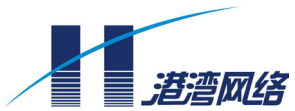
UniWorks VPN Manager 用户手册



UniWorks VPN Manager 用户手册

资料编号	P-1808****-20040520-100（手册编码尚未申请）
产品版本	V1.00
资料状态	发行

手册使用说明

读者对象

本手册的读者对象为安装和使用 UniWorks VPN Manager 系统进行 VPN 业务管理的系统管理员。本手册需要读者熟悉以太网和组建局域网的概念和术语。

内容介绍

本手册详细介绍了 UniWorks VPN Manager 系统的安装和使用方法，是 VPN 业务管理人员了解本系统并顺利完成系统安装与使用的指导文档。《UniWorks VPN Manager 用户手册》共分为两个部分：

第一部分 安装 UniWorks VPN Manager 系统

通过阅读本部分内容，用户将对本系统的用途、特点和版本信息等有一个全面的了解，并可进行本系统的正确安装。具体包括以下内容：

章序号	题目	内容描述
第1章	UniWorks VPN Manager 系统概述	简要讲述UniWorks VPN Manager 系统的功能、特点及版本说明。
第2章	系统构建	讲述UniWorks VPN Manager系统的运行环境构建和安装、卸载方法。

第二部分 配置 UniWorks VPN Manager 系统

通过阅读本部分内容，用户将了解使用本系统的相关知识，并可利用本系统完成 VPN 业务管理。具体包括以下内容：

章序号	题目	内容描述
第3章	相关知识	讲述与使用本系统相关的网络基本知识及其它相关知识。
第4章	系统启动	介绍系统后台服务和前台的组成、功能，以及如何启动它们，并进入管理系统。
第5章	客户管理	讲述客户管理的内容、作用和相关操作。
第6章	业务管理	讲述业务管理的内容、相关技术原理和操作。
第7章	告警管理	讲述告警管理作用和相关操作。
第8章	日志管理	讲述日志管理的内容、作用和相关操作。

手册约定

手册中有关图标的约定如下：

图标	说明
 注意	这个图标表示提醒用户注意事项。
 提示	这个图标主要给出一些与正文相关的信息，同时给用户一些指引，协助用户更好的理解正文的内容。

获取技术支援

港湾网络有限公司建立了以总部技术支援中心、区域技术支援中心和本地技术支援中心为主体的完善的三级服务体系，并提供全天候 24 小时×365 天的电话热线服务。客户在产品使用及网络运行过程中遇到问题时请随时与港湾网络有限公司各地方的服务支持热线联系。请客户到www.harbournetworks.com获取各地服务支持热线电话。此外，客户还可通过港湾网络有限公司网站及时了解最新产品动态，以及下载需要的技术文档。

目录

第一部分

安装 UniWorks VPN Manager 系统

1 UniWorks VPN Manager 系统概述

1.1 简介

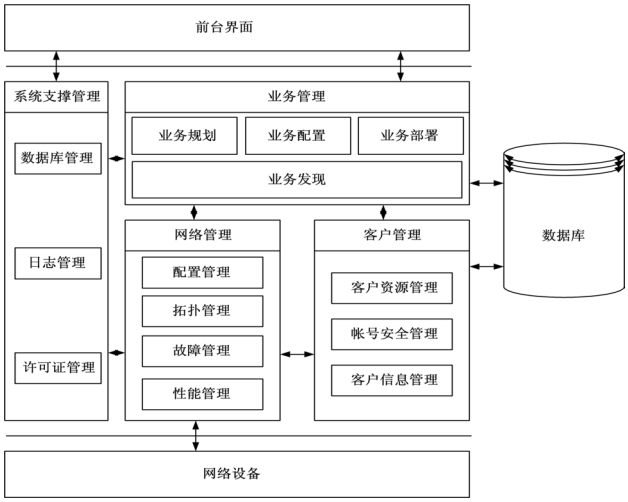
UniWorks VPN Manager 系统是港湾网络有限公司推出的 MPLS VPN 业务管理软件产品。该产品主要用于 MPLS VPN 业务的规划、配置、部署和管理，可以为系统管理人员提供一个直观便捷、图形化的配置管理界面，从而，取代通过命令行进行不同设备配置和管理的大量烦琐操作，减轻工作负担。

UniWorks VPN Manager 系统与港湾网络有限公司的 PowerHammer 系列路由器和 BigHammer 系列交换机产品结合使用，可以为客户提供完善地组建和管理 MPLS VPN 网络的解决方案。

1.1.1 系统组成

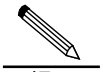
UniWorks VPN Manager 系统组成如下图所示：

图1-1 系统组成



各模块的主要功能如下：

- 前台界面：是图形化的 GUI 用户接口。通过前台界面，将网络运行状况、网络拓扑以及用户关心的相关信息以直观的图形或表格形式呈现给客户。UniWorks VPN Manager 系统可实现后台服务与前台界面的分布式管理，方便用户在远程登录和操作系统。
- 业务管理：业务管理构建在网络管理和客户管理的基础上，是整个 UniWorks VPN Manager 系统的核心部分，主要功能包括：发现网络中已存在 VPN 业务，响应和创建 VPN 业务请求，部署 VPN 业务以及维护 VPN 业务拓扑。
- 系统支撑管理：主要是一些支持系统运行的外围模块。其中包括：数据库管理、系统许可证管理以及日志管理。数据库管理已经实现 Oracle、MySQL 以及 PostgreSQL 等流行的数据库系统；日志管理是整个系统都必须使用的，能够记录系统运行的整个过程，保证对系统中的增加、修改或删除等操作做必需的记录。
- 网络管理：位于 VPN 业务管理系统的最底层，负责和设备通信，能够支持不同厂商的设备，屏蔽各个厂商设备的硬件差异。通过网络管理可以采集网络设备基本信息、维护网络拓扑、下发配置、接收设备告警信息、采集设备性能数据，为整个系统的运行提供基本数据。
- 客户管理：主要用于管理客户信息、客户帐号信息以及客户资源信息。通过客户管理，可以响应客户的申请，让客户通过客户管理系统帐号登录并使用系统；通过权限管理给予不同操作员以不同权限来保证 UniWorks VPN Manager 系统的分级管理，保证系统的安全性；通过客户管理，客户还可以增加客户资源，包括：客户站点以及客户边缘设备等。



目前， UniWorks VPN Manager 系统 V1.00 版本暂不支持业务发现功能。

主要工作流程如下：

用户通过系统前台进行系统登录，然后，根据具体的 VPN 业务需求，配置 VPN 业务并下发配置命令，所有与设备有关的信息均通过网络管理模块向网络设备发送；在完成 VPN 的配置和命令下发后，网络设备会反馈相关的信息并通过网络管理模块上传，一方面存入数据库作为备份供以后分析和查询使用，一方面直接上传给业务管理模块，供业务管理系统实时处理。为了保证系统的安全性， UniWorks VPN Manager 系统提供了完善的日志管理，可以记录客户的每一步操作并将日志存入数据库系统以供以后查询使用。

1.1.2 系统特点

UniWorks VPN Manager 系统的技术架构具有如下特点：

- 分布式设计：分布式软件结构，使系统可分布可集中，设置灵活；
- 多线程设计：支持多线程，提高系统性能，提高 CPU 利用率；
- 组件化设计：按照组件化的设计思想，后台服务全部是组件化实现；
- 存储灵活：提供了多种可选的数据库存储接口，包括 Oracle、MySQL 和 PostgreSQL，可以在系统启动后通过系统配置界面进行数据库的选择和端口的配置；
- 可配置界面风格：采用先进的设计思想，用户可根据个人喜好来灵活的选择界面风格，实现个性化界面，同时系统预定义了多种可选择界面风格供用户参考。

1.2 版本说明

UniWorks VPN Manager 系统 V1.00 for Windows 版本支持的设备种类包括：

- 港湾网络有限公司的 PowerHammer 系列路由器
- 港湾网络有限公司的 BigHammer 系列交换机


注意

1、 UniWorks VPN Manager 系统主要专注于 VPN 业务的部署和维护，对于网络的连通性，比如 IPv4 和 MPLS 网络是否连通并不做检测；

2、 在本系统开始安装并运行以前必须保证用户的网络支持 MPLS 协议并且保证网络系统的连通性。

数据保存的基本方式包括：

- 数据库（Oracle、MySQL 或 PostgreSQL），主要用于保存客户信息、设备信息以及设备的故障及性能信息
- 提供 TXT 文本格式的告警信息保存

UniWorks VPN Manager 系统默认使用的主要 Socket 端口包括：

- 端口 162（UDP）
- 端口 11748（TCP）


注意

如果这几个端口被其它应用程序使用，UniWorks VPN Manager 系统需另行配置才可正常运行。

2 系统构建

2.1 硬件环境

UniWorks VPN Manager 系统安装在 PC 服务器上，其硬件配置要求如下：

- CPU 频率不小于 1.5GHz
- 硬盘容量不小于 40G 字节
- 内存不小于 512M 字节
- 具有网络连接设备

建议配置：

- HP PC Server ML-350 XEON 2.4G
- 40G SCSIHD
- 1024M 内存
- 100/1000M 以太网卡


提示

UniWorks VPN Manager 系统的 V1.00 版本暂不支持 SUN 服务器。

2.2 软件环境

系统的软件环境主要包括：

- 操作系统：Windows 2000 Server / Professional，Windows XP
- 数据库：Oracle、MySQL 或 PostgreSQL


提示

本手册有关界面及操作的讲解全部基于 Windows 2000 Professional。

2.3 UniWorks VPN Manager系统安装

安装 UniWorks VPN Manager 系统前须先安装数据库并启动数据库服务。

安装数据库并启动数据库服务


提示

请将数据库系统安装在磁盘空间比较大的路径下，因为在系统运行过程中，将有大量的数据存储在该路径下，需占用很大空间。建议磁盘可用空间大于 1G。

以安装 MySQL 为例，在安装光盘上找到 mysql-4.0.20c-win 目录，进入本目录，然后直接双击运行本目录下的 setup.exe 即可开始安装 MySQL 数据库：

1. 运行 setup.exe 后弹出 MySQL 系统安装主界面；
2. 点击“Next”按钮，出现“Information”信息窗口；点击“Next”按钮，进行下一步安装，弹出“Choose Destination Location”对话框；
3. 在“Choose Destination Location”对话框中，用户可以通过“Browse”按钮选择安装路径，请确定所选路径下具有足够的磁盘空间。系统默认安装路径为“C:\mysql”。安装路径选好后，点击“Next”按钮进行安装类型的选择，弹出“Setup Type”对话框；
4. 在“Setup Type”对话框中，选择“Typical”安装类型，点击“Next”安装 mysql 数据库即可，用户可以看到系统安装进度条，此步骤需要几分钟的时间（具体时间因 PC 服务器的硬件配置及软件系统的不同而略有差异）；
5. 数据库安装完毕后，弹出“Setup Complete”对话框，提示用户安装已经完成，用户点击“Finish”按钮即可结束安装。
6. 接下来，向 Windows 系统注册数据库服务。首先在 Windows 命令行下进入 MySQL 安装目录下的 bin 目录（默认是 c:\mysql\bin），执行“mysqld-nt --install”即可。
7. 最后启动数据库服务。打开“控制面板—管理工具—服务”，双击 MySQL 项，弹出对话框后点击“启动”按钮即可。

设置访问数据库服务方式

在数据库设置了密码，或者设置了非默认端口，以及数据库与 UniWorks VPN Manager 系统不在同一台计算机上的情况下，需要通过环境变量通知安装程序访问数据库服务器的方式。具体方法如下：

1. 在桌面上，右键单击“我的电脑”，选择“属性”菜单；
2. 选则“高级”并点击“环境变量”按扭；
3. 点击“新建”按扭，在“变量名”一栏添入环境变量名称（参考表 2-1 ），在变量值一栏设置正确的信息，最后点击“确定”就加入一条变量；
4. 将所有需要设置的变量设置完成后（如果不设置将会使用缺省值），点击“确定”，使刚加入的变量生效。

表2-1 环境变量表

环境变量名称	缺省值	说明
MYSQL_USERNAME	root	MySQL数据库用户名
MYSQL_PASSWORD	空	MySQL数据库用户密码
MYSQL_HOST	localhost	MySQL数据库主机地址
MYSQL_PORT	3306	MySQL数据库主机端口

安装 UniWorks VPN Manager 系统


注意

安装 UniWorks VPN Manager 系统前，请先确认数据库服务已经启动。

安装程序在光盘的 UniWorksVPN Manager 目录下，您可以直接运行光盘上 UniWorks VPN Manager 目录下的 uvm-1.0-win32.exe，或把 UniWorks VPN Manager 目录下的所有文件拷贝到本地，再运行 uvm-1.0-win32.exe。主要安装过程描述如下：

1. 运行 uvm-1.0-win32.exe 后，将会弹出解压缩界面，进行解包过程，等解包成功以后就会弹出 UniWorksVPN Manager 系统安装对话框；
2. 点击“下一步”按钮，出现“软件版权协议”窗口。用户必须认真阅读《港湾网络有限公司 UniWorks VPN Manager 软件产品最终用户使用许可协议》内容。用户确认同意协议内容请点击“接受”按钮，进行下一步安装，

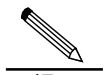
弹出“安装类型”对话框；点击“拒绝”按钮则退出安装；

3. 在“安装类型”对话框中，只有一个选项，就是“完全”；对于目的文件夹，默认的是“C:\Program Files\harbournetworks \UniWorks VPN Manager”目录下，可以点击“浏览”按钮来修改默认的安装路径，选择完毕，点击“下一步”，弹出“选择组件”窗口，直接点击“下一步”，弹出选择“选择安装文件夹”窗口；
4. 在“选择安装文件夹”窗口，程序文件夹下面键入合适的文件夹名称，或者使用默认的文件夹“UniWorks VPN Manager”，点击“下一步”继续，会弹出一个“开始安装”对话框；
5. 在“开始安装”对话框中列出了，上几步列出的安装选项，如果对于那些不满意可以依次点击“上一步”退回到前面的界面就行修改，具体请参看以前的步骤，如果对选项满意请点击“安装”按钮，开始 UniWorks VPN Manager 系统的安装，用户可以看到系统安装进度条，此步骤需要几分钟的时间（具体时间因 PC 服务器的硬件配置及软件系统的不同而略有差异）。


注意

为了避免文件冲突，确保 UniWorks VPN Manager 系统正确安装和运行，请将 UniWorks VPN Manage 系统安装在一个独立目录下。

UniWorks VPN Manager 系统安装完成后，可在 Windows 的“开始－程序”中看到 ‘UniWorks VPN Manager’程序组，在程序组下可看到 ‘UniWorks VPN Manager’和‘VpnManagerUninstall’两个快捷方式，其中‘UniWorks VPN Manager’用来启动 UniWorks VPN Manager 系统的前台。


提示

卸载说明：

用户可通过运行安装目录下的卸载程序 VpnManagerUninstall.exe、“开始—程序—UniWorks VPN Manager”程序组中的快捷方式“VpnManagerUninstall”或在“控制面板—添加/删除程序”中卸掉本系统。

第二部分

配置 UniWorks VPN Manager 系统

3 相关知识

3.1 概述

本章对网络和路由基本知识、MPLS(Multi-Protocol Label Switching，多协议标签交换)协议和 VPN（Virtual Private Network，虚拟专用网）技术等进行了简要介绍。了解和掌握这些知识，将有助于您更好的理解和使用 UniWorks VPN Manager 系统。

3.2 网络基本知识

3.2.1 OSI（开放系统互联）参考模型

开放系统互联参考模型（OSI）是为解决不同供应商提供的设备之间的通信问题而提出的。通常情况下，不同厂家开发的网络结构和专用协议是不兼容的，为此国际标准化组织设计了 OSI 模型，将网络层次分为 7 个不同的级别，并为不同级别的数据通信建立了一套规则来解决这些兼容性问题，使来自不同厂家的设备可以互相通信。OSI 模型的层次如下图所示：

图3-1 OSI 模型的层次

7	应用层
6	表示层
5	会话层
4	传输层
3	网络层
2	数据链路层
1	物理层

在该模型中，报文起源于发送信息的计算机的应用层，然后逐步传递到物理层，再

通过网络媒介传递到接收计算机的物理层，最后传递到接收机的应用层。OSI 模型各层的说明如下：

第 7 层：应用层，提供网络服务的软件，如文件传输、电子邮件、远程登录等。它在用户程序和网络之间提供接口。

第 6 层：表示层，将传出数据从机器指定的格式转换为一个国际标准格式和将传入数据从国际标准格式转换为机器指定的格式。

第 5 层：会话层，允许建立和终止一个通信路径，确保发送方是可靠的并对建立的一个连接有访问权，协调两个系统之间的通信。

第 4 层：传输层，在发送方和接收方之间提供数据流，并确保数据达到正确的目的地。该层的另一个作用是确保分组以接收方和应用程序能处理的速率发送。在接收方，传输层将分组重新组装成报文，并将其传递到更高层。

第 3 层：网络层，决定分组通过网络时采取的路径。网络层还控制网络接收分组的速率，以避免网络拥塞和能从拥塞中恢复。

第 2 层：数据链路层，提供分组传输、执行错误检测和纠错功能，以确保接收和发送分组包含相同的信息。

第 1 层：物理层，建立计算机设备和网络之间的物理连接，并提供从一个系统到其它系统的比特传输。

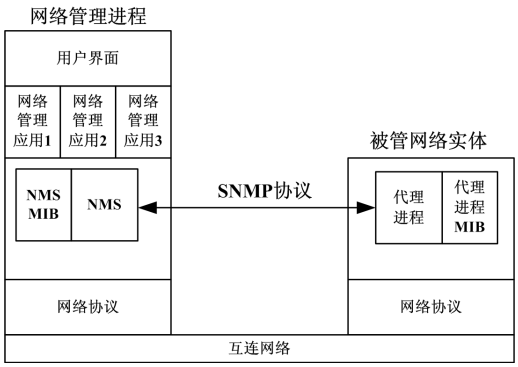
3.2.2 相关网络协议

1. SNMP（简单网络管理协议）

SNMP 是数据网络中使用的最通用的管理协议。它提供了一种从网络设备获得信息并将信息发送到网络设备的手段。SNMP 基于管理员－代理模型，使用管理信息库（MIB）来交换管理员和代理之间的信息。使用 SNMP 协议，管理员通过发送请求到运行在受控设备上的代理来查询和修改每个受控设备的状态和配置信息。所有命令使用 UDP/IP 协议，这意味着管理员和代理之间的通信是无连接的。SNMP 作用于应用层。SNMPV2c 包括 SNMPV1 的基本功能，并增加了新的报文类型、标准化多协议支持、改进的安全性、新 MIB 对象和一种与 SNMPV1 共存方式。SNMPV2c 可用于要使用较少的网络资源来检索大量的管理信息的场合。

SNMP 参考模型如下图所示：

图3-2 SNMP 参考模型



SNMP 参考模型说明了 SNMP 网络管理框架的一般总体结构，以及系统中各个组成部分及其相互关系。其中，主要构成包括：互连网络、网络协议、网络管理进程和被管网络实体。

1） 互连网络

在 SNMP 参考模型中，互连网络是指采用相同协议，通过网关相连的一个或多个网络的集合。如果所实现的全局编址方案正确，采用了标准化的协议，采用的路由选择方案能保证报文的及时可靠传送，则任意两个端点之间都可以互相通信。

采用 SNMP 时，与此相关的网络协议主要是 TCP/IP。

2） 网络协议

网络协议就是使互连网络能够实现通信的规则。对于采用 TCP/IP 通信的互连网络来说，各种协议分别在组成 TCP/IP 协议集的 4 层协议中运行。举例来说，一台主机会至少在每一层实现一个协议。网络协议常常称为“协议栈”：

- 协议栈中的低层是指最“靠近”硬件的部分。在 TCP/IP 协议集中，这一层称为网络接入层。其主要功能是提供主机与网络间的可靠数据互换。存在很多种网络访问协议，每一种协议都对应于可以连接互连网络上的多种不同类型网络；
- Internet 层负责将数据从源主机传送到目的主机。Internet 层的主要部件是 IP（Internet 协议）。IP 是无连接的数据协议，它并不保证端到端的可靠传输。IP 的特性包括有指定服务类型、Internet 层编址、分片和重组、检验和初步的安全性。Internet 层的另一个重要协议是互连网控制报文协议（ICMP），用来报告差错和拥塞；

- 传输层负责两个进程间的端到端的数据传输，要么用可靠的 TCP，要么用不保证可靠的 UDP；
- TCP/IP 协议栈中的高层网络协议是处理层或应用层。这一层直接为端用户或应用程序提供服务，如 Telnet、FTP、SMTP 和 SNMP 等。

3） 网络管理进程

网络管理进程通过网络协议和 SNMP 协议与互连网络中被管理的网络实体通信，主要包括 4 个部件：

- 网络管理站（NMS）：是监视控制代理进程的处理实体，代理进程在互连网中也是起管理作用的。NMS 及其代理进程形成一个共同体。NMS 可以对每个代理的 MIB 中的特定对象进行读写操作，即管理相应的网络设备。NMS 也可以将每个代理中有关的管理信息存储在自己的本地数据库中；
- 网络管理站的 MIB 和数据库：网络管理站的管理信息库中含有本共同体中所有代理 MIB 的主清单。如果网络管理站要控制每个代理的 MIB 变量，那么它必须知道或能够发现该变量的存在。通常，网络管理站会在其本地数据库中存有自己的 MIB 和额外的管理信息；
- 网络管理应用程序：网络管理应用程序将 SNMP 数据转换成网络管理用户可用的信息。它包括一大堆程序，用于轮询代理、进行 set 和 get 请求，以及处理接收到的陷井报文。网络管理应用程序实现了越来越多非常有用的网络管理功能；
- 网络管理用户界面：端用户是通过用户界面来使用网络管理进程设备的。大多数网络管理进程提供图形用户界面（GUI）来表达性能统计数据、帐务汇总、故障报告、配置清单、创建查询表格、拓扑图等等。

