Computer Science and Application 计算机科学与应用, 2017, 7(8), 793-803
Published Online August 2017 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2017.78091

Hans汉斯

Design and Implementation of VPN Experiment Based on Windows Server 2012

Yanfeng Jiang

College of Computer, North China Institute of Science and Technology, Beijing
Email: jiangyf376@163.com

Received: Aug. 8th, 2017; accepted: Aug. 21st, 2017; published: Aug. 28th, 2017

Abstract

The use of VPN technology can reduce the cost of users; connection is convenient and flexible, the transmission data is safe and reliable, and complete the full control of the initiative. This paper introduced the concept and characteristics of VPN, and focused on the design and implementation of VPN experiment. Experiments have proved that using VPN technology can reduce cost, its connection is convenient and flexible, data transmission is safe and reliable, and can complete the full control of the initiative.

Keywords

VPN, Remote Access, Experimental Design

基于Windows Server 2012的VPN实验设计与实现

姜延丰

华北科技学院，计算机学院，北京
Email: jiangyf376@163.com

收稿日期：2017年8月8日；录用日期：2017年8月21日；发布日期：2017年8月28日

摘　要

VPN技术的使用能够使用户降低成本；传输数据安全可靠；连接方便灵活；以及对主动权的完全控制。论文介绍了VPN的概念和特点，重点介绍VPN实验的设计与实现。实验证明，利用VPN技术可以降低成本；连接方便灵活；传输数据安全可靠和完全控制主动权。

文章引用: 姜延丰. 基于 Windows Server 2012 的 VPN 实验设计与实现[J]. 计算机科学与应用, 2017, 7(8): 793-803.
DOI: 10.12677/csa.2017.78091

关键词

VPN，远程访问，实验设计

1. 引言

随着宽带网络的发展，网络安全问题逐渐成为人们关注的焦点。虚拟专用网(Virtual Private Network)作为网络安全技术应用，因其具有降低用户成本；传输数据安全可靠和连接方便灵活等特性，而在教育、科研和企业等领域得到了迅速的应用[1] [2] [3]。文中主要讨论 VPN 概念和特点，重点介绍 VPN 实验的设计与实现。该实验在 Windows Server 2012 环境下完成，主要实现基于 PPTP 和 L2TP 的远程访问 VPN 技术。

2. 相关技术[4] [5]

2.1. VPN 的概念

VPN (Virtual Private Network 虚拟专用网)。指的是在公用网络上建立专用网络的技术。之所以称为虚拟网主要是因为整个 VPN 网络的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台(如 Internet, ATM, Frame Relay 等)之上的逻辑网络，用户数据在逻辑链路中传输。

2.2. VPN 的特点

1) 降低成本

通过公用网来建立 VPN，就可以节省大量的通信费用，而不必投入大量的人力和物力去安装和维护 WAN(广域网)设备和远程访问设备。

2) 安全性高

VPN 主要使用三个方面技术(即通信协议、数据加密和身份认证技术)保证数据通信的安全性。

3) 网络协议支持

VPN 支持最常用的网络协议，这样基于 IP, IPX 和 NetBEUI 协议网络中的客户机都可以很容易地使用 VPN。这意味着通过 VPN 连接可以远程运行依赖于特殊网络协议的应用程序。新的 VPN 技术可以全面支持如 AppleTalk, DECNet, SNA 等几乎所有的局域网协议，应用更加全面。

4) 容易扩展

如果企业想扩大 VPN 的容量和覆盖范围，企业需做的事情很少，而且能及时实现，因为这些工作都可以交由专业的 NSP 来负责，从而可以保证工程的质量，更可以省去一大堆麻烦。企业只需与新的 NSP 签约，建立账户；或者与原有的 NSP 重签合约，扩大服务范围。VPN 路由器还能对工作站自动进行配置。

5) 完全控制主动权

借助 VPN，企业可以利用 ISP 的设施和服务，同时又完全掌握着自己网络的控制权。比方说，企业可以把拨号访问交给 ISP 去做，由自己负责用户的查验、访问权、网络地址、安全性和网络变化管理等重要工作。

2.3. Windows Server 2012 系统对 VPN 的支持

Windows Server 2012 系统支持四种类型的 VPN，即 PPTP, L2TP/IPSec, SSTP 和 IKEv2 VPN。

1) PPTP (Point to Point Tunneling Protocol，点对点隧道协议)

PPTP，该协议是在 PPP 协议的基础上开发的一种新的增强型安全协议，支持多协议虚拟专用网(VPN)，可以通过密码身份验证协议(PAP)、可扩展身份验证协议(EAP)等方法增强安全性。可以使远程用户通过拨入 ISP、通过直接连接 Internet 或其他网络安全地访问企业网。PPTP 协议是点对点隧道协议，其将控制包与数据包分开，控制包采用 TCP 控制。PPTP 使用 TCP 协议，适合在没有防火墙限制的网络中使用。

