

WAN Accelerates the Application of VPN in Group Enterprises

Guanghai Zhou Hequn Wang

Anhui Tongguan Intelligent Technology Co., Ltd., Tongling, Anhui, 244000, China

Abstract

This paper discusses the application of WAN accelerated VPN technology in the network interconnection of overseas units and headquarters of Tongling Non-ferrous Group. First, a basic principle of the technique is briefly introduced. Then, the author will systematically test and analyze the effect of this technology in practical application, focusing on the efficiency and stability of network connection. The results show that the WAN accelerated VPN technology significantly improves the quality of network connectivity, reduces latency and packet loss, and provides an efficient and stable solution for the group's remote office. This research not only provides theoretical support for the network construction of Tongling Nonferrous Metals Group, but also provides a reference for other enterprises in the network optimization in similar scenarios.

Keywords

WAN acceleration; VPN technology; TCP application acceleration

广域网加速 VPN 在集团企业中的应用

周广辉 王鹤群

安徽铜冠智能科技有限公司, 中国 · 安徽 铜陵 244000

摘 要

论文探讨了广域网加速VPN技术在铜陵有色集团下属驻外单位与总部网络互联中的应用, 简要介绍了该技术的基本原理, 对该技术在实际应用中的效果进行了系统的测试与分析, 重点关注网络连接的效率和稳定性。研究结果显示, 广域网加速VPN技术显著提升了网络连接的质量, 减少了延迟和丢包现象, 为集团公司的远程办公提供了一个高效、稳定的解决方案。这一研究不仅为铜陵有色集团的网络建设提供了理论支持, 也为其他企业在类似场景下的网络优化提供了借鉴。

关键词

广域网加速; VPN技术; TCP应用加速

1 概况

在网络领域, 虚拟私人网络 (VPN) 是一种远程访问技术, 旨在通过公用网络构建专用网络^[1]。VPN 技术使得集团下属驻外单位能够通过互联网与总部网络互联, 员工无论身处何地, 只要连接互联网, 即可安全访问集团内网的授权资源。这一技术显著拓展了企业员工在生产和经营管理中的地域和空间, 因而在企业中得到了广泛应用。

随着信息化和网络化管理的深入, VPN 为集团公司与驻外单位之间的网络互联提供了有效解决方案。然而, 现有 VPN 架构和协议在面对多样化的管理内容 (如视频信息等多媒体内容) 时逐渐显露出局限性, 无法满足日益增长的需求。因此, 亟须研究新型 VPN 架构, 以提升其安全性和性能, 更好地支持管理和移动应用。

技术创新和广域网优化技术为传统 VPN 注入了新活

力。经过几年的发展, 广域网优化技术已获得广泛认可, 通过优化传输协议和应用层协议, 有效降低了因互联网线路丢包和延迟导致的业务交付不稳定^[2]。同时, 压缩缓存技术减少了链路传输中的冗余数据, 降低了带宽占用, 避免了企业升级带宽的需求。基于应用层的流控管理技术也为核心业务提供了高效的传输保障。这些进展推动了广域网优化技术与 VPN 的融合, 成为新的技术演进方向。

2 广域网加速技术在 VPN 隧道通信中的应用与流量需求优化

2.1 安全组网

广域网加速 VPN 通过三个方面提供完整的安全保障: VPN 隧道接入、隧道中数据传输和接入访问授权。

2.1.1 基于网关的硬件特征码认证

接入 VPN 后, 用户将访问组织内网资源, 因此需严格确认设备身份。为确保网关的唯一性, 采用基于 CPU、硬盘和网卡的硬件特征码进行认证, 通过校验接入网关的硬件证书与已录入的分支端网关证书匹配, 实现身份唯一性确

【作者简介】周广辉 (1973-), 男, 中国安徽无为, 硕士, 高级工程师, 从事企业信息化、工业智能化研究。

认。这种方法相较于传统认证方式，具有不可复制和不可盗用的优势。

2.1.2 双向权限控制、应用级别细致控制

总部仅对分支开放必要的共享应用服务器资源，同时对总部内网和内部服务器进行隔离，以防止病毒和攻击等风险。通过广域网加速 VPN 设备的双向权限控制功能，可以严格限制分支与总部之间的访问范围，细化到 IP 段、IP、端口和协议，从而合理管控，增强安全性，降低风险。

2.2 快速组网

2.2.1 高效流压缩

广域网加速 VPN 通过高效流压缩技术解决数据冗余问题，采用流压缩、IP 包压缩和动态压缩的综合方案。与传统文件压缩方式不同，LZO 和 GZIP 实现了压缩比与系统性能消耗之间的最佳平衡，确保最低的系统资源消耗和最大的压缩效果。此外，流压缩采用边压缩边传输的方式，进一步加快数据输出，从而整体提升数据加速效果。