4） 被管网络实体

就是含有代理进程的网络设备。它也要用网络协议和 SNMP 协议在互连网上与网络管理进程的 NMS 通信。被管网络实体包含 2 个关键部件：

- 代理进程：是处理实体，从所在共同体中的 NMS 接收请求，如果请求合法就进行处理，最后发出适当的响应。代理进程也可以配置成要发送陷井报文，以报告异步预定义的事件。代理进程利用操作支持程序操作本地数据结构以提取和设置它所控制的各个 MIB 对象。
- 代理进程的 MIB：代理进程的管理信息库是它所关心的变量集合。构成特定代理管理信息库的 MIB 组决定于该设备的功能和所要管理的资源。

2. TCP/IP（传输控制协议/网际协议）

TCP/IP 是两个使用最广泛的 Internet 协议。

TCP 提供 IP 网络上的数据传输，作用于 OSI 模型的第 4 层，能够向发送方提供到达接收方数据包的传送信息。当传送过程中出现数据包丢失情况时，TCP 可以重新发送丢失的数据包直到数据成功到达接收方或者出现网络超时。TCP 还可以识别重复信息，丢掉不需要的多余信息，使网络环境得到优化。如果发送方传送数据的速度大大快于接收方接收数据的速度，TCP 可以采用数据流控制机制减慢数据的传送速度，协调发送和接收方的数据响应。

IP 作用于 OSI 模型的第 3 层，除了可以提供网络路由之外，还具有错误控制以及网络分段等众多功能。

TCP/IP 作为一个互连设备和网络的共同起源，广泛用于连接使用不同技术的计算机。大多数管理解决方案需要 TCP/IP 作为信息源和信息载体。

3. UDP（用户数据报协议）

UDP 是一种允许一台机器上的应用程序与另外一台机器上的应用程序交换数据报而不需要确认或保证传递的协议。UDP 作用于 OSI 模型的第 4 层，即传输层。其与 TCP 的明显区别是不具备复杂的可靠性与控制机制。TCP 提供的是面向连接（即在传输前就建立好了点到点的连接）的、可靠的数据流传输，而 UDP 提供的是非面向连接（即在数据传输前不建立连接，而是在每个中间节点对数据包进行路由）的、不可靠的数据流传输。当强调传输性能而不是传输的完整性时，如音频和多媒体应用，UDP 是一个好的选择。把 SNMP 建立在 UDP 上的部分原因是设计者认为当发生网络阻塞时，UDP 较低的开销使其有更好的机会去传送管理数据；当强调数据传输的完整性、可控制性和可靠性时，则 TCP 是当然的选择。

4. ICMP（Internet 控制报文协议）

ICMP 是伴随 IP 一起必须实现的协议。ICMP 的 RFC 编号是 792。它利用 IP 服务发送各种反映差错和状态的报文。现在有 13 个 ICMP 报文，每个报文的类型值都是唯一的。ICMP 报文及其相应的类型值如下表所示：

表3-1 ICMP 报文类型

报文	类型值
回声（ECHO）回答	0
目的地址不可达	3
源站抑制	4

重定向	5
回声（ECHO）请求	8
超时	11
参数不可理解	12
时间戳请求	13
时间戳回答	14
信息请求	15
信息回答	16
地址掩码请求	17
地址掩码回答	18

ICMP 协议最著名的地方是其在 PING（Packet Internet Groper）程序中的应用。PING 会发出一个类型为回声请求的 ICMP 报文，然后等待回声回答，这样就可以确认在两个端点之间存在 IP 连接。例如，可以用命令：

```
ping 192.168.0.1
```

来测试本机是否可以跟 IP 地址为 192.168.0.1 的设备连接通信。

如果设备连通，将出现以下信息：

```
PING 192.168.0.1 : 56 data bytes.
Press Ctrl-c to Stop.

Reply from 192.168.0.1 : bytes=56: icmp_seq=0 ttl=128 time=10 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=1 ttl=128 time=5 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=2 ttl=128 time=5 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=3 ttl=128 time=5 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=4 ttl=128 time=5 ms

----192.168.0.1 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss

round-trip(ms) min/avg/max = 0/36/100
```

如果设备没有连通，将出现以下信息：

```
PING 192.168.0.1 : 56 data bytes.
Press Ctrl-c to Stop.

Request time out.
Request time out.
Request time out.
Request time out.
```

```
Request time out.

----192.168.0.1 PING Statistics----
5 packets transmitted, 0 packets received, 100% packet loss
```

3.2.3 网络硬件设备

基本的网络通信设备包括中继器、集线器、网桥、交换机、路由器。这些设备工作在 OSI 模型的不同层，使用不同的网络协议和执行不同的任务。如下表所示：

表3-2 工作在 OSI 模型不同层上的设备

OSI 模型的层次		该层上的协议	该层上的硬件设备
7	应用层	SNMP Berkeley Services ARPA Services	网关
6	表示层		
5	会话层		
4	传输层	TCP UDP	
3	网络层	IP/IPX ICMP ARP/RARP	路由器 交换机
2	数据链路层	IEEE802.X DHCP MAC地址	网桥 交换机
1	物理层	10Base2 10Base5	简单中继器 集线器

1. 网关

网关工作在应用层，可以包含 OSI 模型的所有层。网关是一个计算系统，通过编程可以实现任何复杂的协议转换和协调，如 IP 和 IPX 之间的转换。

2. 路由器

路由器工作在网络层，其作用是连接两个使用不同技术的网络，并提供分组从一个网络传递到另一个网络的智能解决办法，还能在多个集线器和网桥之间转发流量。

3. 网桥

网桥工作在数据链路层，其作用是允许网络可以具有不同的物理信号，但又具有兼容的数据链接寻址模式。在信息从一个网段流向另一个网段时，对于不需要通过骨干网转发的信息，网桥将进行过滤，从而减少骨干局域网上的流量。网桥的通常用

法是允许在一个以太局域网上的用户与一个令牌环局域网上的用户相互通信。

4. 交换机

交换机工作在数据链路层，其作用是将数据发送到目的地，该目的地由分组的低层介质访问控制（MAC）地址决定。交换机象网桥那样，对流量进行限制，且不识别网络协议。现在，新的交换设备是多层交换，或路由交换，这种设备工作在第 3 层，通过路由器智能与交换机效率的结合，从而在数据路由时可以以较高的速度进行。

5. 集线器

集线器工作在物理层。集线器只是一个多口中继器，可以用来增加整个网络的大小和在一个单一网段上的节点数量。集线器允许隔离子网错误，且能在不中断整个网络的情况下向一个网段增加节点。

6. 简单中继器

简单中继器工作在物理层，通常用于将两个网段连接成一个大段，或扩展一个已存在的网段。两个网段之间对传递的报文不进行过滤。简单中继器能对数据信号进行加强，因此可以用来扩展传送距离。简单中继器没有内置网络智能，通常严格用于信号传播。

3.2.4 网络分类

1. 按地理位置分类

网络按地理位置分类，包括：

- 局域网（Local Area Network，简称 LAN）：一般限定在较小的区域内，小于 10km 的范围，通常采用有线的方式连接起来；
- 城域网（Metropolis Area Network，简称 MAN）：规模局限在一座城市的范围内，10～100km 的区域。
- 广域网（Wide Area Network,简称 WAN）：网络跨越国界、洲界，甚至全球范围。

目前局域网和广域网是网络的热点。局域网是组成其它两种类型网络的基础，城域网一般都加入了广域网。广域网的典型代表是 Internet 网。

2. 按拓扑结构分类

网络的拓扑结构是指网络中通信线路和站点（计算机或设备）的几何排列形式。

网络按拓扑结构分类，包括：

- 星型网络：各站点通过点到点的链路与中心站相连。特点是：很容易在网络中增加新的站点，数据的安全性和优先级容易控制，易实现网络监控，但中心节点的故障会引起整个网络瘫痪。
- 环形网络：各站点通过通信介质连成一个封闭的环形。环形网容易安装和监控，但容量有限，网络建成后，难以增加新的站点。
- 总线型网络：网络中所有的站点共享一条数据通道。总线型网络安装简单方便，需要铺设的电缆最短，成本低，某个站点的故障一般不会影响整个网络。但介质的故障会导致网络瘫痪，总线网安全性低，监控比较困难，增加新站点也不如星型网容易。

树型网、簇星型网、网状网等其他类型拓扑结构的网络都是以上述三种拓扑结构为基础的。

3. 按传输介质分类

网络按传输介质分类，包括：

- 有线网：采用同轴电缆和双绞线来连接的计算机网络。同轴电缆网是常见的一种连网方式，它比较经济，安装较为便利，传输率和抗干扰能力一般，传输距离较短；双绞线网是目前最常见的连网方式，它价格便宜，安装方便，但易受干扰，传输率较低，传输距离比同轴电缆要短。
- 光纤网：光纤网也是有线网的一种，但由于其特殊性而单独列出，光纤网采用光导纤维作传输介质。光纤传输距离长，传输率高，可达数千兆 bps，抗干扰性强，不会受到电子监听设备的监听，是高安全性网络的理想选择。不过由于其价格较高，且需要高水平的安装技术，所以现在尚未普及。
- 无线网：采用空气作传输介质，用电磁波作为载体来传输数据，目前无线网联网费用较高，还不太普及。但由于联网方式灵活方便，是一种很有前途的连网方式。

局域网通常采用单一的传输介质，而城域网和广域网采用多种传输介质。

4. 按通信方式分类

网络按通信方式分类，包括：

- 点对点传输网络：数据以点到点的方式在计算机或通信设备中传输。星型网、

环形网采用这种传输方式。

- 广播式传输网络：数据在共用介质中传输。无线网和总线型网络属于这种类型。

5. 按使用目的分类

网络按使用目的分类，包括：

- 共享资源网：使用者可共享网络中的各种资源，如文件、扫描仪、绘图仪、打印机以及各种服务等。Internet 网是典型的共享资源网。
- 数据处理网：用于处理数据的网络，例如科学计算网络、企业经营管理用网络。
- 数据传输网：用来收集、交换、传输数据的网络，如情报检索网络等。

目前网络使用目的都不是唯一的。

6. 按服务方式分类

网络按服务方式分类，包括：

- 客户机/服务器网络：服务器是指专门提供服务的高性能计算机或专用设备，客户机是用户计算机。这是客户机向服务器发出请求并获得服务的一种网络形式，多台客户机可以共享服务器提供的各种资源。这是最常用、最重要的一种网络类型。不仅适合于同类计算机联网，也适合于不同类型的计算机联网，如 PC 机、Mac 机的混合联网。这种网络安全性容易得到保证，计算机的权限、优先级易于控制，监控容易实现，网络管理能够规范化。网络性能在很大程度上取决于服务器的性能和客户机的数量。目前针对这类网络有很多优化性能的服务器称为专用服务器。银行、证券公司都采用这种类型的网络。
- 对等网：对等网不要求文件服务器，每台客户机都可以与其他每台客户机对话，共享彼此的信息资源和硬件资源，组网的计算机一般类型相同。这种网络方式灵活方便，但是较难实现集中管理与监控，安全性也低，较适合于部门内部协同工作的小型网络。

7. 其他分类方法

如按信息传输模式的特点来分类的 ATM 网，网内数据采用异步传输模式，数据以 53 字节单元进行传输，提供高达 1.2Gbps 的传输速率，有预测网络延时的能力。可以传输语音、视频等实时信息。

另外，还有如企业网、校园网，根据名称便可理解。

从不同的角度对网络有不同的分类方法，每种网络名称都有特殊的含意。几种名称

的组合或名称加参数更可以看出网络的特征。千兆以太网表示传输率高达千兆的总线型网络。

了解网络的分类方法和类型特征，是熟悉网络技术的重要基础之一。

3.3 操作系统

UniWorks VPN Manager 系统 V1.00 for Windows 版本的操作系统为 Windows 2000 Server / Professional 或 Windows XP。

本手册主要涉及 Windows 2000 操作系统的功能或操作，但不作详细说明。有关 Windows 2000 操作系统的知识，请用户参考操作系统随带的文档资料。

3.4 路由基本知识

3.4.1 概述

路由是路由器最基本的功能。在 HOS 软件系统中，采用了控制与转发分离的技术。路由协议作为控制信令协议，负责计算出路由；转发引擎按照路由协议给出的路由来进行转发操作。

什么是路由呢？

事实上整个数据通信网络的基础架构有点类似于现实生活中的城市交通网络。数据通信网络解决从一个设备到另一个设备之间的报文通讯问题。现实生活中人们也面临着从一个地方到另一个地方的交通问题。

要解决交通问题，首先得有地址的概念。这样可以把问题精确地描述成类似从“西三环北路 21 号”到“王府井 1 号”如何走。在 TCP/IP 网络中，IP 地址相当于城市交通中的地址，路由就相当于每个路口的路标牌，指导每个报文在十字路口该往哪走。在现实生活中，当然不必每到一个路口就去看路标，这是因为我们有记忆罢了。

下面要引入网段（或称为子网）的概念。在上面的地址“西三环北路 21 号”中“西三环北路”就是一个网段（平时我们往往称为“XX 路”），“21 号”是在这个网段的一个号码。在所有实际可寻址的网络中，其实都假定一个子网的地址在逻辑上都在一起。要是 010 打头的电话号码有的在北京，有的在深圳，那 PSTN 就乱套了。

在有了 IP 地址的概念和一个子网的地址逻辑上在一起的前提后，就可以路由了。

路由协议起的作用就是把整个城市的地图给画出来，在每个路口详细地标上路标牌。

3.4.2 IP路由

IP 路由是 IP 协议三层转发的控制信息，它说明最终达到某个网段的"下一跳"应转发到哪里。一条 IP 路由的主要内容是：a）目的地址及掩码 b）下一跳地址或出接口。其中目的地址及掩码描述目的地信息；下一跳地址或出接口描述在本路由器中应该如何转发符合本路由目的地址描述的报文。目的地址及掩码相同的路由称为相同的路由。

IPv4 通讯可以分为单播、组播、广播三大类。通常的 IP 数据通信都使用单播方式，即每个报文的接收者有一个明确的唯一的 IP 地址，主要用以实现点对点的通信。IP 组播可以支持用户将一个数据流发送给特定的多个接收者，支持组播的网络会自动在适当的位置复制 IP 组播报文，而不需要数据源重复发出多份数据，可以显著节省网络带宽占用，从而较好地实现了单点对多点的通信。而广播方式是无条件地发送给所有 IP 设备，所以它只少量应用在本地网段内部。

广播不需要路由协议，因为网络中的每个三层设备都不允许转发广播报文。这也是为什么局域网存在广播风暴，而三层网就不存在的原因。单播和组播就需要不同的路由协议。

3.4.3 IP路由协议

路由协议就是根据特定的判断标准和算法，计算出网络中到不同子网的最佳路径的协议。

根据不同的报文，路由协议分成单播路由协议和组播路由协议两类。

根据适用的范围，路由协议分成 IGP（Interior Gateway Protocol）和 EGP（Exterior Gateway Protocol）。

根据采用的算法不同，单播路由协议分成距离矢量协议（Distance-Vector）和链路状态协议（Link State）；组播路由协议分成密集模式（Dense Mode）和稀疏模式(Sparse Mode)。

目前主流的单播路由协议有 RIP v1/v2、OSPF v2、BGPv4，另外，兼容 CISCO 的 IGRP 和 EIGRP 私有协议，主流的组播路由协议是 PIM；这些动态路由协议在 HOS 软件中都能提供完善的支持。

IGP&EGP

要介绍 IGP&EGP，需先了解自治系统的概念。

自治系统（AS）：网络中遵循同一管理策略的设备，称为一个自治系统。

光看定义，有点莫名其妙。举几个例子就明白了。象电信 169 网是个自治系统，中国教育网是个自治系统。自治系统是个逻辑上的概念，不是地域上的。自治系统更强调的是非技术层面对网络的划分，一般来说不同运营商的网络就是不同的自治系统。

IGP 就是在一个自治系统内部的路由协议。在一个自治系统内，主要考虑技术层面上的事情，以最短的时间、最小的开销寻找路由就是 IGP 的职责，它们的判断依据往往是网络带宽、时延等等。

EGP 是跨自治系统的路由协议。在这一层面上，往往有很多非技术因素在左右路由的选择。比如 Sprint 会选择由欧洲去五角大楼的数据最好不要经过阿拉伯地区，在技术上就转化成不要选择途径阿拉伯 Router 的路由。比如有的国家的网络出口往往会屏蔽一些地址。（以上只是举例，不代表本公司的立场和观点）

EGP 就往往重点不在如何计算路由上，在于如何提供各种粒度的路由策略，供网络管理员来实施。

目前，EGP 协议只有一种：BGP，其他路由协议，如 RIP、OSPF、IGRP 和 EIGRP 都是 IGP。它们在 TCP/IP 协议栈中的位置如下图所示：

图3-3 路由协议在 TCP/IP 协议栈中的位置

<table>
<tr><td>BGP</td><td>RIP</td><td rowspan="2">OSPF</td><td rowspan="2">EIGRP</td><td rowspan="2">IGRP</td></tr>
<tr><td>TCP</td><td>UDP</td></tr>
<tr><td colspan="2">IP</td><td colspan="3">Raw IP</td></tr>
<tr><td colspan="5">链路层</td></tr>
<tr><td colspan="5">物理层</td></tr>
</table>

下面对 RIP、OSPF 和 BGP 做简要介绍。

■ RIP（路由信息协议）

RIP（Routing Information Protocol ，路由信息协议）是所有路由协议中最简单的协议，在实际使用中有着广泛的应用。RIP 是基于 Distance-Vector（简称 D-V）算法的协议，它的协议信息封装在 UDP 数据报文中。RIP 文档见于 RFC 1058、RFC 2082、RFC 2453。

当路由器启动以后，首先通过运行 RIP 协议的端口分别向外发送一个 RIP request

报文。在此以后，每隔 30 秒向外发送一次更新报文。对于某一条从其他路由器学习到的路由信息，如果在 180 秒内没有收到这条路由信息的更新报文，就将这条路由信息标志为不可达；若在其后 120 秒内仍未收到更新报文，就将该条路由从路由表中删除。

RIP 使用跳数（Hop Count）来衡量到达信宿机的距离，称为路由权值（Routing Metric）。在 RIP 中，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，RIP 规定 metric 取值为 0 到 15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。较小的取值范围使 RIP 不适用于大型网络。

RIP 以规则的时间间隔及在网络拓扑改变时发送路由更新信息，发送者记为下一跳。RIP 路由器只维护到目的的最佳路径（具有最小度量值的路径）。更新了自己的路由表后，路由器立刻发送路由更新把变化通知给其它路由器，这种更新是与周期性发送的更新信息无关的。

为了适应快速的网络拓扑变化，RIP 规定了一些与其它路由协议相同的稳定特性。例如，RIP 实现了 split-horizon 和 hold-down 机制来防止路由信息的错误传播。此外，RIP 的跳数限制也防止了无限增长的路由环。

如果路由器有缺省路由存在，RIP 将会把 0.0.0.0/0 作为缺省路由向外通告。网络 0.0.0.0/0 并不存在，RIP 把 0.0.0.0/0 视为缺省网络路由(最后一站的网关)。RIP 路由信息将向指定网络上的接口发送出去，如果 RIP 启动后没有配置接口网络，RIP 不向外界发布任何更新信息。

HOS 的 RIP 版本 2 支持纯文本、MD5 认证、路由汇总、可变长度子网掩码(VLSM)。

为了提高性能，RIP 协议支持水平分割算法，对路由的更新采用触发更新的方式，并允许引入其它路由器学到的路由。

■ OSPF（开放最短路径优先协议）

OSPF（Open Shortest Path First，开放最短路径优先协议）是一类内部网关协议(Interior Gateway Protocol)，它可以计算和设置一个自治系统中各个路由器的路由表。

OSPF 是 IETF 组织开发的一个基于链路状态的路由协议。在 IP 网络上，OSPF 通过收集和传递链路状态（Link State）来动态地发现路由。 每个支持 OSPF 协议的路由器都维护着一份描述整个自治系统网络拓扑结构的数据库（LSDB），该数据库是收集所有路由器的链路状态广播（LSA）而得到的。 根据链路状态数据库，各路由器会构建一棵以自己为根的最短路径树（SPF Tree），这棵树给出了到自治系统中

各节点的路由。

■ BGP（边界网关协议）

BGP（Border Gateway Protocol，边界网关协议）是一种自治系统间的动态路由协议，它的基本功能是在自治系统间自动交换无环路的路由信息，通过交换带有自治系统号(AS)序列属性的网络可达信息，来构造自治系统的拓扑图，从而消除路由环路，并使得基于自治系统级别的策略控制得以实施。

