

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 12/56 (2006.01)

H04L 12/46 (2006.01)



[12] 发明专利说明书

专利号 ZL 03804854. X

[45] 授权公告日 2009 年 12 月 2 日

[11] 授权公告号 CN 100566284C

[22] 申请日 2003.2.27 [21] 申请号 03804854. X

[30] 优先权

[32] 2002. 2. 28 [33] SE [31] 0200640 - 1

[86] 国际申请 PCT/SE2003/000326 2003. 2. 27

[87] 国际公布 WO2003/073707 英 2003. 9. 4

[85] 进入国家阶段日期 2004. 8. 30

[73] 专利权人 艾利森电话股份有限公司

地址 瑞典斯德哥尔摩

[72] 发明人 J·贝克曼 K·诺尔伦德

A·恩斯特伦 L·芒努松

J·克普曼

[56] 参考文献

EP 1071296 A1 2001. 1. 24

WO 0051290 A2 2000. 8. 31

审查员 程小亮

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 李亚非 王忠忠

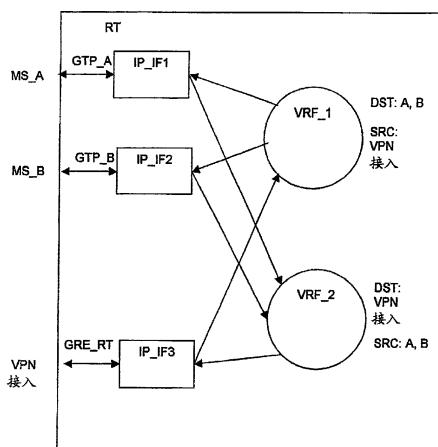
权利要求书 2 页 说明书 8 页 附图 8 页

[54] 发明名称

虚拟专用网络及其中的路由器

[57] 摘要

已经展示了包括服务至少一个虚拟专用网络(VPN)的网关 GPRS 支持节点(GGSN)的网络，由此网关 GPRS 支持节点对每个互连网协议(IP)接口展包括至少两个虚拟专用网络(VPN)路由/转发实体。此外还公开了带有方向特定属性的路由器。



1. 一种路由器 (RT) , 包括至少两个 IP 接口 (IP_IF1; IP_IF2; IP_IF3) , 由此每个 IP 接口与各自的虚拟专用网络 (VLAN1; VLAN2; VLAN3) 相关, 所述路由器还包括至少两个转发表 (VRF_1; VRF_2) ,

由此所述转发表的第一张表 (VRF_1) 用于将业务路由到给定的 IP 接口 (IP_IF1; IP_IF2) , 并且

所述转发表的第二张表 (VRF_2) 用于路由自同一给定的 IP 接口 (IP_IF1; IP_IF2) 出现的业务。

2. 如权利要求 1 所述的路由器, 其中在一个 IP 接口 (IP_IF1; IP_IF2) 上接收到的且涉及一个给定的虚拟专用网络 (VLAN1; VLAN2) 的分组被转发到涉及另一虚拟专用网络 (VLAN3) 的另一 IP 接口 (IP_IF3) 。

3. 如权利要求 1 或 2 所述的路由器, 由此第一个 IP 接口 (IP_IF1) 与向移动站提供双向连接性的第一个隧道 (GTP_A) 相耦合, 第二个 IP 接口 (IP_IF3) 与向公司网络提供双向连接性的隧道 (GRE_RT) 相耦合。

4. 如权利要求 3 所述的路由器, 包括向移动站提供双向连接的第三个 IP 接口 (IP_IF2) , 配置所述路由器以使在第一个 IP 接口 (IP_IF1) 上的移动站与第三个 IP 接口 (IP_IF2) 上的移动站通信时, 业务被通过第二个 IP 接口 (IP_IF3) 路由。

5. 包括拥有至少两个 IP 接口 (IP_IF1; IP_IF2; IP_IF3) 的路由器 (RT) 的网络, 由此每个 IP 接口与各自的虚拟专用网络 (VLAN1; VLAN2; VLAN3) 相关, 路由器还包括至少两个转发表 (VRF_1; VRF_2) ,

其中所述转发表的第一张表 (VRF_1) 用于将业务路由到第一 IP 接口 (IP_IF1) , 所述转发表的第二张表 (VRF_2) 用于路由自第一

IP 接口 (IP_IF1) 出现的业务，

其中在第一 IP 接口 (IP_IF1) 上接收到并涉及第一虚拟专用网络 (VLAN1) 的分组被转发到涉及第二虚拟专用网络 (VLAN3) 的第二 IP 接口 (IP_IF3)，

其中第一个 IP 接口 (IP_IF1) 与向移动站提供双向连接的第一个隧道 (GTP_A) 相耦合，第二个 IP 接口 (IP_IF3) 与向公司网络提供双向连接的隧道 (GRE_RT) 相耦合，并且

其中第三个 IP 接口 (IP_IF2) 向移动站提供双向连接，路由器被配置成，以使在第一个 IP 接口 (IP_IF1) 上的移动站与第三个 IP 接口 (IP_IF2) 上的移动站通信时，业务被通过第二个 IP 接口 (IP_IF3) 路由。

6. 根据权利要求 5 的网络，包括远程路由器，所述网络被配置为使得从一个移动站 (MS_A) 到另一移动站 (MS_B) 的分组被转发到该远程路由器 (R)，该远程路由器有选择地进行策略决策。

7. 根据权利要求 5 或 6 的网络，其中所述路由器被配置为使得在第三个 IP 接口 (IP_IF2) 上的移动站与第一个 IP 接口 (IP_IF1) 上的移动站通信时，业务也被通过第二个 IP 接口 (IP_IF3) 路由。

8. 如权利要求 6 的网络，其中远程路由器包括防火墙。

9. 如权利要求 6 的网络，其中所述路由器 (RT) 包括在 GGSN 节点中。

虚拟专用网络及其中的路由器

技术领域

本发明涉及 TCP/IP 路由及转发领域，尤其涉及虚拟专用网络（VPN）中的概念。

本发明的主要申请是带有高 VPN 可扩展性需求的 IP 路由器，例如 GPRS(通用分组无线电服务)网络中的 GGSN(网关 GPRS 交换节点)。本发明涉及 WPP5.0 (无线分组平台)。

背景技术

虚拟专用网络 (VPN) 是被远程管理的网络的扩展。这种网络是用基于 IP 或不基于 IP (例如 ATM) 的协议，通过隧道效应在局域网上实现的。在扩展这些网络到移动分组数据网中时，单个节点必须处理大量 VPN。这暗示着所有这些对 VPN 的扩展的管理和配置必须由管理移动分组网络的管理员管理。在 (例如) GPRS (通用分组无线电服务) 中，GGSN (网关 GPRS 交换节点) 连接移动网络到被远程管理的网络。图 1 展示了这种带有 GGSN 的 GPRS 网络的示意性概观。