2) L2TP (Layer 2 Tunneling Protocol，第二层隧道协议)

它结合了 PPTP 协议以及第二层转发 L2F 协议的优点，能以隧道方式使 PPP 包通过各种网络协议，包括 ATM、SONET 和帧中继。但是 L2TP 没有任何加密措施，更多是和 IPSec 协议结合使用，提供隧道验证。L2TP 使用 UDP 协议，一般可以穿透防火墙，适合在有防火墙限制、局域网用户，如公司、网吧、学校等场合使用。

3) SSTP (Secure Socket Tunneling Protocol，又称安全套接字隧道协议)

安全套接字隧道协议(Secure Socket Tunneling Protocol, SSTP)是一种 VPN 隧道的形式，提供了一种通过 SSL3.0 通道传输 PPP 或 L2TP 流量的机制。SSL 利用密钥协商提供传输级别的安全性。通过 TCP 端口 443 使用 SSL，允许 SSTP 通过几乎所有的防火墙和代理服务器，除了需要身份验证的 Web 代理。这种 SSTP 只适用于远程访问，不能支持站点与站点之间的 VPN 隧道。

4) IKEv2 (Internet Key Exchange V2，因特网密钥交换版本 2)

ikev2, Internet 密钥交换协议，它是一个用于通讯双方协商加密的一个协议。由 Internet 安全关联和密钥管理协议(ISAKMP)和两种密钥交换协议 OAKLEY 与 SKEME 组成。解决了在不安全的网络环境(如 Internet)中安全地建立或更新共享密钥的问题。

Windows 2012 系统支持以下两种方式的 VPN，即远程访问 VPN 连接(Remote Access VPN connection)和站点对站点 VPN 连接(Site To Site VPN connection)。其中远程访问 VPN 连接的 VPN 客户端在远程利用无线网络、局域网等方式连上因特网后，就可以通过因特网与公司 VPN 服务器建立 VPN，并通过 VPN 与内部计算机安全地通信。

对于站点对站点 VPN 连接是连个局域网的 VPN 服务器都连接到因特网，并通过因特网建立 VPN，它让两个网络内的计算机之间可以通过 VPN 来安全地通信。

3. 实验内容设计与实现

3.1. 实验目的

了解 VPN 的使用场合；

理解 VPN 的配置及原理；

掌握 VPN 的配置方法。

3.2. 实验环境

PC (windows server 2012 R2)1 台，两块网卡，交换机 2 台，PC (windows 7)2 台，直通双绞线 4 根。

3.3. 实验拓扑

实验的组网图如图 1 所示。

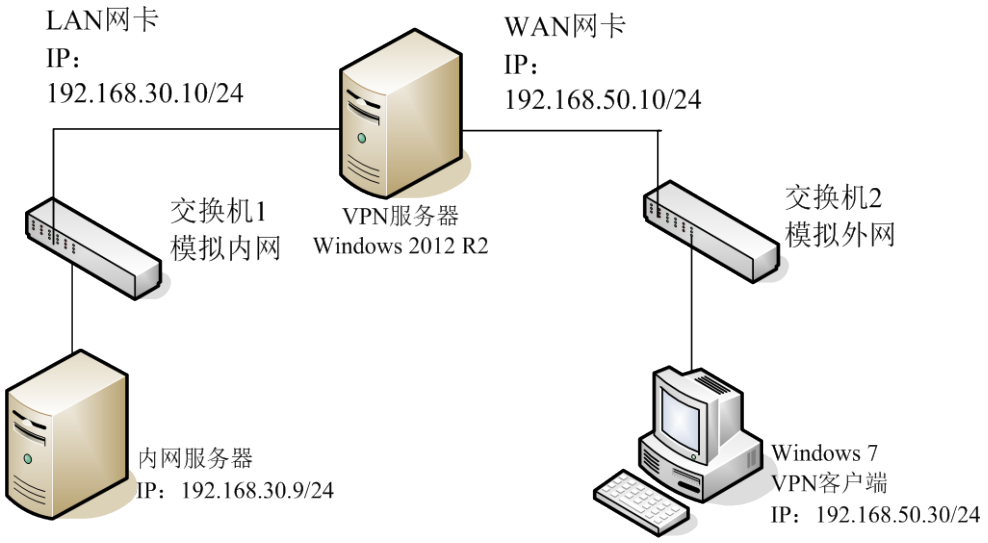

Figure 1. Experimental topology
图 1. 实验拓扑

3.4. 实验过程与主要实验步骤[6] [7]