运行 BGP 协议来交换路由信息的路由器被称为 BGP 发言人（BGP Speaker），和它通信的其它的 BGP 发言人，被称为它的邻居（peer）。BGP 作为高层协议，使用 TCP 作为其传输层协议，通过建立可靠的传输层连接来交换报文。一旦和邻居间的传输层连接建立后，连接双方就各自发送 Open 报文来协商参数，参数确认后，双方就可以通过发送 Update 报文来交换路由信息。初始的数据流是整个的 BGP 路由表，之后只有在路由信息发生变化时，才发布路由更新信息，以此来减少 BGP 传播路由所占用的带宽。BGP 通过周期性地发送 keepalive 报文来确保连接的有效性，如果有错误发生，就发送 Notification 报文，并关掉连接。

当 BGP 从其不同邻居收到同一网络地址路由信息时，它总是选择最佳的路由对外发布。BGP 提供了多个路径属性来权衡最佳路由。路径属性是 Update 报文的一个域，标识了 Update 报文中的网络可达信息（即路由的网络地址）的属性，如起源、下一跳、自治系统路径等。BGP 通过对各路径属性的优先值来判断最佳路由。通过配置或者改变路径属性，BGP 可以提供多种过滤和 route-map 等丰富有力的策略配置手段，来控制路由的传播。

BGP 连接有两种类型：IBGP(Internal BGP)和 EBGP(External BGP)。在同一自治系统中建立的 BGP 连接称为 IBGP，不同自治系统间的 BGP 连接为 EBGP。本地的 BGP 协议对 IBGP 和 EBGP 邻居使用不同的处理机制。当从 EBGP 邻居收到的路由信息，如果是最佳路由，本地的 BGP 协议就将它转发给其他的所有邻居；如果是从 IBGP 邻居收到的路由信息，本地的 BGP 协议只会将它转发给其他的 EBGP 邻居，而不会转发给其他的 IBGP 邻居。所以运行于同一自治系统中的 BGP 邻居，为了路由选择和路由策略的一致性，要求全连接(Fully meshed)，即在同一自治系统内的任意两个运行 BGP 的路由器间都要有 IBGP 连接。为避免全连接所带来的巨大开销，在 HammerOS 中引入了反射器和联盟等配置。

BGP 协议自使用以来已经经历了 4 个版本。它最早的三个版本分别是 RFC1105（BGP-1）、RFC1163（BGP-2）、RFC1267（BGP-3）。当前使用的是 RFC1771（BGP-4），它支持基于无类域间路由 CIDR(Classless Interdomain Routing)的路由聚合

（Routes Aggregation），可以有效的减少日益增大的路由表，这是比较早版本的一个重要改进。目前，BGP-4 正迅速成为事实上的 Internet 外部路由协议标准。

3.5 MPLS(多协议标签交换)

Internet 在近些年中的爆炸性增长，为 Internet 服务提供商(ISP)提供了巨大的商业机会，同时也对其骨干网络提出了更高的要求，人们希望 IP 网络不仅能够提供 E-Mail、上网等服务，还能够提供宽带、实时性业务。ATM 曾经是被普遍看好的能够提供多种业务的交换技术，但是由于实际的网络中人们已经普遍采用 IP 技术，纯 ATM 网络已经不可能，现有 ATM 的使用也一般都是用来承载 IP。因此人们就希望 IP 也能提供一些 ATM 一样多种类型的服务。

MPLS（Multiprotocol Label Switch，多协议标签交换）就是在这种背景下产生的一种技术，它吸收了 ATM 的 VPI/VCI 交换的一些思想，无缝地集成了 IP 路由技术的灵活性和二层交换的简捷性，在面向无连接的 IP 网络中增加了 MPLS 这种面向连接的属性。通过采用 MPLS 建立“虚连接”的方法，为 IP 网增加了一些管理和运营的手段。

MPLS 的最早原型是 90 年代中期由 Ipsilon 公司率先推出的 IPSwitching 协议，其目的主要是解决 ATM 交换机如何更好地支持 IP，该协议使 ATM 交换机成为一台路由器，因而具有 ATM 交换机的高性能，突破了传统路由器的性能限制。一时间 Ipsilon 名声大震。当时路由器厂家实现标签交换的目的是为了解决 IP 路由查找不能达到线速的问题（因为 IP 路由查找采用的是最长地址匹配的方式，在路由器端口速度达到 155M 或 622M 时软件查找会有困难）。这些早期不同厂家的标签交换的实现存在互通问题，所以在 1997 年 IETF 成立一个负责标签交换标准化的工作组---MPLS 工作组。它独立于各个设备实现厂家。现有的 MPLS 相关协议和草案基本上来自于这个工作组和它后来派生出来的流量工程工作组和 MPLS VPN 工作组。

随着网络处理器技术的迅速发展，2.5G 甚至 10G 端口的路由线速查找都已经不成问题，MPLS 应用也逐步转向 MPLS 流量工程和 MPLS VPN 等。在 IP 网中，MPLS 流量工程技术成为一种主要的管理网络流量、减少拥塞、一定程度上保证 IP 网络的 QoS 的重要工具。在解决企业互连，提供各种新业务方面，MPLS VPN 也越来越被运营商看好，成为在 IP 网络运营商提供增值业务的重要手段。

采用 MPLS VPN 技术可以把现有的 IP 网络分解成逻辑上隔离的网络，这种逻辑上

隔离的网络应用可以是千变万化的：可以用在解决企业互连、政府相同/不同部门的互连、也可以用来提供新的业务，如为 IP 电话业务专门开辟一个 VPN，以此解决 IP 网络地址不足和 QoS 的问题，也可以用 MPLS VPN 为 IPv6 提供开展业务的可能。

在 MPLS 越来越被看好的同时，反对使用 MPLS 的声音同样越来越尖锐。主要的反对声音来自于 AT&T 的两位 Internet 研究者—安全权威 Steve Bellovin 和网络运行专家 Randy Bush。MPLS 的反对者认为 MPLS，尤其是 MPLS VPN 对 IP 网络来说是一个灾难。认为 MPLS 彻底破坏了 IP 网络的现有结构，在 IP 网上增加了复杂的、难于管理和控制的 VPN 结构，在 VPN 数量很多的时候会严重影响骨干网的稳定性和可扩展性。另外象三层 MPLS VPN 的安全也是一个问题，在 VPN 配置错误时，错被配进 VPN 的客户在 VPN 中没有任何阻拦。MPLS 的反对者认为 MPLS 是没有必要的，解决 VPN 采用 IPSec 是一种更好、更安全、对现有网络改动也最小的解决方案。 MPLS 的反对者认为给有拥塞的链路扩容也会是解决网络拥塞的更简单的办法。

以上观点虽然有些极端，但是 MPLS 技术确实给运营商提出了新的挑战，在实施 MPLS 时整个网络管理的复杂度明显增加。如使用流量工程时需要对网络流量进行全面周期性测量、使用 MPLS VPN 需要针对每一个 VPN 管理一个 VPN 路由表。在有成千上万个 VPN 的时候，管理成千上万个 VPN 路由表会是一个非常头痛的事。所以并不是所有的 VPN（如 Site 很少、端口速度又小的 VPN）都要用 MPLS/BGP VPN，能用 IPSec 或专线的不必一定要用 MPLS/BGP VPN。MPLS/BGP VPN 比较适用于 Site 较多、端口速度大的 VPN。MPLS 的另一个问题是标准还有待完善，很多都是草案，这些草案常常也只有一两个设备商支持，有些问题如 MPLS QoS、二层 VPN 互通、三层 VPN 跨域都还在发展之中，安全性也确实要差一些。

目前，MPLS 标准代表了在多层次交换领域持续解决方案中的最新结果。MPLS 的主要目标就是将标签交换与传统的网络层路由集成起来。这种集成可以提高数据转发过程中的效率，并且能够给网络带来一些高级的 QoS（Quality of Service，服务质量，即指流量优先）功能。

传统的 IP 数据转发是逐跳式的，每个转发数据的路由器都要根据 IP 包头的目的地址查找路由表来获得下一跳的出口。由于路由匹配遵循最长匹配原则，所以迫使几乎所有的路由器的交换引擎必须用软件来实现。

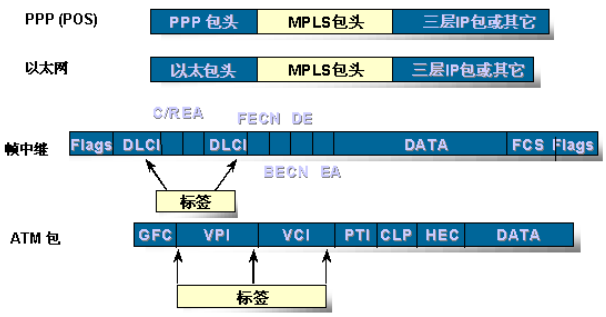
MPLS 环境中，通过网络的最佳路由是事先确定的。然后，当数据报文进入 MPLS 网络时，入口设备使用第三层报文头中的信息来将报文分配到预定路径的某一条

上。这种分配是通过将一个引用端到端路径的标签（Label）附加到数据报文中来实现的。该路径上随后的路由器使用标签中的信息来决定下一跳的设备，对第三层报文头进行大量的分析和分类将只在入口点进行。

MPLS 的标签是定长的 20 位，路由器可以分析定长的标签来做数据包的转发。这是标签交换的最大优点，定长的标签就意味这可以用硬件来实现数据转发。

MPLS 的包头位于二层和三层之间，俗称 2.5 层。MPLS 可以承载的报文通常是 IP 包（当然也可以改进直接承载以太包、ATM 的 AAL5 包、甚至 ATM 信元等）。可以承载 MPLS 的二层协议可以是 PPP、以太网、ATM 和帧中继等。MPLS 包头在协议栈中的结构如下图所示：

图3-4 MPLS 结构图



其中，对于 PPP 或以太网，MPLS 分别采用 PPP 包头或以太网包头进行二层封装；对于 ATM 或帧中继，MPLS 则分别采用 VPI/VCI 或 DLCI 做为转发的标签。

MPLS 可以看做是一种面向连接的技术。通过 MPLS 信令或手工配置的方法建立好 LSP（Label Switched Path，标签交换路径）以后，在标签交换路径的入口把需要通过这个标签交换路径的报文打上 MPLS 标签，中间路由器在收到 MPLS 报文以后直接根据 MPLS 报头的标签进行转发，而不用再通过 IP 报文头的 IP 地址查找。在 MPLS 标签交换路径的出口（或倒数第二跳），弹出 MPLS 包头，还回原来的 IP 包（在 VPN 的时候可能是以太网报文或 ATM 报文等）。

通常使用的建立 MPLS 标签交换路径的信令有 LDP、BGP 扩展等，其中 LDP 是用来建立标签连接通路，LDP 的标签分配模式有 DoD（Downstream On Demand，下游按需分配标签模式）和 Du（Downstream Unsolicited，下游主动标签分配模式）两种方式，LDP 能够建立到某个目的路由或目的子网的 LSP，它的路由的每一跳是根据路由表确定的，也就是说 LDP 建立的 LSP 只是把需要转发的 IP 报文打包成 MPLS，实际走的路径还是和原来的 IP 包走的路径一样。LDP 建立的 LSP

没有平衡流量的功能，只能起到建立虚连接的作用。BGP 协议的各种扩展则可以为 MPLS VPN 建立跨 AS 域的外层承载隧道，或者是 VPN 应用分配 VPN 的内层标签。

3.6 VPN（虚拟私有网络）

3.6.1 概述

VPN（Virtual Private Network，虚拟私有网络）是利用公共网络来构建的私有专用网络技术，也常称虚拟专用网。用于构建 VPN 的公共网络包括 Internet、帧中继、ATM 等。在公共网络上组建的 VPN 象企业现有的私有网络一样提供安全性、可靠性和可管理性等。

“虚拟”的概念是相对传统私有网络的构建方式而言的。对于广域网连接，传统的组网方式是通过远程拨号连接来实现的，而 VPN 是利用服务提供商所提供的公共网络来实现远程的广域连接。

VPN 是中小企业从自建专网向利用运营网络的重要途径。通过部署 VPN，可利用广泛覆盖、高带宽的骨干运营网络来实现企业网的互连，可为企业节省大量的建设费用。

VPN 的应用还远不局限于企业内部网络的互连。对于已建有专网的大企业集团，利用 MPLS VPN 可以实现数据、语音和视频等多种业务的承载，实现各种业务系统之间的隔离。MPLS VPN 在保证业务 QoS 和系统安全隔离方面具有天然优势。

3.6.2 IP VPN技术分析

1. 传统的 IP VPN

传统的 IP VPN 技术包括 GRE/IPSec、L2TP 等，业务的关键特性集中于公网的边缘设备，数据报文在穿透公网时采用 IP 隧道技术。骨干网设备只需完成标准的 IP 转发功能，而不需要也不可能知道 VPN 用户的存在，目前常用的 LAN-to-LAN VPN 技术是 IPSec。

IPSec（IP Security）是一组开放协议的总称，它是在特定的通信方之间通过在 IP 层加密和数据源验证等手段，保证数据包在 Internet 网上的私有性、完整性和真实性。IPSec 采用 AH （Authentication Header）和 ESP （Encapsulating Security

Payload）安全协议，不会对用户、主机或其它 Internet 组件造成影响，用户可以选择不同的硬件或软件加密算法，不影响其它部分的实现。

IPSec 提供以下网络安全服务：

- 私有性：在传输数据包之前进行加密，保证数据的私有性；
- 完整性：在目的地验证数据包，保证数据包在传输过程中不被修改；
- 真实性：IPSec 端验证所有受 IPSec 保护的数据包；
- 防重放：防止数据包被捕捉后重新投放上网，即目的地拒绝旧的或重复的数据包，这一过程是通过报文的序列号来实现的。

IPSec 在两个端点之间通过建立安全联盟（Security Association）进行数据传输，该安全联盟定义了数据保护使用的协议、算法和安全联盟的有效时间等属性。IPSec 在转发加密数据时新产生的 AH 和/或 ESP 附加报头，可用于保证 IP 数据包的安全性。IPSec 包括隧道和传输两种工作方式：在隧道方式，用户的整个 IP 数据包用于计算附加报头且被加密，附加报头和加密用户数据封装在一个新的 IP 数据包中；在传输方式，仅传输层（如 TCP、UDP）数据用于计算附加报头，附加报头和被加密的传输层数据放置在原 IP 报头的后面。

AH 报头用以保证数据包的完整性和真实性，防止黑客截断数据包或向网络插入伪造的数据包。考虑到计算效率，AH 没有采用数字签名方式，而是采用安全哈希算法对数据包进行保护，AH 不对用户数据进行加密。AH 在 IP 包中的位置（隧道方式）如下图所示：

图3-5 AH 处理示意图

ESP 对需要保护的用户数据加密后再封装到 IP 包，可保证数据的完整性、真实性和私有性。ESP 头在 IP 包中的位置（隧道方式）如下图所示：

图3-6 ESP 处理示意图

AH、ESP 方式可以单独使用，也可同时使用。

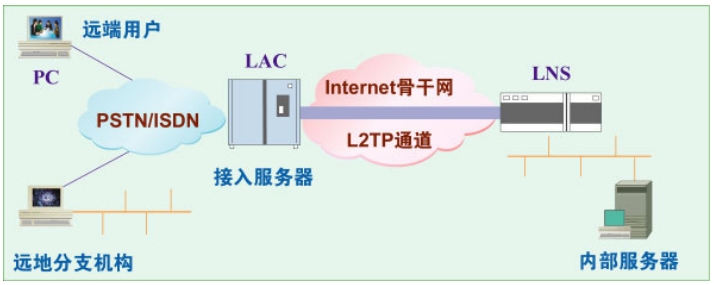
通过 IPSec 协议，数据可安全地在公网传输，不必担心数据被监视、修改或伪造。IPSec 提供两个主机间、两个安全网关间或主机与安全网关之间的数据保护。

在两个端点之间可以建立多个安全联盟，结合访问控制列表（Access-list），IPSec 可对不同的数据流实施相应的保护策略。安全联盟具有方向性（单向），通常两个

端点之间存在着四个安全联盟，每个端点两个，一个用于数据发送，一个用于数据接收。

L2TP 是应用最广泛的 VPN 二层隧道协议，它可用于远程用户拨号 VPN。采用 L2TP 构建的典型的 VPN 结构如下图所示：

图3-7 典型的拨号 VPN 业务示意图



其中：LAC 表示 L2TP 访问集中器（L2TP Access Concentrator），它附属在交换网络上的具有接入功能和 L2TP 协议处理能力的设备，通常是一个网络接入服务器 NAS（Network Access Server），通过 PSTN/ISDN 为用户提供网络接入服务；LNS 表示 L2TP 网络服务器（L2TP Network Server），它是用于处理 L2TP 协议服务器端部分的软件。

在一个 LNS、LAC 对之间存在着两种类型的连接：一种是隧道（Tunnel）连接，它定义了一个 LNS、LAC 对；另一种是会话（Session）连接，它复用在隧道连接之上，表示承载在隧道连接中的每个 PPP 会话过程，一个隧道连接可以承载多个会话连接。L2TP 的连接维护和 PPP 数据传送是通过 L2TP 消息的交换来完成的，这些消息再通过 UDP 的 1701 端口承载于 TCP/IP 之上。L2TP 消息可分为控制消息和数据消息，控制消息用于隧道连接和会话连接的建立和维护，数据消息则用于承载用户的 PPP 会话数据包。

控制消息的参数用属性值对 AVP（Attribute Value Pair）来表示，它使协议具有很好的扩展性，此外在控制消息的传输过程中还应用了消息丢失重传和定时检测通道连通性等机制来保证 L2TP 层传输的可靠性。L2TP 数据消息的传输不采用重传机制，不保证传输的可靠性，这可通过上层协议（如 TCP）来保证。数据消息的传输可根据应用的需要灵活地采用流控或非流控机制，甚至可在传输的过程中动态地使用消息序列号激活消息的顺序检测和流控功能。在采用流控的过程中，对于失序消息的处理采用缓存重排序的方法来提高数据传输的有效性。

此外，L2TP 还具有以下特性：

- 身份验证机制：与 PPP 类似，L2TP 可对隧道端点进行验证，不同的是，PPP

可以采用 PAP 方式以明文传输用户名和密码，而 L2TP 则必须使用类似 PPP CHAP 的验证方式；

- 内部地址分配：LNS 置于企业网的防火墙之后，可对远端用户的地址进行动态分配和管理，并支持 DHCP 和私有地址应用（RFC1918），远端用户分配的地址不是 Internet 地址，而是企业内部的私有地址，既方便地址管理又增加了安全性；
- 网络计费：可在 LAC（通常为 ISP）和 LNS（通常为企业）两处同时计费，前者产生帐单，后者用于付费和审计，L2TP 能够提供数据传输的出入包数、字节数和连接的起始/结束时间等计费数据；
- 可靠性：L2TP 协议支持备份 LNS，若某主 LNS 不可达，则 LAC（接入服务器）可重新与备份 LNS 建立连接，进而增加 VPN 服务的可靠性和容错性；
- 网络管理：L2TP 协议是标准的 RFC 协议，MIB 也制定了 L2TP 标准，可以通过统一的 SNMP 网络管理方案进行网络维护和管理。

2. MPLS VPN

MPLS VPN 是一种基于 MPLS 技术的 IP-VPN，是在网络路由和交换设备上应用 MPLS 技术，简化核心路由器的路由选择方式，结合传统路由技术的标签交换实现的 IP 虚拟专用网络（IP VPN），可用来构造宽带的 Intranet、Extranet，满足多种灵活的业务需求。经过几年的发展，MPLS VPN 技术已经走向成熟，并逐渐得到认可，成为业界公认的网络发展方向。

MPLS VPN 的主要优点包括：

- 运营管理简单：可在统一的网管上进行基于 VPN 的配置，而不需要一段段地对链路进行配置，可对每个 VPN 端口进行监测；
- 可承载多种业务：可承载包括图像、语音和数据等在内的多种业务；
- 服务质量有保证：可执行复杂的 DiffSever 等 QoS/CoS 协议，针对不同的业务，提供相应的服务质量保证，有效地实现多种业务的可靠承载；
- 可进行复杂的访问控制：通过用户控制访问列表，可进行复杂的访问控制，满足用户分层或星型互联的需求；
- 支持大型多业务网络：该技术是为了解决大型运营网络虚拟专线业务而提出的，可实现不同业务系统之间的隔离，解决多业务承载和安全问题。

MPLS VPN 在具有上述优点的同时，也具有协议复杂的缺点，对设备性能提出了较高的要求，成本也高，但是随着技术的成熟，设备价格迅速下降。同时，MPLS VPN 的大规模运营对网管也提出了更高的要求，不仅要实现设备和网络的管理，

还要实现业务管理功能，如基于 VPN 业务的管理。

在 MPLS VPN 模型中，网络是由骨干网和各用户 Site 组成，VPN 实际上就是对 Site 集合的划分，一个 VPN 对应一个或由若干 Site 组成的集合。这种集合必须遵循如下规则：即两个 Site 之间只有至少同时属于一个 VPN 定义的 Site 集合，才具有 IP 连通性。

MPLS VPN 体系包含的基本组件包括 PE（Provider Edge Router，骨干网边缘路由器）、CE（Custom Edge Router，用户网边缘路由器）、P Router（Provider Router，骨干网核心路由器）和 VPN 用户站点（Site）。

其中：

- PE：存储 VRF，处理 VPN-IPv4 路由，是 MPLS 三层 VPN 的主要实现者；
- CE：分布用户网络路由；
- P Router：负责 MPLS 的转发；
- Site：是 VPN 中的一个孤立 IP 网络，一般来说，不通过骨干网不具有连通性，公司总部、分支机构都是 Site 的具体例子。CE 路由器通常是 VPN Site 中的一个路由器或交换设备，Site 通过一个单独的物理端口或逻辑端口（如 VLAN 方式、FR 子接口等）连接到 PE 设备。

