

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

H04L 12/26

H04L 12/46 H04L 12/56



[12] 发明专利申请公开说明书

[21] 申请号 02161139.4

[43] 公开日 2003 年 10 月 15 日

[11] 公开号 CN 1449162A

[22] 申请日 2002. 12. 20 [21] 申请号 02161139.4

[30] 优先权

[32] 2001. 12. 20 [33] EP [31] 01403312.0

[71] 申请人 阿尔卡塔尔公司

地址 法国巴黎

[72] 发明人 汉斯·玛利亚·保罗·德奈维

丹尼·乔斯·戈德里斯

[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

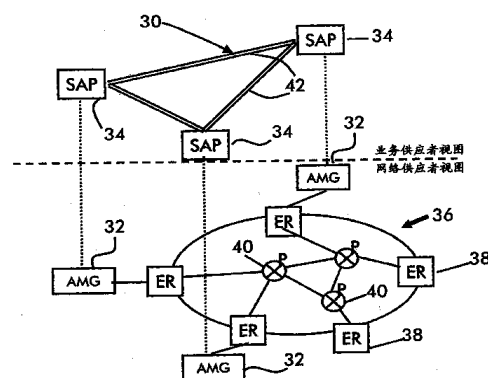
代理人 吴丽丽

权利要求书 6 页 说明书 17 页 附图 8 页

[54] 发明名称 使用虚拟业务网络结构的电信系统

[57] 摘要

一种用于互连终端用户的电信系统，它包括一个或多个互相连接的虚拟业务网络(VSN)，每一个都与数据传送网络相关联。每个虚拟业务网络提供聚集数据流的服务质量(QoS)保证，并包括一个虚拟业务网络控制器(VSNC)，以控制虚拟业务网络的资源并在想要通过上述相关联的数据传送网络传送的每个数据流上执行按用户的许可控制。再者，每个虚拟业务网络有一个在电信系统的终端用户之间提供服务质量保证的可接通性协议。这个可接通性协议包括 VSN 的附着点(TAP)的位置并且对应于数据传送网络的对等点(PP)，一个在虚拟业务网络之间交换路由信息的协议，以及每个 VSN 的至少一个虚拟业务网络控制器(VSNC)的位置，这个虚拟业务网络控制器用于在 VSN 之间交换资源信令消息并对终端用户数据流执行端对端许可控制。



- 1、一种包括数据传送网络和虚拟业务网络（VSN）的电信系统，该虚拟业务网络（VSN）用于跨越数据传送网络为用户数据流提供预定服务质量（QoS）
5 保证，其特征在于，该虚拟业务网络包括一个虚拟业务网络控制器（VSNC），它适应于控制所述虚拟业务网络的资源，并在每个想要通过上述数据传送网络传送的用户数据流上执行按用户的许可控制。
- 2、如权利要求1的电信系统，其特征在于，所述数据传送网络是一个虚拟专用网络（VPN），它适应于为虚拟业务网络提供一个保证的数据传送容量。
- 10 3、如权利要求1的电信系统，其特征在于，所述虚拟业务网络控制器（VSNC）适应于管理（VSN SLA）所述数据传送网络的资源。
- 4、如权利要求1的电信系统，其特征在于，所述用户数据安排在数据分组中。
- 5、一种适应于使终端用户互连的电信系统，它包括多个互连的虚拟业务网络（VSN），每个所述虚拟业务网络都与一个数据传送网络相关联，
15 其特征在于，每个所述虚拟业务网络（VSN）适应于向聚集数据流提供服务质量（QoS）保证，
并且每个所述虚拟业务网络包括一个虚拟业务网络控制器（VSNC），适应于控制所述虚拟业务网络的资源，并在每个想要通过上述数据传送网络传送的数据流上执行按用户的许可控制，以及
20 每个所述虚拟业务网络有在所述电信系统的终端用户间提供服务质量保证的一个可接通性协议。
- 6、一种如权利要求5的电信系统，其特征在于，所述可接通性协议包括：
— 虚拟业务网络的附着点（TAP）的位置，所述附着点对应于数据传送网络的对等点（PP），并且通过所述附着点数据在虚拟业务网络之间进行交换，
25 — 一个在虚拟业务网络之间交换路由信息的协议，以及
— 每个虚拟业务网络的至少一个虚拟业务网络控制器（VSNC）的位置，所述虚拟业务网络控制器适应于在虚拟业务网络之间交换资源信令信息并对终端用户数据流执行端对端许可控制。
- 30 7、如权利要求6的电信系统，其特征在于，所述交换路由信息的协议是基

于因特网协议[IP]寻址进行的。

8、如权利要求5的电信系统，其特征在于，每个虚拟业务网络由业务供应者（SP）所有，所述业务供应者从拥有与所述数据传送网络对应的传送区域的网络供应者（NP）租用传送容量。

5 9、如权利要求8的电信系统，其特征在于，所述电信系统包括一个域间路由装置，它包括存储装置，适应于存储虚拟路由表，以识别彼此间有对等协议的业务供应者，由此，由于所述虚拟路由表，所述终端用户通过这样识别的业务供应者的业务水平规范（SLS）互相连接。

10 10、如权利要求9的电信系统，其特征在于，每个业务供应者具有相关联的虚拟业务网络控制器（VSNC: 88, 92, 96），适应于以按流量为基础，在来自终端用户的到来数据流请求上执行许可控制，并将所述数据流请求转发到与前述业务供应者有对等协议的一个预定的其它业务供应者的虚拟业务网络控制器。

15 11、如权利要求10的电信系统，其特征在于，业务供应者（SP）的虚拟业务网络控制器（VSNC）包括带宽验证装置，适应于沿终端用户之间的业务水平规范（SLA）的端对端链验证可用的带宽。

12、如权利要求9的电信系统，

20 其特征在于，域间路由装置包括一个输入边界路由器（BR）和一个输出边界路由器（BR），其中，网络是一个因特网，业务供应者（SP）是一个应用服务供应者（ASP）。

13、如权利要求10的电信系统，其特征在于，公共地址被用于在定义所述业务水平规范（SLS）的对等虚拟业务网络（VSN）之间进行交换，并用于唯一识别终端用户。

25 14、如权利要求12或13的电信系统，其特征在于，同一公共地址被安装在多个虚拟路由器功能中，以便通过不同的应用服务供应者达到同一用户目的地。

15、一种用在如权利要求14的传送网络中的虚拟路由器，其特征在于，所述虚拟路由器包括存储装置，用于存储有关可接通性业务水平协议的信息，所述信息通过下述内容确定特定的业务供应者能达到哪些用户：

30 一在虚拟业务网络之间的物理对等点，

- 配置网络元件的虚拟业务网络识别标记, 以及
- 虚拟业务网络的虚拟业务网络控制器的 IP 地址。

16、一种提供电信系统的方法, 所述电信系统包括一个虚拟业务网络(VSN), 用于向数据传送网络中的用户数据流分配数据网络资源, 所述虚拟业务网络根据商定的服务质量(QoS)保证来控制通过所述数据传送网络的所述用户数据流, 该方法的特点在于, 所述虚拟业务网络进一步建立用户许可准则(VSN SLA)以便控制在所述数据网络中的数据流许可。

17、一种提供具有多个互连虚拟业务网络(VSN)的电信系统的方法, 每个虚拟业务网络与一个数据传送网络相关联, 并根据商定的服务质量(QoS)保证控制通过其相关联数据传送网络的用户数据流,

该方法的特点在于, 每个所述虚拟业务网络进一步建立用户许可准则(VSN SLA), 以便控制在其相关联的数据传送网络中的数据流许可, 从而获得所述商定的服务质量(QoS)保证,

并且每个所述虚拟业务网络建立终端用户间的可接通性协议, 所述可接通性协议通过所述电信系统提供服务质量保证。

18、根据权利要求17的方法, 其特征在于, 所述可接通性协议包括:

- 虚拟业务网络的附着点(TAP)的位置, 所述附着点与数据传送网络的物理对等点对应,

- 在虚拟业务网络之间交换路由信息的协议, 和

- 用于在虚拟业务网络之间交换资源信令消息和用于对用户数据流实行端对端许可控制的虚拟业务网络控制器(VSNC)的位置。

19、一种在具有虚拟业务网络控制器的虚拟业务网络(VSN)中提供服务质量保证(QoS)的方法, 其特征在于该方法包括下列步骤:

- 存储网络拓扑和/或资源信息;

- 存储用户服务质量信息;

- 监视来自授权用户的业务请求; 以及

- 根据服务质量信息分配资源。

20、一种在具有两个或多个对等虚拟业务网络(VSN)的电信系统中提供服务质量(QoS)有保证的通信的方法, 其特征在于该方法包括:

- 在每个网络中提供用户服务质量保证;

- 在虚拟业务网络之间提供网络业务水平保证;
 - 在每个虚拟业务网络中存储系统拓扑和/或资源和/或可用性信息;
 - 将通过一个发送主机的归属网络从发送主机接收的、寻址到不与归属网络相连的目的地主机的业务请求转发到对等的虚拟业务网络;
 - 5 —在对等虚拟业务网络中确定它们是否与目的地主机连接; 和
 - 在目的地主机与之连接的对等虚拟业务网络中, 发送确认信息以建立具有所需服务质量的连接。
- 21、一种如权利要求 20 的方法, 其特征在于, 该方法包括在虚拟业务网络的入口点上实行业务水平规范的步骤。
- 10 22、一种如权利要求 20 的方法, 其特征在于, 目的地终端与之连接的虚拟业务网络的身份被插入在转发的请求之中, 在归属虚拟业务网络和目的地虚拟业务网络之间的路径中的下一个中继段虚拟业务网络的身份被包含在归属虚拟业务网络和每个介入的下一个中继段虚拟业务网络上的转发请求之中。
- 23、在两个或多个对等域内虚拟业务网络之间配置一个域间虚拟业务网络的方法, 其特征在于,
- 15 —跨越每个域建立域业务水平规范 (VSN SLA);
- 在对等域内虚拟业务网络对之间建立域间业务水平规范;
- 控制每个域中的资源可用性以便在对应网络管理系统的控制下遵守该域业务水平规范;
- 20 —控制对等虚拟业务网络的域之间的资源可用性以便遵守域间业务水平规范。
- 24、如权利要求 23 的方法, 其中域内虚拟业务网络业务量受到对应虚拟业务网络控制器的控制, 该方法的特点是, 路由信息被存储在虚拟路由环境之中, 并且路由信息从虚拟路由环境被传递到虚拟业务网络控制器。
- 25 25、如权利要求 24 的方法, 其特征在于, 所述路由信息通过带外信令被传递。
- 26、如权利要求 25 的方法, 其特征在于上述路由信息通过使用边界网关协议或替换的路由协议会话被发送。
- 30 27、如权利要求 24 的方法, 其特征在于, 所述路由信息包括数据流的入口/出口信息。