图 2 展示了在两个移动站之间有业务的例子。这个例子展示了 GGSN 的管理员不得不管理保护移动站免于相互干扰的分组过滤规则。移动站间的业务不能从远程管理的网络上监控。

一种已知的解决方案是基于进行分组转发的分组过滤的一种实现。通过定义从一个接口或隧道转发所有业务到另一接口或隧道的分组过滤器，转发表中的路由信息将不被考虑，并且业务也将被强制到远程网络。

对该问题另一已知的 WPP 解决方案是直接把来自一个接口/隧道的业务映射到另一接口或隧道中，而不根据目标 IP 地址进行转发决策。这种已知解决方案称为 APN (访问点名) 路由。

上述解决方案的缺点是冗余性差，因为分组过滤器 (或映射表) 不是被动态更新并且分组被转发去的接口或隧道可能由于链路或网络问题而不可用。

图 3 展示了两个节点 A 和 B 以及物理连接到以太网段 ETH_S 的

路由器 R。两个虚拟专用网络 VPN_1 和 VPN_2 是在公共以太网段 ETH_S 上实现的。节点 A 包括第一个和第二个 IP 接口 IP_IF1 和 IP_IF2。IP 层 3 上的 IP 接口 IP_IF1 和 IP_IF2 被通过 ARP (自动请求协议) 协议映射到给定的单一层 2MAC (介质访问控制) 以太网地址 ETH_IF1。

同样地，接口 IPIF3 和 IP_IF4 被映射到节点 B 的以太网接口 ETH_IF2。IP 接口 IP_IF5 和 IP_IF6 被映射到路由器 RT 上的 ETH_IF2。

节点 A 的 IP_IF1 和节点 B 的 IP_IF3 构成了第一个虚拟专用网络 VPN_1。节点 B 的 IP_IF4 和路由器 RT 的 IP_IF6 构成了第二个虚拟专用网络 VPN_2。可以在各个 VPN 上的各个 IP 接口之间传递 IP 分组。对各个 VPN 的不同 IP 接口来说，似乎以太网段是专有的。

图 4 展示了从图 3 所示的网络的 VPN_1 上的 IP 接口 IP_IF3 发送到 IP_IF1 的示例 IP 分组。该 IP 分组被封装在一个以太分组中，源地址是 ETH_IF2，目标地址是 ETH_IF1。它的以太网类型标识是“VLAN”类型-虚拟局域网-并携带对应的网络标识符 VPN_1 以及属于正在使用的 IP 协议版本的第二个以太网类型标识符 Ipv4。在以太网有效载荷 ETH_PL 中，提供了上面提到的 IP 源和目标地址以及 IP 有效载荷。该分组由以太网循环冗余校验值 ETH_CRC 结束。

图 5 中，所展示的示例性的现有技术的网络包括路由器 RT，RT 通过转发表 VRF_1 提供第一个虚拟专用网络 VPN_1，VRF_1 为 IP 接口 IP_IF1、IP_IF2 和 IP_IF3 提供互连性。路由器还通过转发表 VRF_2 提供第二个虚拟专用网络 VPN_2，VRF_2 为 IP 接口 IP_IF5 和 IP_IF6 提供互连性。

发明内容

本发明的第一个目标是阐明允许根据业务方向有选择地路由的路由器。

这个目标是这样实现的：

根据本发明的一种路由器，包括至少两个 IP 接口，由此每个 IP 接口与各自的虚拟专用网络相关，所述路由器还包括至少两个转发表，

由此所述转发表的第一张表用于将业务路由到给定的 IP 接口，并且

所述转发表的第二张表用于路由自同一给定的 IP 接口出现的业务。

第二个目标是给出允许在不同的专用网络之间通信的路由器。

这个目标是这样实现的，其中在一个 IP 接口上接收到的且涉及一个给定的虚拟专用网络的分组被转发到涉及另一虚拟专用网络的另一 IP 接口。

根据本发明的包括拥有至少两个 IP 接口的路由器的网络，由此每个 IP 接口与各自的虚拟专用网络相关，路由器还包括至少两个转发表，

其中所述转发表的第一张表用于将业务路由到第一 IP 接口，所述转发表的第二张表用于路由自第一 IP 接口出现的业务，

其中在第一 IP 接口上接收到并涉及第一虚拟专用网络的分组被转发到涉及第二虚拟专用网络的第二 IP 接口，

其中第一个 IP 接口与向移动站提供双向连接的第一个隧道相耦合，第二个 IP 接口与向公司网络提供双向连接的隧道相耦合，并且

其中第三个 IP 接口向移动站提供双向连接，路由器被配置成，以使在第一个 IP 接口上的移动站与第三个 IP 接口上的移动站通信时，业务被通过第二个 IP 接口路由。

第三个目标是给出允许在具体接口上强制业务的系统。

这个目标是这样实现的，网络包括远程路由器，所述网络被配置为使得从一个移动站到另一移动站的分组被转发到该远程路由器，该远程路由器有选择地进行策略决策。

第四个目标是给出分组控制被延迟到公司网络的系统。

这个目标是这样实现的，其中所述路由器被配置为使得在第三个 IP 接口上的移动站与第一个 IP 接口上的移动站通信时，业务也被通过第二个 IP 接口路由。

依照本发明的另一方面，为了提高 VPN 网络中的安全性，希望来自移动终端的所有业务（即 IP 分组）总会通过家庭网络而行。这就使得 VPN 管理员能够指定要施加到去往移动终端和来自移动终端的业务的分组过滤规则。这与分组去往与分组所来自的移动网络扩充相同或不同无关。不强制业务到家庭网络，则必须由 VPN 网络的移动扩展的管理员而不是由家庭网络的管理员配置分组过滤规则。

从下面对优选实施方案的详细描述可以看到本发明的更多优势。

附图说明

图 1 展示了 GPRS 网络体系结构的总体图示。

图 2 展示了 GPRS 网络中执行路由的已知方法。

图 3 展示了在以太网段上实现虚拟专用网络 (VPN) 的已知方式。

图 4 展示了图 3 中所用的分组。

图 5 展示了提供两个 VPN 网络的现有技术的路由器。

图 6 展示了依照本发明的路由器的第一实施方案。

图 7 展示了依照本发明的 VPN 网络的第二实施方案，包括从节点 A 到节点 B 的分组流。

图 8 展示了与图 7 相同的 VPN 网络，包括从节点 B 到节点 A 的分组流。

图 9 展示了 GPRS 网络中本发明的应用，

图 10 展示了依照本发明的第四实施方案。

具体实施方式

依照本发明，对每个 IP 接口使用多个 VRF(VPN 路由/转发实体)。例如，IP 接口可以是双向 IP-中-IP 隧道或以太网上的 IP 接口。用于路由来自给定接口的业务的转发表不能路由业务到相同 IP 接口。这个区别使得能够让一个方向上的业务属于一个 VRF 而另一个方向上的业务属于另一 VRF。此外，如果接口有多个对等实体，每个对等终点可以属于不同的 VRF。