3.4.1. 实验环境及通用步骤

按图 1 所示正确连接线缆，其通用步骤如下：

1) 配置 VPN 服务器：修改计算机名称为 HK-VPN-S，设置连接“交换机 1”的网卡 IP 地址为 192.168.30.10/24，并重命名网卡名称为 LAN；设置连接“交换机 2”的网卡 IP 地址为 192.168.50.10/24，并重命名网卡名称为 WAN；安装“远程访问服务器”，配置 VPN 服务器；创建 VPN 用户，并允许用户“远程拨入”。

2) 配置 VPN 客户端 W7：在 PC 上设置 IP 为：192.168.50.30/24，建立 VPN 连接，连接到 VPN 服务器。

3.4.2. 配置 PPTP 的 VPN 服务器

步骤 1 在**服务器管理器**界面中单击**仪表板**处的**添加角色和功能→选择服务器角色**界面时，勾选**远程访问**复选框→单击“添加功能”按钮→**角色服务**界面时，勾选 **Direct Access 和 VPN (RAS)**复选框→直到出现**确认安装选项**界面时单击“安装”按钮，安装完“远程访问服务器”后，点击“关闭”按钮。

步骤 2 在**服务器管理器**界面→单击**工具→路由和远程访问**→点击“打开 RRAS 管理控制台”→右击“HK-VPN-S”→单击“配置并启用路由和远程访问”→在向导中选中“远程访问(拨号或 VPN)”→在“远程访问”界面勾选 VPN→进入“VPN 连接”界面选择连接到 Internet 的网络接口，本例中网络接口选 WAN，如图 2 所示。接着进入“IP 地址分配”界面，选择“来自一个指定的地址范围”单选按钮→进入“地址范围分配”界面，单击“新建”按钮，在弹出的“新建 IPv4 地址范围”对话框中输入起始地址为 192.168.30.11，结束地址为 192.168.30.20，如图 3 所示。接下来直接点“下一步”→点击“完成”完成配置。

步骤 3 创建 VPN 用户。在“计算机管理”中创建“hk-vpn”用户，密码为 123456，并勾选密码永不过期。接着右击“hk-vpn”选择“属性”命令，如图 4 所示，在弹出 hk-vpn 属性对话框中点击“拨入”选项卡，选中“允许访问”单选按钮，然后点击“确定”按钮，如图 5 所示，至此，VPN 服务器的配置告一段落，下面将在客户机上进行验证。