28、如权利要求 24 的方法，其特征在于，域间业务水平规范使对等虚拟业务网络的请求进行分级。

29、一种跨越包括两个或多个对等虚拟业务网络的域间虚拟业务网络发送数据流的方法，

5 其特征在在于，虚拟路由（VR）环境与每个虚拟业务网络的域的边缘路由器（ER）和边界路由器（BR）相关联地被安装，以保证在对应虚拟业务网络中的内部数据流被包含在分配给该虚拟业务网络的资源之中，

该内部数据流流向从数据流目的地地址和虚拟路由环境确定的适当边缘路由器或边界路由器，

10 并且流向被传送到或通过另一个虚拟业务网络的边界路由器的数据流在该另一个虚拟业务网络中受到另一个虚拟路由环境的控制，所述另一个虚拟路由环境与所述另一个虚拟业务网络的域的边缘路由器或边界路由器相关联地被安装。

30、一种在包括多个对等虚拟业务网络的电信系统中在业务供应者（SP）和

15 和用户之间建立数据流的方法，该方法的特点在于：

— 用户发送一个请求到应用控制服务器（MMCS），以获得一个请求的业务，

— 在虚拟业务网络环境中业务供应者将一个唯一的 IP 地址分配到用户，

— 用户和业务供应者通过应用控制服务器协商请求的服务质量（QoS），

20 — 应用控制服务器通过中间虚拟业务网络控制器对目的地应用控制服务器启动呼叫资源信令，以及

— 每个虚拟业务网络控制器检查资源并将请求转发到下一个中继段虚拟业务网络控制器。

31、一种如权利要求 30 的方法，其中从请求方的详情识别入口，并使用将目的地 IP 地址映射到下一个中继段虚拟业务网络的路由表从下一个中继段和

25 对等点确定出口。

32、一种提供预定服务质量（QoS）给用户的虚拟业务网络（VSN），该虚拟业务网络是一个数据网（36）上的一个虚拟覆盖（30），该虚拟业务网络包括两个或多个互相连接的接入点（ER），通过所述接入点用户和/或其它主机被连到网络上，

30 其特征在在于，所述虚拟业务网络包括存储器装置，用于存储虚拟路由表和

识别每个用户的 QoS 保证的信息, 并且包括一个虚拟业务网络控制器(VSNC), 适应于根据对应的服务质量(QoS)保证基于每个数据流分配网络资源。

5 33、一种如权利要求 32 的虚拟业务网络, 其中数据网络支持一个或多个业务网络, 其特征在于, 对于至少一个虚拟业务网络(VSN), 数据网络包括置于至少一对边缘路由器(ER: 38)之间的一个或多个核心路由器(P: 40), 其中上述虚拟业务网络的核心路由器和边缘路由器保持上述虚拟业务网络的一个虚拟路由环境。

10 34、一种如权利要求 32 的虚拟业务网络, 其特征在于, 虚拟业务网络控制器(VSNC)对于每个请求通过虚拟业务网络(VSN)传送的数据流执行按数据流的许可控制。

35、一种适应于按预定服务质量(QoS)保证控制虚拟业务网络(VSN)中的数据流的虚拟业务网络控制器(VSNC),

15 其特征在于所述控制器包括存储器装置, 该装置包括一个第一存储区, 用于存储识别网络可用性的信息, 和一个第二存储区, 用于存储识别预定服务质量保证的信息,

并且所述控制器进一步适应于根据服务质量信息基于每个数据流控制网络资源的分配。

20 36、一个分组网络, 包括两个或多个虚拟业务网络, 其特征在于, 对于每个虚拟业务网络, 与该虚拟业务网络相关联的边缘路由器和桥接路由器包括对该虚拟业务网络唯一的虚拟路由环境, 并且每个所述虚拟路由环境包含对其虚拟业务网络唯一的路由信息。

要么要求跨越全球的所有“业务接入点”之间的端对端管道，要么要求多路分用在（千兆节）边界网路（Border Routers）上的 Int Serv 流。在这两种情况下，可缩放性问题妨碍问题的解决。

发明内容

5 本发明提供了解决问题的办法，它适应于单域和多域等级，并且可缩放为进行全局操作。这个想法创造了一个类似于虚拟专用网络（Virtual Private Networks (VPN)）的系统[RFC 2547: E. Rosen, Y. Rekhter “BGP/MPLS VPNs”，1999年3月]，它传送公共业务，例如声音和视频，要求严格的服务质量保证。这个系统叫作虚拟业务网络（Virtual Service Network）或 VSN。VSN 所有者
10 从网络供应者（NP）那里租用传送容量并自己使用这些资源对终端用户提供公共业务。基本上，VSN 是在 VPN 的端点和按终端用户（per-end-user）流量许可控制之间的具有 QoS 保证的 VPN。

VSN 一般具有局部覆盖，例如单网络传送域或单一自给系统。因此在 VSN 中的聚集分组流或通信包络（例如“管道”）的 QoS 可以根据 Diff Serv 技术获
15 得。不过，Diff Serv 不足以向在 VSN 的通信包络中的单一应用或流量提供 QoS。因此，每个 VSN 受到所谓 VSN 控制器（VSN C）的许可控制服务器的控制，该控制器控制 VSN 资源，对于每个想通过 VSN 的流量执行按流量（per-flow）许可控制。

由于 VSN 只具有局部覆盖，它们需要和其它 VSN 对等（peering）以具有全
20 球范围的公共终端用户业务。与终端用户之间的这种对等或可接通性协议主要包含三种类型的信息：

第一：VSN 的附着点的位置，称为转接接入点（Transit Access Point (TAP)）或对应物理对等点（PP）。通过这个点分组可以在 VSN 之间交换；

第二：在 VSN 之间交换路由信息的协议。每个 VSN 具有自己的路由，即按
25 照 IP 地址的终端用户可接通性。对等 VSN 交换这个信息，从而获得大的地理覆盖以及；

第三：VSN 控制器的位置，使得资源信令消息可以在 VSN 之间进行交换，使得能够对于用户流进行端对端的许可控制。

主要操作如下：

30 端对端流通过一些 VSN 需要所有对应的 VSN 控制器的容许。按流量

使用虚拟业务网络结构的电信系统

5 技术领域

本发明涉及一个使用虚拟业务网络结构的电信系统，用于提供实时的多媒体和要求服务质量(QoS)的其它终端用户业务。这种业务通常跨多个网络提供者域、基于因特网协议(IP)服务质量在分组化的网络上提供。

背景技术

- 10 面对下一代网络的域间 IP QoS 的供给的主要问题之一是，这些业务要求沿整个数据通道的延迟，跳动，分组损失和可利用资源有严格的保证。多种解决办法被提出了。它们包括：集中业务 IP QoS 技术(Int Serv)[RFC 1633: R. Braden, D. Clark and S. Shenker, "Integrated Services in the Internet Architecture: an Over view", 1994 年, 6 月; 这里提到的所有 RFC (Requests
- 15 For Comments), 是来自因特网工程特别工作组(IETF)标准化体系的标准, 其中更多的细节可以在因特网网址上找到(<http://www.ietf.org/>), 区分业务 IP QoS 技术(DiffServ)[RFC 2475: S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang and W. Weiss, "An Architecture For Differentiated Services", 1998 年 12 月], 和 Int Serv 与 Diff Serv 的结合[RFC 2998: Y. Bernet, P.
- 20 Ford, R. Yavatkar. F. Baker, L. Zhang, M. Speer, R. Braden, B. Bavier, J. Wroclawski, E. Felstaine. "A Frameuork for Integrated Services Operation over Diff Serv Networks" 2000 年, 11 月] IP QoS 技术。Int Serv 根据按照资源预留协议(RSVP)的资源预留(在每个中继段中, 按多媒体应用, 沿数据通道的信令)。这种解决办法对于核心路由器是不能缩放的, 结果这种技
- 25 术未能得到发展。

- Diff Serv 在单域中提供边对边(edge-to-edge)的保证(即, 每个 DiffServ 代码点), 以便用于分组流的聚集。在多域应用中它没有提供解决办法, 同时也不清楚如何将其用于提供因特网协议服务质量给个人多媒体业务。Int Serv 和 DiffServ 结合方法涉及将 Int Serv(微型)流多路传输到 Diff Serv(预先构
- 30 成的, 单域)边对边管道。这个概念不能延伸到域间应用(例如, 因特网)。这

(per-flow)的资源请求可通过多种方法被传递到第一 VSN 的 VSN 控制器。如果第一 VSN 具有足够资源容纳这个流量,第一 VSN 控制器将通过专用资源信令协议发送按流量的资源请求到下一个 VSN 的 VSN 控制器。用这种方式,按流量的资源请求通过映射到流量中的分组将通过的 VSN 序列上的 VSN 控制器序列,并且每个 VSN 控制器检查在它的 VSN 中是否有足够的资源。用这种方式,终端用户应用的端对端 QoS 可以以可缩放的方式被获得。VSN 控制器可以以集中的方式(例如,每 VSN 一个 VSNC)或分散的方式(例如,每个 VSN 的业务接入点一个 VSNC)实现。VSNC 到 VSNC 资源信令协议可以是带外的(例如,对于集中 VSNC)或分散的(例如,对于分散 VSNC);或者是两者的结合(对于网络的特定部分是带内的,而对于网络的其它部分是带外的)。

因此,本发明的第一实施例是一种方法,它提供一个包括虚拟业务网络的电信系统,用于分配数据网络资源到数据传送网络中的用户数据流,该虚拟业务网络根据商定的服务质量保证控制通过上述数据传送网络的用户数据流。

这个方法的特点在于,所述虚拟业务网络进一步建立用户许可准则,以便控制上述数据网络中的许可数据流。

这个方法可以作为在物理传送层和终端用户数据流之间的虚拟层而被实现。

根据本发明的进一步的实施例,本发明公开一种提供具有多个互连虚拟业务网络(VSN)的电信系统的方法,每个虚拟业务网络与数据传送网络相关联,并根据商定的服务质量(QoS)保证控制通其相关联数据传送网络的用户数据流。

该方法的特点在于,每个所述虚拟业务网络进一步建立用户许可准则(VSN SLA),以便控制在其相关联的数据传送网络中的数据流许可,从而获得所述商定的服务质量(QoS)保证,并且每个所述虚拟业务网络建立终端用户间的可接通性协议,所述可接通性协议通过所述电信系统提供服务质量保证。

