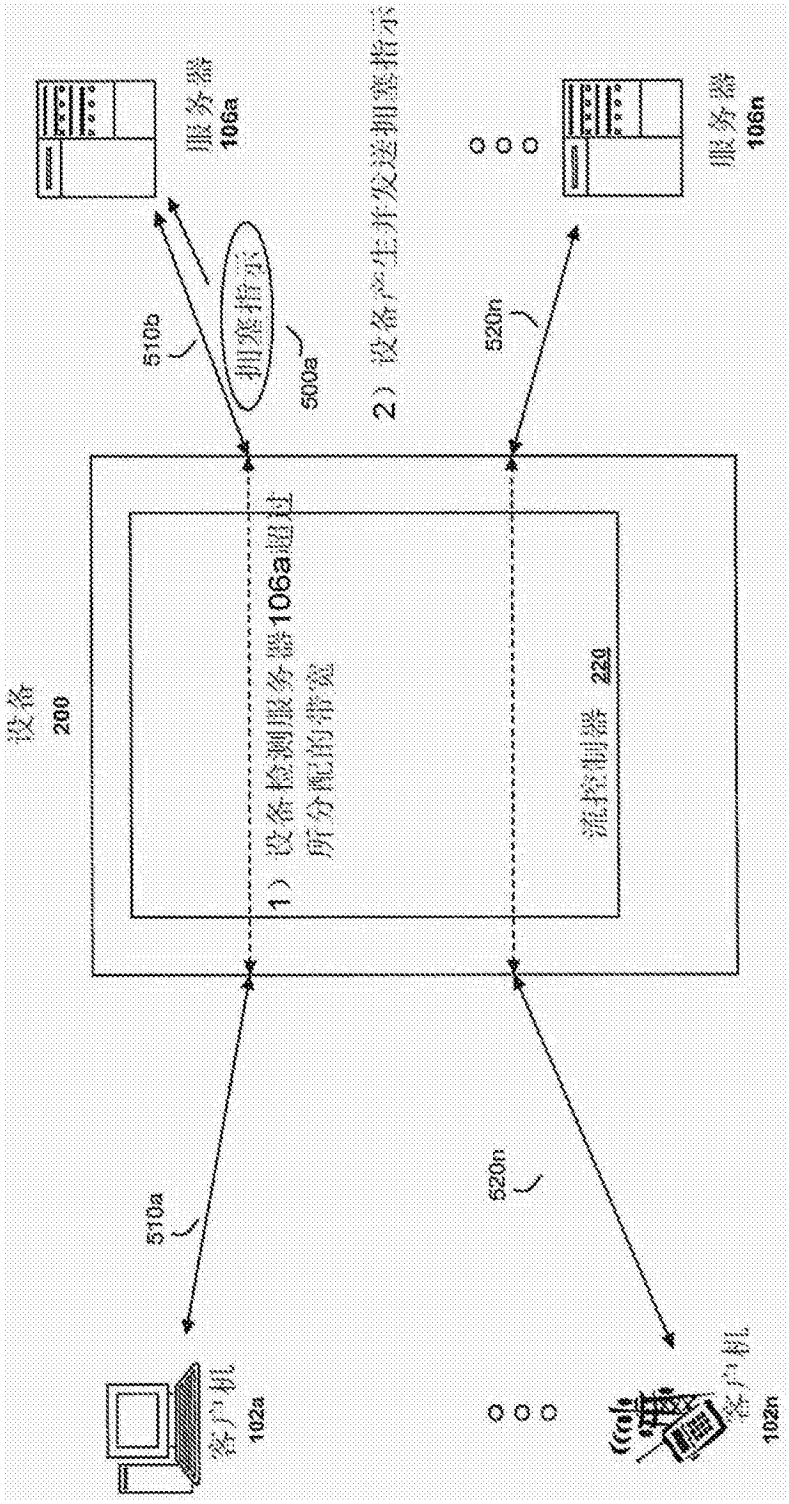

服务器
106a
服务器
106n
拥塞指示
500a
510a
520n
2）设备产生并发送拥塞指示
设备
200
1）设备检测服务器106a超出
所分配的带宽
流控制器 220
510a
520n
客户机
102a
客户机
102n

