学位论文精选

基于 IP 骨干网的虚拟专用网理论与实现

李秀忠
（信息产业部电信科学技术研究院，北京 100088）

[摘要] 讨论了虚拟专用网（VPN），尤其是 IP－VPN 的相关方面。在此基础上分析了 IP－VPN 的虚拟专用路由网（VPRN）和虚拟专用局域网（VPLS）两种类型。着重讨论了 VPRN 的两种实现机制——边界网关协议/多协议标记交换（BGP/MPLS）和虚拟路由器（VR），并进行了比较。实现了一种 VPLS——虚拟局域网（VLAN）。最后从理论上探讨了基于网络的 VPN 的服务质量（QoS）并提出了一种 VPN QoS 的实现途径。

[关键词] 虚拟专用路由网（VPRN）；虚拟专用局域网段（VPLS）；边界网关协议/多协议标记交换（BGP/MPLS）；虚拟路由器（VR）；最坏情况加权公平排队（WF^2Q）；随机早期检测（RED）
[中图分类号] TP393 [文献标识码] A [文章编号] 1009－1742（2002）03－0084－08

1 VPN 综述

随着网络尤其是网络经济的发展，企业规模日益扩大，客户分布日益广泛，合作伙伴日益增多，于是企业在自身网络的灵活性、安全性、经济性、扩展性等方面提出了更高的要求。虚拟专用网（VPN）以其独具特色的优势，赢得了越来越多的企业青睐。

1.1 VPN 应用分析

虚拟专用网（VPN），指利用公共的网络设施（包括公共因特网及服务提供商（SP）的传输网）来模拟专用网络的技术总称。从逻辑上看，VPN 是叠加在公共网络之上的专用网络。

VPN 代表了当今网络发展的最新趋势，它综合了传统数据网络安全和服务质量（QoS）的性能优点和共享数据网络结构简单与低成本的特点，能够提供远程访问，外部网和内部网的连接，价格比专线或者帧中继网络要低得多。而且，VPN 在降低成本的同时满足了对网络带宽、接入和服务不断增加的需求，因此，VPN 必将成为未来企业传输业务的主要工具。

1.2 IP－VPN[1]

实现 VPN 功能可以有几种机制，通常依据 VPN 使用的隧道机制可以分为下面两种：

1）建立在链路层虚连接（异步转移模式（ATM）的永久虚电路（PVC），帧中继（FR））基础上的 VPN；

2）基于 IP 隧道的 VPN，VPN 通过网络层隧道通信。

IP－VPN 定义为：在 IP 骨干网络上模拟专有的广域网（WAN）。IP 骨干网络包括 Internet 和服务提供商（SP）的 IP 骨干网。

利用公共 IP 骨干来组建 VPN，要求 IP－VPN 实现机制能够满足客户的应用需求，它包括以下方面：

1）*VPN 内传输的数据与承载 VPN 的 IP 骨干数据无关* 因为 VPN 的数据有可能是多协议的（非 IP），还有 VPN 内采用的 IP 地址并不是全球统一分配的唯一的地址[2]。

2）*数据安全* 使用 VPN 的客户要求某种等级的数据安全。

3）*QoS 保证* 在租用线专网和基于 PVC 的

[收稿日期] 2001－10－11；修回日期 2001－11－16
[作者简介] 李秀忠（1977－），男，山西交口县人，硕士，信息产业部电信科学技术研究院助理工程师

VPN，用户从 SP 可以得到带宽和延迟的保证，在 IP－VPN 下，客户也有相应的 QoS 要求。

IP－VPN 有几种分类方法，分别对应于不同的情况。

1）基于客户端设备（CPE）和基于网络 VPN 的划分，并非出于技术的考虑，而主要是依据 SP 和 VPN 客户之间对于维护 VPN 运作的责任划分。这种不同的划分或多或少引起了技术差异。基于 CPE 的 VPN，VPN 的功能主要集中到各种各样的客户端设备，例如防火、边缘路由器或者专门的 VPN 终端设备。在这种情况下，VPN 的运行通常是由用户自己来维护，SP 仅提供传输基础。基于网络的 VPN，VPN 的运行由 SP 来维护，VPN 的功能也集中在 SP 的骨干设备上（如骨干网的接入路由器）。