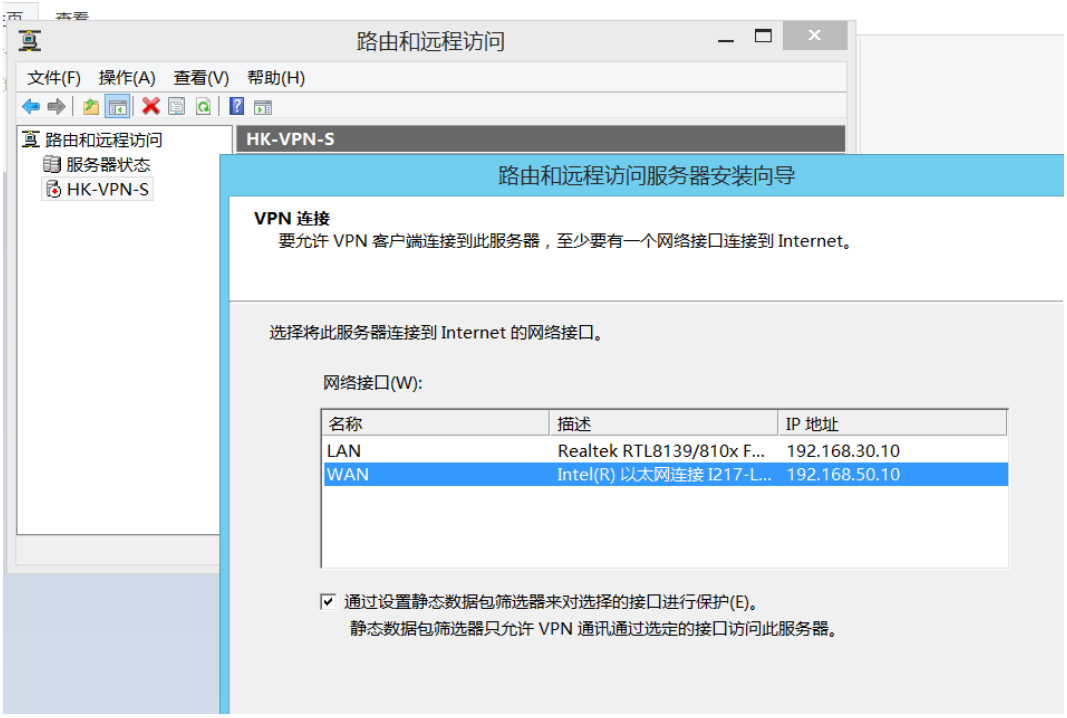

Figure 2. VPN external network interface
图 2. VPN 的外网接口

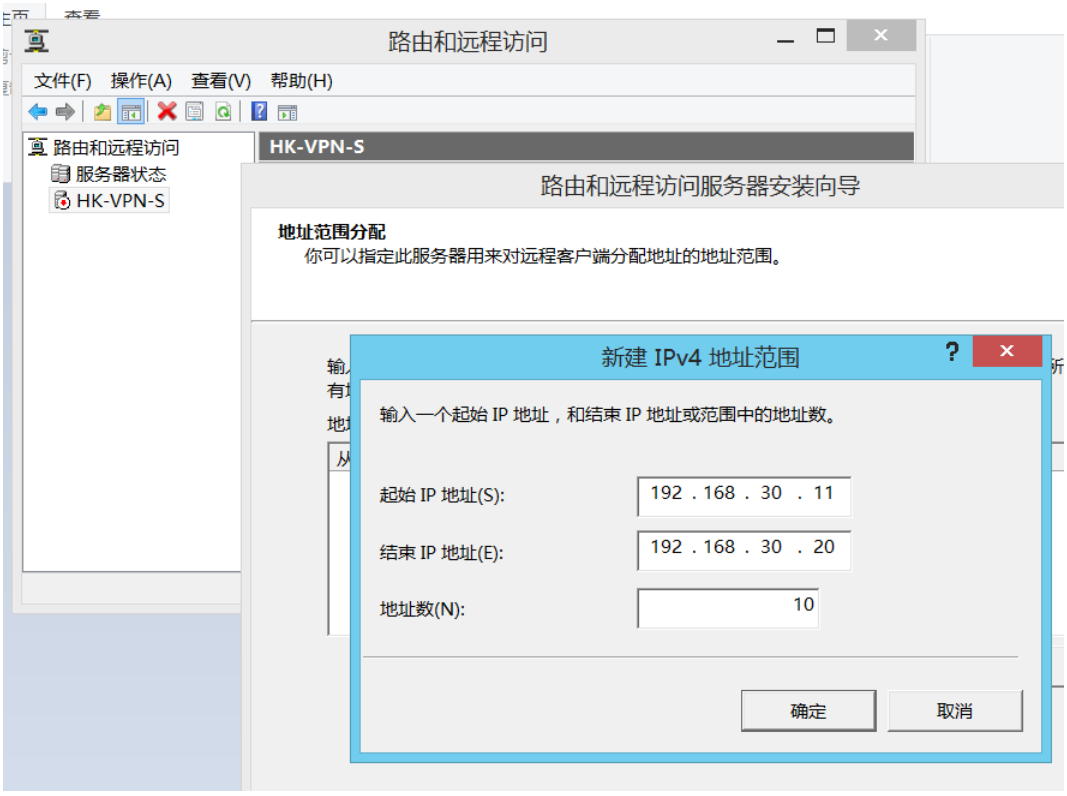

Figure 3. VPN address range
图 3. VPN 地址范围

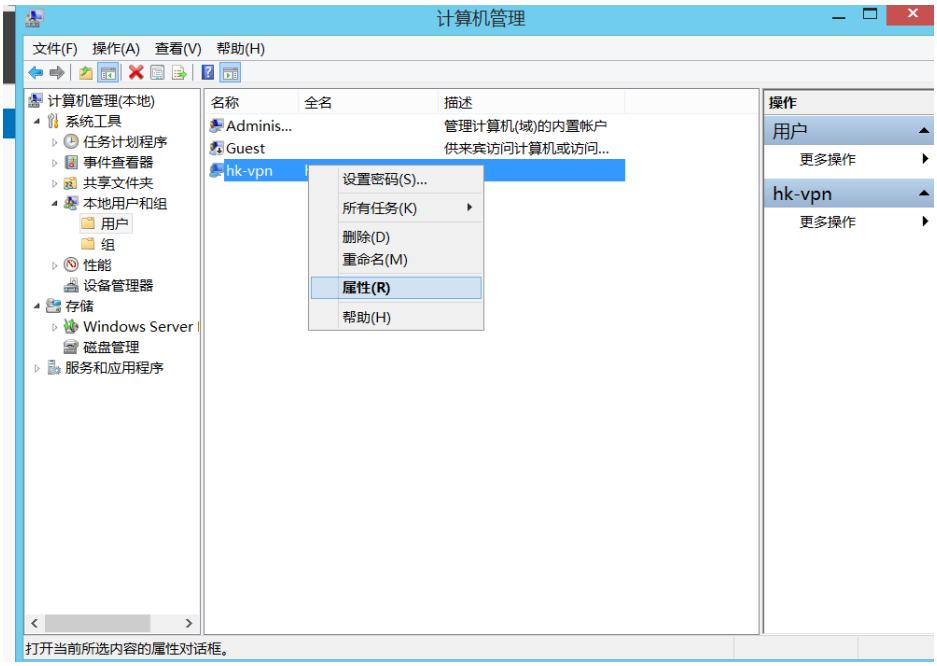

Figure 4. User attributes
图 4. 用户属性

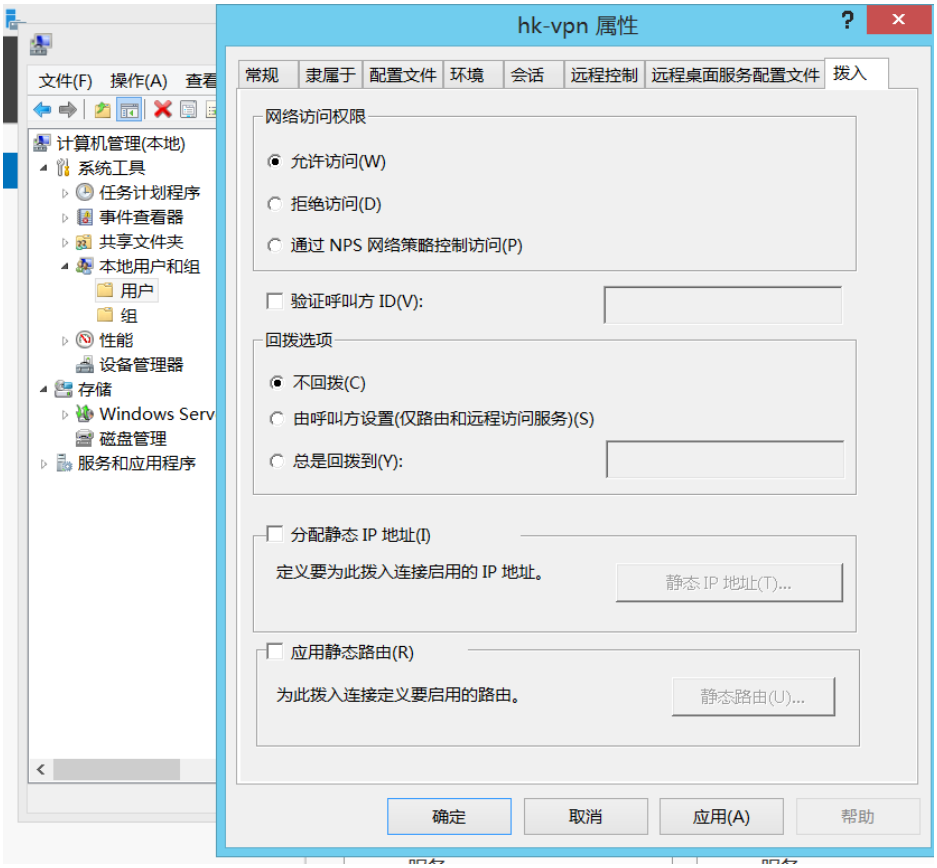

Figure 5. Setup allows access
图 5. 设置允许访问

步骤 4 在 Windows 7 中配置 VPN 客户端验证测试。Windows 7 IP 设为 192.168.50.30/24。在“控制面板”→网络和 Internet→网络和共享中心→设置新连接或网络→连接到工作区→使用我的 Internet 连接(VPN)→“键入要连接的 Internet 地址”界面，输入 VPN 服务器的 IP 地址(192.168.50.10)及目标名称(VPN 连接)如图 6 所示，进入“键入您的用户名和密码”界面，设置 VPN 的用户名与密码，勾选“记住此密码”复选框如图 7 所示。创建成功后，便可连接到 VPN 服务器。VPN 类型选择 PPTP 如图 8。

