WINAPN 移动客户端

使用说明书

Powered by APN GW Architecture

WINAPN

Installation & Configuration Guide

For APN GW 200/200A/2000/2500/5000 Series

【Text Part Number: T05-10-11-G12】

Document Status: Approved

Data: 11/Oct/2005

Documentation also available on CD-ROM and the Website

声　明

本公司对本手册的内容保留在不通知用户的情况下更改的权利。未经本公司书面许可，本手册的任何部分不得以任何形式手段复制或传播。

NOTICES

We reserves the right to make any changes in specifications and other information contained in this publication without prior notice and without obligation to notify any person or entity of such revisions or changes.

目 录

关于本手册

概述

本手册适用与 APN GW 系列产品的工程师、用户。本手册主要描述了在安装、使用、调试 APNGW 软件客户端的使用说明。

WINAPN 支持 PSK 和证书版本。PSK 是通过用户名、密码来验证的一种方式，证书版本是通过证书来实现验证和管理的，选择的时候可以参考以下原则：

硬件支持：APNGW 所有系列。

软件	特点	选择原则
PSK 版本	使用简单、APNGW 端设置也相对简单	■ 如果并发用户（即同时使用软件客户端接入 APNGW 的用户）较少，而要求使用方便快捷，推荐使用 PSK 模式； ■ 如果并发用户较多而且对安全性要求较高，可选择证书方式； ■ 证书模式分文件证书和 USB 证书，USB 证书成本较高，但是证书存储在 USBKEY 里面可随身携带，相对安全较高。
文件证书版本	使用、配置较复杂，但是稳定性和安全性比 PSK 版本优越。	
PSK 证书版本		
证书管理程序	使用证书版本，需要借助第三方可信赖的 CA 中心颁发证书。如无可信赖 CA 中心，本证书管理程序可协助用户自建一个小型 CA，同时也可以对其他 CA 颁发的证书进行管理导入 USBkey 等操作。	

阅读指南

如果您使用 PSK 版本，请阅读第一章即可。

证书版本使用过程中，每个公司应设立一个统一的证书管理员。

- 如果您使用证书版本， 您可直接阅读第二章。并根据您选择的证书版本的型号（USB 证书或文件证书），可选读相应的章节。
- 如果您是证书管理员，您需要阅读第二章和第三章，便于对所颁发的证书进行统一的维护和管理。

第一章 PSK 客户使用说明

本章描述了 PSK 客户端的使用说明。适合于使用 PSK 版本的 WINAPN 用户和 APN 设备管理员。

一．系统需求

操作系统：Windows 2000/Windows XP/Windows 2003

系统配置：CD-ROM（用于安装程序）

APN 版本号：20050930 及以上版本

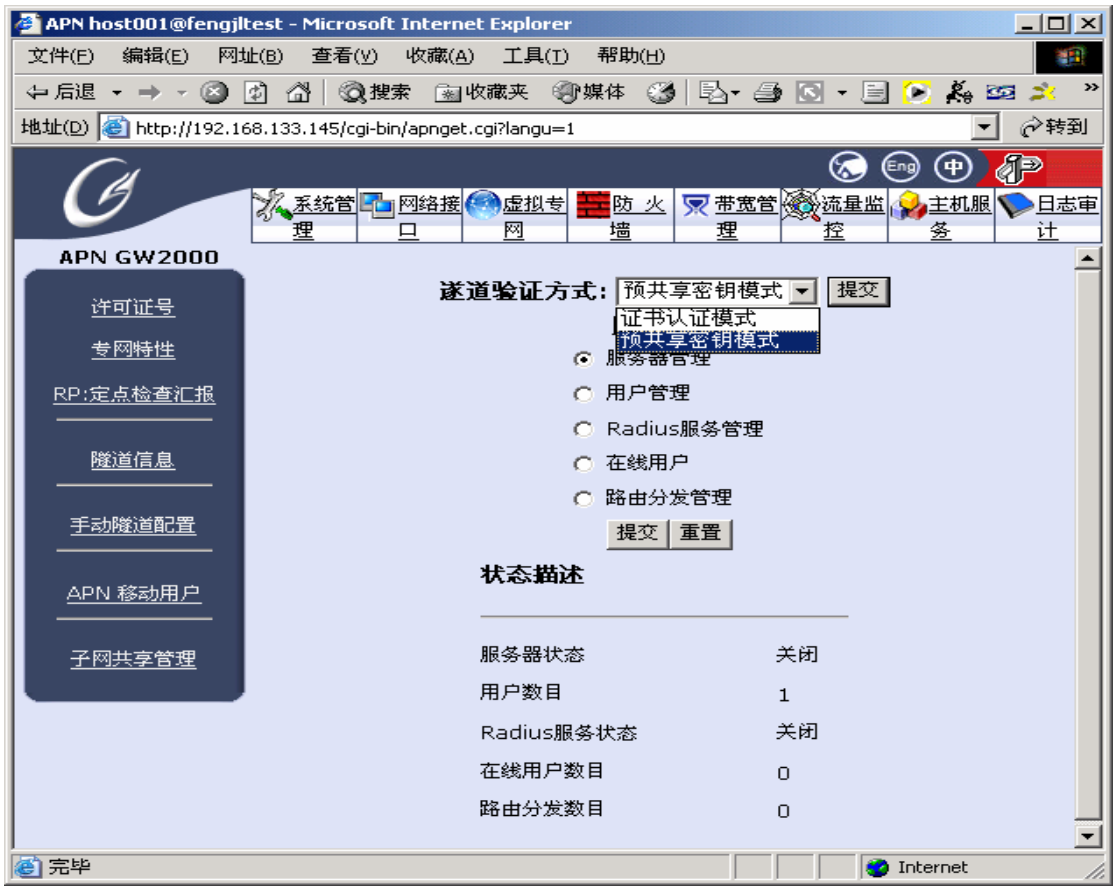
WINAPN 版本号：2.0

二．APNGW 设备服务器端配置

1．选用“预共享密钥模式”

当前“APN 移动用户”支持“PSK 认证模式”和“证书认证模式”两种，必须先选用“预共享密钥模式”。

通过 IE 浏览器进入 APN 终端的 web 管理页面，进入“虚拟专网”→“APN 移动用户”，在“隧道认证方式”中，通过“编辑”功能，选用“预共享密钥模式”。如下图所示：