2）根据 VPN 的应用范围，可以有接入（Access）VPN，内联网（Intranet）VPN，外联网（Extranet）VPN。

3）根据 IP－VPN 实现的具体机制，依据 SP 边缘设备所起的作用的不同，可以有如下划分：

·虚拟租用线（VLL）　SP 边缘设备在进入链路和出去的隧道之间作简单的映射而不察看数据包的内容。

·虚拟专用路由网（VPRN）　提供商边缘（PE）设备执行路由功能，具体说，PE 对进入的 VPN 数据包察看其第三层信息（可能还需要其他信息以区分不同的 VPN），并在此基础上做出路由转发决策，将数据导向合适的出去隧道。

·虚拟专用拨号网（VPDN）　其应用对象为移动办公用户。VPDN 利用公用电话网（PSTN）建立到 SP 的网络接入服务器（NAS）的点到点协议（PPP）会话，SP NAS 利用诸如二层传输协议（L2TP）等隧道协议将该会话延伸至企业网 NAS。

·虚拟专用局域网段（VPLS）　与 VPRN 相比，在 VPLS 中 PE 设备执行桥接功能而非路由功能，具体说，PE 对进入的包的转发决策是建立在其第二层信息（可能还需要其他信息以区分不同的 VPN）的基础上。

2　VPRN 及其两种实现机制

VPRN 是对广域路由网的模拟。在 SP 骨干网上，VPRN 包括执行路由转发功能的 SP PE 路由器，以及连接这些路由器的 IP 隧道构成的网格（见图 1）。

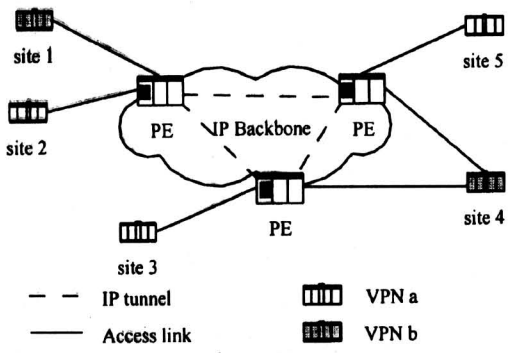

图 1　虚拟专用路由网络参考模型

Fig.1　VPRN reference model

2.1　VPRN 实现需要考虑的几个方面

VPRN 实现需要考虑的一些问题：

1）VPN IP 地址空间专有问题　多个 VPN 以及 SP 骨干网可能使用重叠的 IP 地址。PE 服务于多个 VPN，故需要一种机制来保证各 VPN，以及 SP IP 骨干的 IP 地址空间相互独立。

2）VPN 拓扑　根据不同的应用需求，可能要求不同的 VPN 内部拓扑。如全连接拓扑或 Hub-Spoke 拓扑。

3）数据包转发　由于 PE 为多个 VPN 复用，故必须有一种机制确保 VPN 内的数据不会泄漏到其他 VPN。

4）构建 Extranet 和多种接入模式　VPN 的实现机制需要提供方便组建多个 VPN 之间的 Extranet 的能力。多种接入模式意味着实现机制可以容纳用户节点与提供服务的骨干网的多种连接关系。

基于网络的 VPN 的实现有两种基本的结构，BGP/MPLS 和 VR。

2.2　BGP/MPLS VPN[3]——VPRN 实现之一

在这种实现机制中，多协议标记交换（MPLS）作为骨干网上的隧道机制，使用边界网关协议（BGP）在 VPN 内各节点之间交换路由信息。

该机制中，PE 维护若干相互独立的路由表，接入 PE 的不同的 VPN 节点使用不同的路由表，从而实现数据转发的独立。至于各个 VPN 的路由信息则是通过各个 PE 运行 BGP 实体来维护的。VPN 信息对 SP 网络的核心设备是透明的。

为了适应 VPN 的应用需求，对 BGP 作了若干

扩展：

1）VPN－IPV4 Address Family　PE 上多个 VPN 共用一个 BGP 实体来交换路由信息，为此引入了一种新的地址格式——VPN－IPV4 Address[4]，从而使得 BGP 实体可以处理不同 VPN 内地址重叠的问题。它并不代表路由的来源，也不控制路由的再分配。VPN 数据转发时，只考虑 IP 地址部分。

2）BGP 路由属性和路由过滤　BGP 路由属性是描述一个路由特性的一套参数。输入过滤、决策以及输出过滤都是基于路由属性。为支持 VPN，引入了一个路由属性——路由目标（RT）。RT 属性标志一列节点，通过 RT 属性可以控制 VPN 内的路由不会被扩散到其他 VPN 内。

MPLS 实现了包转发决策与包头内容分离，因此也可以作为一种隧道机制。在 VPN 中使用 MPLS 作为隧道机制，可以利用 MPLS 对流量工程的支持来实现 VPN 的 QoS。