动态压缩技术通过针对不同数据采用优化的压缩策略，实现最佳匹配。这种动态选择策略不仅提高了压缩效率，还降低了系统负载，从而提升整体数据处理速度和业务访问速度。

2.2.2 基于码流特征的缓存技术

广域网加速 VPN 利用流缓存技术，通过分析码流特征显著减少因行为方式导致的冗余。在文件传输过程中，VPN 设备将数据包分拆为多个“碎片”，并为每个“碎片”分配唯一指针，分别存储在本地和目的地主机。当相同内容再次传输时，仅需发送指针，接收端根据指针从本地提取数据进行重组。

通过将“碎片”做得足够小，传递相同内容的概率增大。与传统缓存技术相比，基于码流特征的优化方法结合数据包分片标签和模式匹配算法，确保数据实时性的同时显著降低传流量，提高访问速度。每个指针仅占 9 个字节，却可代表最多 4K 的数据，冗余削减可达 60%~90%。

流缓存流量削减效果见图 1。

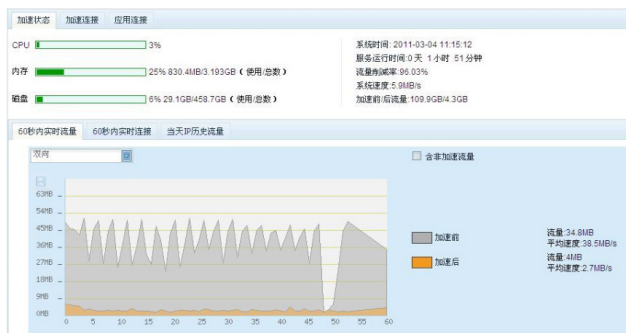


图 1 流缓存流量削减效果

2.3 高丢包、高延时、跨网传输解决技术

在跨省传输、跨运营商或网络质量较差的情况下，常出现高丢包和高延时，导致用户在访问应用时体验不佳，如 ERP 页面加载缓慢、订单录入和数据查询延迟、FTP 文件

下载时间过长等，从而影响工作效率。

广域网加速 VPN 通过采用 HTP 高速传输协议来解决这些问题。

HTP 高速传输协议，高丢包、高延时下大幅提速。

高丢包和高延时对 TCP 协议的传输影响显著。TCP 作为面向连接的可靠传输协议，其设计初衷是在网络条件较差的情况下采用“慢上升、快下降”的拥塞控制机制，以避免过度拥塞^[3]。然而，这一机制在现代网络吞吐能力下限制了跨网访问速度：在良好网络环境中，滑动窗口缓慢增长至最大 64K，而一旦出现丢包，窗口大小会迅速减小，并需重新传输丢失的数据包，导致传输效率低下。

为了解决传统 TCP 的低效传输问题，广域网加速 VPN 引入了 HTP 高速传输协议（High-Speed Transmission Protocol）。HTP 协议通过扩展传输窗口、优化拥塞控制算法和选择性快速重传等技术，提高 TCP 传输效率。在网络条件允许的情况下，HTP 能够迅速提升传输速度至最大吞吐量；在高丢包和高延时环境下，HTP 通过优化的拥塞控制机制适应网络条件，确保传输质量，从而显著提升网络传输速度（见图 2）。

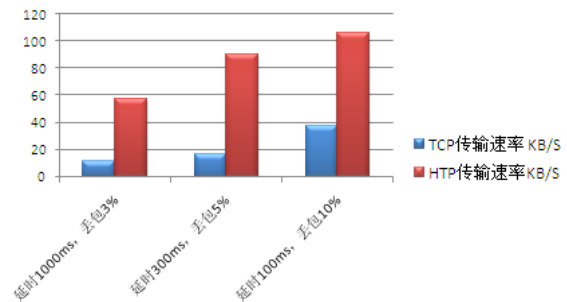


图 2 传输速率柱状图

2.4 应用优化

为满足应用协议优化需求，广域网加速 VPN 设备针对 HTTP、HTTPS、FTP、POP3、SMTP、CIFS、MAPI、Oracle EBS、RDP、Citrix 等协议实施优化机制。这些优化可显著提升 Lotus Notes、Exchange、Outlook、金蝶 EAS、用友 NC、SAP NetWeaver、Oracle EBS、远程桌面和 Citrix 等应用的交互速度。通过协议代理、优化应用交互机制和 WebCache 技术，用户访问体验得以显著改善。