2．启用服务端

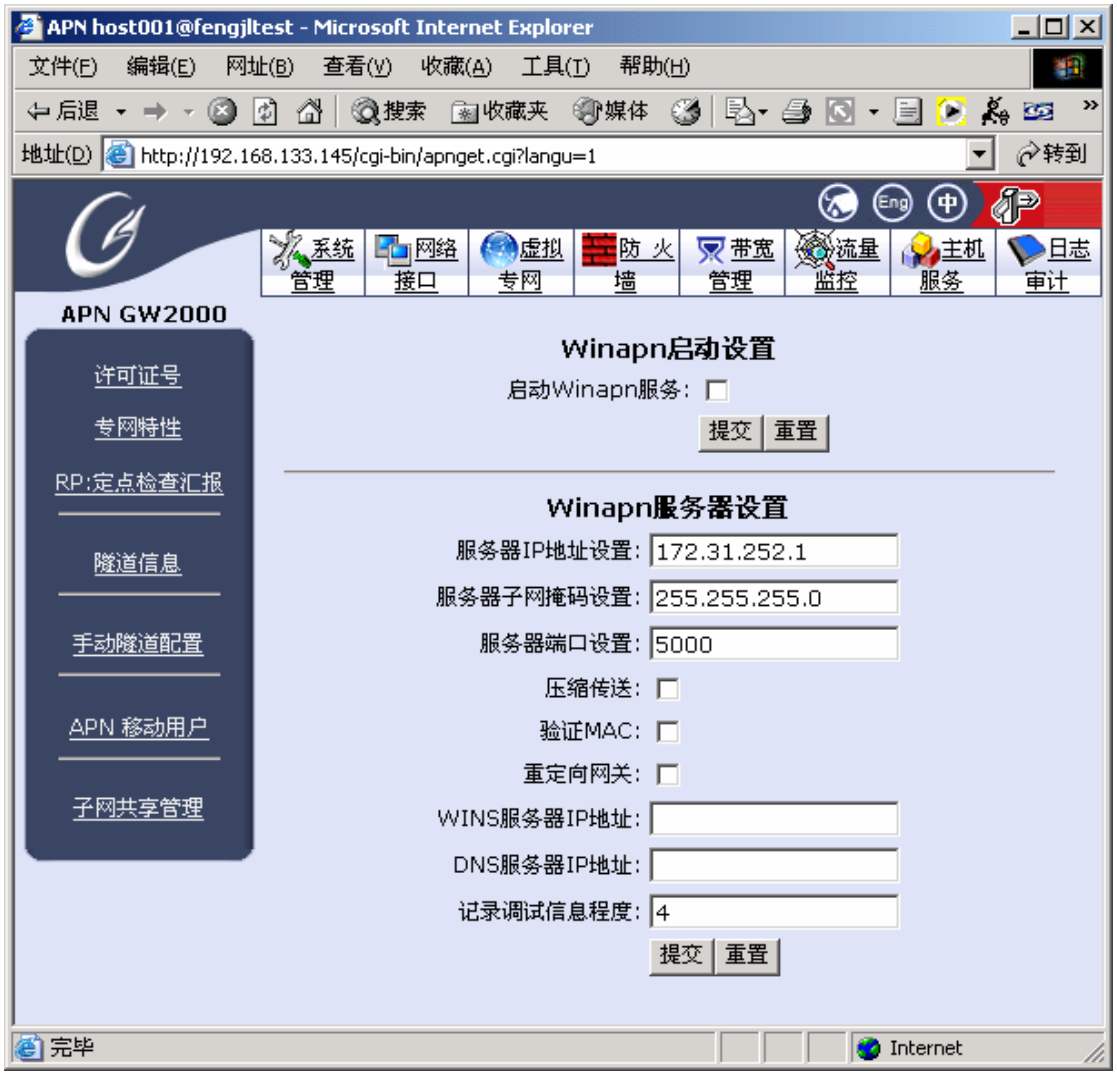
选中“服务器管理”，按“提交”按钮。进入服务端管理页面。对 winapn 服务的一些参数进行设置，详细见下：

■ WINAPN 服务器设置

服务器端设置中，需要规划一段移动用户使用的 IP 地址段，该网段将不允许被重用，否则网络将可能出现不稳定现象，缺省的是 172.31.252.0/24。 用户可以规划使用其他网段。

规划好使用的网段后，需要为设备作为服务端指定一个固定的 IP 地址，比如缺省的是 172.31.252.1/24。在 Web 页面上输入“服务器 IP 地址设置”及其“子网掩码设置”后，按下面的“提交”按钮。如下图所示。

注意：WINAPN 服务使用的地址段不能与 APN 设备的内网口地址相同，也不能与其它互连的节点内网段地址相同。



■ 是否改变“服务器端口设置”选项

该端口为 winapn 客户端接入将使用的端口，为默认为 tcp5000，允许更改为其他的 tcp 端口，比如 5001，另外 winapn 客户端接入的时候将使用到另外一个 udp8500 的端口，该端口不允许修改，即 APN 上的 udp8500 端口将长期被占用。

■ 否使用“压缩传送”选项

该选项为 winapn 客户端接入到 APN 后，之间传输的数据是否压缩的选项，在 APN 端为非 56Kmodem 拨号的情况下不推荐使用，因为进行压缩要耗用 CPU 较多的时钟。

■ 是否“验证 MAC”地址选项

此选项为是否启用对 winapn 接入进行 MAC 地址的验证，启用该选项时候必须在用户管理中针对每个用户 ID 添加相应的 MAC 地址

■ 是否启用“重定向网关”选项

该选项如果启用，则当 winapn 客户端连接上来后，该客户端的计算机的默认网关将变为以上所设置的服务器 IP 地址。

■ WINS 服务器 IP 地址和 DNS 服务器 IP 地址

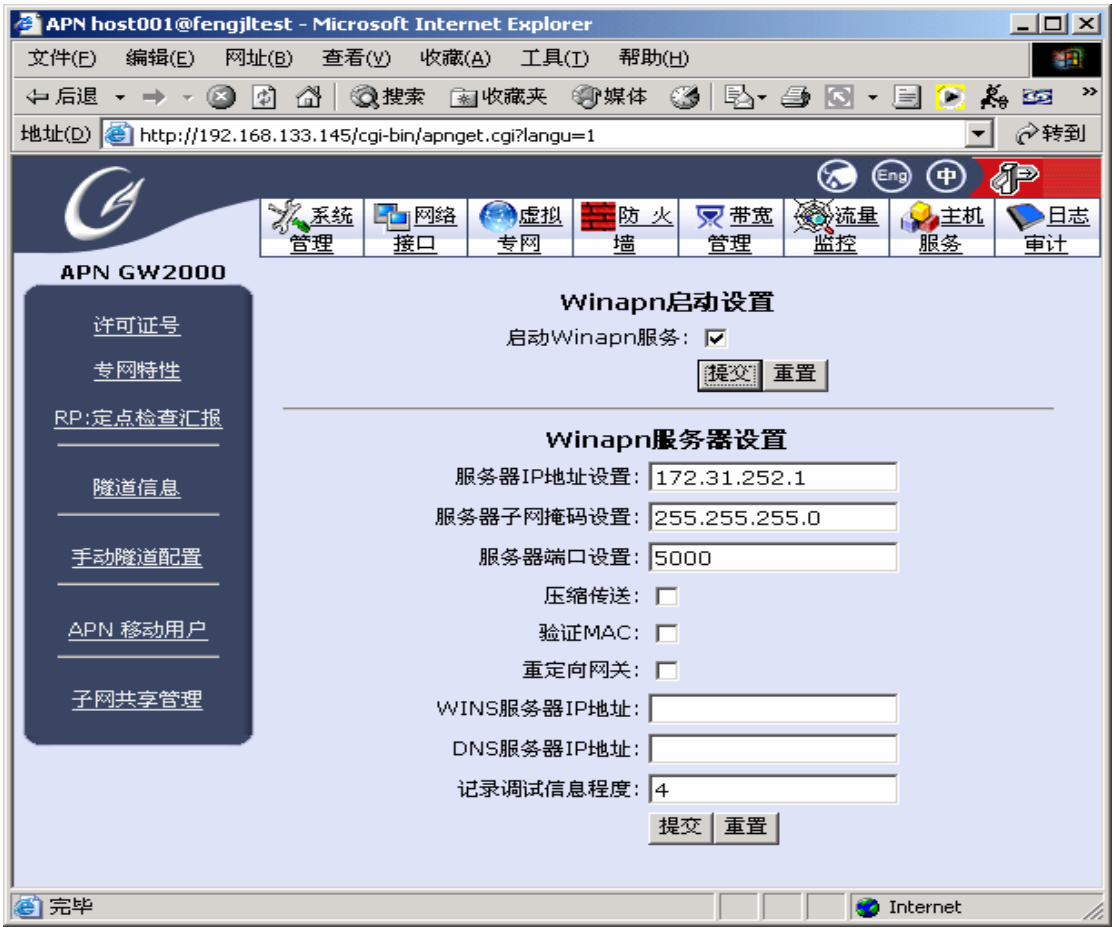
若填写了该信息，则接入的客户端的计算机的 WINS 和 DNS 的首选服务器将变为所设置的服务器 IP。