用户接入 MPLS VPN 的方式是每个 Site 提供一个或多个 CE，与骨干网 PE 连接。在 PE 为该 Site 配置 VRF，连结 PE-CE 的物理接口、逻辑接口、甚至 L2TP/IPSec 隧道绑定的 VRF 上，但不可以是多跳的 3 层连接。

PE-CE 之间的交换路由信息通常选择静态路由，也可通过 RIP、OSPF、BGP、IS-IS 等。静态路由方式可以减少因 CE 设备管理不善等原因造成对骨干网路由产生震荡，避免影响骨干网的稳定性。

MPLS VPN 提供灵活的地址管理方式，它采用单独的路由表，允许每个 VPN 使用单独的地址空间（VPN-IPv4 地址空间），采用私有地址的用户不必进行地址转换 NAT，实际上只有在两个发生冲突地址的用户之间建立 Extranet 通信时才需要进行 NAT。

在 MPLS VPN 中，同一 VPN 的两个 Site 间转发报文时需要使用两层标签，在入口 PE 为报文打上两层标签，第一层（外层）标签在骨干网内部进行交换，代表从 PE 到对端 PE 的一条隧道，VPN 报文打上该层标签即可沿着 LSP 到达对端 PE，此时即可使用第二层（内层）标签，表示报文应该到达哪个 Site，或更具体地到达哪个 CE，找到转发接口。内层标签代表的是通过骨干网相连的两个 CE 之间的一个隧道。

3.6.3 VPN技术在企业的应用

对于已经建设了专网的大型企业集团，通常可采用 MPLS VPN 技术在公共骨干网络上承载多个业务系统，完成各种业务网络之间的隔离，同时提高网络的安全性；对于中小型企业，建设专网的费用高昂，可通过路由器或专用 VPN 网关，采用 GRE/IPSEC 技术，利用运营商公网实现不同地点网络的互联；对于企业的移动用户、小型分支，则可采用拨号 VPN 方式，利用 L2TP 技术接入企业的内部网络。

3.7 MPLS/BGP VPN

MPLS/BGP VPN 是基于 BGP 扩展实现的 L3 MPLS VPN，在 MPLS/BGP VPN 的模型中，网络由运营商的骨干网与用户的各个 Site 组成。所谓 VPN 就是对 Site 集合的划分，一个 VPN 就对应一个由若干 Site 组成的集合。但是必须遵循如下规则：两个 Site 之间具有至少同时属于一个 VPN 定义的 Site 集合，才具有 IP 连通性。其基本组件包括：

- PE（Provider Edge Router，骨干网边缘路由器）：存储 VRF（Virtual Routing Forwarding Instance），处理 VPN-IPv4 路由，是 MPLS 三层 VPN 的主要实现者。
- CE（Custom Edge Router，用户网边缘路由器）：分布用户网络路由。
- P Router（Provider Router，骨干网核心路由器）：负责 MPLS 转发。
- VPN 用户站点（site）：是 VPN 中的一个孤立的 IP 网络，一般来说，不通过骨干网不具有连通性，公司总部、分支机构都是 site 的具体例子。CE 路由器通常是 VPN Site 中的一个路由器或交换设备，Site 通过一个单独的物理端口或逻辑端口（通常是 VLAN 端口）连接到 PE 设备上。

用户接入 MPLS VPN 的方式是每个 Site 提供一个或多个 CE，同骨干网的 PE 连接。在 PE 上为这个 Site 配置 VRF，将连结 PE-CE 的物理接口、逻辑接口，甚至 L2TP/IPSec 隧道绑定到 VRF 上，但不可以是多跳的 3 层连接。

BGP 扩展实现的 MPLS VPN 扩展了 BGP NLRI 中的 IPv4 地址，在其前增加了一个 8 字节的 RD（Route Distinguisher）。RD 是用来标识 VPN 的成员，即 Site 的。VPN 的成员关系是通过路由所携带的 route target 属性来获得的，每个 VRF 配置了一些策略，规定一个 VPN 可以接收哪些 Site 来的路由信息，可以向外发布哪些 Site 的路由信息。 每个 PE 根据 BGP 扩展发布的信息进行路由计算，生成每个相关 VPN 的路由表。

PE-CE 之间要交换路由信息一般是通过静态路由，也可以通过 RIP、OSPF、BGP、IS-IS 等。PE-CE 之间采用静态路由的好处是可以减少 CE 设备可能会因为管理不善等原因造成对骨干网 BGP 路由产生震荡，影响骨干网的稳定性。

PE 与 PE 之间需要运行 IBGP 协议，存在可扩展性问题，但采用路由反射器 RR 可以显著地减少 IBGP 连接的数量。

MPLS/BGP VPN 提供了灵活的地址管理。由于采用了单独的路由表，允许每个 VPN 使用单独的地址空间，称为 VPN-IPv4 地址空间，RD 加上 IPv4 地址就构成了 VPN-IPv4 地址。很多采用私有地址的用户不必再进行地址转换 NAT。NAT 只有在两个有冲突地址的用户需要建立 Extranet 通信时才需要。

在 MPLS/BGP VPN 中，属于同一个 VPN 的两个 Site 之间转发报文使用两层标签来解决，在入口 PE 上为报文打上两层标签，第一层（外层）标签在骨干网内部进行交换，代表了从 PE 到对端 PE 的一条隧道，VPN 报文打上这层标签，就可以沿着 LSP（Label Switched Path，标签交换路径）到达对端 PE，这时候就需要使用第二层（内层）标签，这层标签指示了报文应该到达哪个 site，或者更具体一些，到达哪一个 CE，这样，根据内层标签，就可以找到转发的接口。可以认为，内层标签代表了通过骨干网相连的两个 CE 之间的一个隧道。

UniWorks VPN Manager 系统 V1.00 for Windows 版本支持 MPLS/BGP VPN 的业务管理。

4 系统启动

4.1 概述

用户要利用 UniWorks VPN Manager 系统进行 VPN 业务管理，首先需要确定 UniWorks VPN Manager 系统的后台服务正在运行。确定后台服务正在运行后，用户便可启动 UniWorks VPN Manager 系统的前台程序。

4.2 启动后台服务

Uniworks VPN Manager 系统的后台服务包括：

- 数据库服务：主要负责数据库的连接、数据的实时存储和历史查询。
- UniWorks VPN Manager 服务：负责管理客户端和数据库的连接。

一般情况下，数据库服务会在每次启动 Windows 系统时自动启动，不需要用户手工干涉，用户只需启动 UniWorks VPN Manager 服务。在命令提示符下的启动方式为：

- vpnmanager <初始化文件绝对路径>
- vpnmanager ：不带参数，系统搜索当前目录下的 initCommand.js，如果当前目录下没有 initCommand.js 文件，则得到环境变量 VPNSERVER_INITFILE_LOCATION 指定的初始化文件绝对路径

如果没有找到初始化文件，则系统初始化失败。需要用户重新输入正确的命令参数进行启动。

服务启动成功将给出成功提示信息如下：

```
************************************************
*                                              *
*              欢迎使用港湾网络 VPN 管理系统           *
*                                              *
*                                              *
*                  2004-05-07 V1.0             *
```

```
*                                                  *
****************************************************
****************************************************
*                                                  *
*            [ 1 ] : 显示配置                      *
*            [ 2 ] : 停止服务                      *
*            [ 3 ] : 显示客户端登录信息            *
*            [ 4 ] : 隐藏客户端登录信息            *
*            [ 5 ] : 显示客户端操作信息            *
*            [ 6 ] : 隐藏客户端操作信息            *
*            [ 7 ] : 当前在线用户数量              *
*            [ 8 ] : 启动控制台                    *
*                                                  *
****************************************************
```

4.3 启动前台程序

UniWorks VPN Manager 系统的前台程序主要用于系统配置管理、客户管理以及业务管理等的参数配置。

UniWorks VPN Manager 系统前台程序提供了友好的图形用户界面，可以方便用户简单快捷地管理和监控客户资源、网络运行状态、分析和定位网络故障、部署和配置 VPN 业务，还可以根据系统的配置灵活地选择后备存储数据库，方便快捷地查询系统历史记录，并根据历史数据有效的分析系统性能，方便用户的管理和维护，提高工作效率。

UniWorks VPN Manager 系统前台程序可以在后台服务正确启动以后随时启动。启动方法有两种：

- 桌面快捷方式：UniWorks VPN Manager 系统安装成功以后会在用户桌面上创建一个快捷方式，名为 UniWorks VPN Manager。用户仅需用鼠标双击此快捷方式就可以启动 UniWorks VPN Manager 系统前台。
- 开始菜单启动方式：打开 Windows 的“开始—程序－UniWorks VPN Manager－UniWorks VPN Manager”，启动 UniWorks VPN Manager 系统前台。

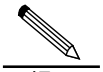
4.3.1 注册

如果您是第一次运行 UniWorks VPN Manager 系统，系统将弹出用户注册窗口，要求输入用户注册信息，包括用户名称和授权许可密钥。以后，您就可以直接进行系统登录了。

4.3.2 登录

前台程序启动以后用户看到第一个界面就是系统的主界面，用户需要先进行系统配置，如：远程启动客户端或者本地启动客户端。对于本地启动客户端需要配置数据库选项，配置成功才可以登录和使用系统。配置步骤如下：

1. 选择主界面上的菜单项‘系统－系统配置’，弹出‘系统配置’界面；
2. 在‘系统配置—选择启动模式’中选择‘作为客户端’；在‘VPN 服务器地址’中填入 VPN 服务器的 IP 地址，在‘VPN 服务器端口’中填入 Socket 端口号，默认为 11748。最后，点击“确定”按钮完成配置。


提示

有两种启动模式可供选择：作为客户端和本地启动。通常情况下，用户只需要使用“作为客户端”模式。

系统配置完成后，用户就可以登录系统了。用户第一次登录时使用系统预置的用户名和密码：

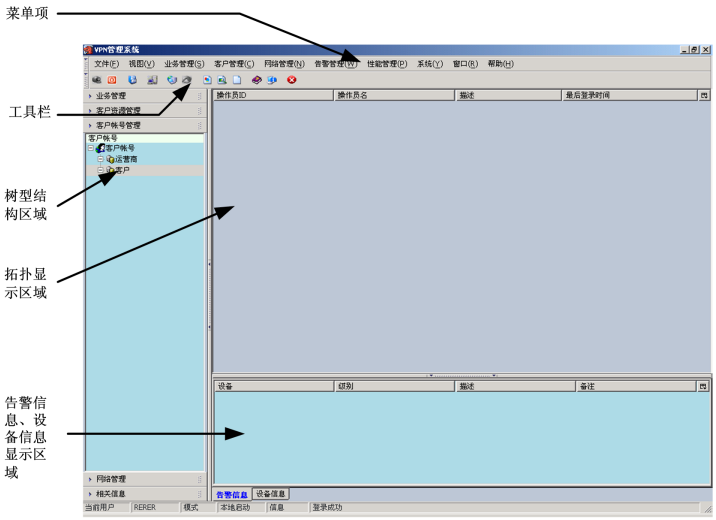
- 客户：admin
- 用户：admin
- 密码：harbour

为了保证系统的安全性，建议用户登录系统后首先修改默认密码。具体方法请参见 5.3 节“客户帐号管理”的相关内容。

4.3.3 前台主界面

UniWorks VPN Manager 系统登录后的主界面如下图所示：

图4-1 登录后的主界面

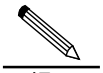


有关菜单项的描述如下表所述：

表4-1 菜单项描述

菜单项	菜单子项		子项功能描述
文件（F）	登录（I）		登录UniWorks VPN Manager系统
	注销（O）		注销当前操作员
	退出（Q）		退出UniWorks VPN Manager系统
视图（V）	常用工具（M）		显示常用工具的开关
	业务管理工具（S）		显示业务管理工具开关
	客户管理工具（C）		显示客户管理工具开关
	网络管理工具（N）		显示网络管理工具开关
	状态栏（B）		显示状态栏开关
	信息栏（I）		显示信息栏开关
业务管理（S）	新建VPN （C）		创建一个新的VPN业务
	修改VPN （M）		修改一个已存在VPN业务属性
	删除VPN （D）		删除一个无用的VPN业务
	管理CERC（G）		创建、修改、删除CERC
	管理VRF		创建、修改、删除VRF
	业务配置（S）		配置VPN业务
	业务部属（T）		部署VPN业务，下发命令
	刷新（R）		刷新一次屏幕显示
客户管理（C）	客户管理（C）	创建客户（N）	创建一个新的客户
		修改客户（M）	修改一个已存在客户
		删除客户（D）	删除一个过期客户
	资源管理（M）	添加站点（S）	添加一个新的客户站点
		修改站点（T）	修改一个已存在客户站点
		删除站点（D）	删除一个无用的客户站点

菜单项	菜单子项		子项功能描述
		添加设备（A）	添加一个新的设备
		修改设备（U）	修改一个已存在客户设备属性
		删除设备（E）	删除一个无用设备信息
		接口管理（I）	管理设备接口信息
	操作员管理（P）	添加操作员（O）	添加一个新的操作员帐号
		修改操作员p（C）	修改一个已存在操作帐号
		删除操作员d（C）	删除一个过期操作员帐号
	刷新（R）		刷新一次屏幕显示
告警管理（W）	参数配置（P）		设置告警参数
	启动（S）		启动告警采集
	停止（T）		停止告警采集
	保存全部告警（A）		保存全部告警信息
	保存已选择的告警（E）		保存已选择告警信息
	删除全部告警（D）		删除全部告警信息
	删除已选择的告警（C）		删除已选择告警
系统（Y）	系统配置（C）		配置系统参数
	日志管理（L）		启动日志管理窗口
	Telnet终端		启动Telnet终端窗口
	拓扑显示（L）		显示拓扑图
	保存拓扑（S）		保存现有拓扑图信息
窗口（R）	设置背景色		设置背景颜色
	设置背景图（I）		设置背景界面图案
	取消背景（C）		设置为无背景
	选择风格（T）	经典（K）	将窗口设置为经典风格显示方式
		现代（M）	将窗口设置为现代风格显示方式
	选择布局	布局1	选择布局方式1
		布局2	选择布局方式2
帮助（H）	帮助信息（H）		启动帮助信息窗口
	关于（A）		启动产品信息窗口



本手册重点讲述 UniWorks VPN Manager 系统 V1.00 for Windows 版本中与业务配置和管理相关的内容，有关视图、窗口和帮助等菜单项的内容不在手册中介绍了，用户在使用本产品的过程中，会很快熟悉和掌握这些方面的操作的。

5 客户管理

5.1 概述

UniWorks VPN Manager 系统的客户管理主要用于完成客户资源管理和权限控制任务。从前面介绍的 MPLS/BGP VPN 原理，可知，UniWorks VPN Manager 系统的客户管理主要就是管理 MPLS/BGP VPN 系统的 PE 和 CE 设备。为了便于管理，客户管理提供了域的组织方式，即允许一个客户下面对应多个站点，每个站点包含多个设备。这样便于设备的查找和组织。对 PE、CE 设备来说，需要获得路由器上的接口，资源管理提供了手工添加和自动获得设备接口的功能。

客户主要分为两种类型：

- 运营商，主要负责管理 PE 设备；
- 业务客户，主要负责管理 CE 设备。

每一个客户下面可以带多个操作员。为了保证系统的安全，可以赋予不同的操作员以不同的权限，使操作员只能操作自己客户范围内的资源。操作员的操作，日志系统都会有记录，这样可以很方便的定位业务数据的变更情况。

UniWorks VPN Manager 系统安装完成后，系统会创建一个默认用户：

- 客户：admin
- 用户：admin
- 密码：harbour

这个用户是超级用户，可以更改所有用户的权限和管理所有用户的资源。同时其他客户，以及他们的操作员也是用这个用户来进行管理的。一般用户在得到分配的用户账号以后，就可以远程登录到 UniWorks VPN Manager 系统来进行远程维护。

利用客户管理提供的资源，业务管理系统才能真正的实现业务的配置和部署。

利用客户管理提供的账户管理，整个 UniWorks VPN Manager 系统才能有效的进行权限管理。

5.2 客户管理

客户管理中对于客户基本资料的维护和管理主要包括创建客户、修改客户以及删除客户。

创建一个客户，一般需要下面的基本内容：

- 客户名称：客户的名称描述；
- 自治域号：客户是属于哪个自治域的，在配置 VPN 业务中需要这个参数；
- 运营商标志：是不是运营商。正如前面所述，运营商是用来管理 PE 设备的，一般业务用户是用来管理 CE 设备的；
- 组织名：一般是哪个单位，或者团体的名字；
- 国家：组织所属的国家；
- 联系地址 1：联系地址；
- 联系地址 2：联系地址；
- 联系方式：比如电子邮件等联系方式；
- 邮政编码：客户的邮政编码；
- 电话：客户联系电话；
- 传真：客户的传真；

其中，客户名称、自治域号和是否为运行商是必填项，其它项可选填。

1. 创建客户

新建一个客户的方法有三种：

- 方法一：点击主菜单栏中的“客户管理－客户管理－创建客户”即可弹出创建客户界面，在创建客户界面中按照规则填写客户名称，管理域码（客户所在的自治系统编号），是否是运营商，以及一些诸如客户组织，客户所在国家联系地址、联系方式、邮政编码、电话和传真等用户资料，点击“确认”按钮即可创建一个新的客户。
- 方法二：点击主界面左侧树型结构列表中“客户资源管理”按钮，在向下拉开的客户资源列表中，右键点击树型结构的根节点“客户资源”弹出快捷菜单，选择其中的“创建客户”项，即可弹出创建客户界面，其余操作请参见上述方法一。
- 方法三：点击主界面左侧树型结构列表中“客户帐号管理”按钮，在向下拉开的客户资源列表中，右键点击树型结构的根节点“客户帐号”弹出快捷菜单，选择其中的“创建客户”项，即可弹出创建客户界面，其余操作请参见上述方法一。

2. 修改客户

修改客户信息有三种方法：

- 方法一：点击主界面左侧树型结构列表中“客户资源管理”按钮，在向下拉开的客户资源列表中，选中要修改的客户，然后点击主菜单栏中“客户管理－客户管理－修改客户”即可弹出修改客户界面，在修改客户界面中按照规则修改一些诸如管理域码，客户组织，客户所在国家联系地址、联系方式、邮政编码、电话和传真等用户资料，点击“确认”按钮即可完成客户修改。
- 方法二：点击主界面左侧树型结构列表中“客户资源管理”按钮，在向下拉开的客户资源列表中，右键点击树型结构树型结构需要修改的客户名称即可弹出快捷菜单，选择其中的“修改客户”项，即可弹出修改客户界面，其余操作请参见上述方法一。
- 方法三：点击主界面左侧树型结构列表中“客户帐号管理”按钮，在向下拉开的客户帐号列表中，右键点击树型结构树型结构中需要修改的客户名称即可弹出快捷菜单，选择其中的“修改客户”项，即可弹出修改客户界面，其余操作请参见上述方法一。

3. 删除客户

在主界面左侧树型结构中的“客户资源管理”或者“客户帐号管理”的树型中找到要删除的客户帐号，然后可以使用以下三种方式删除此客户帐号。

- 方法一：点击主菜单栏中“客户管理－客户管理－删除客户”即删除了客户。
- 方法二：进入左侧树型结构按钮“客户资源管理”中，打开树型结构下拉列表，找到要删除的客户，右键点击在弹出的快捷菜单中选择“删除客户即可。
- 方法三：进入左侧树型结构按钮“客户帐号管理”中，打开树型结构下拉列表，找到要删除的客户，右键点击在弹出的快捷菜单中选择“删除客户即可。

5.3 客户帐号管理

客户管理中每个客户可以根据不同的权限要求创建和分配多个操作员帐号，维护人员根据需要来选择使用不同的操作员来进行操作。每个客户有多个不同的操作员，对于系统的维护和管理来说增加了安全性，容易落实任务与责任，方便客户管理。客户帐号管理主要包括：增加帐号、修改帐号以及删除帐号，其中：

- 操作员名：不超过 30 个字符，可以是中文、字母、数字、下划线的组合。
- 密码：操作员密码，需要二次确认。

- 描述：对这个操作员的描述。

1. 增加帐号

增加帐号有两种方法：

- 方法一：在左侧树型结构点击按钮“客户帐号管理”，在打开的树型结构中选择确定为哪个客户添加操作员，确定客户以后在主菜单下选择“客户管理－操作员管理－添加操作员”弹出“添加操作员”界面，在窗口中填写操作员名称，操作员密码以及描述。填写完毕以后，点击“确定”按钮，增加操作员；点击“取消”按钮，放弃添加。
- 方法二：在左侧树型结构点击按钮“客户帐号管理”，在打开的树型结构中选择确定为哪个客户添加操作员，确定客户以后右键点击客户，弹出快捷菜单，选择“添加操作员”即可弹出“添加操作员”界面，其余步骤请参见方法一。

2. 修改帐号

修改帐号有两种方法：

- 方法一：在左侧树型结构中点击按钮“客户帐号管理”，在打开的树型结构中确定要修改的操作员，在主菜单下选择“客户管理－操作员管理－修改操作员”弹出“修改操作员”界面。在“修改操作员”界面中修改相应的描述以及密码，点击“确定”按钮，确认修改；点击“取消”按钮，放弃修改。
- 方法二：在左侧树型结构中点击按钮“客户帐号管理”，在打开的树型结构中确定要修改的操作员，右键点击选定的操作员，弹出快捷菜单，选择“修改操作员”弹出“修改操作员”界面，修改请参见方法一。