在控制平面，用户设备（CE）与 PE 之间通过各种途径（如外部边界网关协议（EBGP），路由信息协议（RIP），开放最短路径优先（OSPF），静态路由）交换路由信息。PE 之间通过内部边界网关协议（IBGP）交换 VPN 路由信息。需要正确配置接入 PE 的各个客户节点使用的 RT 属性以避免 VPN 之间的信息泄漏。在数据平面，各个客户节点进入的数据包根据其进入接口决定其使用的转发表。在转发表中查找到下一跳信息并进行转发。

此外，该机制还需要考虑 VPN 隧道的复用以及跨越多个 SP 的 VPN 等。

2.3　虚拟路由器（VR）——VPRN 实现之二

在这种机制中，VPN SP 为每个 VPN 提供一组位于 PE 上的 VR 以及连接 VR 的隧道，VR 之间运行普通路由协议（例如 RIP，OSPF 或 BGP）来通告 VPN NLRI 信息。采用其他机制来通告 VPN 成员信息。

虚拟路由器，虚拟表示 VR 是逻辑上的而不是一个单独的物理设备，但具有实际路由器的功能，包括路由维护功能、转发功能、接入控制功能甚至 VR 之间的固定带宽的连接。

在实现时，PE 上的一个 VR 表现为一个路由实体，可以采用进程或线程来实现（见图 2）。VR 是对物理路由器在软件和硬件上的模拟。具体讲，需要有路由功能、转发功能、接入控制功能以及管理与配置。

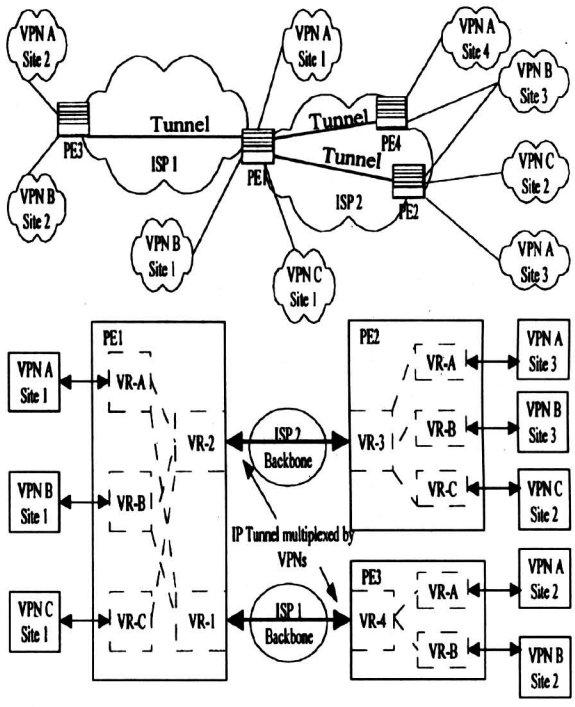

图 2　虚拟路由器参考模型

Fig.2　VR reference model

在 SP 的骨干网，虚拟路由器仅存在于 PE，VR 与 VR 之间的连通性可以利用第二层虚连接或利用 IP 隧道。采用 IP 隧道机制跨越 SP 骨干网，要求对 SP 骨干网拓扑的了解，因此，每个 PE 还需为 SP 骨干网维护一个路由实体（图 2 中的 VR1，2，3，4）。

VPN 的成员信息指 SP 网中包含某一特定 VPN 的 VR 的一组 PE。VPN 的拓扑信息指某一特定 VPN 的一组 VR 之间的连接关系。在 VR 方案中，成员信息和拓扑信息的发现机制是分离的（在 BGP/MPLS 中，二者都是借助于 BGP 及其扩展协议而实现的）。

对于 VPN 成员信息的发现，可以通过目录服务器、详细的管理配置，也可以利用骨干网现有路由协议的扩展，来捎带 VPN 信息（例如 BGP）。对于拓扑信息，只要 VPN 的成员关系确定后，即可借助于 VR 间使用的路由协议来建立 VR 路由会话从而交换 VPN 拓扑信息。