本发明的另一个实施例提供了一种包括数据传送网络和虚拟业务网络(VSN)的电信系统,该虚拟业务网络(VSN)用于跨越数据传送网络为用户数据流提供预定服务质量(QoS)保证。

根据本发明,该电信系统的特征在于,该虚拟业务网络包括一个虚拟业务网络控制器(VSNC),它适应于控制所述虚拟业务网络的资源,并在每个想要通过上述数据传送网络传送的用户数据流上执行按用户的许可控制。

本发明的进一步的实施例提供了一种适应于使终端用户互连的电信系统，它包括多个互连的虚拟业务网络（VSN），每个所述虚拟业务网络都与一个数据传送网络相关联，

5 根据本发明，该电信系统的特征在于，每个所述虚拟业务网络（VSN）适应于向聚集数据流提供服务质量（QoS）保证，并且每个所述虚拟业务网络包括一个虚拟业务网络控制器（VSNC），适应于控制所述虚拟业务网络的资源，并在每个想要通过上述数据传送网络传送的数据流上执行按用户的许可控制，以及每个所述虚拟业务网络有在所述电信系统的终端用户间提供服务质量保证的一个可接通性协议。

10 特别是，可接通性协议最好包括：

— 虚拟业务网络的附着点（TAP）的位置，所述附着点对应于数据传送网络的对等点（PP），并且通过所述附着点数据在虚拟业务网络之间进行交换，

— 一个在虚拟业务网络之间交换路由信息的协议，以及

15 — 每个虚拟业务网络的至少一个虚拟业务网络控制器（VSNC）的位置，所述虚拟业务网络控制器适应于在虚拟业务网络之间交换资源信令信息并对终端用户数据流执行端对端许可控制。

本发明的另一实施例是一种在具有两个或多个对等虚拟业务网络（VSN）的电信系统中提供服务质量（QoS）有保证的通信的方法。

该方法的特征在于包括：

20 — 在每个网络中提供用户服务质量保证；

— 在虚拟业务网络之间提供网络业务水平保证；

— 在每个虚拟业务网络中存储系统拓扑和/或资源和/或可用性信息；

— 将通过一个发送主机的归属网络从发送主机接收的、寻址到不与归属网络相连的目的地主机的业务请求转发到对等的虚拟业务网络；

25 — 在对等虚拟业务网络中确定它们是否与目的地主机连接；和

— 在目的地主机与之连接的对等虚拟业务网络中，发送确认信息以建立具有所需服务质量的连接。

本发明的另一实施例是在两个或多个对等域内虚拟业务网络之间配置一个域间虚拟业务网络的方法。

30 该方法的特征在于：

- 跨越每个域建立域业务水平规范 (VSN SLA);
 - 在对等域内虚拟业务网络对之间建立域间业务水平规范;
 - 控制每个域中的资源可用性以便在对应网络管理系统的控制下遵守该域业务水平规范;
- 5 — 控制对等虚拟业务网络的域之间的资源可用性以便遵守域间业务水平规范。

本发明的另一个实施例提供了一个用在传输网络中的虚拟路由器, 它包括存储装置, 用于存储有关可接通性业务水平协议的信息, 所述信息通过下述内容确定特定的业务供应者能达到哪些用户:

- 10 — 在虚拟业务网络之间的物理对等点,
- 配置网络元件的虚拟业务网络识别标记, 以及
 - 虚拟业务网络的虚拟业务网络控制器的 IP 地址。

进一步的实施例是提供了一种在包括多个对等虚拟业务网络的电信系统中在业务供应者 (SP) 和用户之间建立数据流的方法。

15 该方法的特点在于:

- 用户发送一个请求到应用控制服务器 (MMCS), 以获得一个请求的业务,
 - 在虚拟业务网络环境中业务供应者将一个唯一的 IP 地址分配到用户,
 - 用户和业务供应者通过应用控制服务器协商请求的服务质量 (QoS),
 - 应用控制服务器通过中间虚拟业务网络控制器对目的地应用控制服务器
- 20 启动呼叫资源信令, 以及
- 每个虚拟业务网络控制器检查资源并将请求转发到下一个中继段虚拟业务网络控制器。

附图说明

- 图 1 是目前的 QoS 问题的高层视图;
- 25 图 2 是解释包括在虚拟业务网络结构中的任务和协议的原理图;
- 图 3 是单域虚拟业务网络结构图;
- 图 4 是单域虚拟业务网络的逻辑互连或对等; 物理实现在图 6 中解释;
- 图 5 是 VSN 参考结构和 VSN 控制器; 实现这个结构要求本发明的三个新的思想; 在下面图中进行解释;
- 30 图 6 解释在对等 VSN 之间的 SLS 的缝合;

图 7 是根据契约信息的, 跨越网络边界的 VSN 的虚拟路由器中的选择路由设施,

图 8 是 VSNC (在控制平面中) 和虚拟路由器 (在数据平面中) 之间的路由信息对准。

5 具体实施方式

问题的陈述

图 1 是要解决的问题的高层视图, 即在终端用户 10 和 12 之间提供端对端的 QoS。终端用户也可能是一个物理设备, 例如是一个视频点播服务器。端对端通路包括接入部分 14 和核心部分 16。接入媒体网关 (AMG) 18.1 和 18.2 被安
10 排在网络的边缘。AMG 是在网络边缘上的终端用户业务量的任何聚集器 (aggregator) 的通用术语, 例如, 宽带接入服务器 (非对称数字用户线路接入), GGSN (通用移动通信系统接入), 一个网关, 等等。终端用户可以用几种方式启动它的业务, 例如声音或视频。图 1 是通过应用信令协议 (例如: 会话启动协议或 H.323) 来启动业务, 其中用户发送信令信息到业务供应者的应用控制实
15 体, 称为一个 MMCS (多媒体呼叫服务器) 20.1 和 20.2, 例如经过呼叫信令 19 互连的一个守门装置或是一个 SIP 代理业务系统。其它启动业务的装置也是可以的, 例如, 接入业务供应者的门户网站。在任何情况下, 应用控制实体, 例如 MMCS, 决定用户对业务的接入, 并因此, MMCS 20.1 和 20.2 也控制 AMG, 如在 21 处所示。后一设备注意按流量的业务量调节并产生统计量, 它被用于计帐
20 和计费的目的。MMCS 处理用户业务请求并通过配置 AMG 以允许某种流量通过而控制网络的接入。

在接入网络 14, 即从终端用户到 AMG, 提供 QoS, 对于大多数今天的接入技术而言是已经解决的问题, 例如 ATM (异步传输模式), xDSL 接入或无线 UMTS (通用移动通信系统) 接入。因此, 提供端对端的 QoS 到终端用户应用相当于,
25 在任何两个存取集中器, 即 AMG 之间提供 QoS, 所述 AMG 能够通过因特网 (IP) 或任何大的传送网络组, 例如, 经过边缘路由器 (ER) 22.1 和 22.2 而互连接。

关于所涉及的任务和协议的专门术语

图 2 在概念上表示, 包括在终端用户业务提供中的不同的任务和协议。基
30 本的思想是建立虚拟专用网 (VPN), 它传送公共业务, 例如声音和视频, 并要求

严格的服务质量 (QoS) 保证。这样一个 VPN, 称为一个虚拟业务网络 (VSN)。
VSN 的所有者, 叫做业务供应者 (SP), 它从一个叫做网络供应者 (NP) 的, 传
送基础结构的所有者那里租用容量。所租用的容量通过 SP 和 NP 之间的合同协
议描述, 叫作 VSN 业务水平协议 (VSN SLA)。业务供应者使用这些 (租用的)
5 资源提供公共业务给终端用户。虽然图 2 给出了网络供应者 (Network Provider)
和业务供应者 (Service Provider) 之间的 1 对 1 关系, 实际上, 任一对任一
的关系是可能的。网络供应者可以提供租用的传送容量给任何数量的业务供应
者。业务供应者可以有带有多于一个的网络供应者的 VSN SLA, 以便获得更大
的用户群覆盖。如果多个网络供应者需要和远处终端用户连通, 则它们必须有
10 连通性协议, 以便交换“分组”, 因为这些今天就存在于因特网中 (并非新事物)。
如果需要多个业务供应者以与远地终端用户连通, 则这些业务供应者应该具有
可接通性协议, 例如今天各国的话音操作人员所拥有的。

单域虚拟业务网络

图 3 是虚拟业务网络 (VSN) 30, 它覆盖一个单一传送域。VSN 是在对应于
15 一个在 VSN 中的业务接入点 (SAP) 34 的接入媒体网关 (AMG) 32 之间的一个虚
拟覆盖网络。它被业务供应者拥有, 业务供应者使用 VSN 作为基础结构以提供
终端用户业务。VSN 对集中在 AMG 之一上的所有终端用户提供业务。VSN SLA
主要描述 VSN 拓扑 (SAP 的数目, 在 SAP 之间的连通性, 例如, 全网连通性)
和在每组可达到的 SAP 之间的 QoS 特性 (通过量, 最大延迟, 等等)。

20 图 3 的下部是传送网络 36, 它包括边缘路由器 38, 通过它, 接入媒体网关
(AMG) 与网络 and 核心路由器 40 相连, 核心路由器 40 与边缘路由器互相连接。在
边缘路由器 (ER) 38 和核心路由器 (P) 40 中, 服务质量通过使用结合 DiffServ
代码点 (DSCP) 的 Diff Serv 技术而被提供。

25 图 3 的上部是虚拟业务网络, 用 QoS 管道使接入媒体网关 32 或 SAP 34 互
相连接。Diff Serv 为分组聚集提供了良好的 QoS 保证, 例如, 在每对 AMG 之
间的最大延迟或分组损失, 因此在 AMG 32 之间提供了 QoS 管道 42。在 Diff Serv
术语中, 这些 QoS 管道 42 对应于业务水平规范 (SLS)。

30 QoS 管道 42 不必在所有 AMG 32 之间形成一个全网 (full mesh)。这意味
着, 在加到同一虚拟业务网络上的两个 AMG 之间的通信, 可能通过多于一个的
QoS 管道 (图中未示出)。因此, 为了获得在每对 SAP 之间的 QoS 保证, 重要的