图7

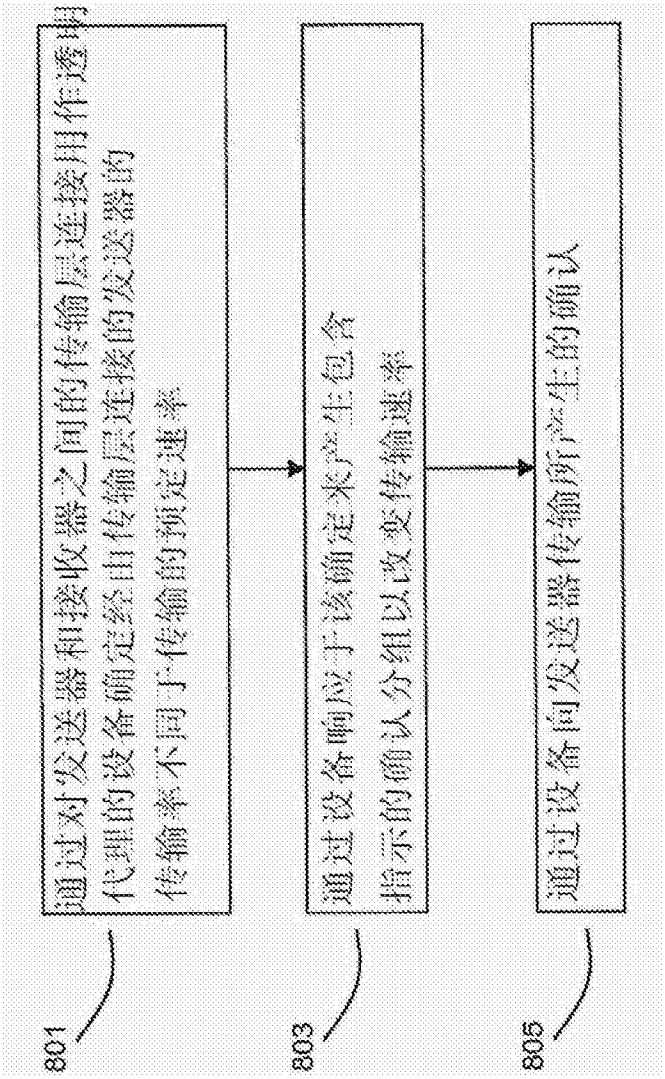

通过对发送器和接收器之间的传输层连接用作透明代理的设备确定经由传输层连接的发送器的传输率不同于传输的预定速率
801
通过设备响应于该确定来产生包含指示的确认分组以改变传输速率
803
通过设备向发送器传输所产生的确认
805

图8

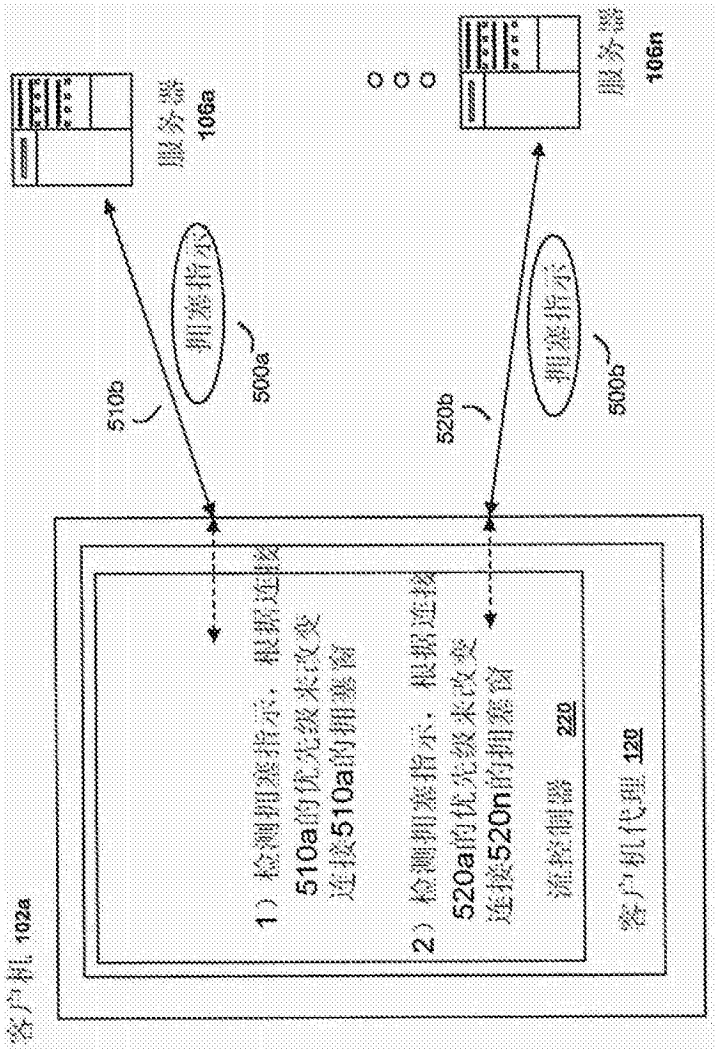

服务器 106a
服务器 106n
拥塞指示 500a
拥塞指示 500b
510a
520b
客户机 102a
1）检测拥塞指示，根据连接510a的优先级来改变连接510a的拥塞窗
2）检测拥塞指示，根据连接520a的优先级来改变连接520n的拥塞窗
流控制器 220
客户机代理 122