2.4　VPRN 总结以及两种实现机制的比较

如上所述，VPRN 的关键在于 SP PE 执行路由转发功能，路由转发涉及到数据平面和控制平

面。控制平面负责维护拓扑信息，控制数据流向。数据平面执行转发功能。在 VPN 环境下，各平面基本功能未变，但需考虑一些相关方面。在控制平面，需要明确各 VPN 的成员，还需要为 PE 上的各个 VPN 逻辑上划分相关资源并且隔离各 VPN 的相关资源，做到各 VPN 之间互不影响。这些资源包括路由信息的通告机制、路由信息表、转发实体、带宽资源。考虑到安全和 QoS 问题，可能还包括各个 VPN 的接入控制策略、数据的安全封装格式、与每个 VPN 客户的 SLA 以及对 VPN 客户数据流的监控等。在数据平面上，任务比较简单，对进入的包映射到正确的 VPN 转发实体进行处理。由此可见，BGP/MPLS 和 VR 两种机制的主要区别不在数据平面而在控制平面，而且主要是在路由信息（拓扑信息）的通告机制上。

对于 VPN 成员关系的确定，BGP/MPLS 直接采用 BGP 协议捎带。VR 没有详细规定一种具体方案，而是列出了几种可选方案，BGP 协议捎带是其中一种。其他方面，诸如路由信息表、转发实体、带宽资源等，两种机制并无明显差别，至少逻辑上表现不出任何差别，其实现机制依具体情况而定。

但是，在路由信息的通告机制上，二者有根本的区别。BGP/MPLS 中，扩展的 BGP 协议被用来通告拓扑信息，而且多个 VPN 共用一个 BGP 协议实体，通过特殊的 BGP 属性 RT，在逻辑上隔离各个 VPN。而在 VR 机制中，引入了 VR 概念，使各个 VPN 的路由信息通告机制隔离得更加彻底，而不仅仅是逻辑上的表现，从而实现了更大的灵活性，允许各 VPN 使用自身的路由协议而互不相关。

上述二者的区别导致了实现机制上的差异。BGP/MPLS 的实现主要是对 BGP 现有协议的扩展。而 VR 的实现则要麻烦得多，需要在一个物理路由器上采用软件技术构造出多个并行的具有实际路由器功能（软件方面：路由信息维护，数据包转发；硬件方面：各种数据接口）的虚拟路由器。涉及到 VR 的动态创建和管理，而且各个 VR 可以动态加载各种路由协议（RIP，OSPF，BGP 等）。

由此可以看出二者的优劣：VR 机制概念清晰，用户容易理解，而且便于以后 VPN 业务的扩展。但缺点是实现较为困难，尤其是在需要支持大量 VR 时（例如 1 000 数量级）；而 BGP/MPLS 实现较为容易，但概念上不如 VR 清晰，而且 VPN 业务的扩展也不方便。

3　VPLS 及其实现——虚拟局域网（VLAN）

VPLS 基本特征在于其数据转发决策基于链路层信息。因此，SP 网络的 PE 设备执行桥接功能。VPLS 利用 SP 的骨干网设施或 Internet 来模拟局域网段。VPLS 服务的一个重要特性便在于其对于协议（网络层以上协议）是透明的，这对企业节点之间的多协议传输是很重要的。

3.1　VPLS 概述

VPLS 实现有其特殊要求。首先，VPLS 隧道中传输的是链路层帧格式而非网络层数据包。其次 PE 执行桥接功能，因此生成树算法（STA）也应被激活来避免环路。还有鉴于广播功能在桥接中的重要性，执行桥接功能的 VPLS PE 必须具有广播的能力。此外，需要某种机制来保证 VPLS 内的数据不会泄漏。但与 VPRN 不同的是，VPLS 的地址是全球唯一，不会重叠的。因此，在具体实现时，无需为每个 VPLS 单独维护一个转发表。VPLS 之间的隔离要求做到：在物理上，一个 VPLS 的帧不会出现在另一个 VPLS 的网段上。

VPRN 和 VPLS 的根本区别在于 VPLS 中 PE 执行桥接而 VPRN 中 PE 执行路由功能。二者的应用范围也不同，其主要差异：

1）VPLS 基于第二层信息，故其扩展性不好；VPRN 基于第三层信息，扩展性好。

2）VPRN 只能用于 IP 网络；而 VPLS 对于多协议网络以及非 IP 网络是合适的。

3.2　VPLS 实现——VLAN

VLAN 是一种在链路层划分广播域的技术。通过 VLAN 来划分广播域，可以充分考虑应用需求，从而使得广播域的分布与流量的分布相吻合。当然，VLAN 还有其他方面的优势：例如提高安全性能，简化网络配置等。但从应用角度来看，VLAN 可以作为 VPLS 的一种实现机制。