■ 记录调试信息程度

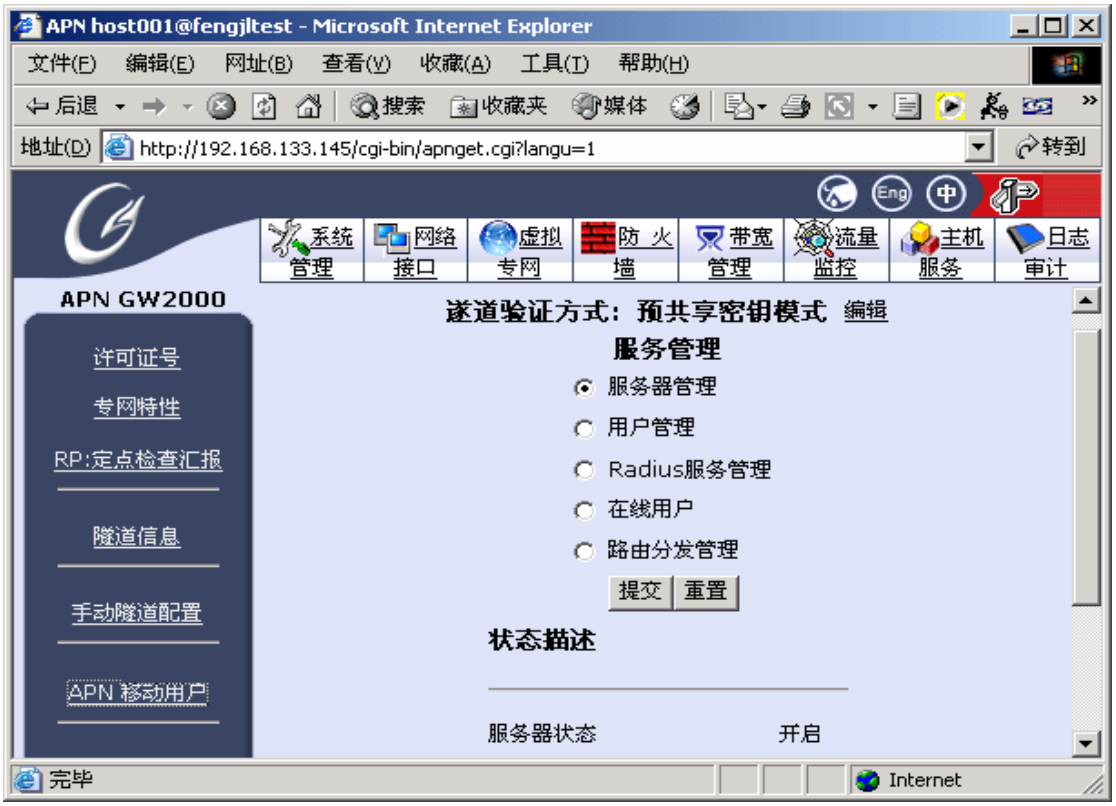
此项为 winapn 使用过程中将产生的日志信息的强度，主要用于技术人员调试使用，默认为 4，不建议客户对该值进行修改。若不希望有 winapn 的相关日志信息的输出，可设置该值为 0。

■ 启动 WINAPN 服务程序

选中“WINAPN 启动设置”下面的“启动 WINAPN 服务”，然后按“提交”按钮。



提交完成后，确认“状态描述”中的“服务器状态”是“开启”。如下图。



3．用户管理

选中“用户管理”，按“提交”按钮。进入用户管理页面。

■ 检查授权数目

不同型号的设备标配的移动用户支持数目是不一样的。进入“用户管理”后，可检查授权数目。在末行一般显示“最大注册人数为: [x]” ，这代表你可以在这里增加 x 个用户账号，“最大在线人数为: [X]” ，表示 APN 当前支持的同时在线的人数为 X。

■ 增加新的用户账号

点击“添加”，然后输入用户名，口令和 IP 地址信息。

- 用户名：客户端接入时认证的账号，可使用字母和数字的任意组合，最长为 32 个字符；
- 口令：客户端接入时认证的账号，可使用字母和数字的任意组合，最长为 32 个字符；
- IP 地址：指定给客户端接入后所获得的虚拟 IP 地址，需要跟服务端设置的 IP 地址在一个网段内。
- MAC：指定移动用户计算机的 MAC 地址，对移动用户名和 MAC 地址的一种绑定。

如下图所示。

■ Radius 服务管理

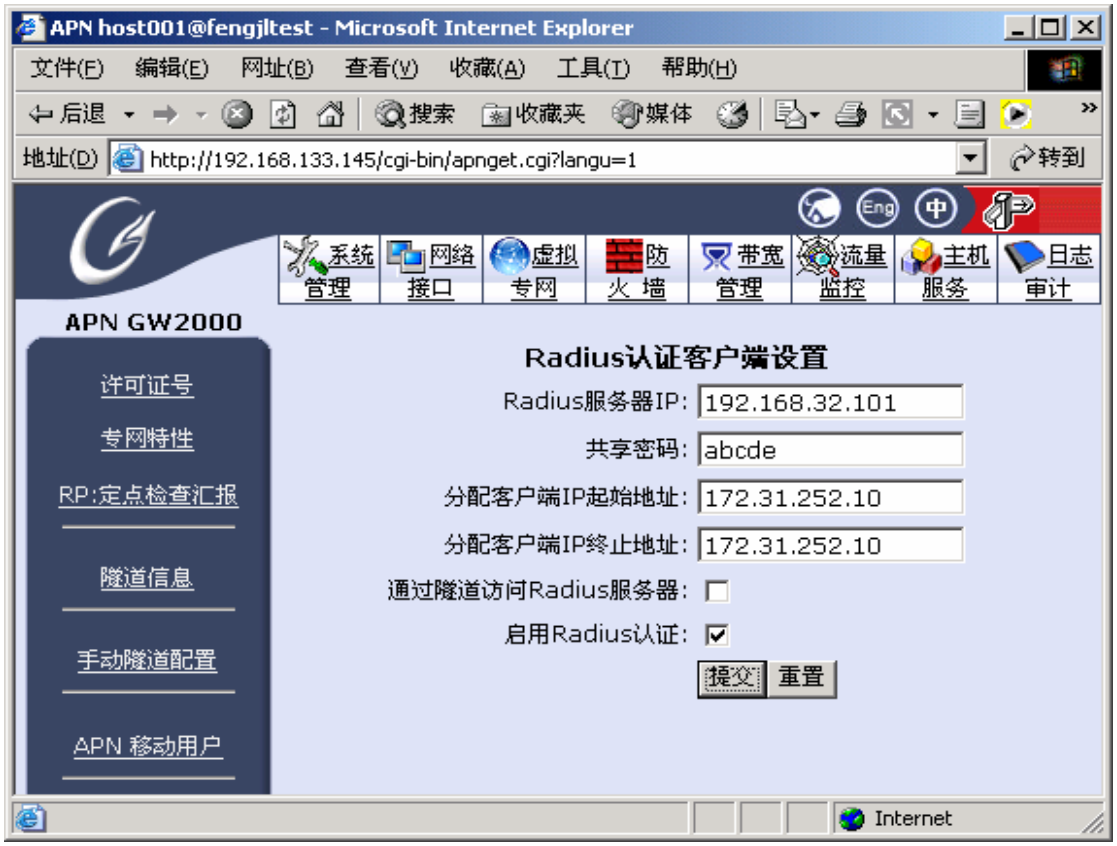
winapn 支持第三方的 Radius 认证方式，该选项为配置 Radius 服务器的一些参数，选中“Radius 服务管理”，按“提交”按钮。进入 Radius 服务管理页面。