图 6 展示了本发明的第一实施方案，包括路由器 RT，它包括路由表 VRF_1 和 VRF_2 以及 IP 接口 IP_IF1，提供对 GTP 隧道 GTP_A 的访问，GTP_A 连接到第一个移动站 MS_A 和 IP 接口 IP_IF2，提供对第二个 GTP 隧道 GTP_B 的访问，GTP_B 连接到移动站 MS_B。该路由器还包括第三 IP 接口 IP_IF3，它连接到 GRE 隧道 GRE_RT，GRE_RT 提供到 VPN 访问网（例如公司内部网）的连接。

如箭头所示，转发表 VRF_1 根据给定分组的目标移动站路由来自 IP 接口 IP_IF3 的分组到 IP 接口 IP_IF1 和 IP_IF2。转发表 VRF_2 路由来自 MS_A 和 MS_B 的分组到 IP 接口 IP_IF3 并进而到 VPN 访问网。由此，移动站 MS_A 和 MS_B 之间的业务可以由 VPN 访问网控制。

图 7 展示了本发明的另一实施方案，其中第一个路由器 RT 通过

IP 接口 IP_IF1、IP_IF2、IP_IF3 连接到以太网段 ETH_S，形成了各自的虚拟专用网络 VLAN1、VLAN2 和 VLAN3，以及以太路由器接口 ETH_IF。该第一路由器包括第一转发表 VRF_1 和转发表 VRF_2。

节点 A 虚拟局域网 VLAN1 连接到路由器，节点 B 通过公共以太网段 ETH_S 上的虚拟局域网 VLAN2 连接到路由器。

第二路由器 R 包括连接公共以太网段 ETH_S 上的 VLAN3 的转发表。第二路由器还连接到互连网。

转发表 VRF_1 为目标 A 定义 IP 接口 IP_IF1 的下一次转发，为目标节点 B 定义 IP 接口 IF2。转发表 VRF_2 定义接口 IP_IF3 为默认的下次转发地址。转发表 VRF_R 为目标 A 和 B 都定义了 IP 接口 IPIF_3。

从移动站 A 发往 B 的分组被沿着箭头 10 经过 IP 接口 IPIF_1 转发到转发表 VRF_2，并接着被转发到 IP 接口 IPIF_3，再到路由器 R，箭头 20，然后再次回到 IP 接口 IPIF_3，并到达转发表 VRF_1。转发表 VRF_1 为目标 B 定义 IP 接口 IPIF_2 作为下次转发地址，接着分组被沿着箭头 30 传输到节点 B。

路由器被配置为，在一个接口 IP_IF1 上的移动站正在和另一接口 IP_IF2 上的移动站通信时，业务被通过第二个接口 IP_IF3 路由。

在图 8 中如箭头 40、50 和 60 所示展示了传输分组的相反路径。应该理解在数据链路层上可以使用许多其它技术。

如上所示，VRF 的转发表只有到属于该 VRF 的流出方向的接口的路由。哪个 VRF 用于转发决策是从接收接口的进入方向的 VRF 配置选择的。流出和进入两个方向上的接口定义都可以扩展成还考虑源和目标对等体（例如通过链路级地址识别）以允许多访问链路上的不同远程对等体（例如路由器）的不同 VRF。

进入和流出方向之间的差异提供了接口可由流出方向上的多个 VRF 使用的可能性。也就是说，若干个 VRF 可以使用相同的流出链路。图 7 中，展示了 VRF_1 和 VRF_2 怎样使用相同的流出链路，例如 IPIF_3。这个特性与基于广播和多播的服务在一起特别有用。一个例子是，它使得能够有独立的多播 VPN 提供几个其它 VPN 能够使用的多播服务。来自多播网络的业务可以被转发到服务的终端用户所连接的另一 VPN 中。这样做的好处是，网络间的公共服务可以使用一个公共

的能够更有效地利用传输链路的网络体系结构。多播网络这样被使用来得到更好的性能，但多播服务目前并不能在 VPN 之间共享，本发明为此提供了一个解决方案。

主发明所解决的 WPP 中的主要问题是它允许 GGSN 节点延迟到远程网络的分组过滤以降低 GGSN 节点的管理员对分组过滤配置的需要。本发明提供朝向外部网络的可扩展路由解决方案。

图 9 依照本发明展示了本发明的第三个优选实施方案，其中两个移动站 MS#1 和 MS#2 之间的业务，MS#1 和 MS#2 属于与拥有 VRF#23 的路由器相同的公司网络。VRF#37 和 VRF#42 用在 GGSN 中，VRF#23 用在路由器中。本发明用在 GGSN 中。对来自移动站的业务使用 VRF#42。对来自路由器的业务使用 VRF#37。VRF#42 有路由器作为转发表中所有路由的下一站。这意味着来自移动站的所有业务都被送往该路由器。VRF#37 有 SGSN(服务 GPRS 支持节点)作为两个移动站的下一站。这意味着来自路由器目标是移动站的业务被送往 SGSN。来自路由器目标不是移动站的业务被送回到路由器，因为 VRF#37 的转发表有一个默认路由指出该路由器作为目标不是移动站的所有业务的下一站。该路由器仅有一个 VRF (VRF#23) 用于所有它的接口。该路由器是一个普通路由器。从某个移动站发出目标是另一移动站的分组被通过 SSGN 送往 GGSN。GGSN 执行转发查找 (使用 VRF#42 的转发表) 并接着把分组路由到路由器。路由器执行转发检查并将业务路由返回 GGSN，因为 VRF#23 的转发表将 GGSN 指作移动站的下一跳转。该 GGSN 再一次进行转发查找 (使用 VRF#37 的转发表) 并随后把分组路由到 SGSN。SGSN 把分组发送到接收移动站。应该注意到，不属于公司网络的第三个移动站将不使用图 3 中所示的隧道。将设置另一平行组的隧道和转发表。

图 9 展示了怎样在不同的管理员之间划分网络管理责任。在这张图中，移动站 MS#1、MS#2 和拥有 VRF#23 的路由器属于相同的公司网络，称为“公司”，并且这个网络的所有管理都由该公司网络管理员负责。举例来说，第一运营商，运营商 1 控制 SGSN 节点，运营商 2 控制 GGSN 节点。在 GPRS 网络管理和公司网络的管理之间有明确的划分。这个例子还展示了，在适用时 SGSN 和 GGSN 运营商之间的划分。对运营商来说向公司网络提供服务是一个强烈的商业事件，使得公司

网络管理员能够为移动站配置分组过滤器并监控所有进出移动站的业务。因为对 GGSN 销售商来说向运营商提供实现本发明的设备是一个强烈的商业事件。应该注意到转发表 VRF#37 和 VRF#42 由运营商 2 依照公司和运营商 2 之间存在的无论什么协议来控制。