是，来自 VSN 的分组是沿着它们的 VSN 的 QoS 管道 (SLS) 进行路由选择的。这要求在每个 VSN 的环境中独立进行路由决定和在边缘路由器及核心路由器中的分组转发。这保证属于特定 VSN 的分组沿着为该 VSN 配置的 QoS 管道进行路由选择，使得不同的 VSN 的分组或“最大努力 (best-effort)” [BE] 分组遵循不同的路由。这意味着，边缘路由器和核心路由器保持每个 VSN 的虚拟路由环境，并且在这个虚拟路由环境内做出路由决定。如果边缘路由器通过不能支持虚拟路由环境的核心路由器互连，在这些核心路由器中的路由决定必须通过打开边缘路由器之间分组的通道而被旁路 (例如使用多协议标记交换 MPLS)。用这种方法，AMG 通过具有 VPN 端点之间的 QoS 管道的 IP VPN 互连。有一些实现 IP VPN 的技术。象已知的 BGP/MPLS (虚拟路由器) [例如 RFC 2547] 的技术用于目前情况是理想的，但是其它 VPN 技术也能很好应用。在一个 VSN 中的路由和 IP 可接通性交换类似于在 VPN 中的情况。接入媒体网关使它们的子网络地址经过路由协议 (例如 Open Shortest Path First 或 BGP [边界网关协议]) 或经过载波静态配置传递到边缘路由器。VPN 路由协议将保证这些地址被传递到属于同一 VSN 的远程边缘路由器和附带的 AMG。

虚拟业务网络的对等

图 4 是两个虚拟业务网络 44 和 46 对等或相互连接。它允许针对所提供的 (终端用户) 业务有大的地区覆盖和有关用户群。目的是，获得全球覆盖，要求在 AMG 之间的任一对任一 QoS 连通性。这是通过 VSN 的互相连接获得的。实际上，一个单一 VSN 仅具有局部覆盖。虽然 IP VPN (和对应的 VSN) 可以在域间扩展以包括多个传送域 (图中未示出)，但 IP VPN 决不能互连所有用户聚集点 (AMG)。这一般要求全球的 AMG 对 AMG 管道，这产生了不可缩放的 VPN。因此，图 4 所示 VSN 的对等是解决问题的重要实施例。

业务供应者 (Service Providers)，拥有 VSN，它将建立与其它业务供应者的对等协议。连接远处终端用户的端对端流量可能沿着 VSN 的连接移动。为了保证一系列业务水平规范 (SLS 或 QoS 管道) 链不被破坏，VSN 需要在对应于转接接入点 (TAP) 48 的一个定义好的点 (称为对等点 (PP) 47) 上进行对等。这个对等点的位置是在业务供应者之间的可接通性协议的一部分。在传送网络基础结构中的 PP 的物理位置可以在边界路由器 (BR) 50 和 52 上，或在相邻传送域的边界路由器之间的链路上。

5 连接到任一个 VSN 的所有用户的覆盖 (在 PP47 的任一边上), 由在 AMG 和对等点之间的一组 (双向的) SLS 或 QoS 管道保证。在图 4 的上部, 这一点通过在任一 SAP 和 TAP 之间的相互连接作了解释。这些仅属于一个 VSN 的本地 SLS 类似于 AMG 之间的 SLS, 并用相同的方法实现。从本地的观点来看, 即从只有一个 VSN 的观点看, TAP (或 PP) 精确地具有和 SAP (或 AMG) 相同的作用。重要的是, SLS 是严格的本地, 即, 在不同 VSN 的 SAP 之间没有直接的 SLS 互连, 见图 4 的上部。这个直接链路对应于域间 SLS, 并表示域间 IP VPN, 而不是两个互连的单域 VSN (或 VPN)。

在对等点上 VSN 的汇合提供了在 TAP 的任一侧上的用户之间的可接通性。
10 在 IP 分组可能流过 PP47 以前, 要求 VSN 交换路由信息。VSN 的虚拟路由环境 (存在于所有边缘路由器和边界路由器之中) 了解关于所有其自身 AMG 的可接通性 (路由) 信息 (类似于图 3 所示)。在一个 VSN 与其它 VSN 对等 (图 4) 的情况下, VSN 虚拟路由必须知道在对等 VSN 中可接通的 AMG 以及可通过此对等 VPN 接通的 AMG。更一般地, VSN 虚拟路由环境必须知道在 (直接地) 对等 VSN
15 中的全部可接通 AMG, 而且知道在可通过具有其自身对等点的对等 VSN 接通的远程 VSN 中的 AMG。这意味着, 如果一个 VSN 对等, 它就变成全球 VSN 间网络的一部分, 就象一个独立网络在与一个已经是因特网一部分的网络对等时就变成因特网的一部分。这可能通过配置 VPN 路由协议从而来自一个 VPN (VSN) 的路由信息被通知到另一个 VPN 而实现。这是实施例的重要部分, 将参照图 6 进一步详细解释。
20

主要操作的描述—参考结构

应用于网络间环境的本发明的主要操作现在参照图 5 进行描述, 它示出了虚拟业务网络 (Virtual Service Network) 参考结构, 即, 上述图 1 中所述 QoS 问题的建议的解决办法。

25 图 5 的下部示出了三个传送域 60, 62, 和 64。左侧和右侧域与接入网络相连; 即, 它们的边缘路由器 (ER) 66.1 和 66.2 直接与终端用户聚集器 AMG 68.1 和 68.2 相连。为了简便起见, 只有一个 AMG (和 ER) 被示出, 但是很清楚, 多个 AMG 与左和右传送域 60 和 64 的边缘路由器相连。中间域 62 被作为一个转接域, 虽然这个域同时可以和 (未示出) 接入网络相连。这些传送域的每一个都
30 受到 (普通的) 网络管理系统 (NMS) 70, 72 和 74 的控制。NMS 通过任一方式

(例如, 命令线路接口命令、简单网络管理协议或公开开放式策略服务器协议)配置相关区域的(边缘,核心和边界)Diff Serv 路由器 66.1, 70.1, 72.1, 72.2, 74.1 和 66.2。区域的边缘和边界路由器能够支持几个路由环境, 例如 BGP/MPLS 虚拟路由器[RFC 2547]。

5 图 5 的中部示出三种虚拟业务网络 76、78 和 80, 如上所述。第一(第二, 等) VSN 所有者从第一(第二, 等)网络供应者那里租用容量, 它在其 AMG 之间和在任一 AMG 68.1 和 68.2 与对等点 82 和 84 之间提供 SLS (或 QoS 管道)。在业务供应者和网络供应者之间的任何 VSN SLA 86 也意味着在边缘和边界路由器 ER 和 BR 中存在专用 VSN 虚拟路由环境(图 5 的下部)。该图示出, 第二(中间)
10 VSN 78 具有在两个对等点之间的 SLS (或 QoS 管道)。第一对等点 82 安排在第一 60 和第二 62 域之间, 而第二对等点 84 安排在第二 62 和第三 64 域之间。如上所述, 可能有 AMG 加到这个域, 甚至可能有更多的连接传送域, 每一个具有专用的对等点。对等点 82 和 84 的存在是在 VSN_1-VSN_2 和 VSN_2-VSN_3 之间可接通性协议的结果。如果没有这种共同的可接通性协议存在在两个 VSN 所有者之间,
15 则在对应的 VSN 之间就没有对应于对等点的 TAP。

在传送网络中 VSN (或 VPN) 的配置是通过网络供应者的 NMS 70, 72 和 74 实现的。VSN 自己的控制, 即在 AMG 中间和在 AMG 与对等点之间的租用资源的控制, 是通过 VSN 控制器 (VSNC) 88, 90 和 92 实现的。VSNC 由 VSN 本身的所有者(业务供应者)所有, 它是新的功能单元, 专用于 VSN QoS 的解决。VSNC
20 可以是现有设备, 例如多媒体呼叫服务器 MMCS 的一部分, 也可以是独立设备。VSN 控制器可以用集中的或分散的方式实现。在前一种情况下, 有例如每个 VSN 一个 VSN 控制器(图 5 所示)。在后一种情况下, 有用于单一 VSN 的多个 VSN 控制器, 例如在 VSN 的每个业务接入点(SAP)/转接接入点(TAP)上的 VSN 控制器。这是一种实施选择方案, 其中两种选项都包含在本发明中。VSNC 的功能将进一
25 步详细解释。

网络供应者拥有的 NMS 和业务供应者拥有的 VSNC 共享包含在 VSN SLA 中的同一(合同)信息, 参考图 3 和 4。这个信息(SLS 或 QoS 管道, 拓扑, 容量等)与例如语音和视频的呼叫建立和拆除的相对动态时间范围(一般几分钟或几小时)相比, 是相对静态的(一般几天或几个月)。NMS 用这个静态信息配置
30 传送网络, 这是一个困难的工作, 但是是在静态基础上进行的。VSNC 在 VSNC

数据库中安装这个信息，并将用这个信息处理业务（或呼叫）请求，所述请求使用（租用的）VSN 资源。例如在单一、集中的 VSNC 的情况下，一个（逻辑的）数据库安装所有有关的 VSN SLA 信息，这些信息包括例如在所有业务接入点之间的 SLS（QoS 管道）的完整格网 - 及其容量。在分布式 VSNC、每个 SAP 一个
5 VSNC 的情况下，VSN SLA 信息也是分布式的。例如在入口 SAP 的 VSNC 仅“看见”在这个 SAP 起动的 SLS（或 QoS 管道），即，这个 VSNC 看见“SLS 的一部分”而不是 SLS 的完整格网。

在这个阶段 NMS 配置网络，VSNC 在 VSNC 数据库中安装虚拟网络信息。不过，在业务或呼叫可以使用 VSN 资源以前，VSN 的路由信息还必须以下述方式在
10 传送和网络供应者设备之间共享。

图 5 的下部示出了在每个边缘和边界路由器中的 VSN 虚拟路由环境（VR）的存在，如参照图 3 所述。路由器中的 VSN VR 保证分组（运载 VSN 供给的业务）沿着该 VSN 的 SLS 或 QoS 管道进行路由选择，即分组的路由决定在 VSN 的 VR 环境中做出。相同的机制被用于保证在传送域或边界路由器之间的分组的路由。
15 在对等 VSN 的 VR 之间的信息交换保证分组将沿着一个 VSN 的 SLS 向对等点移动，并从对等点向前移动，下一个 VSN 的 SLS 接管它。重要的是注意，如果 VSN 不具有可接通性协议，则它们的 VR 将不交换路由信息（通过域间链路）。这个机制的可能实现如图 6 和 7 所示。

存在于运载 VSN 的 SLS 的边缘和边界路由器中的所有 VR 环境之中的专用
20 VSN 的路由信息必须由 VSN 控制器 VSNC 已知。实际上，VSN 控制器必须知道分组将跟随的 SLS 的序列（最终将在其自身 VSN 中和在对等 VSN 中）。因此，VSNC 必需知道在 VSN 的虚拟路由环境中采取的路由决定。实际上，VSNC 的基本的路由要求是双重的。