■ 配置及启用 Radius 认证支持

当用户具有自己的 Radius 服务器时，可以使用 APN GW 设备的 Radius 客户端连接此服务器，使用其提供的认证服务。

配置：

- Radius 服务器 IP：指定 APN GW 设备可以访问的 Radius 服务器的 IP 地址。此服务器可以在本地、Internet 或者隧道对端网络内；
- 共享密码：Radius 客户端访问服务端使用的密码；
- 分配客户端 IP 起始地址：指定 WINAPN 客户端认证后 APN GW 分配给它的 IP 地址段的开始 IP，必须跟 WINAPN 服务端配置的 IP 地址在一个网段内；
- 分配客户端 IP 终止地址：指定 WINAPN 客户端认证后 APN GW 分配给它的 IP 地址段的结束 IP，必须跟 WINAPN 服务端配置的 IP 地址在一个网段内；
- 通过隧道访问 Radius 服务器：如果 Radius 服务器处于隧道对端的网络内，请选中此项；
- 启用 Radius 认证：启用 Radius 客户端连接 Radius 服务端。

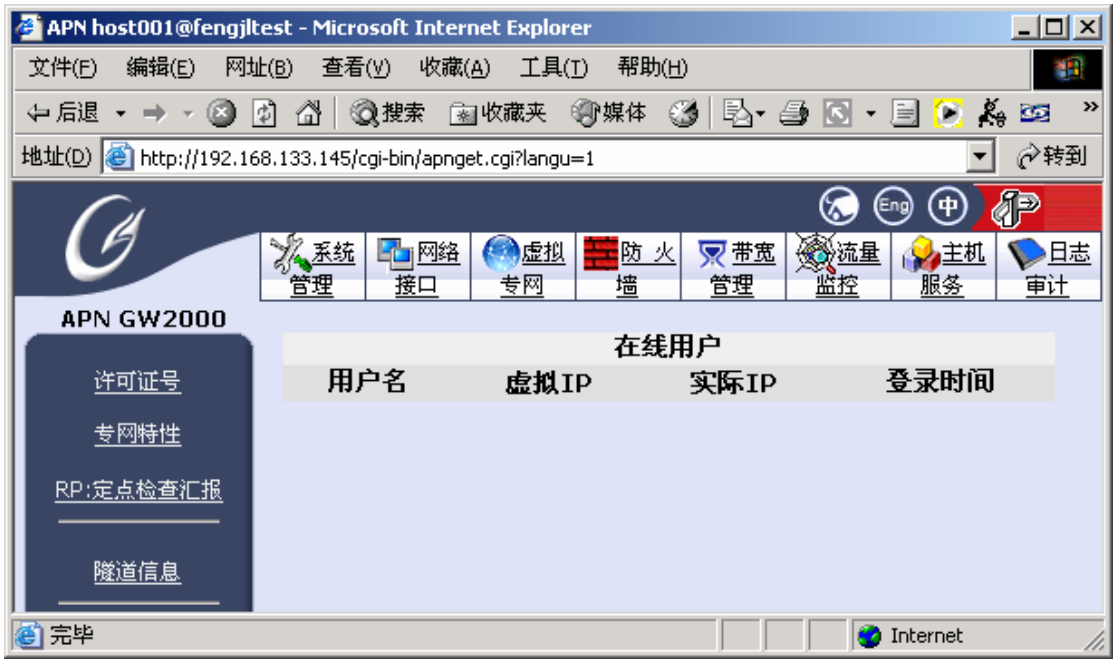


■ 在线用户

将显示当前在线的用户信息，注：当 winapn 客户端为异常下线的时候，该异常用户的在线信息将会 30 秒后被刷新。

选中“在线用户”，按“提交”按钮。进入在线用户查看页面。

如下图所示。在线用户页面显示已经登陆的用户名，有 APN GW 服务端指定的虚 IP 地址，客户端计算机的实际 IP 地址和连接时间等信息。



■ 路由分发管理

这里分发的路由信息就是让移动用户客户端能获取相关的路由信息。详细使用方法参看后面的常见问题。

■ 状态描述

1.服务器状态：查看服务器程序是否为启动状态

2.用户数目:当前已经设置好的用户数目

3.Radius 服务状态:查看当前是否启用了 Radius 服务器的认证方式

4.在线用户数目：查看当前在线用户的个数

5.路由分发数目:查看已经配置的路由分发条目

三．客户端安装

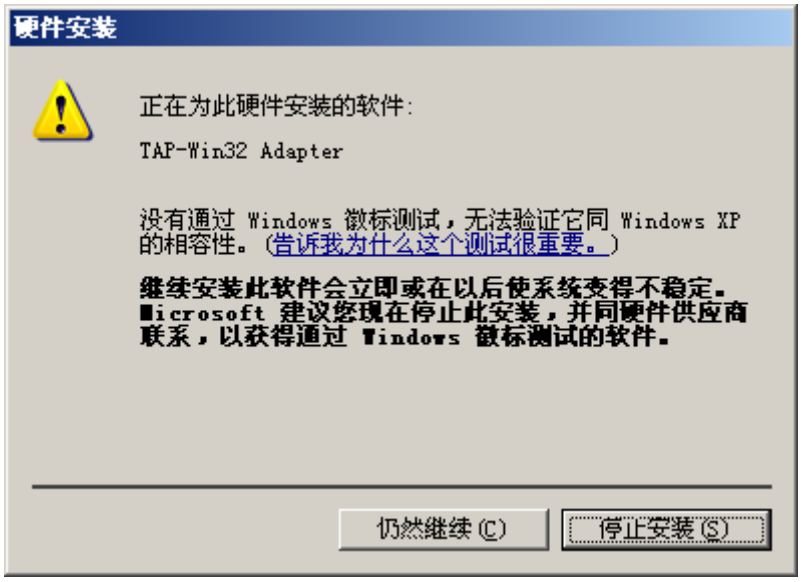
将附件中所带的光盘插入光驱，打开光盘中的客户端软件的安装目录，运行该目录中的 setup.exe 文件，根据安装向导提示进行，直到将此程序正确安装到你的电脑上。

如果从互联网或者其他方式得到此客户端安装包，请解压后运行目录中的 setup.exe。

重点注意事项：

安装过程中，当提示输入序列号时，请查看附件中的光盘或请向奥联科技工程师咨询。

安装过程中，当提示安装“TAP-Win32 Adapter”虚拟网卡时，请按“仍然继续”。如下图所示（WIN XP）。



安装完成后，请确认计算机的“网络连接”中，增加了一个“TAP-Win32 Adapter”的“本地连接”。如果没有，请重新安装，并且注意在提示安装虚拟网卡时一定要选择“仍然继续”。