已经实现了路由分组到接口的相反方向的 VRF 的功能。如果要支持 ICMP 消息的话，这是有必要实现的。相反方向的 VRF 容易找到，因为 ICMP 消息是为流出接口产生的，并且随后可以像分组已经到达了那个接口那样处理分组。VRF 中的转发表可以由路由后台程序更新。

路由后台程序从不同的接口接收它们的路由信息并把这些接口看作属于不同的路由区域。通过分离这些接口的进入和流出方向，可以配置路由协议以过滤要发往不同接口的信息。由此，可以分离路由更新的方向；如果用于路由通知的路由协议支持双向链路的话。

本发明可以用于（例如）Ipv4 和 Ipv6。Ipv4 和 Ipv6 接口都可以是双向或单向的。本发明为路由器（或主机）提供把双向接口看作两个同时的单向接口的能力，因为对等路由器（或主机）把路由器（或主机）上的接口看成双向接口。换句话说，如果不希望以这种方式处理的话，周围的网络环境并不受使用本发明的影响。

本发明有很高的潜力解决 IP 路由的不同领域中的许多现有的和将来的问题，因为它是对 IP 路由和转发环境中怎样对待接口的一种基础改变。

缩写

ATM 异步传输模式

APN 在 GPRS 骨干网中，访问点名字（APN）是对 GGSN 的引用。为了支持 PLMN 内的漫游，内部 GPRS DNS 功能被用来转换 APN 到 GGSN 的 IP 地址。

GGSN 网关 GPRS 支持节点

GPRS 通用分组无线电服务

GSM 全球数字移动电话系统

ICMP 互连网控制消息协议（RFC 792）

IP 互连网协议（RFC 791）

IPIFIP 接口

SGSN 服务 GPRS 支持节点

TCP 传输控制协议 (RFC 793)

TCP/IP 协议组，包括 IP、TCP、UDP、ICMP 和其它协议

UDP 用户数据报协议 (RFC 768)

