计算机科学 2000Vol. 27№. 7

VPRN 成员信息传播方法及比较

The Methods of VPRN Membership Information Dissemination and their Comparison

王永卫　周明天

（电子科技大学计算机科学与工程学院　成都 610054）

Abstract　VPRN is the most complicated type of VPN. The first step to construct a VPRN is to disseminate the membership information. This paper introduces some methods of dissemination with the emphasis on analyzing and comparing them.

Keywords　VPN, VPRN, Membership information, Dissemination

1　引言

IP VPN 可以定义为采用 IP 设施（包括公共 Internet 网和专用 IP 主干网）模拟专用广域网设施，因其既有专用网络的可靠性，又不需要专用网络的投资，而且灵活多变而越来越受到网络厂商和用户的青睐。IP VPN 可分为虚拟租用线、虚拟专用路由网（VPRN）和虚拟专用拨号网等类型，其中 VPRN 最为复杂、应用于多点路由器连接构成的 VPN。

在 VPRN 中，属于同一个 VPRN 内的多个 ISP 边界路由器以隧道方式安全连接或任意拓扑结构互连构成主干。每个用户边界路由器通过专用线路（租用线、ATM 或帧中继）连接到一个或多个 ISP 边界路由器上，见图 1。用户边界路由器将可达性信息传递给直接相连的 ISP 边界路由器，ISP 边界路由器相互交换可达性信息并将其传递给相邻的用户边界路由器，这些可达性信息就可用于 VPN 分组的路由。

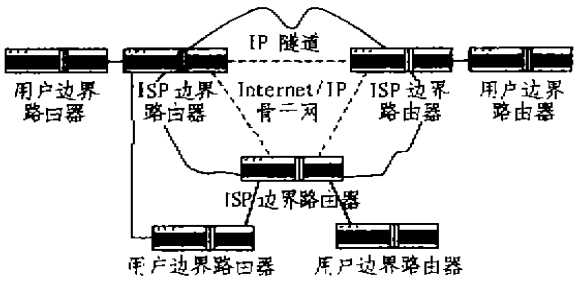

图 1　VPRN 图

VPRN 组建的第一步就是要确定 VPN 的成员，即通过某种渠道使得一个 ISP 的边界路由器知道哪些路由器和它同属于一个 VPN。这包括 2 个方面：一是判别标准。路由器通过 VPN ID 来判别其同组成员，因为 VPN 大多跨越多个自治系统，所以 VPN ID 必须具有全球唯一性。VPN ID 可以由全球唯一组织标识符加上 VPN 索引构成，也可以用自治系统号替代全球唯一组织标识符，不过后者不如组织标识符通用，因为 VPN 网不一定就拥有自治系统号。第二步是将这些 VPN 成员信息有效地传播出去为同组成员所知，这就需要相应的 VPRN 成员信息传播方法。

2　VPRN 成员信息传播方法

2.1　目录查询

某个 VPN 成员的信息，可只包括 VPN ID 号，还可以加上其他信息如 ISP 边界路由器与连接的用户边界路由器的 ID 号等，并将它们配置在一个目录中。路由器通过某些机制如 LDAP，基于自己的 VPN ID 配置来查询该目录。

2.2　显式管理库配置

可以定义一个 VPRN 管理信息库（MIB），有了该 MIB，中央管理系统将通过参与 VPRN 的路由器的身份标识来配置这些路由器。该机制允许管理站进行严格的授权控制，但配置管理系统范围之外的路由器却很困难。由于目录方法也可以利用 MIB 来将 VPRN 成员信息推送到各参与路由器中，所以该方法也可视为目录方法的子集。

2.3　利用路由协议捎带

每个路由器都要通过路由协议交换信息，因此可以将 VPN 信息附在路由信息之上自动传送过 IP 主干网。每个路由器广告信息可以包括路由器所相连的 VPN ID 和能够让其他路由器确定 ID 的足够的信息，还可以包含到某些路由器的路由信息。其他的路由器

王永卫　博士生，研究方向为 IP 网络技术。周明天　教授，博士生导师，主要研究领域为计算机网络，分布对象技术和网络与信息系统安全等。

检查接收到的路由广告信息，通过检查符合本地 VPN ID 与否来确定所包含的信息是否与所配置的 VPN 相关。

捎带方法之一是通过使用 OSPF 的 opaque LSA 选项功能；此外还可以通过 BGP-4 来实现，即将 VPN 成员信息包括在 Multiprotocol Extension Attribute 或者 BGP communities attribute 中。