图9A

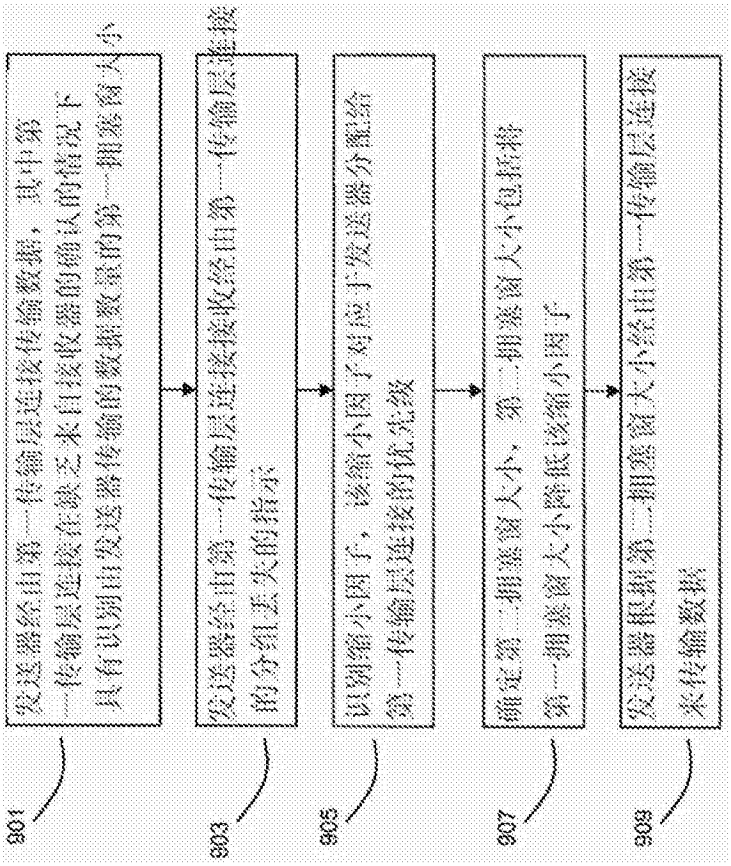

发送器经由第一传输层连接传输数据，其中第一传输层连接在缺乏来自接收器的确认的情况下具有识别由发送器传输的数据数量的第一拥塞窗大小
901
发送器经由第一传输层连接接收经由第一传输层连接的分组丢失的指示
903
识别缩小因子，该缩小因子对应于发送器分配给第一传输层连接的优先级
905
确定第二拥塞窗大小，第二拥塞窗大小包括将第一拥塞窗大小降低该缩小因子
907
发送器根据第二拥塞窗大小经由第一传输层连接来传输数据
909

图9B

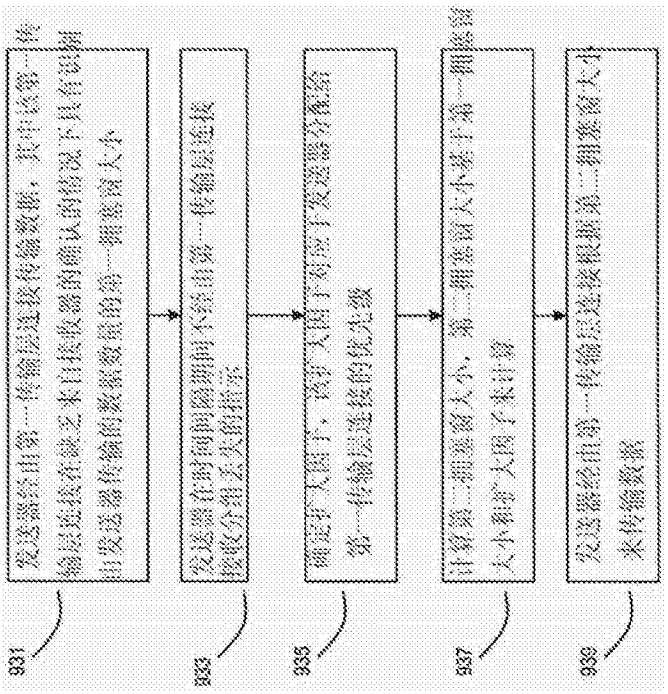

发送器经由第一传输层连接传输数据，其中该第一传输层连接在缺乏来自接收器的确认的情况下具有由发送器传输的数据数量的第一拥塞窗大小
931
发送器在时间周期期间不经由第一传输层连接接收分组丢失的指示
933
确定扩大因子，该扩大因子对应于发送器分配给第一传输层连接的优先级
935
计算第二拥塞窗大小，第二拥塞窗大小基于第一拥塞窗大小和扩大因子来计算
937
发送器经由第一传输层连接根据第二拥塞窗大小来传输数据
939

图9C