3. 删除帐号

删除操作员帐号有两种方法：

- 方法一：在左侧树型结构中点击按钮“客户帐号管理”，在打开的树型结构中确定要删除的操作员，在主菜单下选择“客户管理－操作员管理－删除操作员”即删除选定操作员。
- 方法二：在左侧树型结构中点击按钮“客户帐号管理”，在打开的树型结构中确定要删除的操作员，右键点击选定的操作员，弹出快捷菜单，选择“删除操作员”即删除选定操作员。

5.4 客户资源管理

客户资源主要包括 PE 和 CE 设备。为了便于管理，系统建立了站点和区域的管理单位。对非运营商用户来说，用站点来组织 CE 设备；对运营商来说，用站点/区域来组织 PE 设备。域和站点一般而言有地理上的含义。为了添加设备，需要首先创建站点/区域资源。对于路由器，添加到系统之后，还要对它的接口进行管理。如添加某些接口等。添加接口可以手工，也可以自动添加。

5.4.1 站点/区域管理

客户可以有一个或者多个站点/区域，站点/区域管理工作主要包括：添加站点/区域、修改站点/区域以及删除站点/区域，其中：

- 站点 ID：是站点的唯一数字标识，由系统特定的 ID 分配机制来分配，能够确保 ID 的唯一性。
- 客户：站点所隶属的客户。
- 站点名称：不超过 30 个字符，可以是中文、字母、数字、下划线的组合。
- 站点描述：对站点的简单描述

1. 添加站点

添加站点有两种方法：

- 方法一：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，确定要增加站点的客户，在主菜单下选择 “客户管理－资源管理－添加站点”即可弹出“添加站点”界面；在“添加站点”界面中，正确填写站点名称，站点位置以及站点描述，点击“确定”按钮，确定增加站点；点击“取消”按钮，放弃添加。
- 方法二：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，确定要增加站点的客户，右键点击客户弹出快捷菜单，选择“添加站点”即可弹出“添加站点”界面，余下步骤参见方法一。

2. 修改站点

修改站点有两种方法：

- 方法一：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，确定要修改的站点，在主菜单下选择：“客户管理－资源管理－修改站点”弹

出“修改站点”界面；在“修改站点”界面中，根据需要修改站点名称，站点位置以及站点描述，点击“确定”按钮，确定修改站点；点击“取消”按钮，放弃修改站点。

- 方法二：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，确定要修改的站点，右键点击要修改站点弹出快捷菜单，选择“修改站点”弹出“修改站点”界面，余下步骤参见方法一。

3. 删除站点

删除站点有两种方法：

- 方法一：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，确定要删除的站点，在主菜单下选择 “客户管理－资源管理－删除站点”，可删除所选站点。
- 方法二：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，确定要删除的站点，右键点击要修改站点弹出快捷菜单，选择“删除站点”，可删除所选站点。

5.4.2 设备管理

设备管理主要是管理 PE 和 CE 设备。对于运营商客户，管理的是 PE 设备，对于一般的业务用户，管理的是 CE 设备。操作人员可以根据需要添加、修改和删除 PE、CE 设备。添加 PE、CE 设备，一般需要设置下列选项：

- 设备名称：设备的名称
- 设备描述：设备的简单描述
- 管理 IP：一般设为 loopback 地址
- 厂商：在下拉框中选择，有港湾、思科和华为，目前支持港湾
- 用户名：登录路由器的用户名
- 登录密码：登录路由器的密码
- 配置密码：配置路由器的密码
- 写团体字：SNMP 写团体字，一般为 prviate
- 读团体字：SNMP 读团体字，一般为 public

同时系统会自动分配设备 ID、客户 ID 和区域 ID。

1. 添加设备

添加 CE、PE 设备有两种方法：

- 方法一：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，确定要增加 CE 设备的站点，在主菜单下选择“客户管理－资源管理－添加设备”即可弹出“添加设备”界面；在“添加设备”界面中，正确填写设备名称，设备描述等信息，点击“确定”按钮, 确定增加设备；点击“取消”按钮,放弃添加。
- 方法二：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，确定要增加设备的站点户，右键点击站点弹出快捷菜单，选择“添加设备”即可弹出“添加设备”界面，余下步骤参见方法一。

2. 修改设备

修改设备有两种方法：

- 方法一：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，确定要修改的设备，在主菜单下选择 “客户管理－资源管理－修改设备”即可弹出“修改设备”界面；在“修改设备”界面中，根据要求修改设备名称，设备描述等信息，点击“确定”按钮，确定修改设备；点击“取消”按钮，放弃修改设备。
- 方法二：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，确定要修改的设备，右键点击要修改设备弹出快捷菜单，选择“修改设备”即可弹出“修改设备”界面，余下步骤参见方法一。

3. 删除设备

删除设备有两种方法：

- 方法一：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，确定要删除的路由器设备，在主菜单下选择“客户管理－资源管理－删除设备”，即可删除所选的 PE/CE 设备。
- 方法二：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，确定要删除的路由器设备，右键点击要修改站点弹出快捷菜单，选择“删除设备”，即可删除所选的 PE/CE 设备。

5.4.3 接口管理

接口是系统的关键资源，在 UniWorks VPN Manager 系统中，命令的下发都是对接口进行操作，所以接口管理是资源管理中的重要部分。接口管理包括添加接口、修改接口、删除接口和浏览接口。添加接口的主要配置信息包括：

- 接口 ID：接口的 ID 标识
- 接口名称：接口的名称
- 接口描述：接口的简单描述
- 接口类型：常见的类型有 Ethernet、Loopback 和 FrameRelay 等
- 接口状态：可以选择 up 或者 down
- 接口 IP 地址：接口的 IP 地址

系统除了支持手工添加接口以外，还支持自动添加接口。

自动获取接口信息，需要设备支持 SNMP，并且要打开 SNMP 服务。

启动接口管理有两种办法：

- 方法一：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，选中要管理的设备，在主菜单下选择“客户管理－资源管理－接口管理”即可弹出“接口”界面；
- 方法二：进入左侧树型结构按钮“客户资源管理”，打开树型结构下拉列表，选中要管理的设备，右键点击站点弹出快捷菜单，选择“接口管理”弹出“接口管理”界面。

接口管理界面的布局如下：

- 左边是接口的列表，列表的下方是“自动获取接口”按钮。
- 右边是接口的相关信息，以及增加、修改、删除和浏览接口的按钮。

1. 添加接口

打开接口管理界面以后，单击“添加“选项，将会允许用户输入接口 ID、接口名称、接口类型、接口状态和接口的 IP 地址等信息。输入完毕以后，单击“添加”按钮，添加的接口就会在接口列表中显示。

2. 修改接口

打开接口管理界面以后，单击“修改”选项，将允许用户修改接口的名称、类型、状态和接口的 IP 地址等信息。接口的 ID 由于是设备提供的，不允许修改。修改完毕以后，单击“修改”按钮，相应的接口内容就会发生改变。

3. 删除接口

打开接口管理界面以后，单击“修改”选项，将允许用户删除接口。单击“删除”按钮，即可删除接口。

4. 自动获得接口

系统支持自动获得接口。打开接口管理界面以后，单击“读取设备接口列表”按钮，将通过 SNMP 获得设备的接口信息。所以要想使用自动获得接口功能，必须保证要访问的设备提供 SNMP 服务。

5. 浏览接口

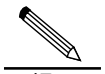
打开接口管理界面以后，可以看到系统默认的接口管理状态为“浏览”，用户可以点选已有的设备接口来浏览接口的参数配置。

6 业务管理

6.1 概述

业务管理构建在网络管理和客户管理的基础上，是整个 UniWorks VPN Manager 系统的核心部分。

UniWorks VPN Manager 系统的业务管理主要是对 VPN 业务的管理，主要功能包括业务规划、业务配置以及业务部署。


提示

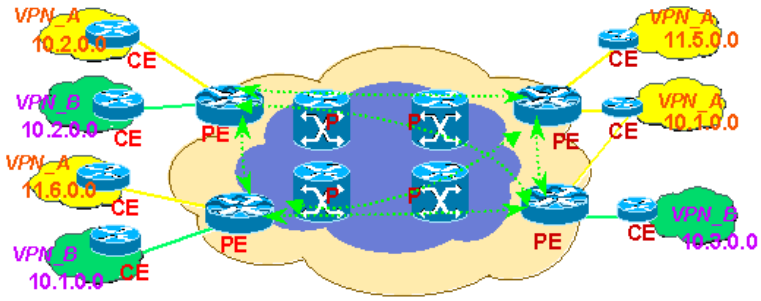
目前，UniWorks VPN Manager 系统 V1.00 的 Windows 版主要实现 MPLS/BGP VPN 的业务管理。

MPLS/BGP VPN 中涉及到的一些基本概念包括：

- P 网 (Provider_Network，服务商网络)：由服务商管理控制的 VPN 的骨干网络。
- C 网 (Customer_Network，用户网络)：由用户管理控制的网络。
- CE 路由器 (用户边沿路由器)：用户网络中用来接入服务商骨干网的路由器。
- 站点(SITE)：C 网中直接互联的部分子网的集合。一个站点可通过一条或多条 PE/CE 链路接入 VPN 骨干网。
- PE 路由器 (服务商边沿路由器)：P 网中连接 CE 路由器的路由器。
- P 路由器 (服务商核心路由器)：P 网中的骨干路由器，对 VPN 的信息透明，即 P 路由器内部没有 VPN 的信息。

MPLS/BGP VPN 是三层 VPN，用户可以保留原来的 IP 地址。一个典型的 MPLS/BGP VPN 的网络结构如下图所示：

图6-1 MPLS/BGP VPN 的网络结构



VPN 的骨干网由 MPLS_LSR 构成。PE 路由器即为边缘 LSR（Label Switch Router，标签交换路由器），P 路由器即为核心 LSR。PE 路由器通过 MP_BGP 将 VPN 的信息分发到其它的 PE 路由器，P 路由器并不参与 VPN 信息的维护。与 VPN 相关的信息主要有 VPN_IPV4 地址、扩展团体属性、VRF 标签等。P 路由器一般不启动 BGP，也没有任何 VPN 的信息。

PE 路由器在 P 网内部运行 MPLS，与 CE 路由器运行普通 IP。P 路由器和 PE 路由器运行共同的 IGP。PE 路由器之间为 MP_iBGP 完全网状逻辑连接，即每个 PE 路由器都需与其它所有的 PE 路由器建立 MP_iBGP 逻辑会话。PE 与 CE 路由器之间可选择运行以下路由协议交换路由信息：EBGP、OSPF、RIPV2、静态路由。CE 路由器安装常规路由软件，不需支持 MP_BGP 或 MPLS。

PE 路由器维护多个独立的路由表，包括全局路由表：由所有的 PE 路由器和 P 路由器持有，通过 VPN 骨干网的 IGP，如 ISIS 或 OSPF 来生成。为每个 PE 直接相连的 VPN 生成一份路由与转发表也就是 VRF，每个 VRF 仅存有所隶 VPN 的路由信息。

MPLS VPN 的路由转发是靠 BGP 来完成的。BGP 是一个路由选择分配协议，它定义谁可以与使用多协议分支（multiprotocol_extensions）和群体属性（Community_attributes）的人对话。在 MPLS 的 VPN 中，BGP 只向同一个 VPN 中的成员发布有关 VPN 的信息，通过业务分离来提供本机安全性。由于所有的业务都使用 LSP 进行传输，从而确保了额外的安全性。LSP 定义了一个特定的通道穿过网络，这个通道是不可更改的。这种基于标签的模式保证了帧中继和 ATM 连接中的私密性。

在 MPLS VPN 中，服务供应商为每个 VPN 分配一个独有的标识符，称为路由区分符（RD），在服务供应商网络中每一个 Intranet 或 Extranet 的区分符都不同。转发表包含独有的地址，称为 VPN-IP 地址，由 RD 和用户的 IP 地址构成。VPN_IP 地址是网络中每一个端点所独有的，条目存储在 VPN 中每一个节点的转发表中。

当提供 VPN 时，服务供应商而非客户将特定的 VPN 与每一个接口连接。在服务供应商网络中，RD 与每个数据包连接，这样，VPN 就不会被非法者渗透“偷窃”数据流或数据包。用户只要位于正确的物理端口上，有相应的 RD 就可以加入 Intranet 或 Extranet 中。这种设置使 MPLS VPN 基本上不可能被突破，因而可提供人们在帧中继、租赁线路或 ATM 业务中所习惯的相同级别的安全性。

VPN_IP 转发表包含与 VPN_IP 地址上对应的标签，这些标签将应用业务路由到 VPN 中的每一个站点。由于使用标签而不是 IP 地址，因此，用户可以在企业网中保留它们的专用编址方案。每一个 VPN 应用在逻辑上都拥有区分的转发表，以在 VPN 之间分离业务。根据呼入的接口，交换机选择一个特定的转发表，由于有 BGP，这个表只列出 VPN 中有效的目的地。若要建立一个 Extranet，服务供应商则需要在 VPN 之间清晰地配置延及的范围。

MPLS/BGP VPN 的工作流程如下：

1、用户端的路由器 CE 首先通过静态路由或 BGP 将用户网络中的路由信息通知提供商路由器 PE，同时在 PE 之间采用 BGP 的 Extension 传送 VPN-IP 的信息以及相应的标签(VPN 的标签，以下简称为内层标签)，而在 PE 与 P 路由器之间则采用传统的 IGP 协议相互学习路由信息，采用 LDP 协议进行路由信息与标签(骨干网络中的标签，以下称为外层标签)的绑定。到此时，CE、PE 以及 P 路由器中基本的网络拓扑以及路由信息已经形成。PE 路由器拥有了骨干网络的路由信息以及每一个 VPN 的路由信息。

2、当属于某一 VPN 的 CE 用户数据进入网络时，在 CE 与 PE 连接的接口上可以识别出该 CE 属于那一个 VPN，进而到该 VPN 的路由表中去读取下一跳的地址信息，同时，在前传的数据包中打上 VPN 标签(内层标签)。这时得到的下一跳地址为与该 PE 作 Peer 的 PE 的地址，为了达到这个目的端的 PE，此时在起始端 PE 中需读取骨干网络的路由信息，从而得到下一个 P 路由器的地址，同时采用 LDP 在用户前传数据包中打上骨干网络中的标签(外层标签)。

3、在骨干网络中，初始 PE 之后的 P 均只读取外层标签的信息来决定下一跳，因此骨干网络中只是简单的标签交换。

4、在达到目的端 PE 之前的最后一个 P 路由器时，将外层标签去掉，读取内层标签，找到 VPN，并送到相关的接口上，进而将数据传送到 VPN 的目的地址处。

由上可以看出，对 VPN 的管理主要是管理 PE-CE 之间的连接。UniWorks VPN Manager 系统的业务管理主要就是完成对 VPN 内部的 PE-CE 之间连接的配置。

业务管理是 UniWorks VPN Manager 系统的核心业务。当确定了客户的相应资源以后，就需要业务管理来具体的定义用户的业务描述。

业务管理可以从系统主界面的“业务管理”菜单启动。业务管理主要包括业务规划、业务配置和业务数据部署三个方面：

- 业务规划主要涉及 VPN 基本信息、VRF 管理和 CERC 管理三个部分；
- 业务配置主要是引导用户完成具体的业务配置；
- 业务部署主要是具体地把配置命令下发到设备上。

其工作流程为：开始—>业务规划—>业务配置—>业务部署—>结束，有关具体细节将在下面的各个章节中讲述。

需要说明的是，要想使用 UniWorks VPN Manager 系统进行业务管理，需满足如下前提条件：

- 在部署 VPN 业务前，必须保证在 MPLS VPN 网络中的所有路由器都是 IPV4 路由可达的。
- 在每一个路由器上都应该有一个 loopback 迂回地址。
- 每一个路由器都必须有一个可路由的 IP 地址。
- 要配置的路由器需允许 Telnet 连接。
- 要检查配置的路由器，需允许 SNMP 访问。需要错误信息上报的，必须打开 SNMP TRAP 服务。
- 需要访问的路由器需要提供管理员配置密码，需要 SNMP 管理的路由器需要提供可以读和写权限的团体字。

对于港湾网络有限公司的路由器产品来说，打开或者关闭 telnet 服务(配置模式下)的命令为：

service telnet [enable|disable]

如果选择 enable 表示打开 telnet 服务，选择 disable 表示关闭 telnet 服务。可以用 show services 命令查看系统提供的 telnet 服务是否打开；如果显示 Service telnet is **up** 则表明 telnet 已经打开；如果显示 Service telnet is **down** 则表明 telnet 已经关闭。

对一个已经打开 Telnet 服务的交换机，就可以用任何一个有 Telnet 功能的工作站，通过 TCP/IP 网络连接到交换机，从而实现对交换机的配置管理。在 UniWorks VPN

Manager 系统中，大部分的配置命令就是通过 Telnet 方式下发到设备上去的。

打开或者关闭 SNMP 服务(配置模式下)的命令为：

service snmp [enable|disable]

SNMP（Simple Network Management Protocol，简单网络管理协议）提供了一种监控和管理计算机网络的系统方法。SNMP 利用 MIB(Management Information Base)来对对象来定位。同时 SNMP 可以利用陷阱（trap）技术来上报设备信息。

在上面的命令中，如果选择 enable 表示打开 SNMP 服务功能，选择 disable 表示关闭 SNMP 服务。可以利用 show services 命令查看系统提供的 SNMP 服务的状态：

如果显示 Service snmp agent is **up**，表明 SNMP 服务已经被打开；

如果显示 Service snmp agent is **down**，表明 SNMP 服务已经关闭。

配置 SNMP 时，需要对如下参数进行设置：

- Community 字符串：这一字符串提供了一个远程网络管理员配置交换机的用户确认机制。在设备上有两种 Community 字符串：读确认 Community 字符串允许对交换机进行只读访问，缺省值为 public；写确认 Community 字符串提供了对交换机写操作的权限，缺省值为 private。

配置 SNMP 团体属性的命令为：

```
config snmp community [readonly|readwrite] <string>
```

查看 SNMP 团体属性的命令为：

```
show snmp community-string
```

SNMP 有故障自动上报的功能，打开或关闭代理发送 trap 报文功能的命令为：

```
service snmp trap [enable|disable]
```

Trap 服务启动以后，需要为设备指定给哪个设备地址发送 trap 信息，添加 trapreceiver 的命令为：

```
config snmp trapreceiver add <A.B.C.D> version [v1|v2c] {community <string>}*1
```

其中，trapreceiver 是接收 trap 信息的主机；<A.B.C.D>为 trapreceiver 的 IP 地址，v1/v2c 表示 trap 的两个版本；如果这个 trapreceiver 同时还承担着对设备的远程

配置，那么还可以为其设置 community 字符串。

例如，增加一个接收 trap 信息的主机 10.1.30.100，trap 的版本设为 v1 的命令：

```
Harbour(config)# config snmp trapreceiver add 10.1.30.100 version v1
Successfully added trapreceiver IP address is 10.1.30.100
The trap version is v1
The default trap community is public
```

删除 trapreceiver 的命令为：

```
config snmp trapreceriver delete <A.B.C.D>
```

其中〈A.B.C.D>为 trapreceiver 的 IP 地址。

查询 trapreceiver 信息的命令为：

```
show snmp trapreceiver
```

例如，显示 snmp trapreceiver 的配置信息的命令：

```
Harbour(config)# show snmp trapreceiver
IP address            Version        Community
12.12.12.1             v1              public
Total 1 trapreceiver IP address in system.
```


提示

上面列举的是港湾网络有限公司对 Telnet 服务和 SNMP 服务的配置，如果需要对其他公司的设备进行配置，可以参考具体设备厂家的用户手册。

6.2 业务规划

6.2.1 概述

业务规划的主要内容包括规划 VPN 的基本信息、CERC 和 VRF 的设置。 其中：

- VPN 的基本信息包括 VPN 名称、属主和简单的描述信息等。
- CERC 用来规划 VPN 拓扑信息，有两种典型的类型，一种是 full-mesh，一种

是 hub-spoke 类型。

- VRF 主要包括 VRF 的名称、路由区分符（RD），以及对 VRF 的一些必要的设置等。

VPN 的基本信息必须首先填写，只有填写了 VPN 的基本信息，在系统中才能建立一个 VPN 实体。建立了一个 VPN 以后，才可以规划设计 CERC 和 VRF。

业务规划管理主要是规划整个网络的拓扑和 VPN 参数的设定，其主要工作流程是：配置 VPN 基本信息—>配置 CERC—>配置 VRF。

6.2.2 配置VPN基本信息

创建一个 VPN，必须首先输入它的基本信息，包括 VPN 的名称、属主和 VPN 的基本描述信息。

VPN 基本信息是 VPN 在系统中的基本表示，不涉及 VPN 具体的业务信息。业务信息需要在 CERC、VRF 管理中定义。

1. 新建 VPN 基本信息

在主界面的“业务管理“菜单或者在左边的 VPN 树中右键选择“创建 VPN”子菜单项，会弹出一个窗口：

- 在名称一栏中，填入 VPN 的名称；
- 在属主下拉框中，选择 VPN 的属主（下拉框中的数据是从客户系统中获得的）；
- 在描述一栏中，填入对这个 VPN 的简单描述，比如属于哪个组织，创建的目的等等。

2. 删除 VPN

选中要删除的 VPN 后，在上下文菜单或者系统菜单中选择“删除 VPN”，系统将删除该 VPN 中的数据，包括 VPN 中的 VRF、CERC 和 VPN 系统内部的连接信息等所有信息。