四．PSK 客户端使用

1．运行客户端

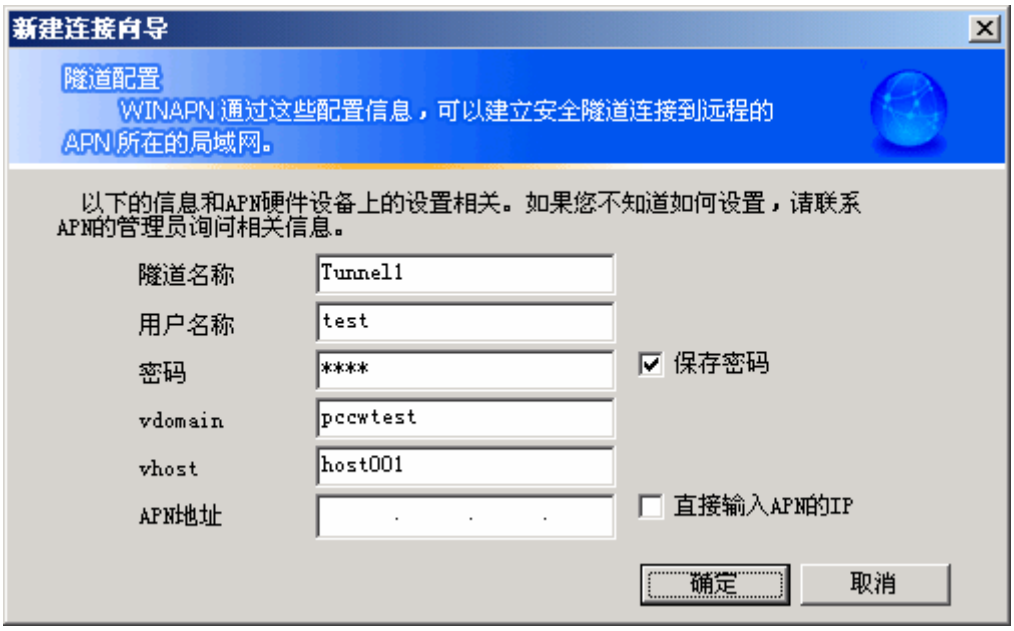
点击“开始”→“程序”→“APN”→“WINAPN”，开始运行 WINAPN 客户端。如下图所示。

2．设置

点击“系统”按钮，进入设置窗口。如下图所示。

■ 2.1 新建一个隧道

点击“隧道”按钮，点击下面的“新建”按钮，进入新建隧道窗口。如下图所示。



“隧道名称” 可以根据需要设置便于管理的字符串，比如以 APN GW 设备终端放置的地方的汉语拼音命名。

“用户名称” APN GW 设备上设置的用户名。

“密码” APN GW 设备上设置的用户名称相对应的密码。

“Vdomain” 要连接的 APN GW 设备终端的组域号。

“Vhost” 要连接的 APN GW 设备终端的节点名。

“APN 地址”和“直接输入 APN 的 IP” 选项表示如果知道了 APN 的公网 IP 地址，可以直接进行连接，不需要填写 VDOMAIN 和 VHOST 信息。

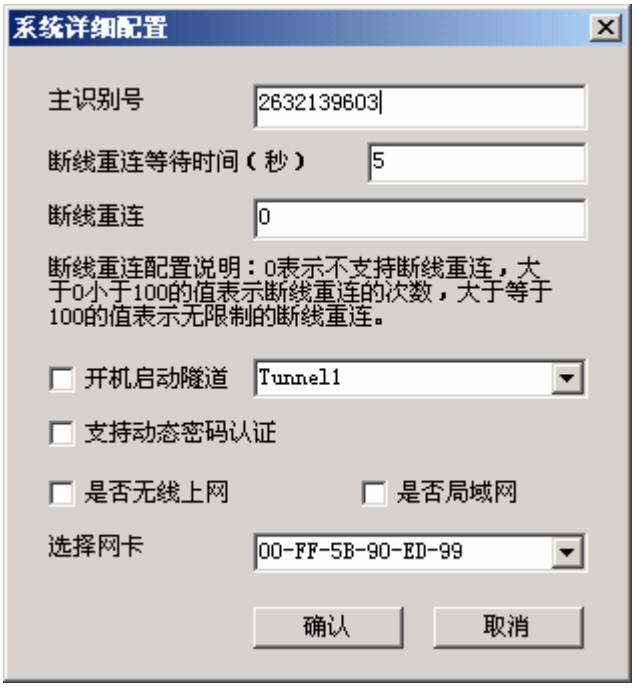
注意：

可以新建多个隧道信息。

■ 2.2 配置

点击“系统”按钮，设备配置中显示了当前 WINAPN 系统中的默认配置，第一行主识别号缺省为“2362139603”，此缺省识别号为厂家 VDN 服务器的识别号。

需要修改这里面的参数请点击下面的“配置”按钮，如下图所示。



“主识别号” 这里要和 APN 上的主识别号要一致。缺省为“2362139603”，此缺省识别号为厂家 VDN 服务器的识别号。

“断线重连等待时间”当网络断开或者其他原因导致客户端没法连接远端设备的时候，客户端自动去连接远端设备的等待时间，默认为 5 S，此参数可以修改，但如果没有特殊情况不建议修改。

“断线重连” 0 表示不支持断线重连，大于 0 小于 1 0 0 表示断线后重连的最大次数，大于或者等于 1 0 0 表示无限制的重连，直道隧道建立起来为止。

“开机启动隧道”一个客户端可导入多条隧道的信息，在这里可以选择计算机开机时是否自动启动客户端软件连接远端设备，以及自动连接哪一条ＶＰＮ隧道。

“运行动态密码认证”该选项只有当 apn 端启用 radius 服务器的时候有效，关于该功能请查阅第三方的 radius 服务器的详细资料。

“是否无线上网”根据当前计算机是否为无线上网方式进行选择。

“是否局域网”此选项只有当 APN 端启用网关重定向，且 APN 的公网口和客户端计算机属于同一个网段的时候有效。

“选择网卡”该选项只有当 APN 端启用了验证 MAC 地址的功能时候生效，启用该功能的时候，在 APN 上绑定的 MAC 地址必须和当前选择的 MAC 地址一致才能够连接成功。

注意：

如果客户的终端设备的许可证是由厂家分发的，此主识别号不需要修改。如果客户的终端设备的许可证是有自有的 VDN 服务模块（GW5000）或者运营商的运营 VDN 平台分发的，需要修改为相对应的主识别号。