首先，如果通过其自身的 VSN 不能达到目的地，VSNC 必须能够找到合适的
25 下一个 VSNC，该下一个 VSNC 对下一个 VSN 的资源许可控制负责。如果 VSN 控制器保存一个路由表，如果目的地不在同一 VSN 之中则映射每个目的地子网掩码到“下一个中继段”（net hop）VSN 控制器，这一点可能被实现。

第二个基本 VSNC 路由要求是，VSNC 必须能够在数据流通路流经虚拟网络时识别其入口点和出口点。这个要求的实现取决于 VSNC 的实现和资源信令机制
30 的性质。有两种极端的情况。第一种情况是，结合带外资源信令的集中 VSNC 实

现, 即, 资源信令消息不沿数据通路上的路由器传送。不在数据通路上的 VSNC, 仍然必须知道 VSN 的虚拟路由表中的信息。这例如可以通过在一个或多个边缘路由器和 VSN 控制器之间建立路由协议会话而实现。用这种方法, VSN 控制器学会在 VSN 环境内被通知的路由选择, 并形成它自己的路由表。

5 第二种情况是结合带内信号的分布式 VSNC 实现(“存在于边界路由器中”)。

在 VSN 中间在虚拟路由环境内路由信息的交换是可跨域传递的。以三个 VSN: VSN_1 , VSN_2 和 VSN_3 的情况为例。如果 VSN_1 和 VSN_2 具有可接通性协议, 从而交换路由信息, 并且如果相同的情况适应于 VSN_2 和 VSN_3 , 则 VSN_1 自动知道 VSN_3 的路由信息。路由协议, 例如 BGP 本身(边界网关协议)的操作保证了这一点。
10 与例如语音和视频的呼叫建立的更动态的时间范围相比, 路由信息的交换也是比较静态的(一般几个小时或几天)。

在这个阶段, 路由信息在对等 VSN 的 VR 环境中间(和超出这个环境)被交换, 并且这个信息可用于 VSN 控制器。现在 VSN 被配置为接收用户对于 QoS 敏感业务的请求(例如语音, 视频等等)。

15 图 5 在左方和右方是集中了用户的接入网络。AMG 是接入集中器, 并且直接与 IP 传送区域的边缘路由器相连(类似于图 1 中的情况)。

现在终端用户 10 通过经由 MMCS 20.1 从其终端发送一个请求到业务供应者 SP 的应用控制服务器来请求, 协商并最后启动一个终端用户业务。这可以通过呼叫信令协议(例如, 会话启动协议[SIP]或 H. 323)来实现。另一种可能是,
20 用户(通过“点击”)选择在 SP 门户网站上的业务。在呼叫信令阶段, 业务供应者 SP 可能分配给用户, 即呼叫者 10, 一个业务(或呼叫)期间的专用 IP 地址。用户终端的地址也可以在终端配置的时刻, 或在拨号因特网接入(例如, 宽带 ATM)时刻获得。这个地址可以是或不是 IP 公共地址。总之, VSN 解决方案独立于寻址问题, 它可能是专用的, 公共的, IPV6 等等。唯一的要求是, 在
25 VSN 路由环境内, 用户 IP 地址应该是唯一的。同时在这个起始呼叫信令阶段, 呼叫者 10 将根据被叫方标志, 通过类似 DNS 的机制, 检索被叫方 12 的 IP 地址。总之, 呼叫信令协议同时处理移动性和漫游状况以及用户鉴别和授权。所有这些, 与图 1 所述的 QoS 问题无关。

用户和业务供应者(SP)必须商定(在呼叫建立期间)业务的 QoS 要求,
30 例如, 要求的通过量, 延迟或分组损失。这个信息可以用许多方式在用户和 SP

之间交换。QoS 请求可以是在呼叫信令协议的“背上”，例如 SIP-SDP（会话描述协议）。例如，对于话音，QoS 要求可以从编解码器类型推断出。另一种可能是，客户在 SP 的门户网站上（通过“点击”）选择业务，并隐含地确定 QoS 要求。还有另一种可能，即用户在带内将其 QoS 请求发送到 AMG（例如通过 R SVP），

5 AMG 依次把信息送入 MMCS 或负责的应用服务器。

在这个阶段，所有用户（参与业务的），它们的物理位置，IP 源和目的地地址都被识别。同时，从应用控制服务器请求业务 QoS 要求（图 5 中的 MMCS）。现在，呼叫资源信令阶段可以开始（见图 5）。呼叫资源信令阶段通过 MMCS 20.1（为呼叫者业务）开始，沿 VSNC 的链向 MMCS 20.2 传送（为被叫方业务）。信

10 令协议（是一个专用协议）可以是带内的（信号不沿着数据通路上的路由器传送）或是带外的。它最好也是两者的结合，例如端对端通路的某些部分是由一个集中（带外的）VSNC 控制，而其它部分是由分布式的（带内的）VSNC 控制。

如果用户（经 MMCS）要求来自 VSN 的资源，则 VSN 控制器需要做两件事情。首先，VSNC 必须检查是否有足够的资源保存在自己的 VSN 中以便容纳所述容量。

15 第二，如果被叫用户没有被加到它自己的 VSN，VSNC 最终还应该运送资源请求到对等 VSN（VSNC）。

根据被叫用户的 IP 目的地地址，VSN 应该确定流量将在哪个 SLS 或 QoS 管道序列上传送（在其自己的 VSN 中）。这意味着，VSN 检索入口和出口 SAP（或 TAP）。入口 SAP 可以根据进行资源请求的一方进行检索：VSN 的客户应该商定

20 特定的入口 SAP 并且应当在从 VSN 请求资源时识别它们本身。为了找到出口 SAP（TAP），VSN 应该找到下一个 VSN 和与该 VSN 相关的对等点。这是根据路由表实现的，该表将目的地 IP 地址映射到下一个 VSN。根据 VSN 业务水平协议，VSN 也了解 QoS 管道的总容量和关于在这些 QoS 管道中的业务量聚集的延迟，抖动的 QoS 保证（VSN SLA 信息）。当与有关 QoS 管道中的所有其它正在进行的呼

25 叫的 VSN 信息相结合时，VSN 可以对新到达的呼叫执行资源许可控制。

因此，在 VSN 中的每个呼叫的许可控制是通过 VSN 控制器执行的（VSNC 17.6）。通过 VSN SLA 86，VSNC 了解 VSN 60 的（租用）资源和拓扑，并处理每个呼叫的资源信令和许可。

如果许可，VSN 控制器将呼叫请求转发到需要跟随同一程序的下一个中继

30 段 VSN 控制器，即，确定下一个中继段 VSN，在其自身 VSN 中的进入和退出点，

以及在进入和退出点之间的路径上的许可控制。当呼叫请求到达服务于被叫用户 12 的远程 VSN 64 的时候，呼叫请求将返回到起始 VSN 60，以在返回通路上执行许可控制。

5 如果沿信令通路的所有 VSNC 都许可业务，则 MMCS 20.1 最终将向用户确认呼叫，并且分组可以开始流动。

边界路由器的实现和操作

图 6 和 7 是 VSN 虚拟路由环境和在 VSN 之间的路由信息交换的实现。虽然本发明的一个实施例利用 BGP/MPLS[RFC 2547]实现，但可以把它扩展到不同传送区域之间的链路，或者类似地，替换实施例包括 iBGP 连接 (RFC 2547) 或
10 eBGP 连接。

业务供应者希望为其客户提供与大量用户的连通性。一个单一 VSN 管理一个单一传送区域，因此，它只能达到有限数量的用户。因此该业务供应者建立与其它业务供应者的可接通性 SLA。这个 SLA 包括

- 15 —可接通性信息，即，一个业务供应者可以达到哪些用户；
- 物理对等点，即，在该处两个 VSN 被物理地连在一起；
- 业务供应者的 VSNC 的 IP 地址；和
- 配置网络元件所需的 VSN 识别标志。

虚拟路由器的概念

当两个业务供应者已经建立这样一个 SLA 的时候，它们的 VSN 应该连接。
20 路由信息然后可以以 BGP 消息的形式进行交换。重要的是，路由信息只是沿特定 VSN 的 SLS 通向上游。这就保证，多媒体分组将仅沿着具有预先提供的、带有严格延迟和带宽保证的 SLS 的通路而被确定路由，路由信息不沿 SLS 序列将被断开的路由通过。这意味着，在 VSN 环境中的多媒体分组的路由决定不同于例如最大努力因特网流量的路由决定。一种获得路由的选择性分配和用于最大
25 努力数据和多媒体业务量的分离路由表的方法是使用 VPN 技术和虚拟路由器。象 BGP/MPLS[RFC 2547]这样的技术可以被采用，但是其它 VPN 技术也将能应用。可以配置虚拟路由器，使得它们仅安装来自己与其建立可接通性 SLA 的对等业务供应者的 BGP 路由。虚拟路由器的另一个优点是，它们使得能够在单一传送网络上支持多个业务供应者，同时每个业务供应者根据他们所具有的可接通性
30 SLA 具有他们自己的路由表。

总之，通过虚拟路由器，VSN 可以：

- 向 SLS 的上方分配路由；
- 根据商业原因，选择性地与其它 VSN 进行对等；
- 在同一骨干网中与其它 VSN 以及可能还有最大努力（BE）因特网共存；

5 以及

- 一只从对等 VSN 形成透明 IP 网络后才根据 IP 目的地地址转发分组。

图 6 示出两个对等 VSN 101 和 102 的 SLS 如何连接，路由信息如何向 SLS 的上游传播。SLS 在网络的入口点被实行，因此，VSN 101 的 SLS 分别在 103.1, 103.2 和 133.3 处实行。VSN B 的两个 SLS 在边界路由器 2(104) 处被实现。

10 边界路由器支持虚拟路由器，所述虚拟路由器是 L3 IP 路由器。用这种方法，IP 技术的无连接和聚集特性被保存下来了。在两个虚拟路由器之间，分组通过通道(tunneling)机制被转发。这可以借助例如 MPLS, ATM 或 IP 通道来实现。应该指出，没有端到端的通道（MPLS）被建立，只有域内通道。

现在描述具有 BGP/MPLS VPN 的 VSN 的实施。

15 VSN 可以基于 BGP/MPLS 虚拟专用网络(VPN) [RFC 2547]，因为它们支持通过 MPLS 通道互相连接的虚拟路由器的概念和 L3 边界路由器的概念。因此，VSN 作为覆盖网络被实现。每个 VSN 取决于它具有的可接通性 SLA 具有它自己的路由表。每个 VSN 的业务量通过 MPLS 标记被识别。当业务量在两个虚拟路由器之间转发时，可能有 MPLS 交换在它们之间，而 VSN 不知道。在这种情况下应该使用两个 MPLS 标记。内部标记用于识别哪个虚拟路由器必须被用于边界路由器中，