步骤 5 进行 VPN 连接测试结果如图 9。

Figure 6. VPN service information
图 6. VPN 服务信息

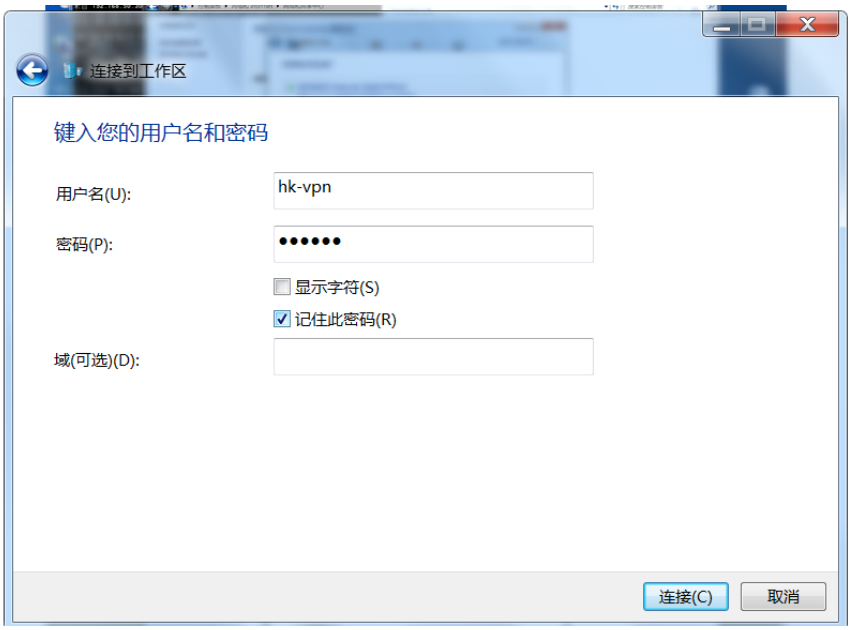

Figure 7. VPN user name and password
图 7. VPN 用户名与密码

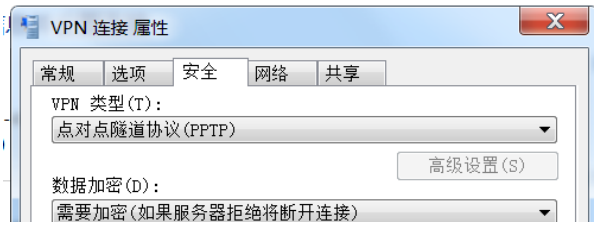

Figure 8. VPN connection properties
图 8. VPN 连接属性

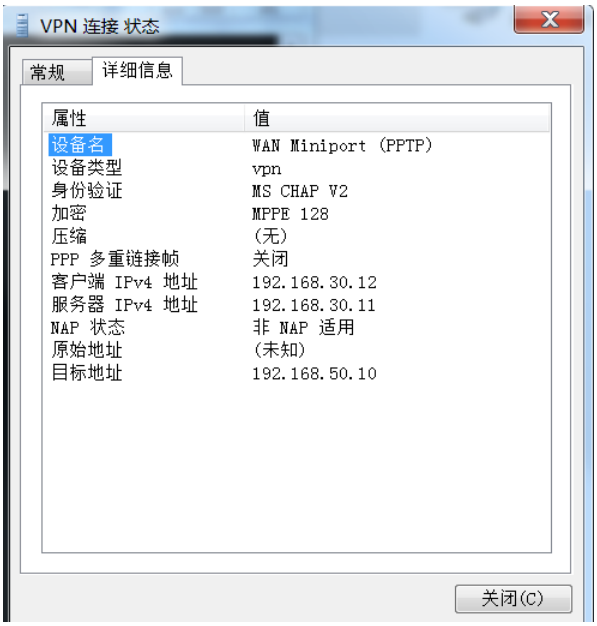

Figure 9. VPN connection details
图 9. VPN 连接详细信息

3.4.3. 配置 L2TP 的 VPN 服务器

L2TP (Layer Two Tunneling Protocol，第二层通道协议)是 VPDN(虚拟专用拨号网络)技术的一种，专门用来进行第二层数据的通道传送，即将第二层数据单元，如点到点协议(PPP)数据单元，封装在 IP 或 UDP 载荷内，以顺利通过包交换网络(如 internet)，抵达目的地。IPSec 协议通过相应的隧道技术，可实现 VPN。该实验使用“预共享密码”方式组建 L2TP 协议的 VPN 网络。

步骤 1 在 Windows Server 2012 服务器端打开“RRAS 管理控制台”窗口，右击“HK_VPN_S”，在弹出的快捷菜单中选择“属性”命令，如图 10 所示。如图 11 所示在“HK_VPN_S 属性”对话框“安全”选项卡选中复选框，并设置密码为 abc456(密码区分大小写)。单击“确定”按钮，右击“HK_VPN_S”→所有任务→点击重新启动，如图 12 所示。

步骤 2 配置 VPN 客户端：Windows 7 系统的设置步骤如下：

1) 在“网络”单击右键→属性→单击更改网络适配器设置→选中 VPN 连接点击右键→属性→如图 13 所示单击“安全”选项卡，在“VPN 类型”下拉列表中选择“使用 IPSec 的第 2 层隧道协议(L2TP/IPSec)”，单击“高级设置”，在弹出的对话框中选中“使用预共享的密钥作身份验证”单选按钮．并输入预共享的密码(abc456)。