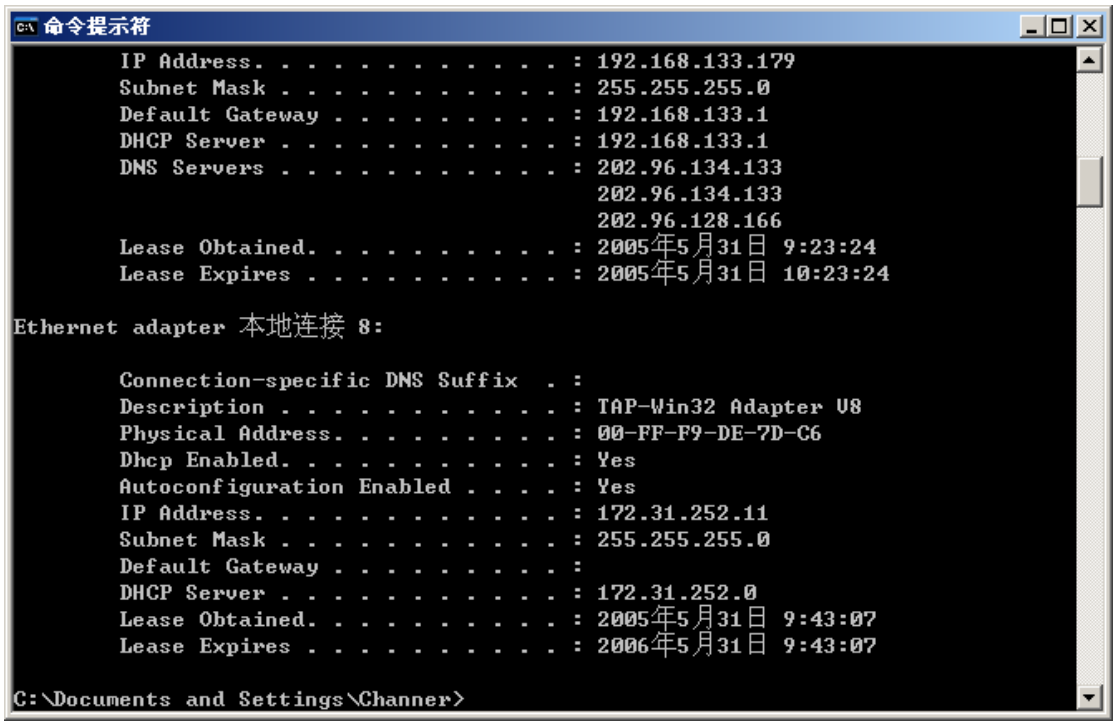
3．连接 APNGW

在“选择隧道”的右边下拉菜单中选择需要连接的隧道标识，然后点“连接”按钮。

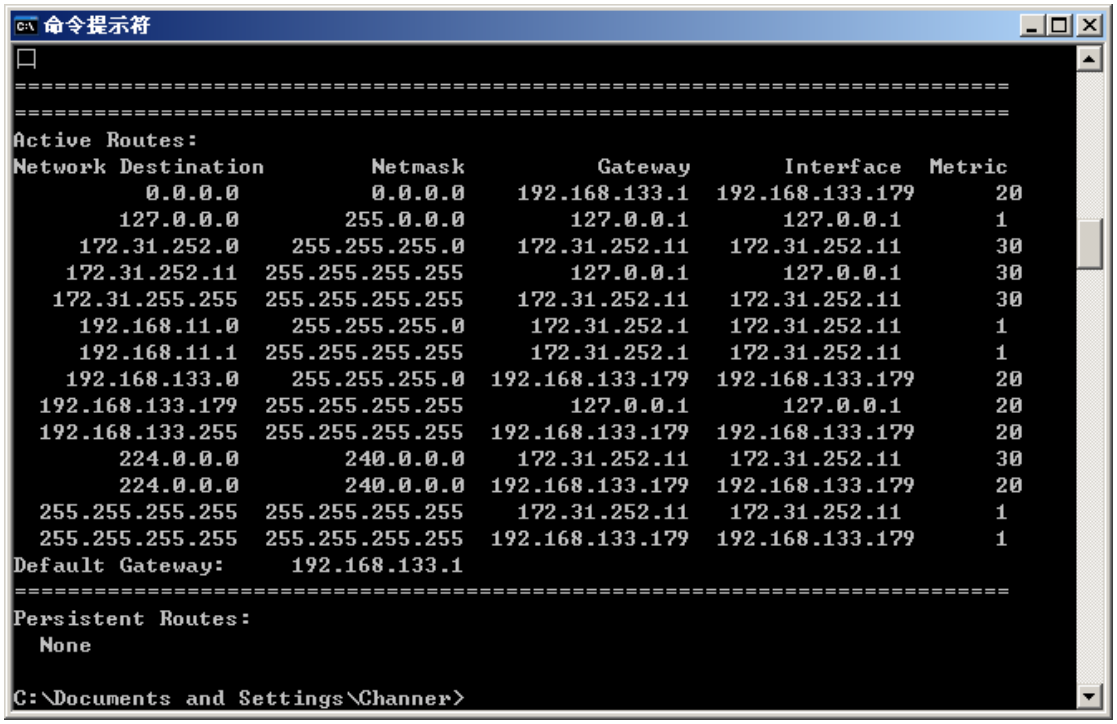
接着开始了连接服务端的过程，如果没有故障的话，可以正常连接到服务端。

4． 连接成功后的检查

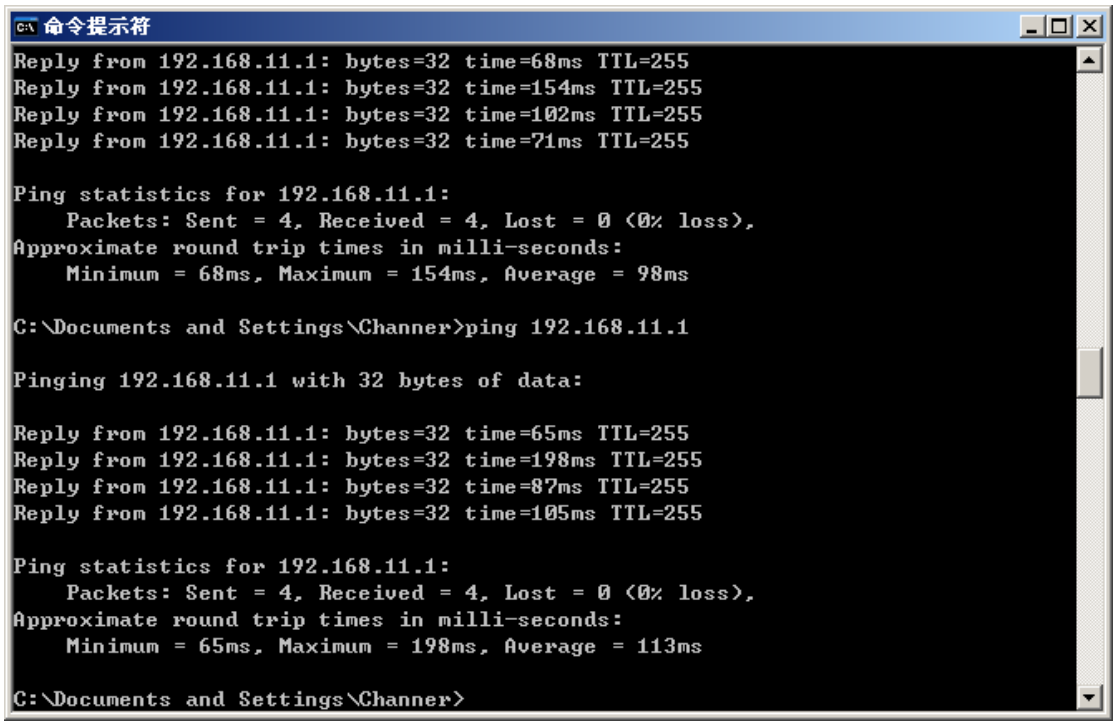
使用 ipconfig 命令查看本地获得的虚拟网口 IP。这个 IP 是 APN GW 上服务端设置的用户管理中跟用户名相对应的 IP 地址。