20 外部标记用于在两个边界路由器之间对分组进行路由选择。

VSN 中的路由分配可以通过 BGP 装置实现。一个 BGP 扬声器发送一个信息到它的对等者以通知路由选择。被交换的 BGP 信息，除 IP 地址和路径（“正常” BGP 更新信息的属性）之外，还包括下面的信息（典型的 VPN/VSN 属性）：

25 — 支持选择性路由分配所需的 VSN/VPN 标识符。如果被在发送和接收 BGP 信息的 VR 的 VSN 所有者之间的对等 SLA 协议允许的话，路由器仅安装所通知的 BGP 路由；以及

— 识别分组的起始 VSN/VPN 所需的 MPLS 标志。实际上，注意该边缘/边界路由器可能支持多个 VPN 和 VSN。如果分组到达边界路由器，这个路由器必须

30 具有一个装置以识别哪个 VPN/VSN 现在应进一步运送分组，和哪个虚拟路由器

环境将进一步确定分组的路由。这是 MPLS 标志的目的，它仅具有在两个边界路由器之间的本地意义。发送边界路由器将把 MPLS 标志（它从 BGP 信息获得的一个值）加到 IP 分组上，从而接收边界路由器知道哪一个 VPN 将承载并转发分组到下游。

5 图 7 解释路由怎样被分配和怎样被选择性地安装在虚拟路由器中。假定在 VSNB, 110 和 VSND, 111 之间只有一个可接通性协议。VSND, 111 的边界路由器, 112, 将例如通过边界路由器 113, 114, 115 广播 BGP 路由通知到所有它的对等网络。这个信息包括 IP 地址, 路径, VSN id 和 MPLS 标志。VSN id 用在 VSNA, B 和 C 的虚拟路由器 113, 114, 115 中, 以检查它们是否应该安装这个路由(即, 10 它们是否具有与 VSN D 的可接通性 SLA)。在图 7 所示例子中, VSN A 和 C 的虚拟路由器忽视 BGP 信息, 但是 VSN B, 110 安装路由并将该路由转发到它的内部对等者。这类似于使用来自[RFC 2547bis]的 BGP/MPLS VPN 结构, 它被扩展到 eBGP 连接, 即在两个域的边界路由器之间的连接。

考虑到在两个边界路由器(即, 虚拟路由器)之间的分组流量, 当分组到 15 达边界路由器时, 它的 MPLS 标志被用于识别正确的虚拟路由器(即, 它识别正确的 VSN)。MPLS 标志然后被去除, 并且在该虚拟路由器中进行正常的 IP 转发。然后, 一个新的 MPLS 标志被加上, 以便识别下一个虚拟路由器。由于 BGP 进行的路由分配, 这个标志值在下一个虚拟路由器上是已知的。

每个虚拟业务网络应该具有一个虚拟业务网络控制器来执行上述功能(集 20 中或分散, 带内或带外实现)。

当 VSNC 接收一个预留请求的时候, 它执行一个许可控制。因此, 它必须识别将在其上传送分组流量的正确 SLS(或 QoS 管道)。然后, 预留请求最后必须被转发到下一个 VSNC。

VSNC 的操作总结如下:

25 一 可从前一 VSNC(或呼叫者)的 IP 地址获得业务量将进入网络的物理对等点, 因为这在业务供应者(或用户/业务供应者)之间的可接通性 SLA 中作了规定。因此, 入口点(SAP 或 TAP)是它自己 VSN 所知道的。

一 然后, VSNC 必须使用在呼叫请求中规定的媒介流量的目的地 IP 地址(即, 目的地 AMG 的 IP 地址), 以便在其路由表中查找目的地是否是在其自己的 VSN 30 中, 如果不在, 需要联系哪一个对等 VSN。这个信息被存储在 VSNC 的路由表中,

并与边缘/边界路由器中的 VSN 虚拟路由环境一致(align)。

—如果地址是本地的, VSNC 显然知道出口 SAP, 而如果地址不是本地的, VSNC 也将知道出口 TAP, 因为表查找提供了下一个中继段 VSN, 而 TAP 就是下一个中继段 VSN 的对等点。

- 5 —为其执行呼叫许可控制的正确的 SLS 现在可以被识别, 因为入口和出口 SAP/TAP 是已知的。

在 VSNC 中的表查找提供下一个 VSNC 的地址, 因为下一个中继段 VSN 和 VSNC 的 IP 地址间的关系从对等业务供应者中间的可接通性协议可以知道。

—预留请求现在可以被转发到下一个 VSNC。

- 10 过程的实现通过图 8 进行描述。

为了执行这个路由功能, VSNC 必须确定媒介流量的分组(为其进行了预留)将遵循哪个路由。因此, 需要安装一个路由表在 VSNC 120, 121, 122 中。这个路由表必须与(虚拟)边界路由器 123, 124, 125 的路由表同步。这可以通过使 VSNC 作为 BGP 扬声器或通过将 VSNC 配置为“CE”(客户设备)—VPN 的设备而实现。通过在边界路由器和 VSNC 之间建立 BGP 连接 128, 控制平面中(VSNC)的路由信息就和传送平面中(在虚拟路由器中)的路由信息同步。