2.4 多播方法

将 VPN ID 通过某种简单的算法单一映射成主干网上多播地址。因此 VPN ID 是唯一的，所以某 VPN ID 所对应的多播地址也是唯一的。这样具有相同 VPN ID 的路由器将属于同一多播组。每个路由器通过多播路由协议向同组成员播送自己的信息。

3 成员信息传播方法比较

1）动态性 VPRN 由多路由器互连而成，随时可能有新的站点加入 VPRN，老的站点也可能退出 VPRN，因此 VPRN 的路由器要能够自动刷新其成员信息，即传播方法应具有动态性。

目录查询动态性显然不好。它需要某些数据库同步机制，例如由边界路由器触发或定期目录轮询，或由目录服务器主动将更新信息推送给边界路由器等，以处理 VPRN 成员变化的情况。显式管理库配置和目录查询也有同样的问题。

利用路由协议捎带和多播方法会自动更新 VPRN 成员信息，动态性很好。

2）拓扑适应性 一般而言，VPRN 是由路由器通过全连接构成的，但它也可以是任意拓扑结构，全连接使得两个站点可不通过第三者就直接通信，从而优化了路由，而且全连接不需要配置路由拓扑信息。但当 VPRN 中 ISP 边界路由器很多时，考虑到伸缩性问题，全连接就不是很合适了，网管策略也可能要求采用非全连接拓扑，例如要求两个站点间的通信必须通过中心管理站即是一例。

目录查询能很好地适应全连接或非全连接拓扑要求，对于全连接，VPN 的完全成员清单将分布到每个路由器上；对于任意拓扑结构，不同的路由器将收到不同的成员清单。

显式管理库配置和目录查询一样，也允许全连接和任意拓扑结构的配置。

采用路由协议捎带方法，网络中所有路由器都看到相同的 VPRN 成员信息，因此很容易支持全连接结构，但要支持任意拓扑结构比较困难，此时需要某些方法对信息进行裁剪，使不同路由器收到不同信息。

利用多播方法和采用路由协议捎带方法有相同问题。同一 VPN ID 路由器知道的信息相同，因此支持全连接结构没问题，但要支持任意拓扑结构比较困难。

3）跨区域性 目录查询可以跨管理域。此时需要用目录到目录协议机制来在不同管理域间的目录系统间传播 VPRN 成员信息。显式管理库配置对于管理系统之外的路由器就很困难。捎带方法在跨越多管理区域时很有效。多播方法也能很好地跨管理区域。

4）安全性 采用目录查询允许在散布 VPRN 成员信息之前先进行授权。显式管理库配置也允许管理站进行严格的授权控制。路由协议捎带方法尚需要某些安全机制用于路由更新，以只允许所有相关的路由器能看到这些捎带信息。而且，由于路由协议的特性，捎带信息也会传给中间路由器，尤其是自治域的边界路由器，并进而转发出去，这使问题更为复杂。

多播方法有安全性。多播路由协议可以采用密钥管理系统和 IPSec 等方式进行加密传输。如 CBT 协议中的中心路由器（或汇合点）就是合法的密钥分发者。

5）对现有路由协议的影响 目录查询和显式管理库配置不需要修改任何路由协议。捎带方法则利用现有路由协议的某些选项，因而对协议有影响。多播方法对协议无影响。

6）效率 当有数据库同步机制时，目录查询和显式管理库配置的成员信息传播都很直接，因而效率高。捎带方法中成员信息随路由协议交换，在有较多路由器的主干网上效率较低。

多播方法在不同情况下用不同的多播路由协议进行。在密集分布模式下用 MOSPF、DVMRP 或 PIM-DM 协议；在稀疏分布模式（如 Internet）采用 CBT 或 PIM-SM 协议。开始建立 VPRN 网时效率较低，以后更新时效率较捎带方法高。

7）基础设施 目录查询和显式管理库配置分别需要一个目录服务器和 MIB 服务器。捎带方法则要求路径上所有路由器都要懂得修改后的路由协议。多播方法需要 VPRN 成员路由器支持多播。

8）网络资源开销 目录查询方式对网络资源占有较少。各 VPRN 路由器发查询信息到目录服务器并由其发回应答信息，只涉及目录服务器和相关路由器，但在跨管理区时因需目录间协议机制，开销有所增加。