UMTS 通用移动电话系统

VPN 虚拟专用网络

VRFVPN 路由/转发实体

WPP 无线分组平台

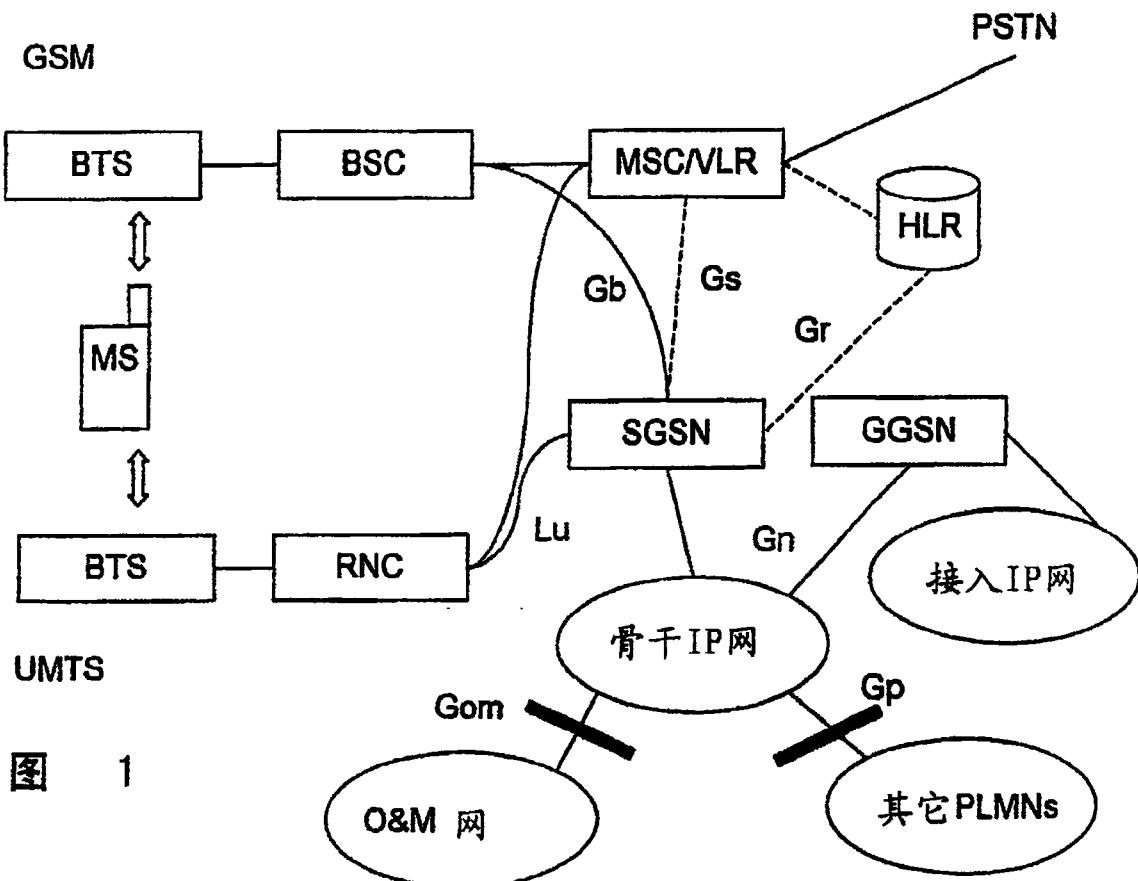


图 1

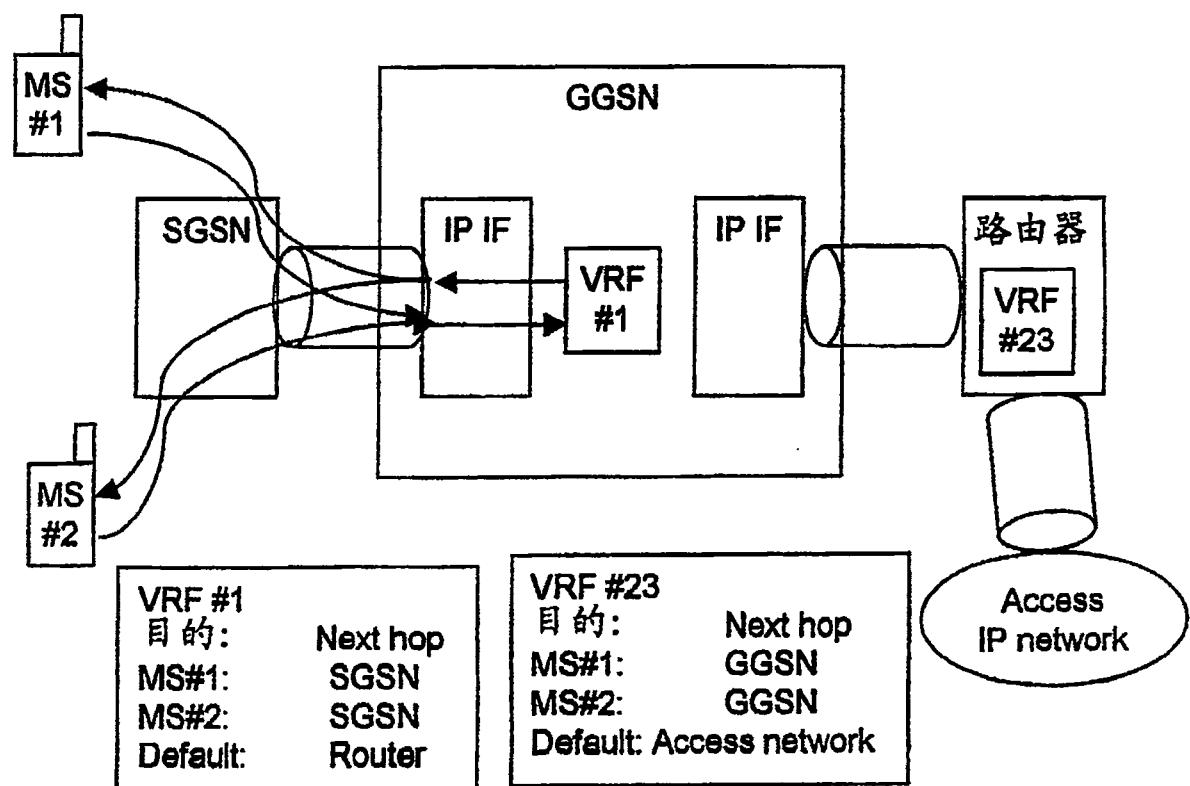