3. 修改 VPN

选中要配置的 VPN，在上下文菜单或者系统菜单中选择“修改 VPN”，会弹出一个窗口：

- 在名称一栏中，可以修改 VPN 的名称。
- 在属主下拉框中，可以重新选择 VPN 的属主（下拉框中的数据是从客户系统

中获得的)。

- 在描述一栏中，可以修改对这个 VPN 的简单描述。


注意

新建 VPN 和删除 VPN 不是等价的。新建 VPN 只是输入 VPN 的一些基本信息，而删除 VPN 则把 VPN 的所有信息包括基本信息、VRF、CERC 等规划以及 CE 和 PE 的连接信息都删除。一旦误操作，系统中将不再包含有这个 VPN 的数据。配置 VPN 修改的信息是 VPN 的基本信息，要改变它里面的其它数据可以参考配置 VRF 信息、配置 CERC，以及业务配置等的相关介绍。

6.2.3 配置CERC信息

一个 VPN 可被组织分割成几个子域，构成几个 CERC（CE routing communities）。一个 CERC 描述了在 VPN 内部的 CE 是如何相互联系的，也就是描述了 VPN 的拓扑结构。CERC 有两种常见的类型：

- hub-and-spoke CERC：这种类型中，有一个或者多个 CE 充当 hub 的角色，其它的 CE 充当 spoke 角色。Spoke 类型的 CE 不能相互访问，必须通过充当 hub 角色的 CE。
- full-mesh CERC：这种类型中，所有的 CE 都是连接在一起的，是一个全连接方式。

对于 full-mesh 类型的 CERC 需要一个 RT（route target）。对于 hub-spoke 类型的 CERC 需要两个 RT，分别作为 HUB RT、SPOKE RT。RT 是 MP-BGP 的扩展团体，是一个 8 字节的值，控制着 VPN 路由信息的分布。

MPLS VPN 中，RT 有两种使用方式：

- 一种是当一个 VPN 的路由被发布到 MP-BGP 中的时候，路由和 VRF 相联系的 RT 建立联系。典型情况下，它是通过 VRF 输出（export）RT 的。
- 一种是每个 VRF 都和一组 RT 捆绑在一起。和 VRF 联系在一起的这些 RT 控制着那些发布过来的路由是否可以导入到本地的路由中来。例如，如果一个 VRF 的输入列表是{a,b,c}，那么那些携带团体名为 a,b,c 的路由信息就可以导入到这个 VRF 中。对 RT，输出控制可以用 Export 命令，表明发出去的路由可以被哪些 PE 上的 VRF 所接收，输入控制可以用 Import，表明可以接收那些路由，如果同时需要输入和输出，可以采用 both 命令，同时导入和导出。

RT 一般有两种表达方式：

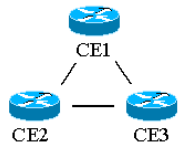
- 与自治系统号（ASN）相关，在这种情况下，RT 是由一个自治系统号和一个任意的数组成；
- 与 IP 地址相关的，在这种情况下，RT 是由一个 IP 地址和一个任意的数组成。

例如：

- 16 位自治系统号：32 位用户自定义的数 ，格式为： 101：3
- 32 位自治系统号：32 位用户自定义的数 ，格式为： 102：3
- 32 位 IP 地址：16 位用户自定义的数 ，格式为 192.3.4.5 : 3

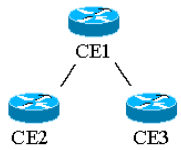
创建一个 VPN 的时候，会默认的创建一个类型为 full-mesh 的 CERC，这个 CERC 作为缺省的。也就是说如果用户不需要配置更复杂的 VPN，那么不需要创建新的 CERC。为了创建更为复杂的网络拓扑，用户需要切断某些 CE 之间的联系，把 CE 分成若干的组，每一个组要么是全连接的，也就是 full-mesh，要么是一个 hub-spoke 模式（当然一个 CE 可以在多个组中）。每一个 CE 组需要它们自己的 CERC。利用 CERC，可以构建复杂的网络拓扑结构。CERC 的两种典型类型和复杂类型分别举例如下所示：

图6-2 CERC1(full mesh 类型)



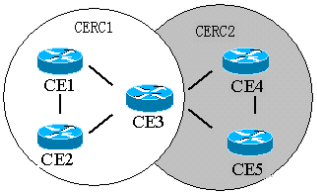
图中，CE1、CE2 和 CE3 是全连接的形式，它们之间可以相互访问。

图6-3 CERC2(hub-spoke 类型)



图中，CE1 为 hub 节点，CE2、CE3 为 spoke 节点，CE2 和 CE3 之间不能直接访问，需要通过 CE1。CE1 可以直接访问 CE2、CE3。

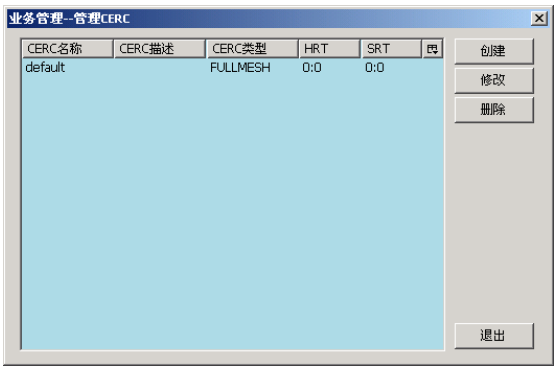
图6-4 复杂类型



图中，CE1、CE2 和 CE3 属于一个 CERC1，CE3、CE4 和 CE5 属于一个 CERC2。同时，CE3 属于两个 CERC1 和 CERC2。

选择业务管理的上下文菜单或者选择系统业务管理菜单中的“管理 CERC”菜单，可以启动管理 CERC 窗口：

图6-5 管理 CERC 窗口



1. 新建 CERC

在上图中，单击“创建”按钮，将出现一个窗口要求用户输入 CERC 的信息。需要填写的 CERC 信息包括：

- CERC 名称：便于记忆的，表明用途的名称；
- CERC 说明：简单的介绍本 CERC 的用途，作为备注；
- CERC 类型：选择要创建的 CERC 是哪种类型：full-mesh 或 hub-spoke 类型。对于 full-mesh 类型，需要输入一个 RT；对于 hub-spoke 类型，需要分别输入一个 hub RT 和一个 spoke RT。

输入 RT 值的方式有三种，单击 RT 右侧的按钮，就可以打开一个窗口：

- 一种是 AS16 + 任意的数值
- 一种是 AS32 + 任意的数值

- 一种是 IPV4 + 任意的数值

RT 配置窗口描述如下：

- 类型选择，具体选择 RD 的类型。
- 管理域输入框，输入管理域的相关值。
- 分配域输入框，输入自己定义的数值。

首先选择类型，如上面所述有三种类型：ASN16、ASN32、IPV4。然后在管理域中输入数值或者 IP 地址，在分配域中输入用户指定的数值。单击“确定”按钮，确认；单击“取消”按钮，不保存这次输入信息。

填写完毕所有的 CERC 信息后，单击“确定”按钮，就可以保存新建的 CERC，确定以后就可以在 CERC 列表中看到 CERC 的表项；单击“取消”按钮，不保存这次创建的 CERC。

2. 删除 CERC

首先在 CERC 列表中选择要删除的 CERC，然后，单击“删除”按钮就可以把选定的 CERC 删除。

1、删除 CERC 前，请确认这个 CERC 不再被任何 VRF 使用；

2、缺省的 Default CERC 不能被删除，而且 Default CERC 的 RT 是 0:0，是不能下发的，用户使用 Default CERC 一定要修改后再使用。

3. 修改 CERC

可以对特定的 CERC 进行重新配置。方法是：在 CERC 列表中选择要配置的 CERC，单击“修改”按钮，就弹出一个窗口，在这里可以重新输入 CERC 的名字、CERC 描述和 CERC 的 RT 等。

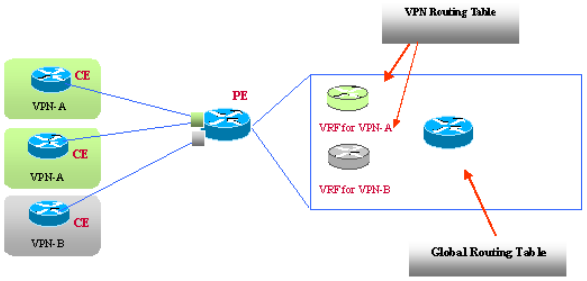
1、重新配置 CERC 时，不能改变 CERC 的类型；

2、修改 CERC 时，应确认这个 CERC 被哪些 VRF 使用，否则随意更改 CERC 的设置，会对业务规划造成一些不必要的麻烦。

6.2.4 配置VRF信息

VPN IP 路由表及相关的 VPN IP 转发表被统称为 VRF（VPN Routing Forwarding Table，VPN 路由及转发表）。VRF 控制着这个 VPN 的导入导出的路由。在 PE 路由器上，为每个 PE 直接相连的 VPN 生成一份路由和转发表。每个 VRF 仅存有所隶属的路由信息。VRF 保存的路由信息和全局的路由信息是分开保存的，示意图如下：

图6-6 VRF 示意图



VRF 与端口关联，端口可以是物理端口、逻辑子端口和虚拟通道的端口。VRF 可以与一个或者多个直接连接的站点相关。如果不同的站点共享同样的路由信息，它们可以共享同一个 VRF。PE 路由器把从直接相连的 CE 路由器学来的路由加入相应的 VRF 中。PE 路由器通过骨干网 IGP 学习的路由被加入到全局路由表中。通过使用独立的 VRF，IP 地址可以在不同的 VPN 中被重复使用。全局路由表由 IGP 维护。PE 路由器可能与其他自治域运行标准的 BGP-4 协议。BGP-4 IPVR 路由进入到全局路由表。MP_BGPVPN_IPV4 路由进入到相应 VRF。

在极端的情况下，可以为连接到 PE 路由器上的每个站点都分配一个 VRF 来存放 VPN 路由，但连接在同一 PE 路由器上的站点如果满足以下三个条件则可以共享一个 VRF：

- 各站点属于同一个 VPN；
- 路由信息相同；
- 站点之间允许相互直接通信。

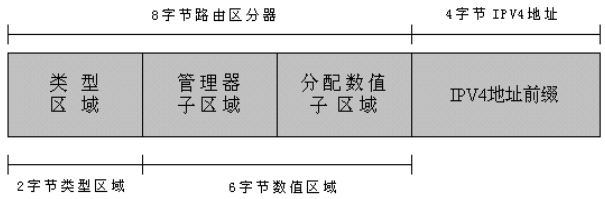
通常 PE 路由器上每个用户的端口与一个特定的 VRF 相关联。

VRF 使用的是 VPN_IPV4 地址，是由 RD 和用户的 IP 地址连接形成的。RD 是路由区别符（ROUTE—DISTINGUISHER）的简称。VPN 路由信息的维护在 P 网内部通过 MP_BGP 完成，由于不同的 VPN 可能使用重复地址段，传统的 BGP 不能处理这种 IP 地址重合的情况，因此设计了 RD。RD 基于 VPN，但是 VPN 的成员

可以不必使用相同的 RD，只需要 VPN_IP 地址在整个 P 网的 VPN 范围唯一。当然一个 VPN 内部的 VRF 最好是用一个 RD 配置。

下面，介绍一下 MPLS VPN-IPV4 的地址结构，以及配置 RD 的一些注意事项。MPLS VPN_IPV4 地址结构如下图所示：

图6-7 MPLS VPN_IPV4 地址结构



VPN-IPV4 地址为 12 字节长，由 8 字节的 RD 以及随后的 4 字节 IPV4 地址前缀组成。8 字节长的 RD 由 2 字节类型区域及 6 字节数值区域组成。类型区域决定数值区域内两个子区域（管理器子区域和分配数值子区域）的长度，同时还决定管理器区域的含义。目前，类型区域定义了两个值：0 和 1。

- 对于类型 0，管理器子区域包括 2 个字节，而分配数值子区域包括 4 个字节。管理器子区域使用自治域号码（ASN）。强烈建议不要使用私有的 ASN。分配数值子区域为来自有服务提供商管理的数值空间，该数值空间用于提供 VPN 服务并与分配使用的 ASN 相关。
- 对于类型 1，管理器子区域包括 4 个字节，而分配数值子区域包括 2 个字节。管理器子区域使用一个 IPv4 地址。强烈建议不要使用私有 IP 地址空间。分配数值子区域为来自由服务提供商管理的数值空间，该数值空间用于提供 VPN 服务并与分配使用的 IPv4 地址相关。对于类型 1 的 RD 配置选项可以使用产生路由的 PE 路由器的回环地址作为 4 字节的管理器子区域，然后选择一个 PE 路由器本地数值作为 2 字节分配数值子区域。

当在 PE 路由器上对 RD 进行配置时，RFC 2547bis 并不要求一个 VPN 内的所有路由使用相同的 RD，而事实上，一个 VPN 内的每个 VRF 可以使用自己的 RD。但是，服务提供商必须确保每个 RD 是全局唯一的。由于这个原因，在定义 RD 时，强烈建议不要使用私有 ASN 空间或私有 IP 地址空间。使用公共 ASN 空间或公共 IP 地址空间确保了每个 RD 全局唯一。全局唯一 RD 提供了一种机制，使每个服务提供商在不与其他服务提供商分配的 RD 发生冲突的前提下，能够管理自己的地址空间并建立全局唯一的 VPN-IPv4 地址。使用全局唯一的 RD 支持以下功能：

- 为一个通用 IPv4 前缀创建不同的路由；
- 为同一系统创建多条全局唯一的路由；
- 通过使用策略来决定哪个数据包应该使用哪条路由。

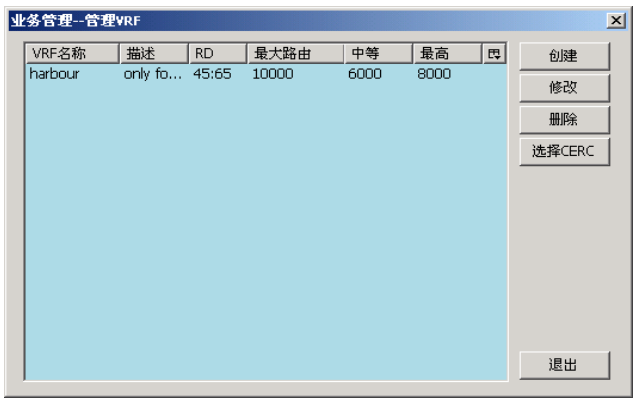
对于 VRF 引入的路由的数量可以利用门限值来进行管理。可以设置最大的门限值，这样当超过了最大的门限值以后，系统将提示超过门限值。同时也提供中等的门限值。

综上所述，一个 VRF 主要包括以下几个部分：

- VRF 名称：便于记忆的一个名字
- VRF 说明：简单的介绍本 VRF 的用途，作为备注
- RD：本 VRF 的路由区别符
- 最大路由：允许本 VRF 导入的路由数量
- 一般门限值：可以设置一般的门限
- 最高门限值：当到达这个门限值以后，将不再加入新的路由

选中 VPN 业务管理中相应的业务后，选择业务管理的上下文菜单或者选择系统业务管理菜单中的“管理 VRF”菜单，可以启动管理 VRF 窗口：

图6-8 管理 VRF



1. 创建 VRF

在上图中，单击“创建”按钮，将出现一个窗口要求输入 VRF 的信息。需要填写的 VRF 的信息包括：

- VRF 名称：便于记忆的一个名字。
- VRF 说明：简单的介绍本 VRF 的用途，作为备注。
- RD：本 VRF 的路由区别符。输入 RD 的时候，单击 RD 旁边的按钮，将弹出一个创建 RD 的窗口。用户需先通过“类型选择”选择 RD 的类型，有三种类型 ASN16、ASN32 和 IPV4 可供选择；然后，通过“管理域”输入框，输入管理域的相关值，数值或者 IP 地址；再通过“分配域”输入框，输入用户指定的数值。单击“确定”按钮，确认；单击“取消”按钮，不保存这次输入的

信息。

- 最大路由：允许本 VRF 导入的路由的数量。
- 一般门限值：可以设置一般的门限。
- 最高门限值：当到达这个门限值以后，将不再加入新的路由。

单击创建 VRF 窗口下面的“确定“按钮，保存 VRF 数据，返回 VRF 管理界面；单击窗口下面的”取消“按钮，不保存 VRF 数据，直接返回到 VRF 管理界面中。


注意

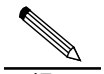
在添加 VRF 时不要重复添加。

2. 删除 VRF

可以删除特定的 VRF。方法是：在 VRF 列表中选择要删除的 VRF，单击“删除”按钮就可以把 VRF 删除。删除以后，在 VRF 列表中将清除相应的 VRF。

3. 修改 VRF

可以对特定的 VRF 进行重新配置。在 VRF 列表中选择要配置的 VRF，单击“修改”按钮，就弹出一个窗口，允许重新设置 VRF 的各个指标，相关说明请参见上面“创建 VRF”的内容。


提示

配置 VRF 信息时可以同时选择 CERC。在上图中单击“选择 CERC”按钮就可以为 VRF 选择特定的 CERC。提供这个功能主要是为熟练的操作人员。建议为 VRF 选择 CERC 的工作在下一个章节讲述的配置 VPN 系统中完成。

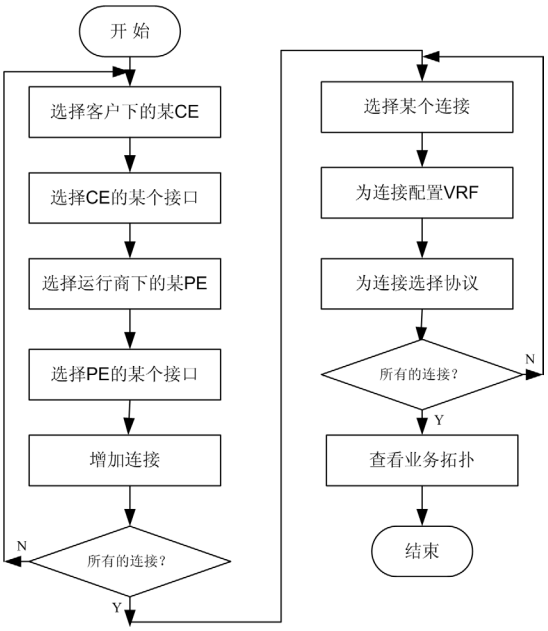
6.3 业务配置

业务配置主要完成客户 CE 和运营商 PE 之间的连接配置。操作员需要为客户 CE 选择特定的接口，与运营商上的 PE 设备某个接口相连，配置这个连接所要用到的 VRF，为这个 VRF 选定 CERC，同时需要为每一个连接配置特定的协议。目前支持的协议主要有 RIP、OSPF、BGP4 和静态路由等。配置 VPN 系统是为客户选

定 CE，选择连接的 PE 设备的工作，在整个规划阶段占有重要的地位。为了方便操作员的使用，在这个部分也可以创建新的 CERC，新的 VRF。当配置结束的时候，业务拓扑就会在系统主界面中显现出来，操作员可以将自己的设计和业务拓扑进行对照，以便做一些调整。

配置 VPN 系统的工作流程如下图所示：

图6-9 配置 VPN 系统的工作流程



具体步骤如下：

步骤**1**　选择业务管理的上下文菜单或者选择系统业务管理菜单中的“业务配置”菜单，可以启动业务配置窗口，业务配置窗口的配置项目如下表所述。

表6-1 业务配置

项目	描述
客户下拉框	提供所有的客户供选择
站点下拉框	提供某客户的站点供选择
CE下拉框	提供某个站点的CE路由器的选择
CE接口列表	选中某个CE以后，列出所有的接口
运营商下拉框	提供所有的运营商供选择
区域下拉框	提供某个运营商下面的区域供选择
PE下拉框	提供某区域下的PE供选择

项目	描述
PE接口列表	选中某个PE以后，列出所有的接口
增加连接按钮	选中PE和CE的接口后，加入到要配置的列表中去
连接列表	所有要配置的列表
配置VRF按钮	为某个选中的连接配置VRF
配置协议按钮	为某个选中的连接配置协议
删除连接按钮	删除某个选中的连接
查看连接按钮	查看某个连接，显示PE、CE接口信息

步骤**2**	在窗口中选择客户下拉框，从中选择某一个客户。
步骤**3**	选择某个客户以后，在站点的列表中出现站点的列表，从中选择某一个站点。
步骤**4**	选择某个站点后，在CE的下拉框中出现CE的列表，从中选择某一个CE。
步骤**5**	选中某个CE以后，在下面的接口列表中，显示出很多的接口，选中一个接口。
步骤**6**	在运营商的下拉框中选择某个运营商，这些运营商的信息是从客户系统得到的。
步骤**7**	选择某个运营商以后，在区域的列表中就会包含这个运营商所有的区域信息。选择一个要连接的PE的区域。
步骤**8**	选择一个区域以后，在PE列表中会包含很多PE，选择一个要连接的PE。
步骤**9**	在PE接口列表中选择一个和CE连接的接口。
步骤**10**	选中两个接口以后，单击窗口中的“添加”按钮，被选中的连接将被添加到窗口下方的列表中。 可以按照上面的步骤加入更多的连接。
步骤**11**	在连接的列表中，选择特定的连接后，可以为这个连接指定某个VRF。单击“配置VRF”按钮，进入管理VRF窗口，可以发现已创建的VRF。同时也可以对VRF进行添加、修改和删除等操作。选择了某个VRF以后，就可以为某个VRF指定CERC。 单击管理VRF窗口中的“选择CERC”，可以打开选择CERC的窗口。在这个窗口中可以看到已创建的CERC。用户可以为VRF指定一个或者几个CERC。如果选择的CERC是Hub-Spoke，那么可以为这个连接指定是用Hub RT还是用Spoke RT。选择Hub,spoke 的方法是：选中列表中的某一个CERC以后，右键可以在上下文菜单中选择。指定CERC的类型以后，在角色一栏中可以看到是HUB或者是SPOKE。然后，单击“选择”，就为选中的VRF选择了这个CERC。一个VRF可以捆绑多个CERC。单击“取消”按钮，将把选中的CERC取消。单击 “确定”按钮保存选择的信息，单击右下脚的“取消”按钮，不保存信息，关闭窗口。