显式管理库配置只涉及 MIB 管理站和相关路由器，网络资源开销小。

在捎带方法中，虽然 VPRN 成员信息只和部分边界路由器有关，但要求所有的中间路由器都要处理和传播这些信息，这将给这些中间路由器的运行和管理带来不能忽略的负担。

多播方法中多播路由协议在构建多播路径树或生成树时因协议种类不同而开销不同。密集模式采用 flooding，开销很大。稀疏模式采用用户驱动构建生成

树且该树为组内所有成员共享，收发分组通过同一棵树，因而开销较小。总体而言，该方法的网络资源开销小于捎带方法而大于目录查询和显式管理库配置。

9）健壮性　目录查询和显式管理库配置以目录服务器和MIB管理站为核心，一旦它们出现问题，就无法提供成员信息。因此从可靠性出发，应设置备份服务器。捎带方法和多播方法不依赖于某一网络组件，因而健壮性很好。

表1总结了上述情况。

表1　各种方法的比较

特性 \ 方法	目录查询	显式管理库配置	路由协议捎带方法	多播方法
动态性	不好 *需数据库同步机制	不好 *需数据库同步机制	好	好
拓扑适应性	好	好	支持全连接结构；支持任意拓扑结构比较困难	支持全连接结构，支持任意拓扑结构比较困难
跨区域性	较好 *需目录间协议	不好	好	好
安全性	有	有	不足	有
对现有路由协议的影响	无	无	有 *需修改路由协议选项	无
效率	高	高	低	低
基础设施	需目录服务器	需MIB管理站	路径上所有路由器识别修改后协议	VPRN成员路由器支持多播
网络资源开销	小	小	大	较大
健壮性	较差	较差	好	好

结束语　本文总结了VPRN成员信息传播的几种方法，并对其在动态性、拓扑适应性、跨区域性、安全性、对现有路由协议的影响、效率、基础设施、网络资源开销和健壮性等方面进行了比较。每种方法各有优点，也有不尽人意之处，只有将多种方法结合起来才能高效、可靠、简洁地进行VPRN成员信息传播。

参考文献

1　Ferguson P, Huston G. What is a VPN?. Available at URL: http://www.employees.org:80/~ferguon/vpn.pdf, April 1998

2　Gleeson, et al. A Framework for IP based Virtual Private Networks. draft-gleeson--vpn-framework-01.txt, Feb. 1999

3　Muthukrishnan and Malis. Core IP VPN Architecture. draft-muthukrishnan-corevpn-arch-00.txt, Oct. 1998

4　Fox B, gleeson B. Virtual Private Networks Identifier. draft-ietf-ion-vpn-id-02.txt, July 1999

5　Jameieson, et al. MPLS VPN Architecture. draft-jamieson-mpls-vpn-00.txt. Aug. 1998

6　Chandra R, Fraina P. BGP Communities Attribute. RFC 1998

7　Coltun R. The OSPF Opaque LSA Option. RFC 2370

8　Waller D, et al. Key Management for Multicast: Issues and Architecture. draft-wallner-key-arch-01.txt

9　Gupta V. Secure, Remote Access over the Internet using IPSec. draft-gupta-ipsec-remote-access-02.txt, Jun 1999

（上接第14页）

参考文献

1　Girard J Y. Linear Logic, Theoretical Computer Science, n°150, 1987

2　Valette R, Courvoisier M. Petri nets and Artificial Intelligence. Modern Tools for Manufacturing Systems, Elsevier Science Publishers, 1993. 385～405

3　Berthomieu B, Diaz M. Modeling and verification of time dependent systems using Petri nets. IEEE Trans. on Software Eng., 1991, 17(3): 259～273

4　Yao Y. A Petri net model for temporal representations and reasoning. IEEE Trans. on Systems, Man and Cybernetics, 1994, 24(9): 1374～1382

5　Cardoso J, et al. Petri net based reasoning for the diagnosis of dynamic discrete event systems. In: 6th Intl Fuzzy Systems Association World Congress, IFSA' 95, Sao Paulo, Brazil, July, 1995. Vol. 1. 333～336

6　de Figueiredo J C A, Perkusich A. Fault and Timing Analysis in Real-Time Distributed Systems: A Fuzzy Time Petri-Net-Based Approach. Intl. J. Fuzzy Sets and Systems, 1996, 83(3): 143～168