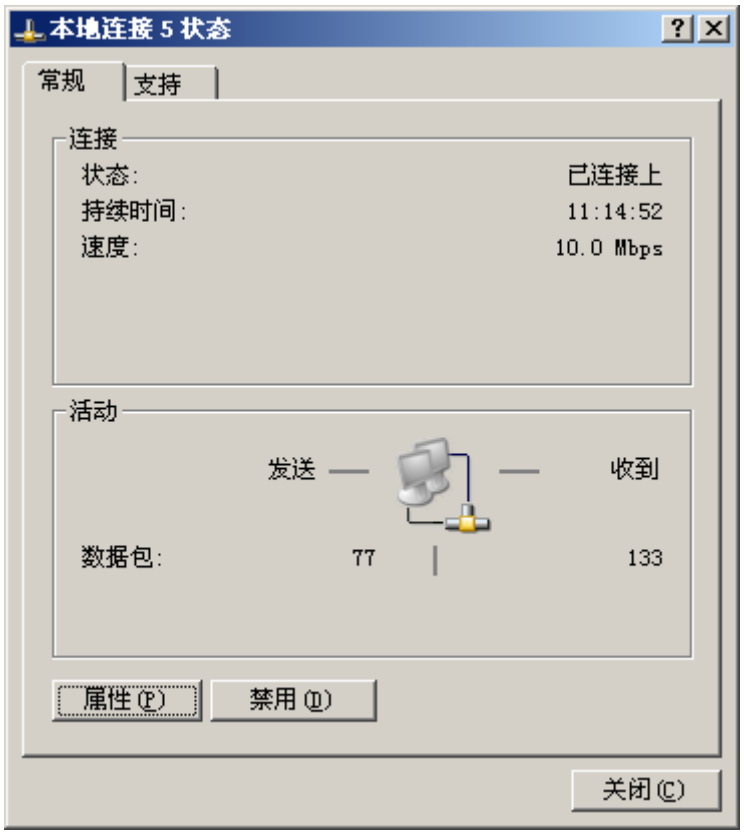
使用 route print 命令查看本地计算机增加的到 APN 内部的静态路由。



使用 ping 命令检查是否跟 APN 内部局域网联通；



检查虚拟网络连接的状态；



5. 查看日志

当连接失败时，可以查看登陆过程的日志，以判断失败原因。当需要向厂家工程师报障时，可向对方提供出错的日志信息。

点击“设置”按钮，进入设置窗口后，点击“日志”按钮。如下图。

在接着弹出的日志信息窗口中，滚动到文件的最后，就可以查看最新的日志信息。

6．常见问题

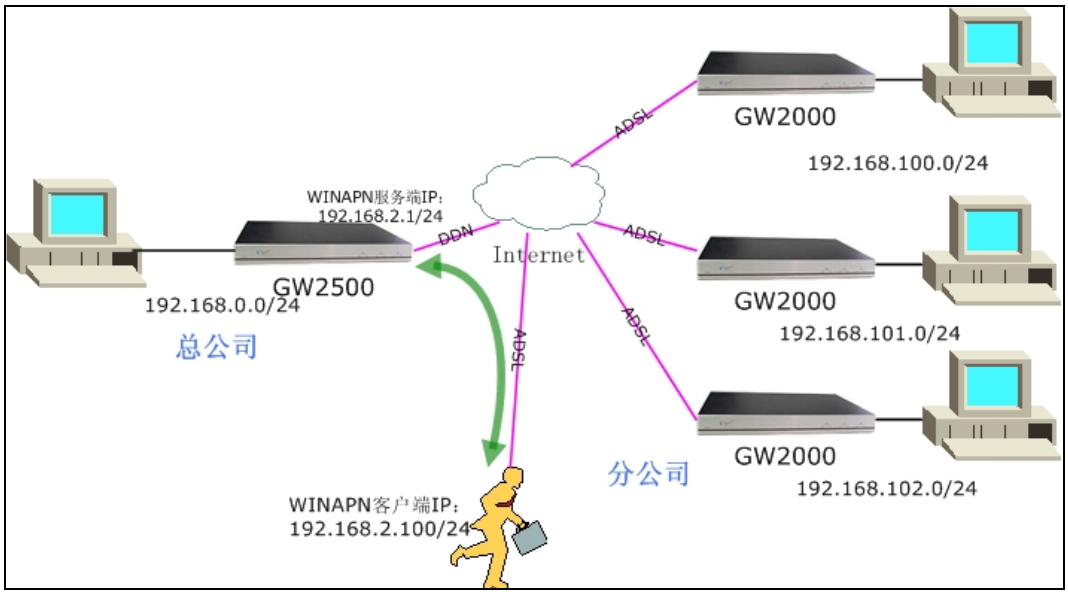
1．我的 APN web 管理界面上根本没有“APN 移动客户端”这一项，我怎么使用 WINAPN 软件客户端？
答：你需要升级你的 APN OS 到 V3.2 buildno 20050517 或以后的版本。

2．在 winapn 服务器端设置中，我可以使用跟内网接口相同的网段吗？
答：你不能使用跟内网接口相同的网段，如内网口网段为：192.168.0.0/24，你在 winapn 服务器端设置中，不能使用 192.168.0.0/24 的网段；
　　你可以使用跟内网口网段完全不同的网段，如：192.168.1.0/24；

3．我可以在防火墙上控制客户端对内网的访问权限吗？
答：可以。
　　你需要启用 APN 设备的 FW3.0 版本防火墙。客户端的 IP 处于[WANIP]区域内。

4．我可以通过客户端登陆到总部的 APN 设备，然后访问所有的节点吗？
答：可以。下面举例说明：

网络拓扑



注：
总公司使用网段 192.168.0.0/24
分公司使用网段 192.168.100-200/24
总部的 WINAPN 服务端使用网段 192.168.2.0/24，需要注意的是，如果需要登陆到总部 APN 的移动用户同时可以访问分公司，建立的隧道必须是包含 WINAPN 客户端使用的地址端，为了便于在总部的 APN 上设置扩大隧道掩码的设置，我们一般设置 WINAPN 服务端使用的 IP 地址段为 APN LAN 本身使用网段相邻的网段；
4.2 APN 端设置

WINAPN 服务端设置，IP 地址为：192.168.2.1，子网掩码为 255.255.255.0。

选中“路由分发”，按“提交”按钮。进入路由分发配置页面。添加一条路由分发，目的网络为 192.168.0.0，子网掩码为 255.255.0.0，此处设置应该包含分公司的所有网段，目的是让客户端登陆成功后，自动的增加通过隧道访问分公司的路由。

在“虚拟专网”→“专网特性”中，选中“扩大子网”，本端地址不需要修改，本端子网掩码修改为 255.255.252.0，修改后的子网掩码应该包含 APN 本身 LAN 使用的网段和 WINAPN 使用的网段，选中“现在激活”，按“提交”按钮；

5．winapn 客户端对操作系统有什么要求？

答：要求操作系统为 win2000/xp/2003 ，目前的版本不支持 98/nt/me。

6．连接 APN 时，出现“There are no TAP-Win32 adapters on this system”的日志提示，并且弹出“Tunnel Engine Close”的警告窗口，这为什么？