可以理解, 此处公开和描述的本发明可以扩展到从全文或附图中所述或明显看出的两个或多个特点的所有替换组合, 所有这些不同组合构成本发明的不同替换方面。

- 20 上述本发明的实施例和修改, 对于熟悉技术的人是明显可以做出的, 它不脱离本发明的范围。

图1

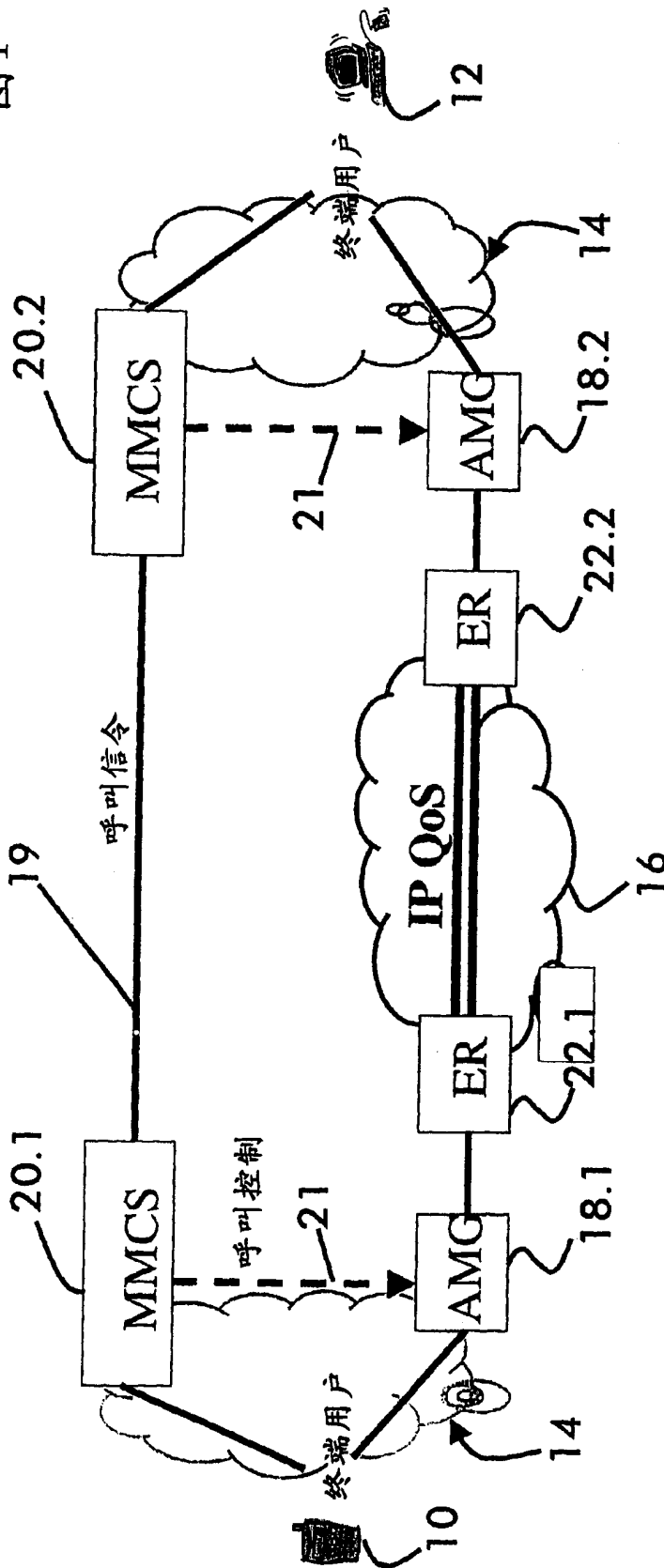
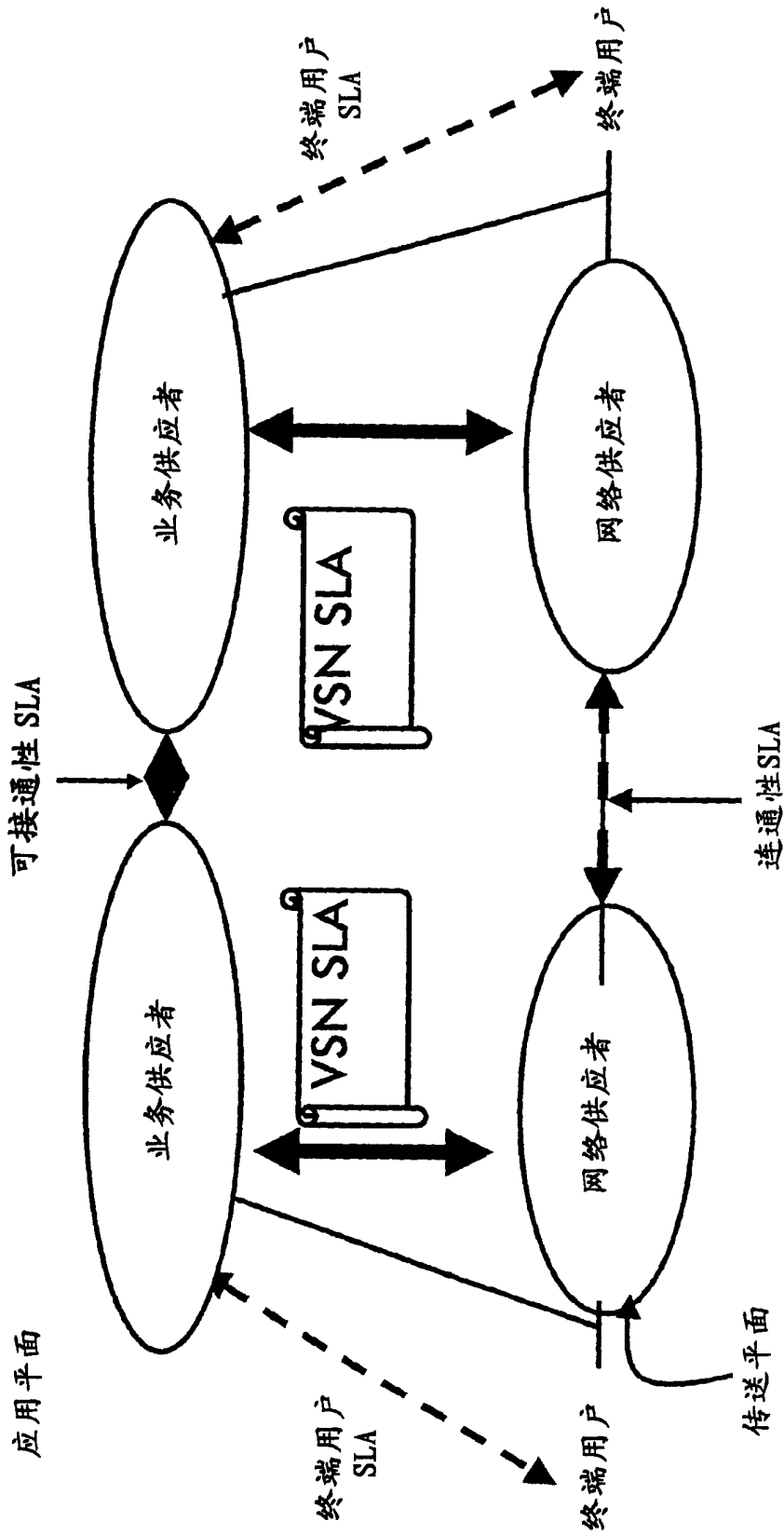
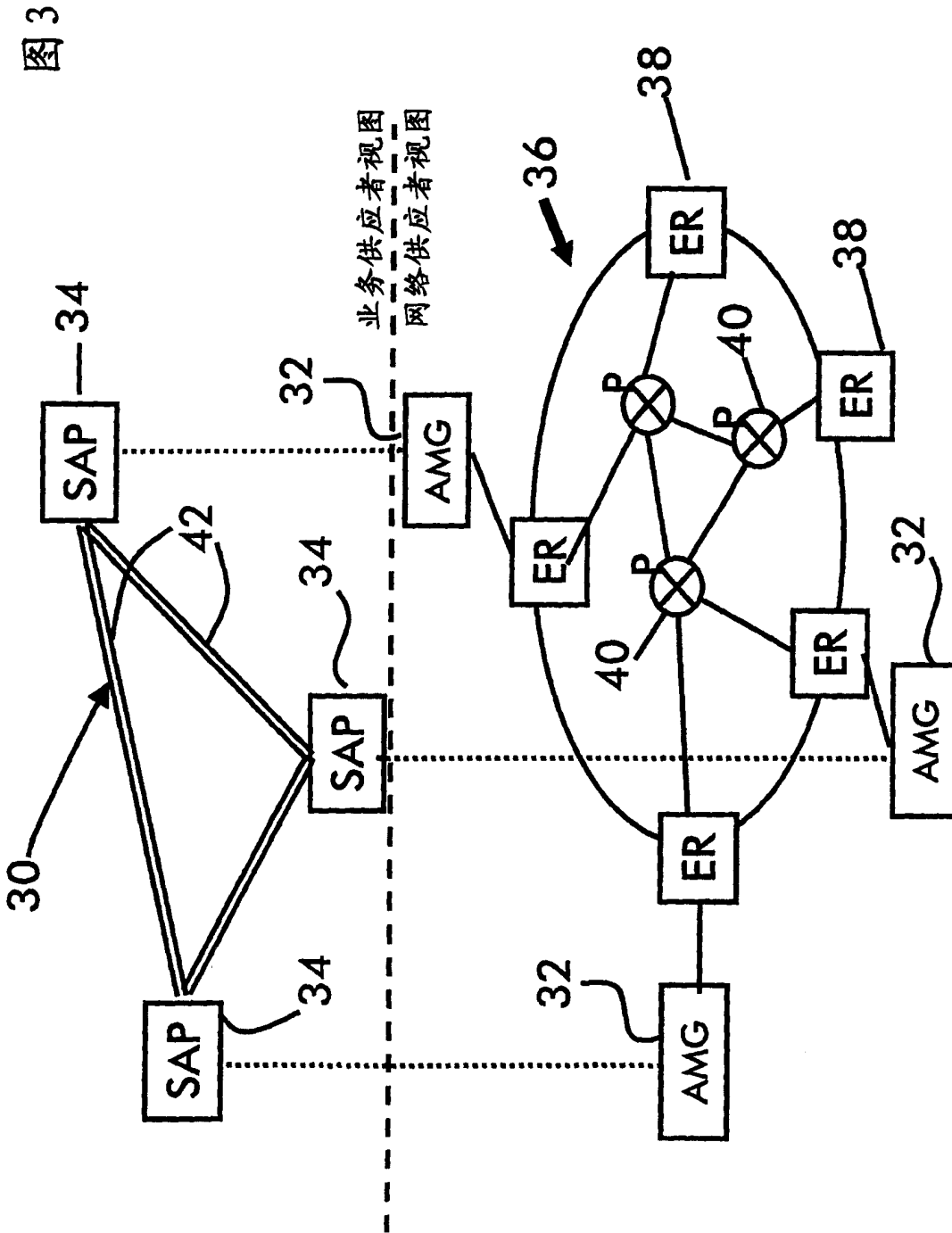