VLAN 划分的依据有多种，常见的有基于端口、基于链路层地址、基于网络层协议等。基于端口是最基本的一种[5]，文中 VLAN 的实现属于这一类的。

基于端口的 VLAN 划分原则很简单，即通过管理配置或其他手段将 VLAN 桥的某几个端口组

成一个 VLAN，VLAN 可以包括多个本地桥，也可以通过 WAN 扩展到其他远端桥。

VLAN 不仅仅限于一个设备，而应该可以通过上连端口扩展到多个 VLAN 桥设备。多个设备可能跨越 WAN。这种应用正符合 VPLS 的概念。此时，一个 VLAN 即可视为一个 VPN。VPN 节点的 CPE 设备接入 VLAN 桥的一个端口，将同一 VPN 的节点接入的所有桥端口配置为一个 VLAN。

下面简单介绍一种已经产品化了的基于端口的 VLAN。这也是笔者所做的主要工作。

作为桥设备，用户的管理对象为端口，端口有两种类型：**a.** 提供以太网接入的 10/100 Mb/s 自适应端口。**b.** 提供上联的逻辑端口，提供与远端设备的互连。

VLAN 转发模块结构图见图 3，下面对各模块功能作简单介绍。

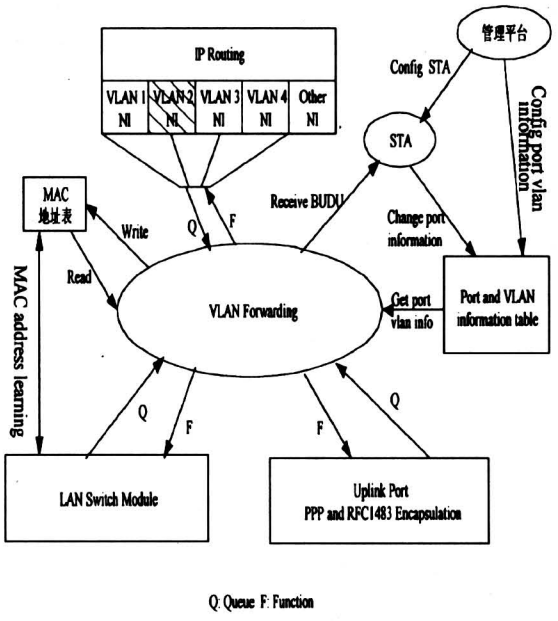

图 3 虚拟局域网模块图

Fig.3 VLAN module

1）VLAN Forwarding 该模块为业务处理核心模块，负责从上联端口、以太端口，以及网络层进入的帧处理，全部体现 VLAN 的转发原则。

2）LAN Switch 该模块负责本地以太端口的业务接入和交换，同时负责 MAC 表的维护。

3）Uplink Module 该模块负责与其他设备的互连。

4）IP Routing 模块 该模块负责不同 VLAN 间的通信。此外，该模块可以作为 VLAN 的缺省网关，从而满足与其他网络互连的需求。

5）STA 避免桥接环境下的环路问题。

6）管理平面 管理和配置。

7）MAC 地址表 该模块负责 MAC 地址信息的维护，包括本地和远端的 MAC 地址，其对应的端口和端口 VLAN 属性。

4 基于网络 VPN 的 QoS——基于 MPLS

VPN 在提供灵活的连通性的同时，必须具有与专线相当的 QoS 和安全特性。

4.1 基于网络 VPN 下客户 QoS 需求

在基于 CPE 的 VPN 情况下（图 4a），其通信模式是节点对节点的，节点之间通常为全连接拓扑。提供的 QoS 有如下特点：提供节点到节点的固定带宽，固定延迟的连接。这种情况下，各节点之间的流量分配由用户来规划，用户数据流的不确定性仅表现在时间上。服务商实行收费和分配资源就相对容易得多。

而在基于网络的 VPN 下，节点通过一种连接形式接入 PE（见图 4b），用户去往 VPN 内所有其他节点的数据都由该连接进入骨干网，此时，VPN 内流量分布的不确定性需要 SP 来处理。即 SP 需要根据 VPN 内流量的分布动态调整网络资源。用户数据流的不确定性不仅表现在时间上，而且表现在空间上。这样的用户数据流是难以估计的，因此，为该用户预留资源、保证其 QoS 以及