重复步骤 11，用户可以为每一个连接配置 VRF，并且为每一个 VRF 选择特定的 CERC。

步骤**12**	在配置窗口中，用户可以为每一个连接选择协议，现在支持的协议有：RIP2、OSPF、BGP4和静态路由等。

重复步骤 12 可以为每一个连接配置特定的协议。

步骤13　配置完成所有的信息后，用户可以在业务拓扑显示中查看到完成配置后的业务拓扑信息，如下图所示。

图6-10 两个 CE 的拓扑

如上所述，描述了配置一个 VPN 的主要步骤，在这些步骤中用户可以查看连接，同时还可以做一些修改。

提示

1、配置 VPN 的过程中，尽管可以管理 VRF 和 CERC 等信息。但这主要是给熟练的操作人员提供一个方便。建议用户在实际使用中，先做好整个网络的规划，完成 VRF、CERC 等资源的创建，然后再对设备进行 VPN 配置；利用 VPN 配置对设备进行配置

2、配置完成后，建议将业务拓扑显示和构思进行比较，检查配置的结果和设想是否一致，并可进行一些调整;

3、配置完成后，在网络拓扑中也会增加相应的拓扑;

4、如果拓扑图没有更新，请单击系统菜单“业务管理”下的“刷新”菜单项;

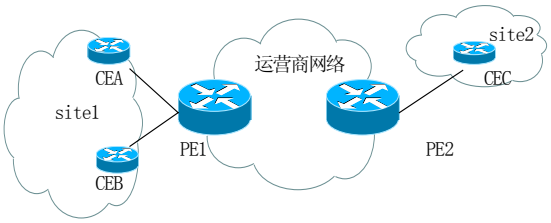
5、配置完成后，在网络拓扑中可以看到 PE 和 CE 的连接情况。

配置案例 1：full-mesh 类型

案例描述

客户甲有三个 CE 设备，想通过 MPLS 网络建立一个全连接的 VPN。组网图如下图所示：

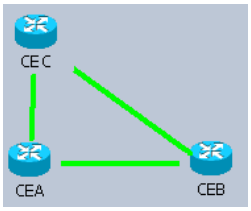
图6-11 full-mesh 类型的应用



配置步骤：

步骤**1**	在客户资源中增加这三个设备，指定它们基本的访问口令、IP地址，在设备的接口管理中增加与PE连接的接口。假设这三个CE设备的名字分别为CEA、CEB和CEC。每个CE设备分别指定一个Loopback地址，增加一个ethernet类型的网络接口，CEA、CEB和CEC设备接口分别为interfaceA、interfaceB、nterfaceC。同时假设CEA、CEB位于站点1，CEC位于站点2。
步骤**2**	计划和这三个设备连接的有两个供应商的PER（Provider Edge Router）PE1、PE2。CEA、CEB分别与PE1相连（这个PE提供两个接口）。CEC与PE2相连。
步骤**3**	输入这个VPN的基本信息，比如它的属主就是这个客户甲，同时可以填写一些基本信息。
步骤**4**	因为这是一个全连接的VPN，所以用户可直接利用系统默认的CERC—full-mesh类型的CERC。
步骤**5**	这个VPN利用一个VRF就可以完成设置，所以配置一个VRF就可以了，这个VRF和默认的CERC相联系。
步骤**6**	具体的配置过程，如同上面业务数据配置所描述的，分别选择客户CE设备和运营商的PE设备，选择接口建立连接，分别配置所设计的VRF和CERC。
步骤**7**	配置完成以后，用户可在拓扑显示中看到业务拓扑信息，如下图所示：

图6-12 业务拓扑信息



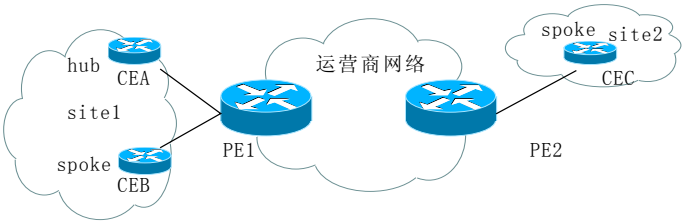
步骤**8**	对照业务拓扑信息后，可以参照下一节业务数据部署，把命令下发到设备上去。

配置案例 2：Hub-spoken 类型

案例描述

客户乙有三个 CE 设备，假设这三个 CE 设备的名字分别为 CEA、CEB 和 CEC。想通过 MPLS 网络建立一个 VPN。但是 CEA 为公司总部，CEB、CEC 都是公司的办事处。公司总部要求能访问两个办事处，两个办事处要求不能直接访问，需要通过公司总部访问。我们可以利用 Hub-spokenVPN 来解决这个问题。组网图如下图所示：

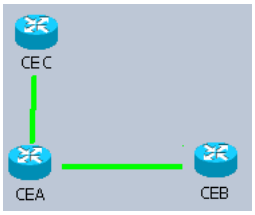
图6-13 Hub-spoken 类型的应用



配置步骤：

步骤**1**	客户资源中增加这三个设备，指定它们基本的访问口令、IP地址，在设备的接口管理中增加与PE连接的接口。每个CE设备分别指定一个Loopback地址，增加一个ethernet类型的网络接口，CEA、CEB、CEC设备接口分别为interfaceA、interfaceB、interfaceC。同时假设CEA、CEB位于站点1，CEC位于站点2。
步骤**2**	和这三个设备连接的是两个供应商的PER（Provider Edge Router）PE1、PE2。CEA、CEB分别与PE1相连（这个PE提供两个接口）。CEC与PE2相连。
步骤**3**	输入这个VPN的基本信息，比如它的属主就是这个客户乙，同时可以填写一些基本信息。
步骤**4**	因为这不是一个全连接的VPN，需要新建立一个CERC，类型为hub-spoken。
步骤**5**	要分别为Hub节点的CE和Spoken节点设置不同的VRF，需要建立两个VRF，一个命名为Vrf_hub，一个命名为VRF_spoken。
步骤**6**	具体的配置过程，如同上面业务数据配置所描述的，分别选择客户CE设备和运营商的PE设备，选择接口建立连接，分别配置所设计的VRF、CERC。同时注意在为公司总部连接的VRF选择CERC的时候，需要指定角色为Hub，办事处的需要指定角色为Spoken。
步骤**7**	配置完成后，将会在拓扑显示中看到业务拓扑信息，如下图所示：

图6-14 业务拓扑信息



这样两个公司办事处的 CE 直接和公司总部相连，而两个办事处不能直接相互访问。

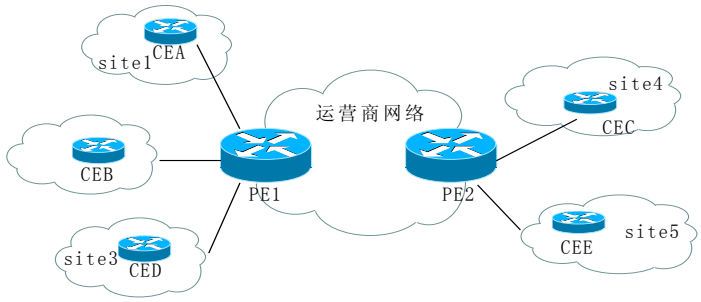
步骤**8**	对照业务拓扑信息后，可以参照下一节业务数据部署，把命令下发到设备上去。

配置案例 3：复杂拓扑类型

案例描述

客户丙有三个站点，site1、site2 和 site3，每个站点包括一台 CE 设备，假设三个 CE 设备的名字分别为 CEA、CEB 和 CEC，通过 MPLS 网络，建立一个 full-mesh 的 VPN。同时客户丙希望 CEA 能够被另外的两个合作伙伴访问，假设两个合作伙伴的站点分别包含一个 CE，命名为 CED、CEE。那么就需要建立两个 CERC1、CERC2。CERC1 包含设备 CEA、CEB 和 CEC，是一个全连接的形式，CERC2 包含设备 CEA、CED 和 CEE，它们是 Hub-spoken 类型的，其中 CEA 是 Hub 站点。组网图如下图所示：

图6-15 复杂拓扑类型的应用

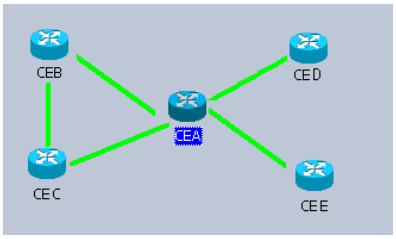


配置步骤：

步骤**1**	客户资源中增加这5个设备，分别属于不同的站点。指定它们基本的访问口令、、IP地址，在设备的接口管理中增加与PE连接的接口。每个CE设备分别指定一个Loopback地址，增加一个ethernet类型的网络接口。

步骤2	和这三个设备连接的是两个供应商的PER（Provider Edge Router）PE1、PE2。CEA、CEB和CED分别与PE1相连。CEC、CEE与PE2相连。
步骤3	输入这个VPN的基本信息，比如它的属主就是这个客户丙，同时可以填写一些基本信息。
步骤4	考虑到这是一个比较复杂的网络拓扑，增加一个Hub-spoken类型的CERC。同时也利用默认的CERC。
步骤5	对CERC1，需要一个VRF。对于CERC2，需要两个CERC，同时考虑到CEA要连接两个CERC，需要单独建立一个VRF，所以一共需要三个VRF，分别命名为VRFA、VRFB和VRFC。VRFA与CERC1、CERC2相关联，主要为CEA设置；VRFB与CERC1相关联，主要是为CEB、CEC设置；VRFC与CERC2相关联，主要是为Spoken节点的CED、CEE设置。
步骤6	具体的配置过程，如同上面业务数据配置所描述的，分别选择客户CE设备和运营商的PE设备，选择接口建立连接，分别配置VRF、CERC。同时注意在为CEA连接的VRF选择CERC的时候，需要选择CERC1和CERC2，并且指定角色为Hub；CEB、CEC的CERC选择CERC1，CED、CEE需要选择CERC2，并且需要指定角色为Spoken。
步骤7	配置完成以后，将会在拓扑显示中看到业务拓扑信息如下图所求：

图6-16 业务拓扑信息



这样 CEA、CEB 和 CEC 可以相互访问，CEA 可以访问 CED、CEE，CED、CEE 可以访问 CEA，但是不能直接访问。

步骤8	对照业务拓扑信息后，可以参照下一节业务数据部署，把命令下发到设备上去。

6.4 业务数据部署

业务规划和业务配置主要是计划阶段，生成的配置并没有具体的下发到对应的设备上去。业务数据部署就是为了完成配置的业务数据真正的部署到设备上去。

选中特定的 VPN，在系统业务管理菜单或者是上下文菜单中，选择“业务部署”菜单项就可以进行业务部署。

业务部署窗口分成左右两个部分：

- 左部分是 PE 列表，列出所有要配置的 PE
- 右部分是命令列表，列出这个 PE 所有要下发的命令

有多少需要配置的设备，列表就有多少项。命令列表显示的是将要对设备发送的命令，如创建一个 VRF，它可能产生的命令如下：ip vrf vrf_1;rd 100:1。

对每一个命令都包括：

- 一个序号，表示顺序；
- 具体的命令；
- 执行的结果，命令是否成功等；
- 执行的状态，表示这个命令的执行状况。

下半部分是一个进度条，表示已经处理的命令的比例。在命令发送的过程中，进度条会相应的增加。所有的命令处理完毕，进度条状态变为 100%。如果中间出现错误，提示业务部署失败。

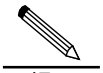
命令执行过程中，需要的时间根据网络状况，可能会有很大的差异。网络拥塞，速度有可能较慢，请耐心等候。

7 告警管理

7.1 概述

告警管理在整个 UniWorks VPN Manager 系统中占据着重要的地位，主要用于监视系统的运行情况，及时发现网络中存在的问题，实时地通过业务拓扑以及输出告警信息的方式，通告管理员，并且保存到日志中，以备管理员的查询。

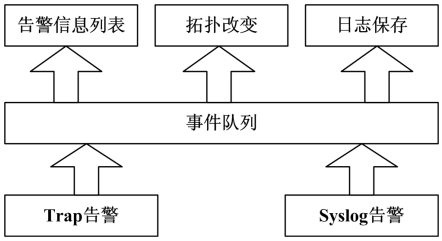
告警管理系统接收设备上报的告警类型包括 Trap 告警和 Syslog 告警。


提示

目前，本版本只接收 Trap 告警。

告警管理系统采用分层的设计模式，其主要工作流程如下图所示：

图7-1 告警管理系统工作流程图



首先接收告警信息，然后转化成统一格式的事件信息，保存到队列中；再根据事件信息的类型，以告警信息列表，或者业务拓扑改变的方式来通告管理员，并将告警信息保存到日志中。

管理员根据告警信息列表可以确定发生故障的具体内容，根据业务拓扑线条的改变（一般用绿色代表正常，红色代表出现故障），可以看出是哪个链路发生了故障。

7.2 告警类型

目前，UniWorks VPN Manager 系统主要处理 Trap 告警。Trap 是根据 mpls-vpn-mib-draft-05 来进行定义的。目前支持的 Trap 类型有：

- mplsVrfIfUp
- mplsVrfIfDown
- mplsNumVrfRouteMidThreshExceeded
- mplsNumVrfRouteMaxThreshExceeded
- mplsNumVrfSecIIlgILblThrshExcd
- mplsNumVrfRouteMaxThreshCleared

为了更好的理解这几个Trap，请先了解一下MPLS-VPN-MIB。

MPLS VPN允许运营商提供三层的VPN服务，可以把用户站点连接到公共网络上，并且提供了与私有网络相同的安全等级。一个VPN包含着多个VRF,VRF在PE路由器上创建，它包含着路由表，以及与这个VRF连接的接口列表。MPLS-VPN-MIB就是用来表述VRF这个结构的。MPLS-VPN-MIB提供了统一的接口，方便操作各个厂商的设备，并且能提供接口失效时相应的告警信息。对一些潜在的威胁，如路由表项过多、无效标签过多、可能受到安全攻击等做出预警。

要想启用这个MIB,首先需要在路由器上启动SNMP,同时在路由器上启动MPLS、BGP等相关协议。

MPLS-VPN-MIB包含多个表和Trap类型,用户可以利用SNMP应用程序来浏览这些表项。MIB库主要包括统计表（Scalar Objects）、实体表（MIB Tables）和告警信息表（Notifications）三部分。

7.2.1 统计表（Scalar Objects）

有关表项描述一下：

表7-1 统计表（Scalar Objects）

MIB Object	功能描述
MplsConfiguredVrfs	在这个路由器上配置的VRF的数量，包括近期删除的VRF
MplsVpnActiveVrfs	在这个路由器上正在被使用的VRF的数量
Mpls VpnConnectedInterfaces	连接VRF的总接口数量
Mpls VpnNotificationEnable	是否允许产生告警信息
mplsL3VpnVrfConfMaxPossRts	表明这个路由器可以保存的路由数量，一般设为0

MIB Object	功能描述
mplsL3VpnVrfConfRteMxThrshTime	设定引发Trap的间隔

7.2.2 实体表（MIB Tables）

实体表（MIB Tables）主要包括：

- Mpls VpnVrfTable
- Mpls VpnInterfaceConfTable
- MplsVpnvrfRouteTargetTable
- MplsVpnVrfSecTable
- MplsVpnVrfPerfTable
- mplsL3VpnVrfRteEntry

1. Mpls VpnVrfTable

Mpls VpnVrfTable表示在路由器上定义的vrf。每一个vrf是用它的名字来引用的。有关表项描述一下：

表7-2 Mpls VpnVrfTable

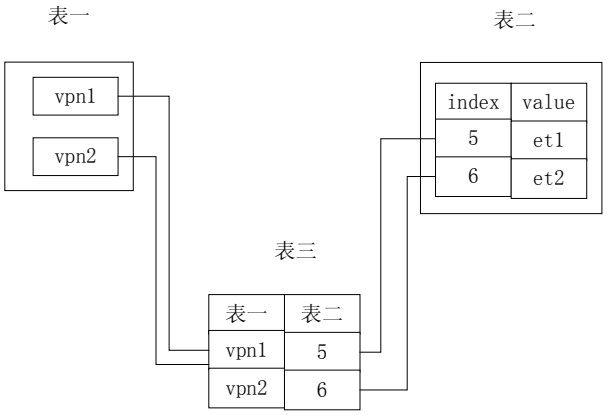
MIB Object	功能描述
mplsVpnVrfName	VRF 的名字，用作索引。注意用作索引的时候，第一个值是字符串的长度，后面是字符串的ASCII代码。例如，“VPN1”表示为4.118.112.110.49
MplsVpnVrfDescription	用来描述这个VRF
MplsVpnVrfRouteDistinguisher	VRF的RD的值
MplsVpnVrfCreationTime	SysUpTime类型的值，表明什么时候创建
MplsVpnVrfOperStatus	vrf的状态，有两种，up和down。当一个VRF是UP的时候，至少有一个和这个VRF联系的接口状态是UP。一个VRF是DOWN的时候，表示没有一个接口和这个VRF联系，或者即便绑定，但是接口的状态不是UP
MplsVpnVrfActiveInterfaces	与这个VRF联系的接口UP的数量
MplsVpnVrfAssociatedInterfaces	与这个VRF相联系的全部接口的数量
MplsVpnVrfConfMidRouteThreshold	中等路由门限，当超过中等门限时，会发一个mplsNumVrfRouteMidThreshExceeded告警信息
Mpls VpnVrfConfHighRouteThreshold	最大路由门限，当超过最大门限时，会发一个mplsNumVrfRouteMaxThreshExceeded告警信息
MplsVpnVrfConfMaxRoutes	最大的路由

MIB Object	功能描述
MplsVpnVrfConfLastChanged	配置发生变化的sysUpTime值
MplsVpnVrfConfRowStatus	增加、删除和修改表项的标志
mplsVpnVrfConStorageType	这个表项现在没有使用

2. MplsVpnInterfaceConfTable

MplsVpnInterfaceConfTable表示一个Vrf和接口相联系。VRF利用的接口是在ifTable中定义的。IfTable定义的是路由器所有的接口列表，MplsVpnInterfaceConfTable就是把一个VRF的表项mplsVpnVrfTable和ifTable联系起来。这三个表的关系如下图所示：

图7-2 MplsVpnInterfaceConfTable 把 mplsVpnVrfTable 和 ifTable 联系起来的关系图



表一：mplsvpnvrftable　表二： ifTable 表三： mplsVpnIfConfTable

有关表项描述一下：

表7-3 MplsVpnInterfaceConfTable 表

MIB Object	功能描述
MplsVpnInterfaceConfIndex	提供一个ifIndex
MplsVpnInterfaceLabelEdgeType	表明是一个运营商边界路由器的接口，还是一个客户的接口
MplsVpnInterfaceVpnClassification	表明这个vpn的种类，1代表Csc；2代表enterprise；3代表InterProvider
MplsVpnInterfaceVpnRouteDistProtocol	路由发布协议，BGP:2，OSPF:3，RIP:4
MplsVpnInterfaceConfStorageType	目前没有使用
MplsVpnInterfaceConfRowStatus	创建、修改和删除的标志

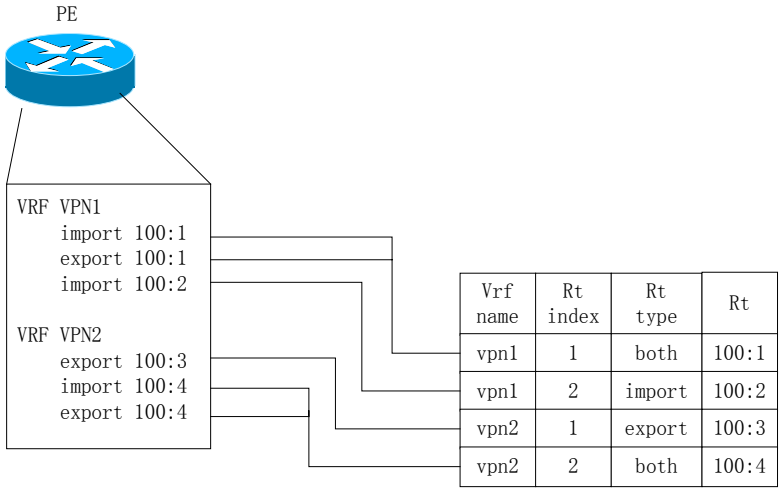
3. MplsVpnVrfRouteTargetTable

MplsVpnVrfRouteTargetTable 用来表示为某个 VRF 定义的 RT 属性（RT 用来控制 VPN 路由信息的发布）。当 VRF 向外发布路由（从 CE 获得）时，会把对应的 RT 设置成 export。VRF 引入的路由使用 import 的 RT 控制，比如一个 VRF 引入的 RT 列表是{A,B,C}，那么那些携带{A,B,C}扩展字的路由被引入。