图2





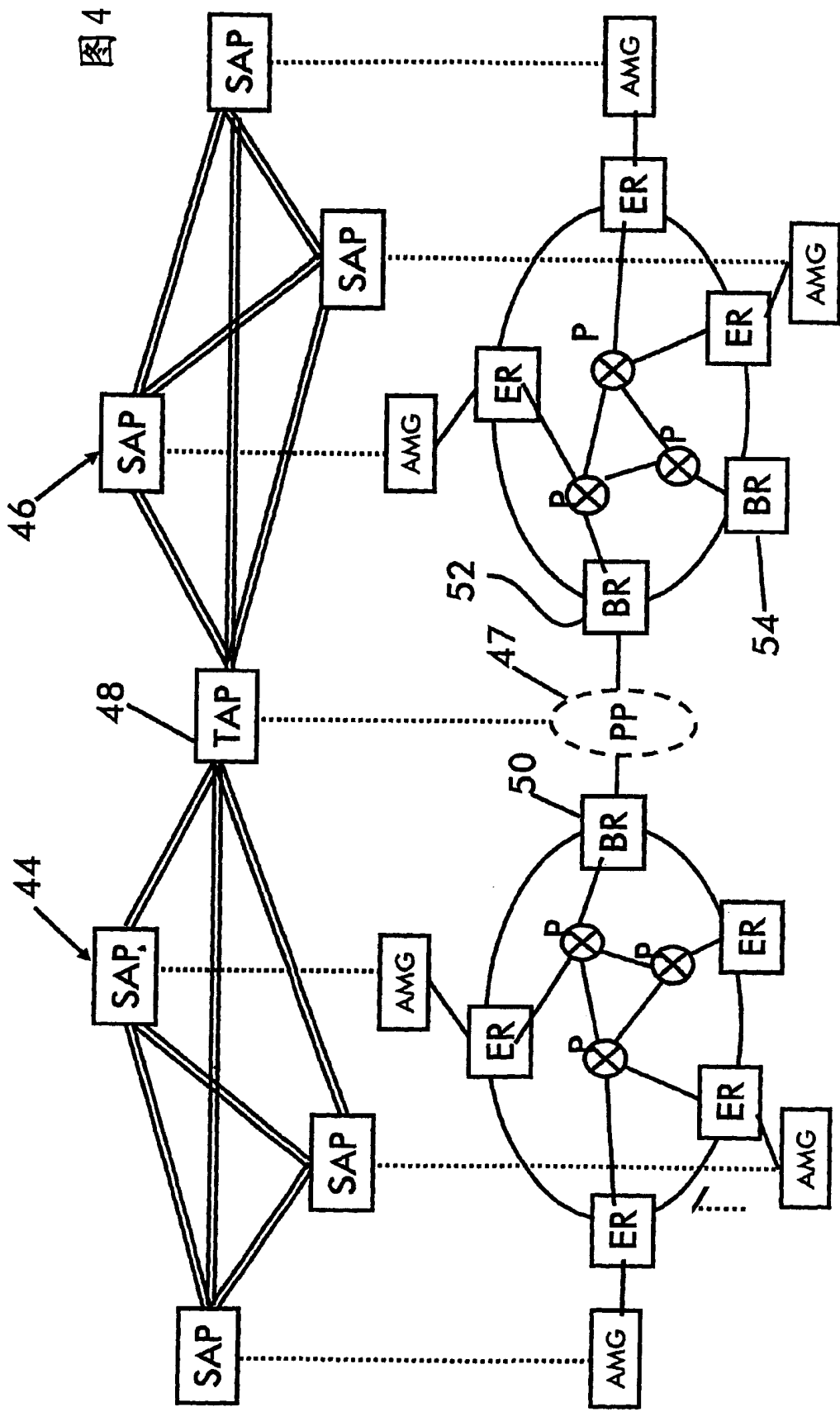


图 4

图5

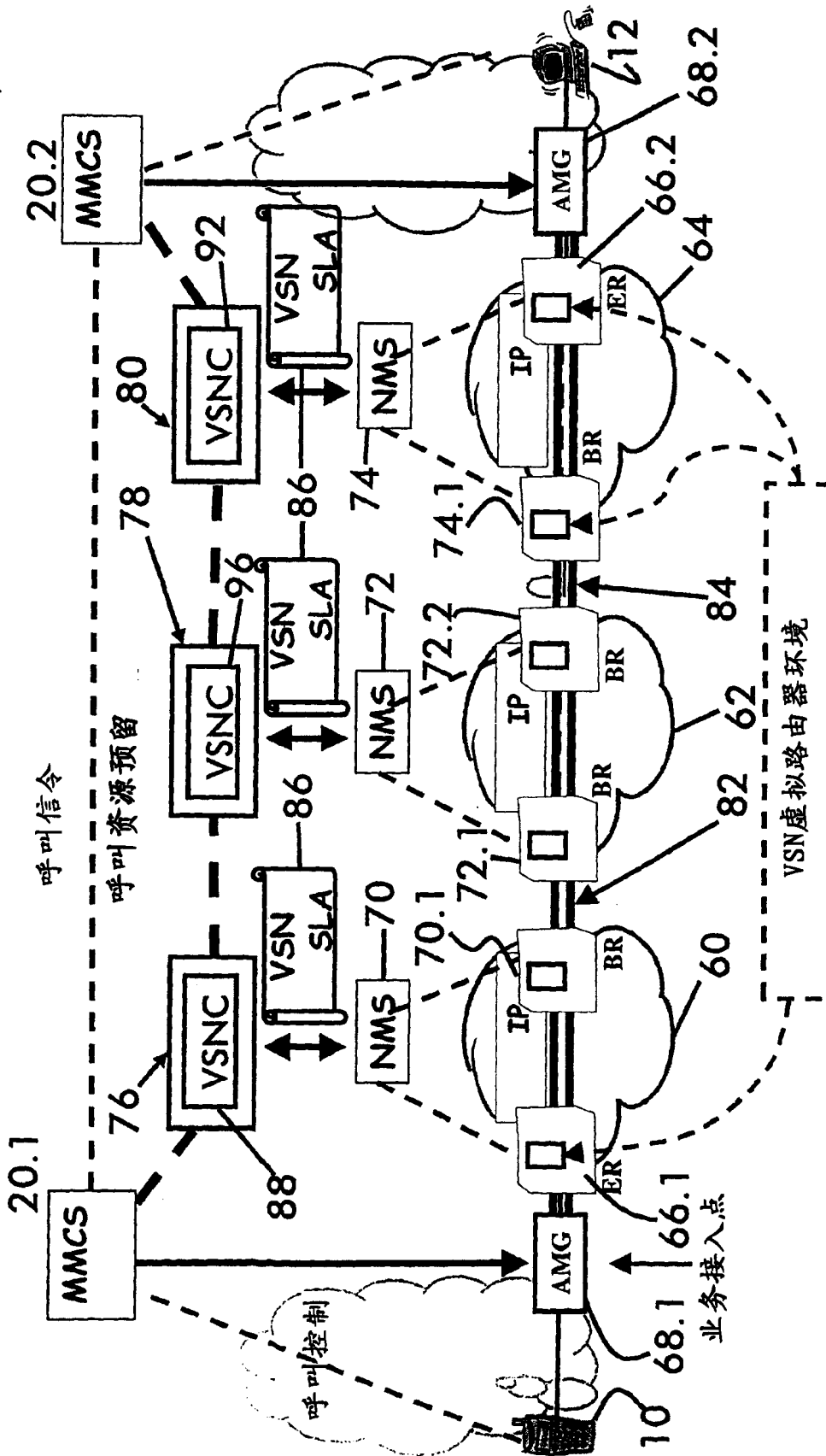


图6

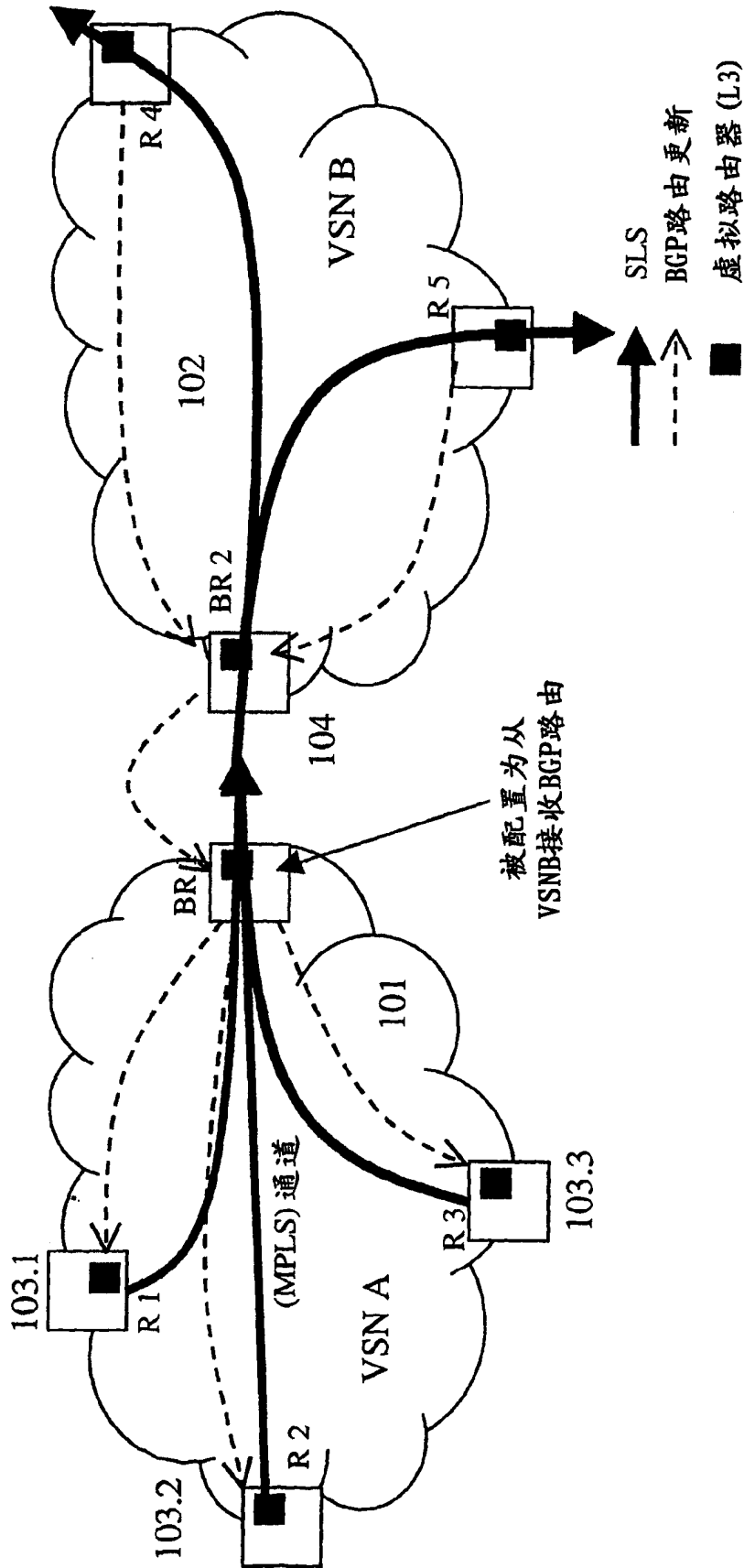


图7

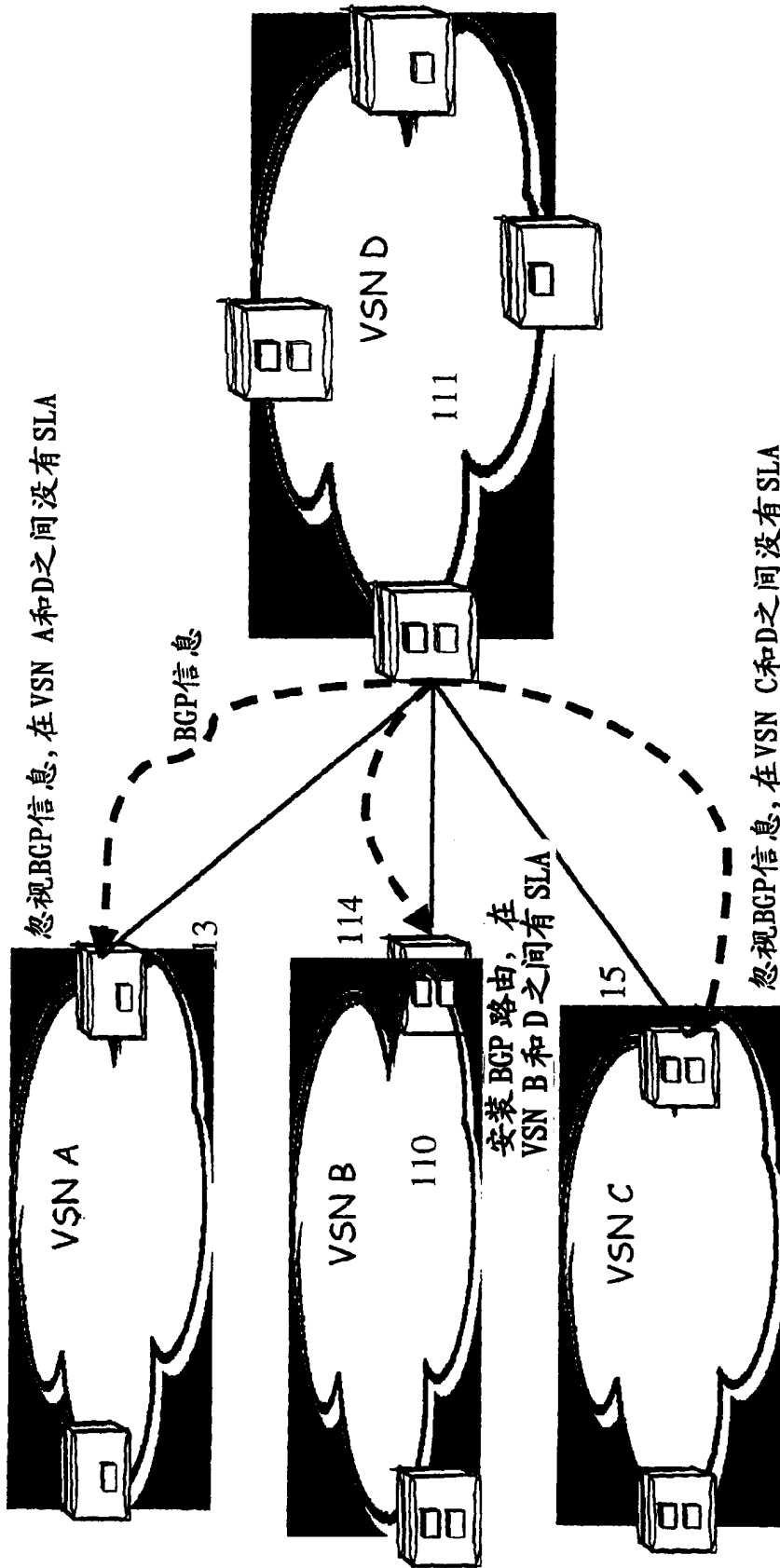


图8