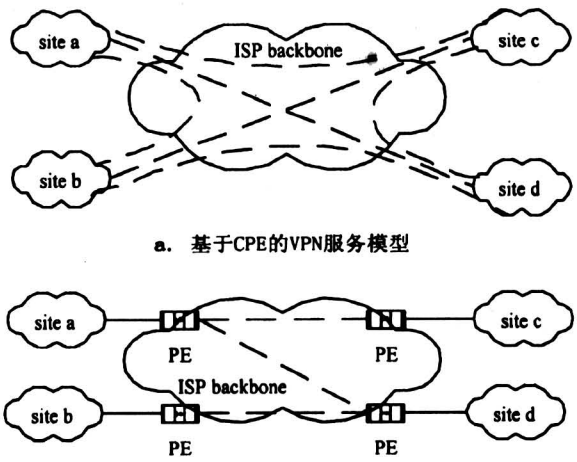

图 4 两种 VPN 的不同服务模式

Fig.4 Two different VPN service mode

收费等均相对困难。

虽然后一种服务模式为 ISP 的管理提出了很大的挑战，但是这种方式对用户的益处是显而易见的：

1）用户不需要详细指明各节点之间的流量分配。

2）这种服务模式可以为用户取得复用效益。

此外用户对 VPN 的需求不仅仅是 Best-effort，这就要求 IP－VPN 可以同时提供多种 QoS 要求的服务。

通过上面对 IP－VPN 的需求分析，可以看出实现基于网络 VPN QoS 需要解决的两个主要方面：

1）估计用户流量在时间和空间上的不确定性，并动态调整网络资源以适应用户流量分布。

2）满足用户对多种 QoS 服务的要求。

4.2　基于网络 VPN QoS 实现

要实现上述两个目标，在很大程度上依赖于 SP 的骨干网对 QoS 的支持能力。假设骨干网具有以下能力：

1）可以同时支持具有不同 QoS 需求的业务。

2）提供动态调整网络资源的手段。

VPN QoS 需要解决的主要问题在于：

1）在 VPN 接入点根据 VPN SLA 对 VPN 数据进行接入控制。

2）根据 VPN 内数据流的动态分布而调整 SP 骨干网络的资源分配。

3）对各服务类型的数据流应用合适的调度策略满足其 QoS。

下面讨论一种解决基于网络 VPN QoS 的方法。假设客户可以通过 VPN 传输具有不同 QoS 要求的数据，如 Best-effort 流，可靠的数据流、语音流、图像传输等。

4.2.1　*方案总体结构*　在该方案中（见图 5），假定 SP 核心为支持流量工程能力的 MPLS 网络，主要的组成有 MPLS 边缘 PE、核心标记交换路由器（LSR）、资源管理器（RM）。

在这个结构中，PE 作为 VPN 接入设备，同时又是 MPLS 域的边缘设备，需要执行以下功能：

1）作为 VPN 接入设备，可以处理 VPN 客户的资源请求，根据现有网络资源的使用情况决定是否接纳该连接。

2）作为 VPN 域的边缘设备，需要具有对用户数据流的监视、分类、标记、整形/丢弃。

3）为了满足不同业务的 QoS，应具有差分服务（DiffServ）功能，具有支持 EF－PHB 和 AS－PHB Group 的各个类的能力[6,7]，并且提供动态配置各个 PHB 占用资源的能力。

4）作为 MPLS 边缘设备，需要执行其相应的功能。

5）根据测量得到的当前各 DS－PHB 的流量分布动态调整它们之间的带宽分配。

6）提供接口供 RM 查询网络资源的使用情况，或定期向 RM 报告资源占用状况。

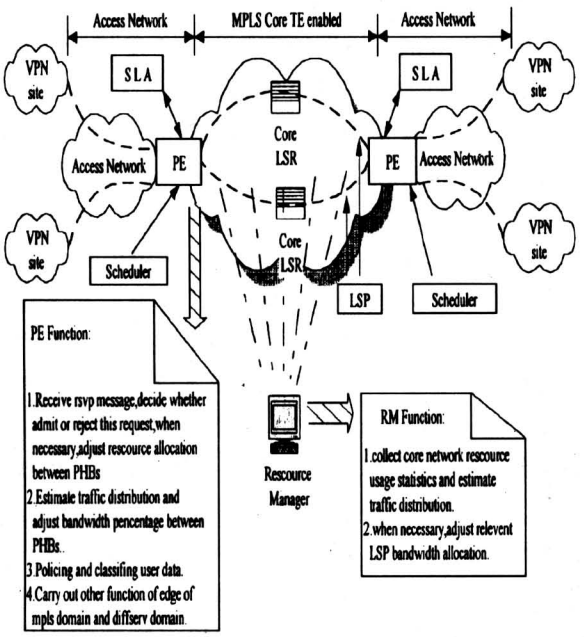

图 5　基于网络 VPN QoS 框架结构

Fig.5　Network-based VPN QoS framework

核心设备为支持差分服务功能的 MPLS 标记交换路由器，具有以下功能：

1）支持 MPLS 以及已定义的流量工程[8]；

2）提供接口供 RM 查询网络资源的使用情况，或者定期向 RM 报告资源占用状况。

资源管理服务器监视 SP 骨干网的当前资源占用状况。根据历史纪录预测网络流量分布，并通过 MPLS 流量工程（TE），调节 PE 之间标记交换路径（LSP）的资源分配和 LSP 的路径。