2) 进行 VPN 连接测试结果如图 14 所示。

Figure 10. RRAS property
图 10. RRAS 属性

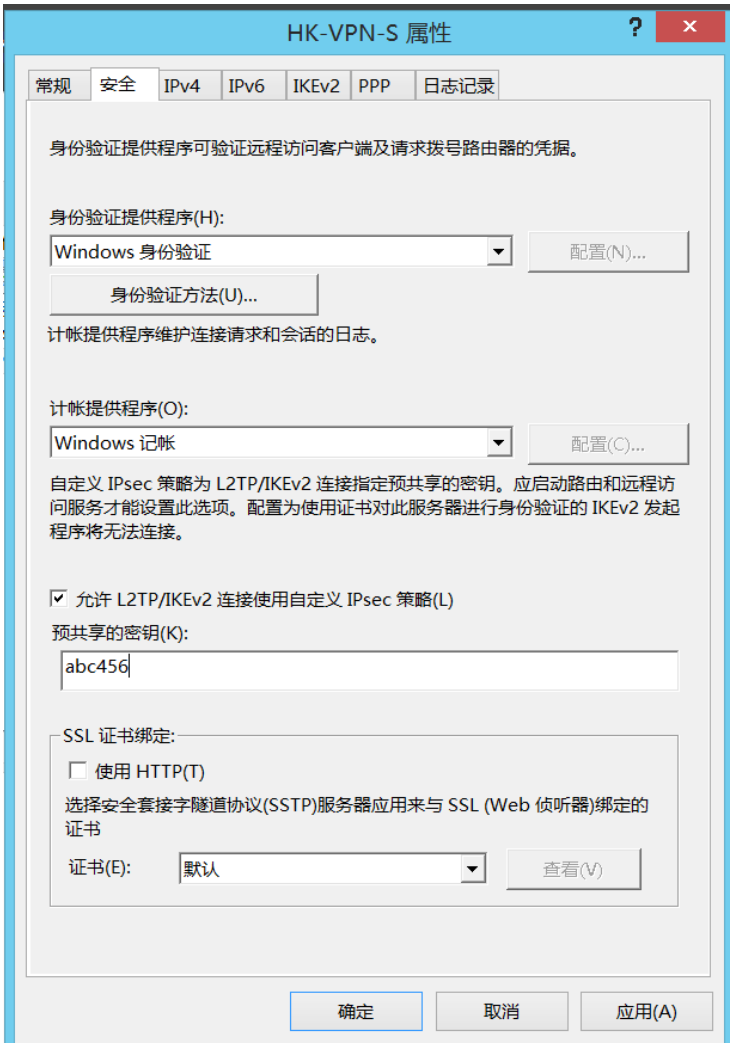

Figure 11. Pre-shared password
图 11. 预共享密码

Figure 12. RRAS reset
图 12. 重启 RRAS

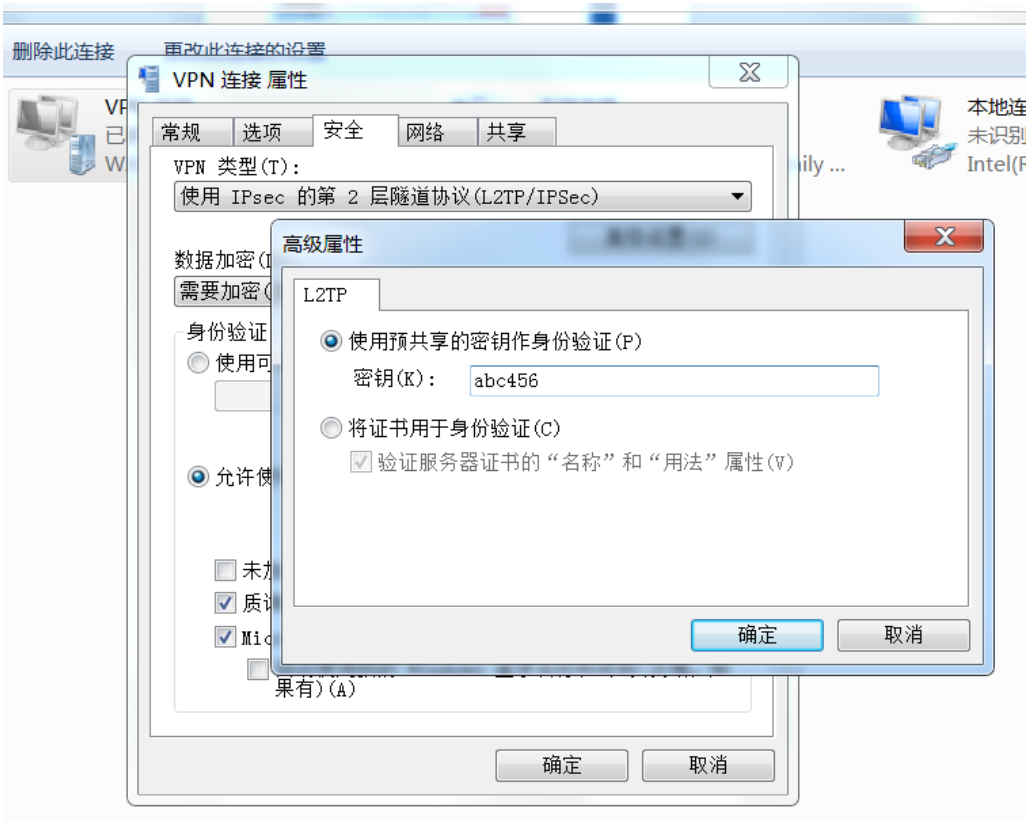

Figure 13. Modify VPN type and set L2TP key
图 13. 修改 VPN 类型及设置 L2TP 密钥

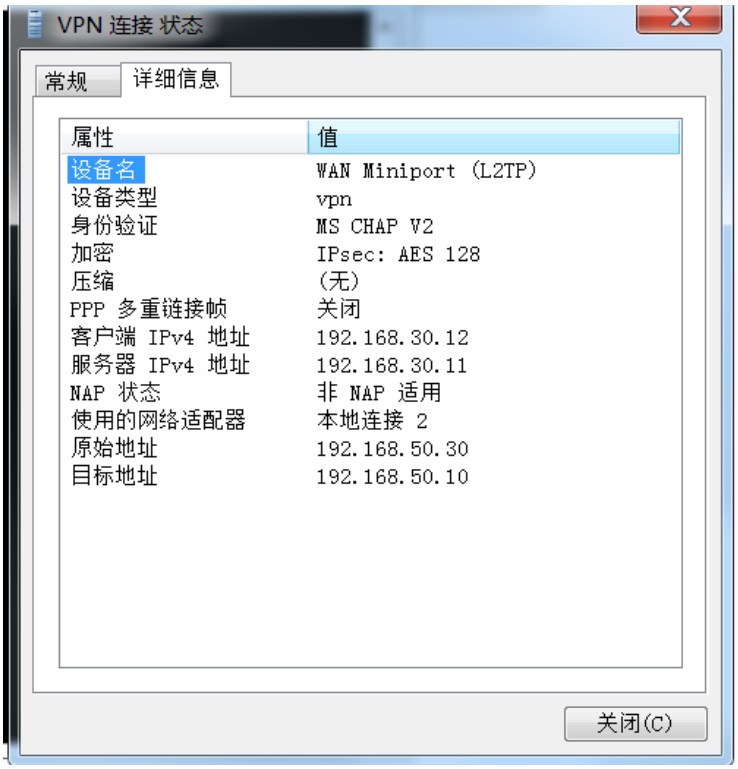

Figure 14. VPN connection
图 14. VPN 连接

4. 结束语

实验证明，利用 VPN 技术能够使用户可降低成本；连接方便灵活；提高传输数据安全可考性并使用户有完全控制主动权。文中重点介绍 VPN 实验的设计与实现。在 Windows Server 2012 环境下要实现基于 PPTP 和 L2TP/IPSec VPN 的远程访问 VPN 技术。SSTP 和 IKEv2 VPN 模式有待进一步实验测试。

致　谢

在此感谢中央高校基本科研业务费资助项目的支持，同时也向所有文献作者与研究相同领域的前辈们表示由衷的感谢。

基金项目

中央高校基本科研业务费资助项目(No.JSJ1202B) (No.3142015022)。

参考文献 (References)

[1] 单家凌. 实验室内 VPN 实验网的组建及测试分析[J]. 计算机时代, 2010(10): 55-57.
[2] 金海, 胡永良. 基于 WINDOWS SERVER 2003 的 VPN 实验环境的构建[J]. 台州学院学报, 2005(12): 17-20.
[3] 庄小妹. VPN 实验教学的设计与实现[J]. 安徽电子信息职业技术学院学报, 2014(6): 21-24.
[4] 王占京, 张丽诺, 雷波. VPN 网络技术与业务应用[M]. 北京: 国防工业出版社, 2012: 1-9.
[5] 罗新, 王会林. 网络实验室 VPN 实验项目的设计与实现[J]. 实验科学与技术, 2012(6): 38-40.
[6] 戴有炜. Windows Server 2012 网络管理与架站[M]. 北京: 清华大学出版社, 2014: 389-486.
[7] 王春海, 宋涛. VPN 网络组建案例实录[M]. 北京: 科学出版社, 2011: 155-172.