MplsVpnVrfRouteTargetTable 是利用 mplsL3VpnVrfName 、mplsL3VpnVrfRTIndex 和 mplsL3VpnVrfRTType 来索引的。

下面是一个具体的实例：

图7-3 MplsVpnVrfRouteTargetTable 说明



有关表项描述一下：

表7-4 MplsVpnVrfRouteTargetTable 表

MIB Object	功能描述
MplsVpnVrfRouteTargetIndex	RT 索引
MplsVpnVrfRouteTargetType	类型，有三种： 1:import 2:export 3:both
MplsVpnVrfRouteTarget	具体的RT值
MplsVpnVrfRouteTargetDescr	具体的描述
MplsVpnVrfRouteTargetRowStatus	用来表示表项的增加，删除，编辑状态

4. MplsVpnVrfSecTable

MplsVpnVrfSecTable主要是提供VRF的安全特性，其扩大了mplsVpnVrfTable，这两个表有相同的索引。有关表项描述一下：

表7-5 MplsVpnVrfSecTable

MIB Object	功能描述
MplsVpnVrfSecIllegalLabelViolations	接收到的不合法的标签数量
MplsVpnVrfSecIllegalLabelRcvThresh	标签数量的限制

5. MplsVpnVrfPerfTable

MplsVpnVrfPerfTable主要是提供性能数据，包括本VRF目前的路由数量，以及增加、删除的路由数量等。有关表项描述一下：

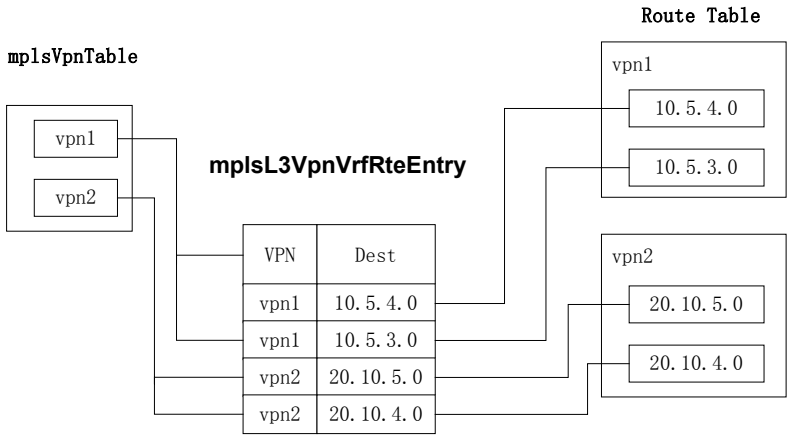
表7-6 MplsVpnVrfPerfTable

MIB Object	功能描述
MplsVpnVrfPerfRoutesAdded	增加的路由数量
MplsVpnVrfPerfRoutesDeleted	从这个VRF删除的路由数量
MplsVpnVrfPerfCurrNumRoutes	当前的路由数量

6. mplsL3VpnVrfRteEntry

mplsL3VpnVrfRteEntry 表示 VRF 内部的路由表。这个表项用 mplsL3VpnVrfName、mplsL3VpnVrfRteInetCidrDestType、mplsL3VpnVrfRteInetCidrDest 、mplsL3VpnVrfRteInetCidrPfxLen 、mplsL3VpnVrfRteInetCidrPolicy、mlsL3VpnVrfRteInetCidrNHopType 和 mplsL3VpnVrfRteInetCidrNextHop 来索引。VRF 和 mplsL3VpnVrfRteEntry 之间的关系如下图所示：

图7-4 VRF 和 mplsL3VpnVrfRteEntry 的关系图



有关表项描述一下：

表7-7 mplsL3VpnVrfRteEntry

MIB Object	功能描述
mplsL3VpnVrfRteInetCidrDestType	IP地址类型
mplsL3VpnVrfRteInetCidrDest	目的IP地址
mplsL3VpnVrfRteInetCidrPfxLen	掩码长度
mplsL3VpnVrfRteInetCidrPolicy	目前没有定义
mplsL3VpnVrfRteInetCidrNHopType	下一跳的类型
mplsL3VpnVrfRteInetCidrNextHop	下一跳的地址
mplsL3VpnVrfRteInetCidrIfIndex	下一跳的转出接口
mplsL3VpnVrfRteInetCidrType	定义路由器是本地的还是远端的
mplsL3VpnVrfRteInetCidrProto	负责向这个VRF增加路由协议
mplsL3VpnVrfRteInetCidrAge	自从路由更新以来的时间
mplsL3VpnVrfRteInetCidrNextHopAS	下一跳的AS号码
mplsL3VpnVrfRteInetCidrMetric1 mplsL3VpnVrfRteInetCidrMetric2 mplsL3VpnVrfRteInetCidrMetric3 mplsL3VpnVrfRteInetCidrMetric4 mplsL3VpnVrfRteInetCidrMetric5	使用这个路由的Metric值
mplsL3VpnVrfRteXCPointer	用于和mpls表联系
mplsL3VpnVrfRteInetCidrStatus	用于表项的编辑

7.2.3 告警信息表（Notifications）

告警信息表（Notifications）主要包括六种告警类型：

- mplsVrfIfUP
- mplsVrfIfDown
- mplsNumVrfRouteMidThreshExceeded
- mplsNumVrfRouteMaxThreshExceeded
- mplsNumVrfSecIllegalLabelThreshExceeded
- MplsNumVrfRouteMaxThreshCleared

其中，mplsVrfIfUP在如下两种情况下发生：

- 和一个 VRF 绑定的接口转化为 up 状态
- 当一个状态为 up 的接口和一个 VRF 绑定时

mplsVrfIfUP 提供两个描述信息：

- MplsVpnInterfaceConfRowStatus：创建、修改和删除的标志
- MplsVpnVrfOperStatus：vrf 的状态，有两种，up 和 down。当一个 VRF 是 UP 的时候，至少有一个和这个 VRF 联系的接口状态是 UP。一个 VRF 是 DOWN

的时候，表示没有一个接口和这个 VRF 联系，或者即便绑定，但是接口的状态不是 UP

MplsVrfIfDown在如下两种情况下发生：

- 和一个 VRF 绑定的接口转化为 down 状态
- 当一个接口和 VRF 消除绑定关系时

MplsVrfIfDown 提供两个描述信息：

- MplsVpnInterfaceConfRowStatus：创建、修改和删除的标志
- MplsVpnVrfOperStatus：vrf 的状态，有两种，up 和 down。当一个 VRF 是 UP 的时候，至少有一个和这个 VRF 联系的接口状态是 UP。一个 VRF 是 DOWN 的时候，表示没有一个接口和这个 VRF 联系，或者即便绑定，但是接口的状态不是 UP

MplsNumVrfRouteMidThreshExceeded、mplsNumVrfRouteMaxThreshExceeded 主要是提供一个预警功能，当 VRF 的路由数量超过一定数量的时候，就引发这两个告警。正如前面所述，VRF 的路由数量会设立一个最大值，一个中等门限；当超过中等门限的时候，就引发 MplsNumVrfRouteMidThreshExceeded 告警，当超过最大路由的时候就发出 mplsNumVrfRouteMaxThreshExceeded 告警。

MplsNumVrfRouteMidThreshExceeded 提供的信息包括：

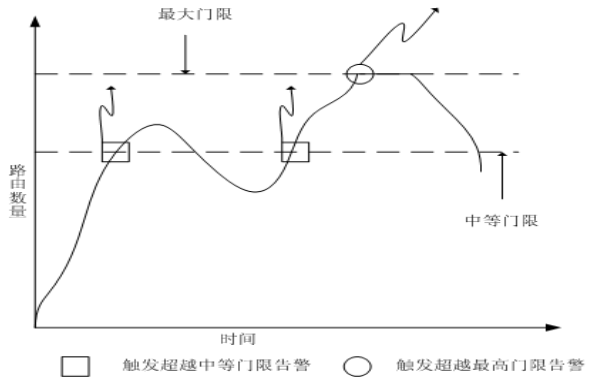
- mplsL3VpnVrfPerfCurrNumRoutes：当前的路由数量
- mplsL3VpnVrfConfMidRteThres：中等门限数值

MplsNumVrfRouteMaxThreshExceeded 提供的信息包括：

- MplsVpnVrfPerfCurrNumRoutes：当前的路由数量
- MplsVpnVrfConfHighRouteThreshold：最大门限数值

这两个 Trap 的关系如下图所示：

图7-5 中等门限和最大门限告警对比



mplsNumVrfSecIllegalLabelThreshExceeded 当接收到的不合法的标签超过设定的数量时，引发这个告警。这个 trap 提供的信息包含 MplsVpnVrfSecIllegalLabelViolations，没有包含设定的门限，是因为发起这个 trap 的时候，收到非法标签的数量正好等于设定的门限，也就是说，现在非法标签的数量和设定的门限是一致的。所以只提供了当前值。

MplsNumVrfRouteMaxThreshCleared 当路由数量下降到最高门限值的时候，发出这个 trap，提示操作员现在路由数量趋于正常。

目前 UniWorks VPN Manager 系统提供的告警除了上面在草案中提到的六种以外，还采集基本的 trap 信息。参照 RFC1215，需要支持的几种 trap 有：coldstart、warmstart、linkdown、linkup、authenticationFailure 和 egpNeighborLoss 等。

其中：

- Coldstart、warmstart 主要是设备的初始化信息。
- Linkdown、linkup 主要是监视接口的状态，当接口连接建立，就发 linkup 信息，当接口连接失败，就发 linkdown 信息。
- AuthenticationFailure 提示 SNMP 验证团体字失败。
- EgpNeighborLoss 通知 egp 对端的邻居失去连接。

同时考虑到 BGP 在 VPN 中的重要应用，增加了 BGP 的 trap，包括 bgpEstablished 和 bgpBackwardTransition 两种。BgpEstablished 主要是通知 BGP 的 FSM 的连接建立，bgpBackwardTransition 主要提示 BGP 的 FSM 从一个较高的状态变为较低的状态。

综上所述，UniWorks VPN Manager 系统采集的告警类型如下表所述：

表7-8 UniWorks VPN Manager 系统采集的告警类型

序号		名称	简单描述
基本TRAP类型	1	Coldstart	发送协议实体已经被重新初始化，表明设备的配置或实体操作可能改变
	2	Warmstart	发送协议已经被重新初始化，但设备的配置和协议实体没有改变
	3	Linkdown	一个通信联系已经失败
	4	linkup	一个通信联系已经建立，受影响的接口被确认为变量捆绑域内的第一个要素：ifIndex事件的名字和值
	5	AuthenticationFailure	设备接收到鉴别不当的SNMP消息
	6	egpNeighborLoss	一个EGP邻居失效
MPLSVPN部分	1	mplsVrfIfUp	在下面两种情况下产生：1、当和一个vrf联系的interface的状态转变为up时； 2、当一个interface的状态为up，和一个VRF联系时。
	2	mplsVrfIfDown	在下面两种情况下产生：1、当和一个vrf联系的interface的状态转变为down； 2、当一个interface的状态为up，和一个vrf拆离时
	3	mplsNumVrfRouteMidThreshExceeded	当vrf里面的路由超过设定的中等门限的时候
	4	mplsNumVrfRouteMaxThreshExceeded	当VRF里面的路由超过设定的最高门限的时候
	5	mplsNumVrfSecIllglLblThrshExcd	当VRF收到错误标签的时候，代表可能的恶意入侵
	6	mplsNumVrfRouteMaxThreshCleared	当vrf的路由从高于最高门限变为低于最高门限时
BGP部分	1	bgpEstablished	当BGP的FSM进入到建立状态的时候
	2	bgpBackwardTransition	当 BGP FSM从一个比较高的状态进入到一个比较低的状态的时候

7.3 告警操作

告警操作主要包括以下几个部分：

- 参数设置：第一次运行系统时，一定要输入要监听的 IP 地址和端口，否则服务不能正常启动；
- 启动/停止服务：用于手工启动和停止告警服务；
- 告警数据的保存和删除：为方便用户查看，用户可以删除告警列表中的全部或特定数据，也可以保存告警列表中全部或特定数据到文件。

对告警列表中的告警信息进行的删除或保存操作不会影响数据库中的告警信息。

7.3.1 参数设置

告警管理的参数配置主要包括：

- 监听的 IP 地址：主要是对多 IP 地址的主机，指定监听哪个 IP 地址；
- 监听的端口：指明监听哪个端口；
- 界面上显示的最大告警数量：允许在界面上显示的告警数量
- 是否在界面上显示：用户可以选择是否在界面上反映接收到的告警
- 是否在拓扑图中显示：用户可以选择拓扑图形是否反映接收到的告警，如果用户选择在拓扑图上显示一些故障，如接口 down，那么 PE 与 CE 之间的连线会变为告警颜色（如红色）。
- 是否随系统启动：如果用户选中该项，表示 UniWorks VPN Manager 系统一启动，故障服务同时启动，如果没有选择，那么必须手工启动该服务。

在主菜单栏中“告警管理”菜单项下选择参数设置，就可以打开参数设置的窗口，操作员可以根据上面的选项，设置参数。在打开的窗口中，点击“确定”按钮保存设置，关闭窗口；点击“取消“按钮不保存设置，关闭窗口。

7.3.2 启动

告警服务可以手工启动，也可以随 UniWorks VPN Manager 系统的启动而启动，手工启动的方法是：在主菜单栏中的“告警管理”菜单项下选择“启动“菜单项，就可以启动告警服务，正常启动服务以后，会弹出一个提示框，提示操作人员服务已经启动。

7.3.3 停止

要停止告警服务，可以在主菜单栏中的“告警管理”菜单项下选择“停止”菜单项，告警服务正常停止，会出现一个对话框，提示告警服务已关闭。

7.3.4 保存全部告警

如果用户选择告警信息在界面上显示，那么时间长了，告警信息列表中可能积累很多的告警信息，这时候，可以利用保存功能保存数据。

在主菜单栏中的“告警管理”菜单项下选择“保存全部告警”菜单项，将允许操作员选择要保存的文件名，保存告警信息。

7.3.5 保存选定的告警

用户不但可以保存全部的告警信息，也可以保存特定的告警信息。要保存特定的告警信息，操作员需要选定告警列表中的某些告警，就可以保存数据了。

在主菜单栏中的“告警管理”菜单项下选择“保存选定的告警”菜单项，将允许操作员选择要保存的文件名，保存选定的告警信息。

7.3.6 删除全部告警

当告警列表中的告警数据太多的时候，可以删除告警数据。

在主菜单栏中“告警管理”菜单项下选择“删除全部告警”菜单项，将允许操作员删除告警列表中的所有告警信息。

7.3.7 删除选定的告警

不但可以删除全部的告警数据，系统也支持删除指定的告警信息。

在主菜单栏中“告警管理”菜单项下选择“删除选定的告警”菜单项，将允许操作员删除告警列表中用户选定的告警信息。


注意

注意启动告警服务以前，应该设定告警参数，特别是要绑定的 IP 地址和端口，否则，服务不能启动。如果没有特定要求，IP 地址可以设为 0.0.0.0，端口一般为 162。

8 日志管理

8.1 概述

日志管理主要是对系统中的各个事件作日志记录。当系统发生某一个故障的时候，可以借助日志管理系统来定位哪个设备和哪个操作人员进行的操作，对故障的排除提供依据。

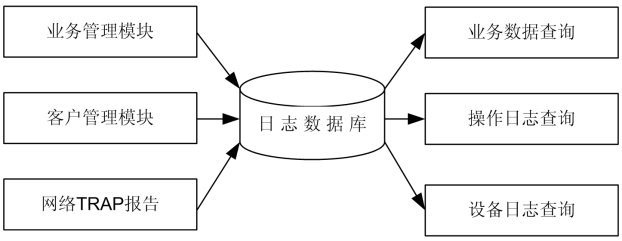
日志管理主要包括操作日志、业务日志和设备日志管理功能，其中：

- 操作日志主要是提供对操作人员操作的查询，比如新建客户、新建操作员等管理信息；
- 业务日志主要是对 VPN 业务的支持，如添加新的 VPN 业务，增加、修改 VRF 和 CERC 信息等业务相关的数据；
- 设备日志是指设备的 Trap 记录，如对设备某个接口的 UP/DOWN 的变化作记录，以便了解设备的运行状况。

UniWorks VPN Manager 系统的 V1.00 版本支持对 TRAP 告警的支持。操作日志和业务日志都在操作人员在操作过程中产生的，设备日志主要是接收到的设备告警信息，自动添加到设备日志中的。

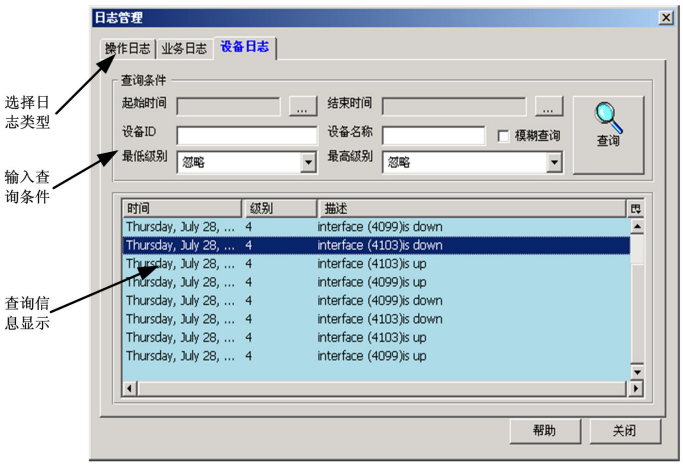
日志管理的结构及工作原理如下图所示：

图8-1 日志管理的结构及工作原理



要对系统进行查询，请选择系统菜单项下的日志管理系统，弹出日志管理窗口，如下图所示：

图8-2 日志管理



输入查询条件，然后，单击“查询”按钮就可以在日志管理窗口的下半部分看到符合查询条件的相关信息了。

8.2 操作日志管理

操作日志管理主要是提供对操作人员操作的查询。查询条件包括：

- 起始/结束时间：按照日志产生的时间，可以选择起始和结束时间；
- 操作员 ID：按照操作员 ID，查询特定操作员的操作日志；
- 操作员名称：按照操作员名称，查询特定操作员的操作日志；
- 模糊查询：输入操作员的关键词，可以搜索出相关操作员的工作日志；
- 最低/最高级别：按照操作员执行操作的重要程度，进行查询。各种不同的操作从特别严重到一些基本的记录信息被赋予于了不同的值，分为以下几挡：忽略、调试信息、一般信息、提示信息、一般告警、告警、错误、一般警告、警告和紧急警告。这些从低到高表示了操作员发生的误操作的错误程度。“提示信息”前的级别说明是操作的一般提示信息。“一般告警“和“错误”之间的信息代表可能操作可能对系统造成一定的影响。“一般警告”级别以上的信息代表操作可能会危及到系统或者业务的正常运行。

如果某一项没有选择或填写，则表示查询此项的所有内容；如果所有查询条件都不选择或填写，则表示查询系统的所有内容。

8.3 业务日志管理

业务日志主要是记录业务的关键日志，如创建、删除和修改 CERC、VRF、VPN 等信息。业务日志管理主要是提供对业务日志的查询。查询条件包括：

- 起始/结束时间：按照日志产生的时间，可以选择起始和结束时间；
- 业务 ID：按照业务 ID，查询特定业务的日志；
- 业务名称：按照业务名称，查询特定业务的日志；
- 模糊查询：输入某些业务的关键词，搜索出相关的日志信息；
- 最低/最高级别：按照业务重要程度，进行查询。各种不同的业务从记录信息到特别重要被赋予于了不同的值，分为以下几挡：忽略、调试信息、一般信息、提示信息、一般告警、告警、错误、一般警告、警告和紧急警告。这些从低到高表示了业务的关键程度。“提示信息”前的级别说明是一般的业务提示信息。“一般告警“和“错误”之间的信息代表可能对系统造成一定影响的业务数据更改。“一般警告”级别以上的信息，代表操作可能涉及到某个系统或者 VPN 业务的正常运行。

如果某一项没有选择或填写，则表示查询此项的所有内容；如果所有查询条件都不选择或填写，则表示查询系统的所有内容。

8.4 设备日志管理

设备日志主要是记录设备的告警信息。目前，UniWorks VPN Manager 系统的 V1.00 版本保存设备的 Trap 信息。设备日志管理主要是提供对设备告警信息的查询，查询条件包括：

- 起始/结束时间：按照日志产生的时间，可以选择起始和结束时间；
- 设备 ID：按照设备 ID，查询特定设备的告警信息；
- 设备名称：按照设备名称，查询特定设备的告警信息；
- 模糊查询：输入某些设备的关键词，可以搜索出相关设备的告警信息；
- 最低/最高级别：按照告警的重要程度，进行查询。各种不同的告警信息被赋予

于了不同的值，分为以下几挡：忽略，调试信息，一般信息，提示信息，一般告警，告警，错误，一般警告，警告，紧急警告。从低到高表示了告警的严重程度。一般来说，“提示信息“以前的信息都是系统的提示信息，代表着设备可能的错误提示，一般不需要人工处理。“一般告警“和“错误”之间的信息，代表着设备出现了问题，需要关注。“一般警告”级别以上的信息，代表着设备出现了严重的故障，需要工作人员及时的处理。


提示

如果某一项没有选择或填写，则表示查询此项的所有内容；如果所有查询条件都不选择或填写，则表示查询系统的所有内容。


注意

UniWorks VPN Manager 系统主要提供告警信息的查询功能，没有提供对告警数据库的维护。有关维护的工作可参照相关数据库的使用说明。