该方案中，隧道复用不仅在不同的 VPN 流之间，而且也在不同的差分服务转发行为等价类（DS－PHB）之间。隧道复用可以取得明显的优

势：

1）骨干网络标记空间的有效利用和标记空间的使用状况稳定，不会因支持的VPN数目和DS-PHB数目变化而变化。

2）复用带来了数据流量分布的相对稳定，从而为骨干网资源管理带来方便。如上所述，VPN单个用户的流量分布具有不可预测性，但不同用户的数据流复用到一个隧道上，以隧道为资源控制单元。那么，复用流表现出来的统计特性相对平稳。

3）不同的DS-PHB流复用到一个隧道上，方便带宽资源在各PHB之间的分配。从而可以在本地完成资源分配而无需RM调整隧道的带宽。

由上可以看出，为适应VPN流量分布的变化，网络资源的动态调节发生在两个层次上，首先是RM根据目前网络的资源情况以及VPN流量分布的预测，对骨干网络VPN隧道——LSP的资源进行调节。RM的调节发生在较长的时段，主要解决由确定性原因引起的流量分布变化。其次就是PE本地的资源调节，即根据当前各PHB的流量动态改变它们之间的资源分配。PE本地调节发生在较短的时段，解决的主要是随机的流量分布变化。

4.2.2 PE资源分配实现机制以及流量分布预测

PE的重要性不言而喻，其功能结构图见图6。其中流量分布预测和资源分配主要是解决各PHB复用一条LSP，并且满足相应的要求。在此，经过比较各种包调度策略、包丢弃规则以及流量分布预测机制，笔者提出了一种流量预测和调度结构，见图7。该调度结构位于每个输出接口（物理的和虚拟的）上。

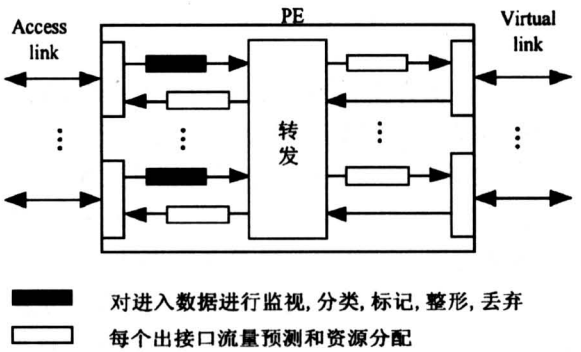

图6 PE功能结构图

Fig.6 PE function chart

其中对EF-PHB采用最大值预测器，而AF-PHB则采用高斯预测器。预测结果控制各个队列的调度权值。采用最坏情况加权公平排队（WF^2Q）规则，对EF-PHB队列实行尾丢弃（DT），而对于AF-PHB实行随机早期检测（RED），并且每个AF-PHB支持三个丢弃级别。

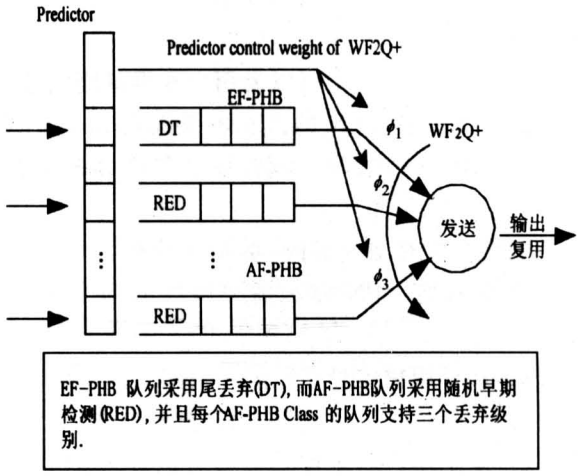

图7 本方案中的服务模型

Fig.7 Service model in our solution

对预测器的选择考虑：因为EF-PHB类流通常为实时业务，故对该类业务采用最大值预测器。虽然可能导致过分配，但由于WF^2Q规则可以实现资源的共享，因此不会浪费资源。而AF-PHB各类通常为数据业务，暂时的拥塞不会影响其性能，故采用高斯预测器。