图 2

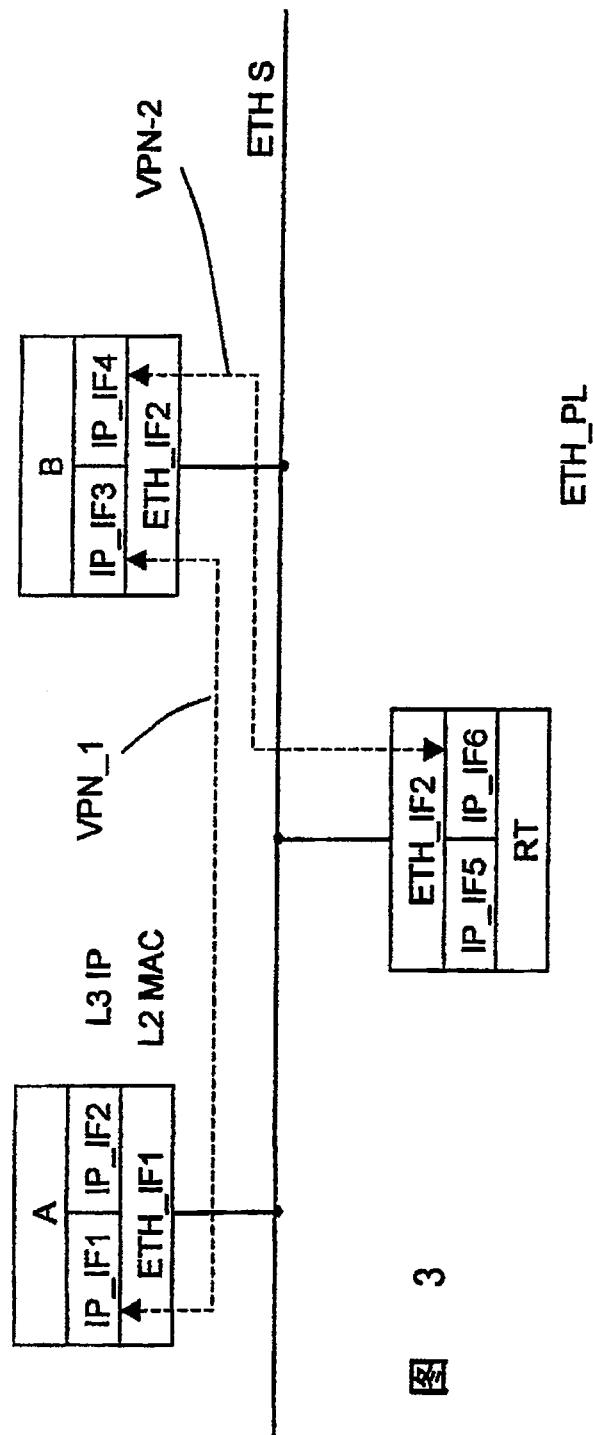


图 3

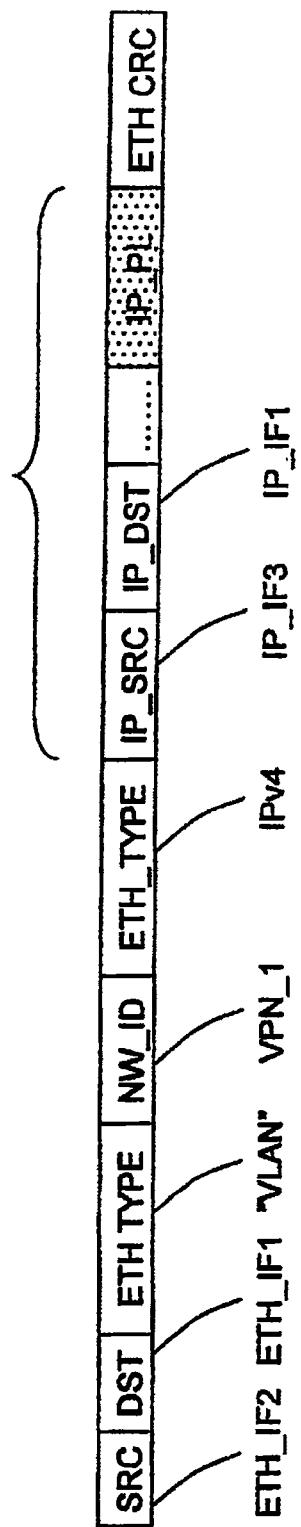


图 4

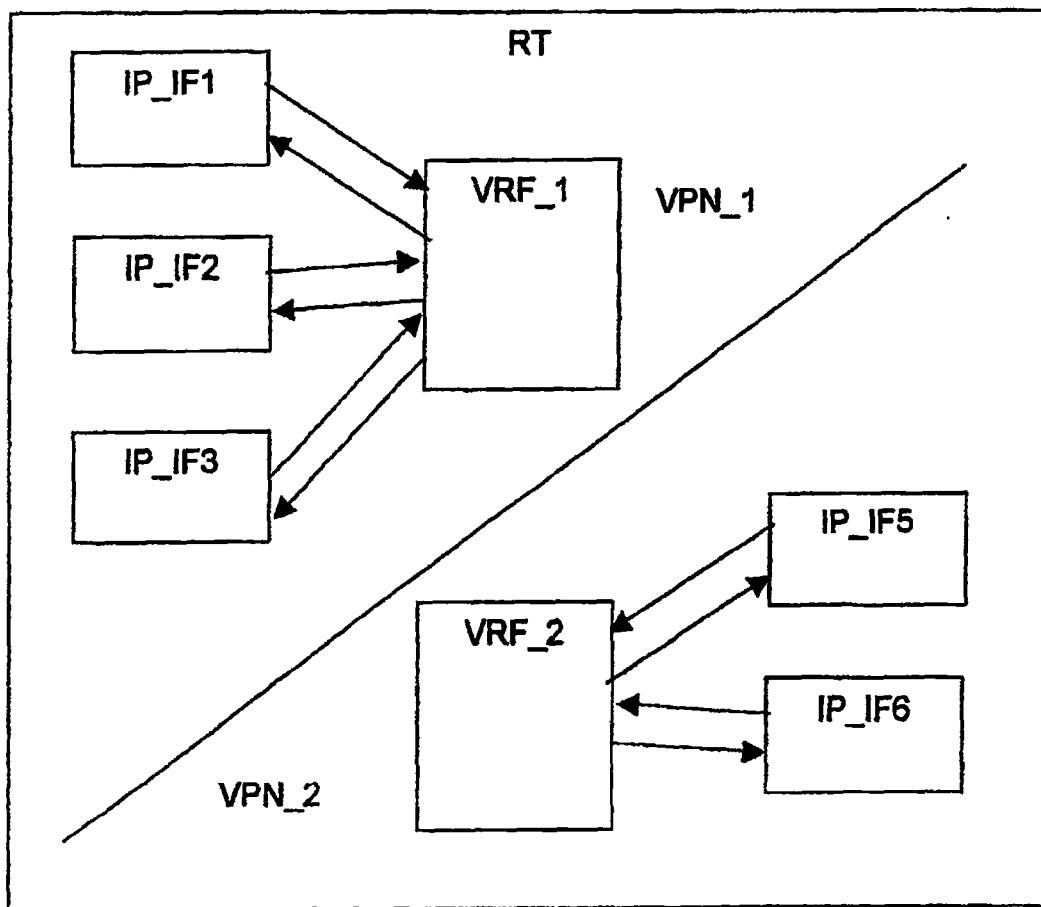