2.5 深度流量管理

通过广域网加速 VPN 流量管理功能，可对线路中的各应用流量进行优先级划分，保障核心业务、适当限制非核心业务（见图 3）。



图 3 深度流量管理

广域网加速 VPN 的流量管理流程分为四个层级：应用

识别、权限控制、通道化管理和线路化管理。首先，通过应用识别确定数据归属，以便进行针对性管理；其次，基于用户权限控制应用使用；然后，对有权限的应用实施通道化带宽保障或限制策略；最后，利用智能报表功能反馈当前策略效果，并进行相应的策略调整，以确保最佳控制效果。

3 采用 HA 模式，提升原有架构可靠性

我单位的业务流量逐年大幅增长，且总部的广域网加速 VPN 网关是集团子公司的核心接入点。目前仅部署一台设备，若出现性能瓶颈或故障，将导致全网业务中断。为应对未来数据量的快速增长，确保全网业务的高可用性和稳定性，总部决定新增两台同型号、同软件版本的广域网加速 VPN 网关，实现双机热备。这样，若任一设备发生故障或断电，将自动切换，保障核心业务系统的稳定运行。

4 应用效果

广域网加速 VPN 显著提升了用户体验，文件收发、网

页访问及 ERP 系统的响应速度均有所提高。所有基于 TCP 的应用在广域网上都能实现不同程度的加速。通过广域网加速 VPN，用户可以快速建立总部与分支的 VPN 链接，无需等待运营商长达数月的专线申请和部署。结合加速功能，VPN 在相同成本下提供了远超专线的访问速度，同时增强了数据安全性。

5 实际测试效果验证

5.1 测试场景说明

测试环境：相同场景下，与普通 IPSEC VPN 进行不同应用效果对比。

测试应用：FTP 下载、HTTP 网页、邮件系统。

5.2 测试数据

FTP 下载测试见表 1。

邮件系统测试见表 2。

HTTP 网页访问测试见表 3。

表 1 FTP 下载测试

测试项目：FTP 下载加速																
测试场景：10Mbps 带宽，延迟 50ms，丢包 1%（建立 VPN，对应用进行访问测试）																
采用测试工具：客户端 PC FlashFXP；																
文件名称：							文件类型：doc/ppt/xls/avi					文件大小：doc12.8M、ppt11.7M、xls10.2M、avi10M				
测试方法：在客户端电脑通过 FlashFXP 从服务器拷贝文件																
1. 不开启加速连接前，通过 FTP 客户端软件从 FTP 服务器下载测试文件，观察传输时间、传输速度																
2. 开启加速连接后，通过 FTP 客户端软件从 FTP 服务器下载测试文件，观察传输时间、传输速度																
测试效果	测试对比	标准 IPSEC VPN 测试（不开启加速）					SANGFOR VPN 测试（不开启加速）					SANGFOR VPN 测试（开启加速）				
		测试文件	第 1 次	第 2 次	第 3 次	平均	测试文件	第 1 次	第 2 次	第 3 次	平均	测试文件	第 1 次	第 2 次	第 3 次	平均
	传输时间（单位：s）	doc	65	55.29	55.8	58.71	doc	44.34	47.47	45.6	45.79	doc	21.82	2.45	2.01	8.76
		ppt	43.37	42.11	44.8	43.41	ppt	37.85	39.5	40.2	39.19	ppt	9.03	2.98	1.76	4.59
		xls	42.99	42.06	43.8	42.96	xls	37.88	38.02	34.4	36.75	xls	2.08	1.55	1.76	1.80
		avi	44.63	44.51	41.5	43.55	avi	32.51	36.02	33	33.83	avi	9.84	1.98	1.78	4.53
	传输速度（单位：kB/s）	doc	207.8	238.8	236	227.67	doc	297.8	278.1	290	288.57	doc	604.9	5070	6410	4028.30
		ppt	257.2	261.6	246	254.97	ppt	291.1	278.9	274	281.30	ppt	1190	3610	6100	3633.33
		xls	249	250.3	240	246.53	xls	278	276.9	307	287.13	xls	4960	6650	5730	5780.00
		avi	233.9	231.5	248	237.87	avi	316.9	286	313	305.17	avi	1020	5080	5660	3920.00
测试结论	在互联网 VPN 场景下，通过对路由器建立的标准 IPSEC VPN、产品建立的 SANGFOR VPN、广域网加速 VPN 产品建立的 SANGFOR VPN+ 加速进行同一场景不同文件的传输对比 IPSEC VPN 与 SANGFOR VPN 效果差距不大，但是经过广域网加速 VPN 加速后传输效果明显提升															