包调度规则通过分配两种本地资源来影响各类业务的性能：通过分配出链路带宽来影响业务流量，通过每个包的服务时间来影响业务的时延。目前已经提出了多种包调度规则，性能各有优劣。具体的分析可以参见文献[9, 10]。其中WF^2Q规则具有较好的性能，而且具有工程上可行的算法WF^2Q+，因此采用WF^2Q调度规则。

队列调度机制仅能影响业务流量和时延，而丢包率则依赖于本地缓存资源的管理，需要利用包丢弃规则。此外，对于TCP流，包丢弃规则也是一种重要的网关拥塞避免机制。目前已有的机制有：尾丢弃（DT），随机丢弃（RD），随机早期检测（RED），性能分析可以参见文献[11]。在图7的方案中，EF-PHB主要支持语音或图像流，通常使用的不是TCP协议。故而，对于EF-PHB使用了DT。而AF-PHB提供不同等级的数据业务，故利用RED来保证AF-PHB Group中每一类的不同

丢弃级别的行为。

5　结语

VPN 的涵盖面非常广，而且 VPN 本身并不仅是一个技术上的概念，更多地是一个服务上的概念，现有标准更多规定了 VPN 服务应满足的需求，而对其实现机制则规定较少。在这种情况下，不同 VPN 实现机制的互通是非常重要的。此外，IP－VPN 提供的 QoS 目前仍未达到专线的水平，这将大大制约 IP－VPN 的市场发展。笔者虽然提出了一种可能的实现机制，但其有效性仍有待下一步实现工作进行检验和修正。还有一些文中未涉及但对于 VPN 服务至关重要的方面：VPN 的管理、计费和安全也有待进一步工作。

致谢：该文是笔者毕业设计的主要成果，在此衷心感谢李朝举导师的悉心指导和谆谆教诲。

参考文献

[1] Gleeson B, Lin A, Heinanen J, et al. A framework for IP based virtual private network [S]. RFC 2764, February 2000

[2] Rekhter Y, Moskowitz B, Karrenberg D, et al. Address allocation for private internet [S]. RFC 1918, February 1996

[3] Rosen E, Rekhter Y. BGP/MPLS VPNs [S]. RFC2547, March 1999

[4] Bates T, Rekhter Y, Chandra R, et al. Multiprotocol extension for BGP4 [S]. RFC2858, June 2000

[5] IEEE Draft Standard P802.1Q/D11. IEEE standards for local and metropolitan area networks: virtual bridged local area networks [S]. IEEE Draft Standard P802.1Q/D11, July 30, 1998

[6] Jacobson V, Nichols K, Poduri K, et al. An expedited forwarding PHB [S]. RFC2598, June 1999

[7] Heinanen J, Telia F, Baker F, et al. Assured forwarding PHB [S]. Group RFC2597, June 1999

[8] Awduche D, Malcolm J, Agogbua J, et al. Requirements for traffic engineering over MPLS [S]. RFC 2702, September 1999

[9] Zhang Hui. Service disciplines for guaranteed performance service in packet-switching networks [J]. Proceedings of the IEEE, 1995, 83 (10): 1374～1399

[10] Bennett J C R, Zhang H. Hierarchical packet fair queuing algorithms [A]. Proceedings of the ACM-SIGCOMM 96 [C], August 1996. 143～156

[11] Floyd S, Jacobson V. Random early detection gateways for congestion avoidance [J]. IEEE/ACM Transactions on Networking, July 1993, 1(4): 397～413

Research and Implementation of IP－VPN

Li Xiuzhong

(*China Academy of Telecommunication Technology, Ministry of Information Industry, Beijing* 100083, *China*)

[**Abstract**] Recently, IP－VPN is proposed as a way satisfying large company's inter-connect requirement because of the prevalence of Internet. But there are some problems to be solved, especially security and QoS. In this paper, one way of network-based VPN QoS is proposed based on analysis of some available QoS algorithms. For IP－VPN, now there are several mechanisms: VLL, VPRN, VPLS and VPDN. This paper places emphasis on VPRN and VPLS. Two kinds of VPRN: BGP/MPLS and VR are discussed and compared with each other. And besides, VLAN, one way of VPLS, is introduced.

[**Key words**] virtual private routed network (VPRN); virtual private LAN segment (VPLS); border gateway protocol / multi-protocol label switch (GP/MPLS); virtual router (VR); worst-case weighted fair queue (WF^2Q); random early detection (RED)