图 5 现有技术

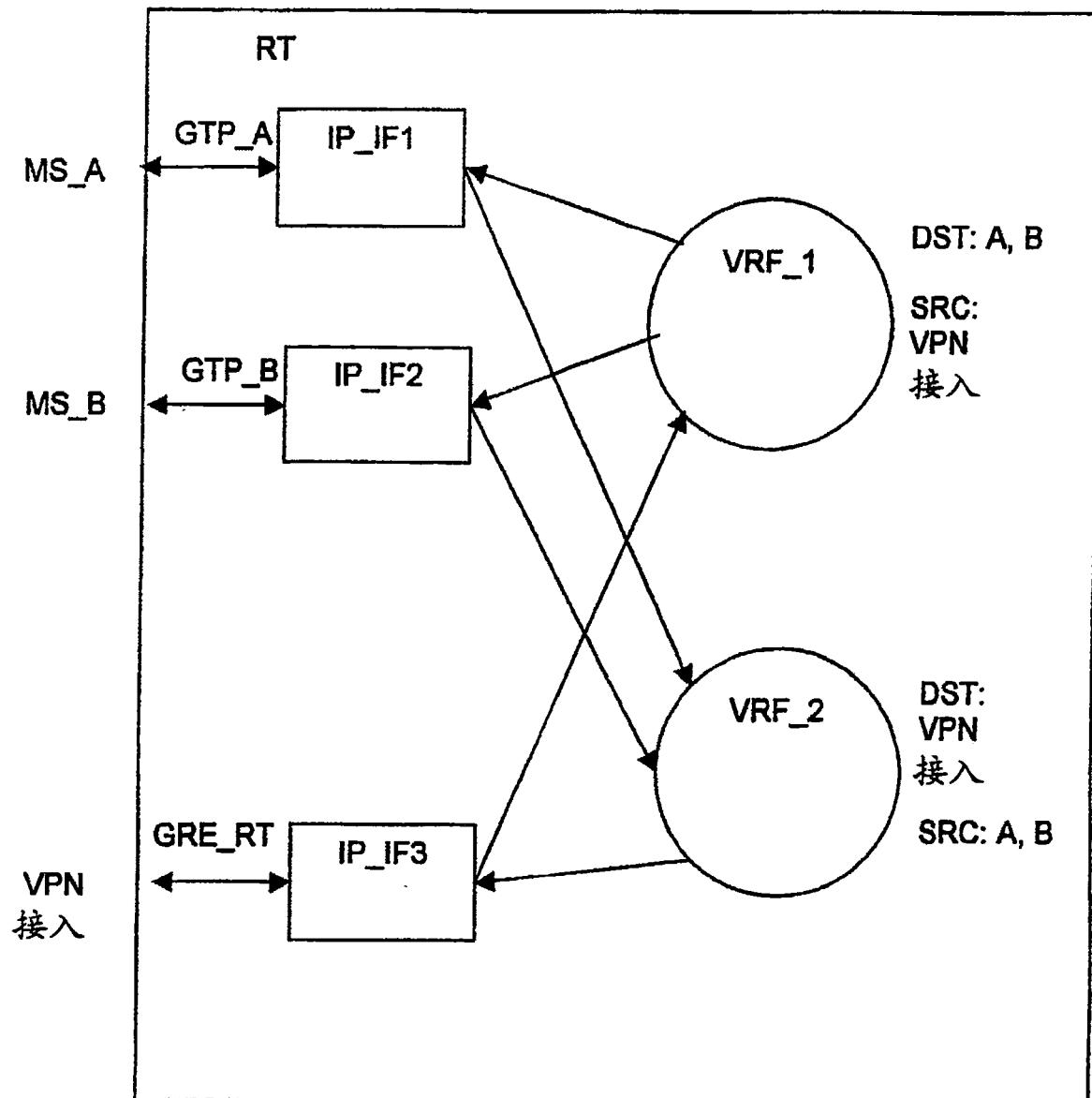


图 6

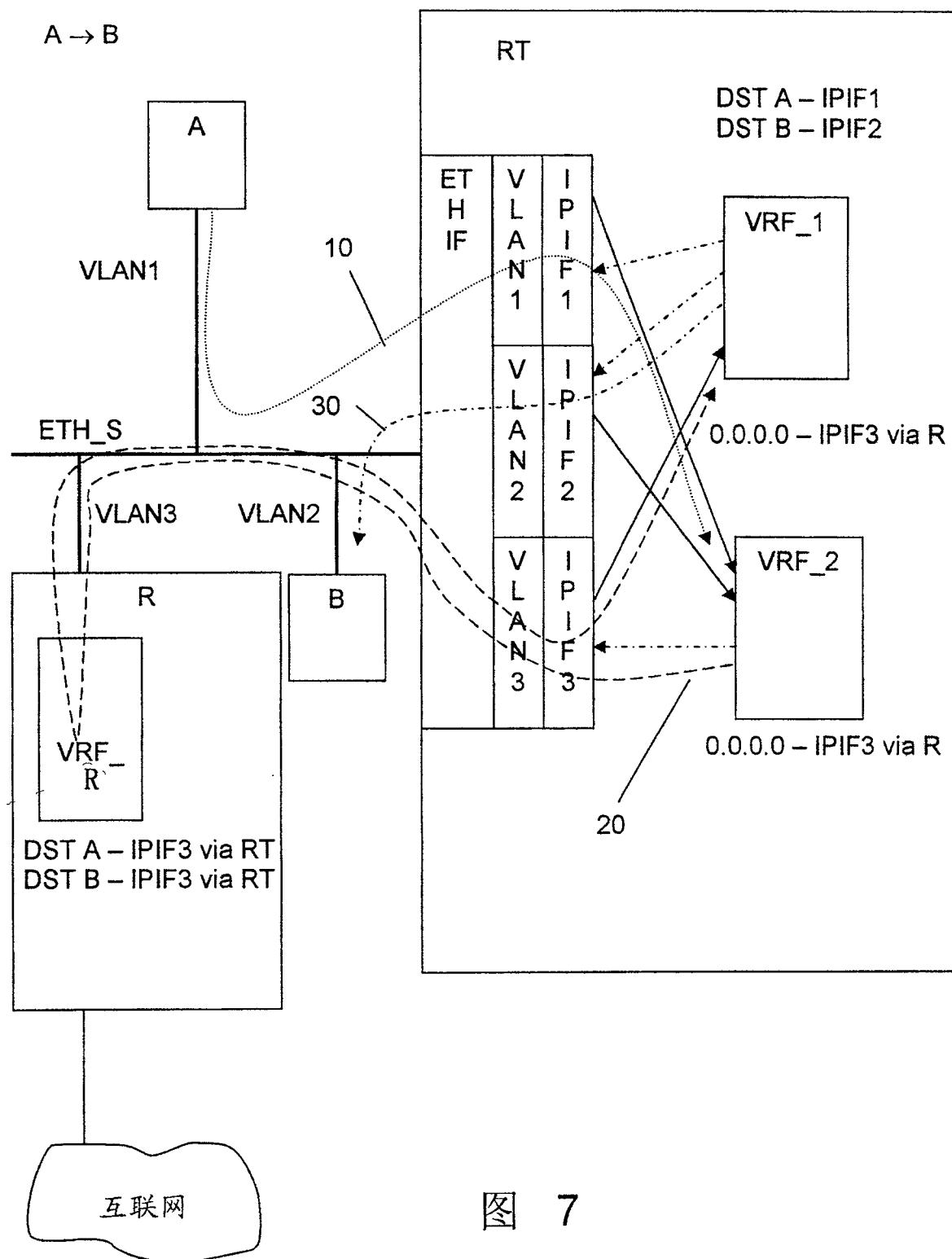


图 7