表 2 邮件系统测试

测试项目：邮件系统访问加速													
测试场景：10Mbps 带宽，延迟 50ms，丢包 1%（建立 VPN，对应用进行访问测试）													
测试应用：email 邮件		测试版本：Windows Server 2008 r2+Exchange 2010+ 客户端 win7											
文件名称：						文件类型：doc				文件大小：12.8M			
测试方法：用 exchange 邮件发送一个 12.8M 的 doc 格式附件，计算发送时间。注意：开加速后测试，先把邮件客户端（outlook）关闭再启动													
1. 不开启加速连接前，发送邮件所需时间													
2. 开启加速连接后，发送邮件所需时间													
测试效果	测试对比	标准 IPSEC VPN 测试（不开启加速）				SANGFOR VPN 测试（不开启加速）				SANGFOR VPN 测试（开启加速）			
		第 1 次	第 2 次	第 3 次	平均	第 1 次	第 2 次	第 3 次	平均	第 1 次	第 2 次	第 3 次	平均
	传输时间（s）	44	42	41	42.33	39	42	41	40.67	23	22	21	22.00
	传输速度（kB/s）	297.89	312.08	319.69	309.62	336.08	312.08	319.69	322.31	569.88	595.78	624.15	595.78
其他备注说明：	在互联网 VPN 场景下，通过对路由器建立的标准 IPSEC VPN、产品建立的 SANGFOR VPN、广域网加速 VPN 产品建立的 SANGFOR VPN+ 加速进行同一场景不同文件的传输对比 IPSEC VPN 与 SANGFOR VPN 效果差距不大，但是经过广域网加速 VPN 加速后传输效果明显提升												

表 3 HTTP 网页访问测试

测试项目：http 应用加速													
测试场景：10Mbps 带宽，延迟 50ms，丢包 1%（建立 VPN，对应用进行访问测试）													
测试工具：HTTP 应用页面、HTTPWATCH（网页检测工具）													
文件名称：http://192.168.43.98/sangfor/static/index.html							文件类型：web 网页						
测试方法：采用 httpwatch 对网页访问进行时间记录，清空 IE 缓存（要求每一次访问网页都要对 IE 缓存进行清除），打开 web 应用同一页面进行对比测试													
1. 加速连接状态里先清除所有缓存，保障测试对比													
2. 不开启加速前 HTTP 页面访问时间记录（要求每一次访问网页都要对 IE 缓存进行清除）													
3. 开启加速后 HTTP 页面访问时间记录（要求每一次访问网页都要对 IE 缓存进行清除）													
测试效果	测试对比	标准 IPSEC VPN 测试（不开启加速）				SANGFOR VPN 测试（不开启加速）				SANGFOR VPN 测试（开启加速）			
		第 1 次	第 2 次	第 3 次	平均	第 1 次	第 2 次	第 3 次	平均	第 1 次	第 2 次	第 3 次	平均
	访问时间（单位：s）	5.277	5.992	5.908	5.73	5.768	4.782	5.345	5.30	4.914	0.895	1.332	2.38
其他备注说明：	在互联网 VPN 场景下，通过对路由器建立的标准 IPSEC VPN、产品建立的 SANGFOR VPN、广域网加速 VPN 产品建立的 SANGFOR VPN+ 加速进行同一场景不同文件的传输对比 IPSEC VPN 与 SANGFOR VPN 效果差距不大，但是经过广域网加速 VPN 加速后传输效果明显提升												

6 结语

本研究探讨了广域网加速 VPN 技术在铜陵有色集团驻外单位与总部网络互联中的应用效果。通过对该技术的原理及实际应用的分析，我们发现其显著提升了网络连接的效率和稳定性，为集团的远程办公提供了可靠解决方案，也为其他企业的网络优化提供了参考。

随着信息技术的发展，网络环境日益复杂，企业对高效、稳定的网络连接需求不断增加。因此，进一步研究和优化广域网加速 VPN 技术将有助于提升企业运营效率。希望本研

究能为后续研究提供启示，推动更多企业在网络技术应用上的探索与实践。

参考文献

[1] 丁健. 计算机网络信息安全管理中 VPN 技术的运用探讨[J]. 信息与电脑(理论版), 2024, 36(16): 151-153+157.

[2] 左勤刚. 广域网加速技术研究与实践[J]. 金融科技时代, 2018(2): 67-69.

[3] 高雅, 郭振华. 广域网并行 TCP 加速系统的研究与实现[J]. 电子技术应用, 2013, 39(6): 96-99.