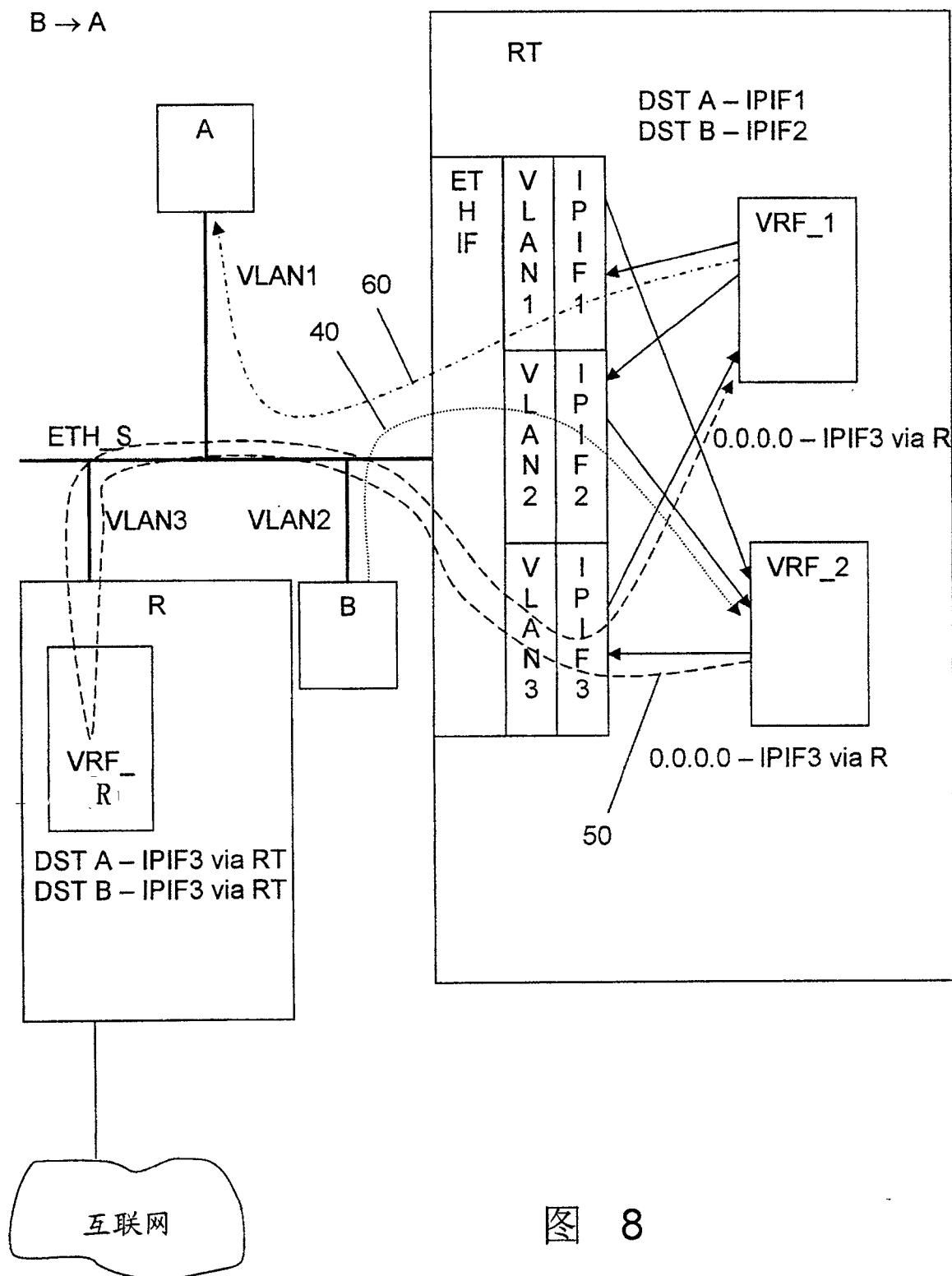


图 8

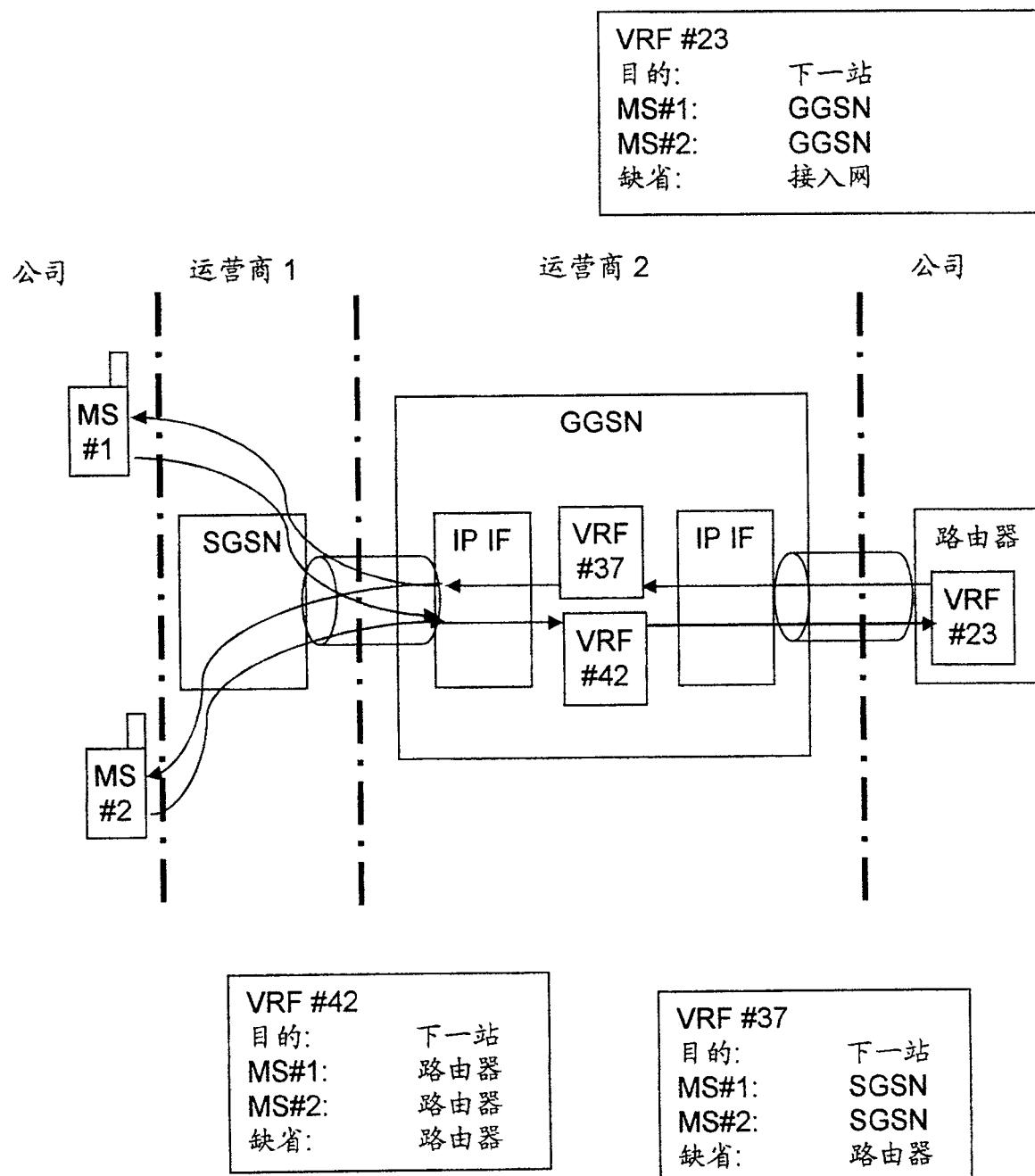


图 9

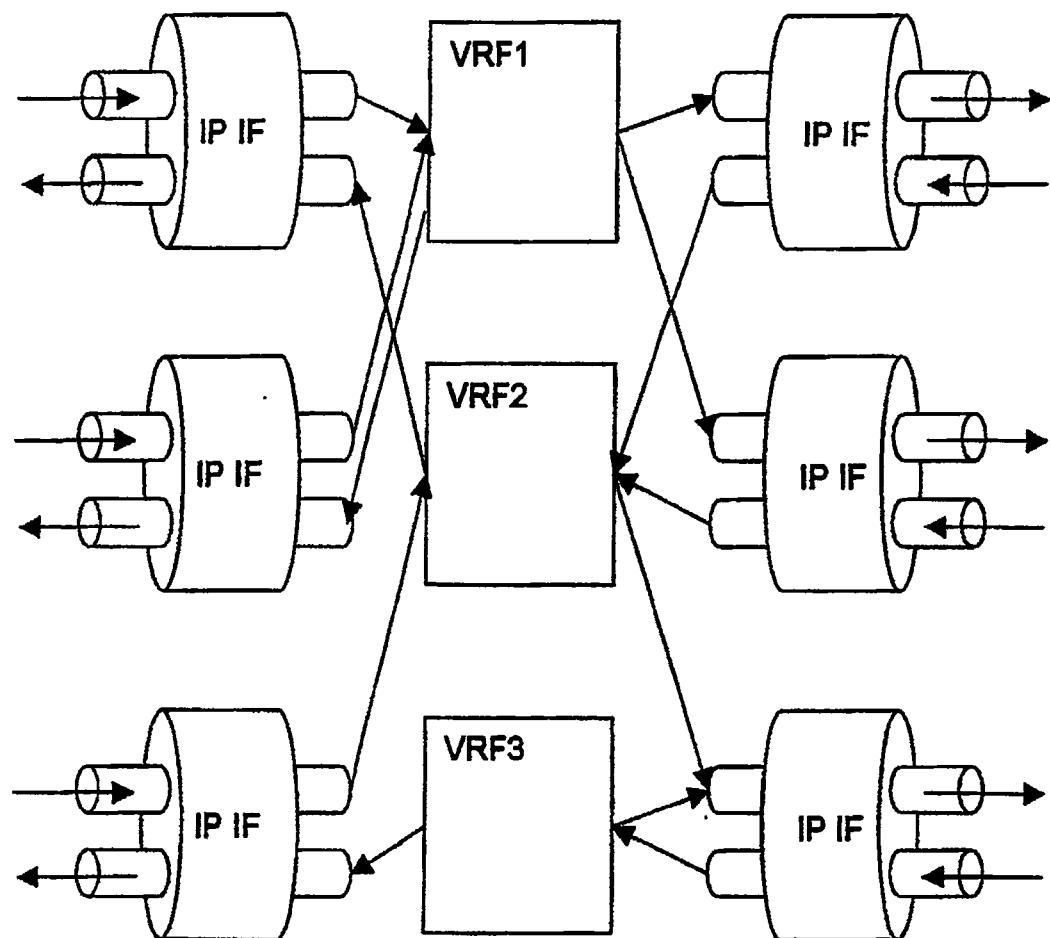


图 10