答：请检查计算机是否有“TAP-Win32 Adapter”的本地连接。如果没有，请重新运行安装程序，选择“remove”，完成后，再次运行安装程序。

7．我的客户端已经成功连接 APN 设备，并且我能 ping 通 APN 设备的 LAN 口地址，但不能 ping 通 APN 局域网内的计算机，这是为什么？怎么解决？

答：这主要是局域网的计算机没有到达 WINAPN 使用 IP 地址段的路由。

解决办法：

检查内部网络路由设置，把目的网段是 WINAPN 使用的 IP 地址段的路由指向 APN 设备的内网口。

五．在线升级

奥联公司的研发人员对产品的功能一直在不断完善和增加，通过在线升级功能，你可以非常方便的连接到我们公司的升级服务器，对软件客户端进行升级。

点击“在线升级”按钮，点击“登陆设置”下面的“在线升级”按钮，进入在线升级窗口。如下图所示。

点击“在线升级”按钮可以进行对软件的升级。如下图，点击下一步进行对升级的查询。

连接到服务器查询后可知软件是否需要更新，如下所示：

从上图中可以看出通过对升级服务器的查询发现有新的软件版本，点击更新，以后的升级过程则无需进行人工进行操作即可完成。

第二章 证书版客户使用说明

本章主要描述了证书版本的客户端使用方法，适合于使用证书版本的 apn 移动客户端用户。

一、系统需求

操作系统：Windows 2000/Windows XP/Windows 2003

系统配置：CD-ROM（用于安装程序）

二．客户端软件安装

将附件中所带的光盘插入光驱，打开光盘中的客户端软件的安装目录，运行该目录中的 setup.exe 文件，根据安装向导提示进行，直到将此程序正确安装到你的电脑上。

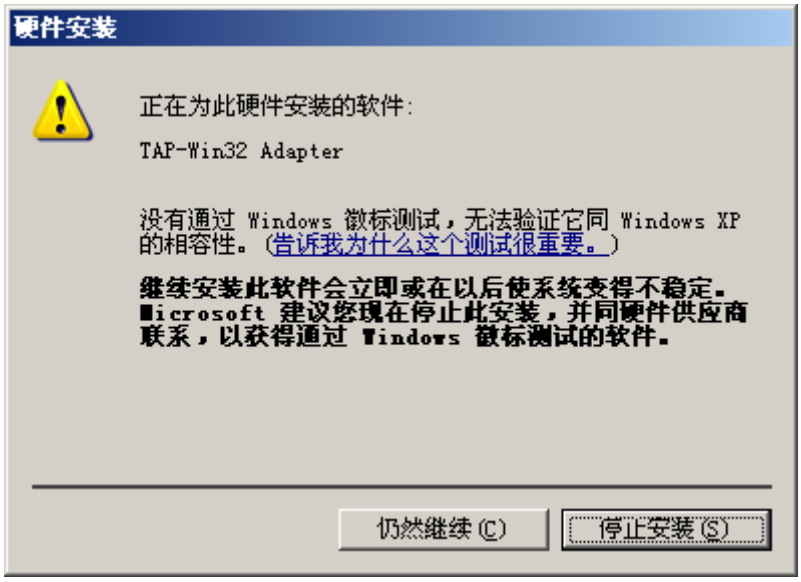
如果从互联网或者其他方式得到此客户端安装包，请解压后运行目录中的 setup.exe。

重点注意事项：

最新发布的客户端软件版本，是一个完整的客户端软件，里面包括了 PSK 模式、文件证书模式、USB KEY 证书模式的，同时包括了证书管理软件，安装过程中可以有选择的安装。选择安装哪一种，是按照在安装过程中输入的序列号来区分的，如下图所示：

其中的序列号见光盘上的标签，或者可以咨询奥联技术支持工程师。

安装过程中，当提示安装“TAP-Win32 Adapter”虚拟网卡时，请按“仍然继续”。如下图所示（WIN XP）。



安装完成后，请确认计算机的“网络连接”中，增加了一个“TAP-Win32 Adapter”的“本地连接”。如果没有，请重新安装，并且注意在提示安装虚拟网卡时一定要选择“仍然继续”。

三．文件证书客户端使用

1．运行客户端

点击“开始”→“程序”→“WINAPN”）开始运行文件证书 WINAPN 客户端。如下图所示。

2．设置客户端

点击“系统”按钮，进入设置窗口。如下图所示。

2.1 证书

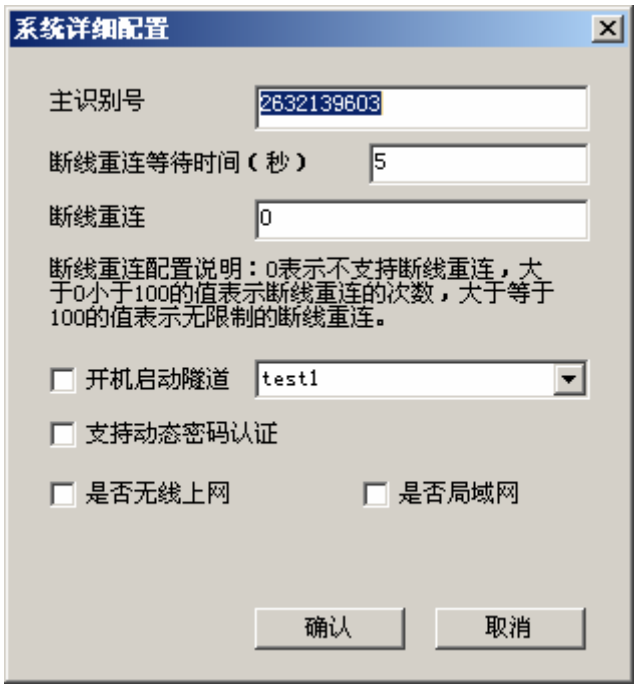
重要：在证书配置时，需要将证书管理软件所分发的或者第三方证书机构分发的用户软件端的证书保存在本地计算机。

点击“证书”按钮，点击“查找文件”按钮，选择用户软件端的证书，按“确定”按钮。在“证书口令”空格中输入生成用户软件端证书时的私钥保护口令，然后按右边“提交”按钮。如下图所示。

2.2 配置

在系统主窗口中选择配置选项，能看到一些相关的配置信息，如下图所示：

点击配置按钮可以进行相关信息的重新配置，如下图所示：



主识别号：APNGW 终端设备上设置的 VDN 服务器的识别号。缺省为“2362139603”，此缺省识别号为厂家 VDN 服务器的识别号。

注意：

如果客户的终端设备的许可证是由厂家分发的，此主识别号不需要修改。如果客户的终端设备的许可证是有自有的 VDN 服务模块（GW5000）或者运营商的运营 VDN 平台分发的，需要修改为相对应的主识别号。

断线重连等待时间：当网络断开或者其他原因导致客户端没法连接远端设备的时候，客户端自动去连接远端设备的等待时间，默认为 5 S，此参数可以修改，但如果没有特殊情况不建议修改。

断线重连：0 表示不支持断线重连，大于 0 小于 1 0 0 表示断线后重连的最大次数，大于或者等于 1 0 0 表示无限制的重连，直道隧道建立起来为止。

开机启动隧道：一个客户端可导入多条隧道的信息，在这里可以选择计算机开机时是否自动启动客户端软件连接远端设备，以及自动连接哪一条ＶＰＮ隧道。

支持动态密码认证：该选项只有当 apn 端启用 radius 服务器的时候有效，关于该功能请查阅第三方的 radius 服务器的详细资料（该功能只有 PSK 版本支持）

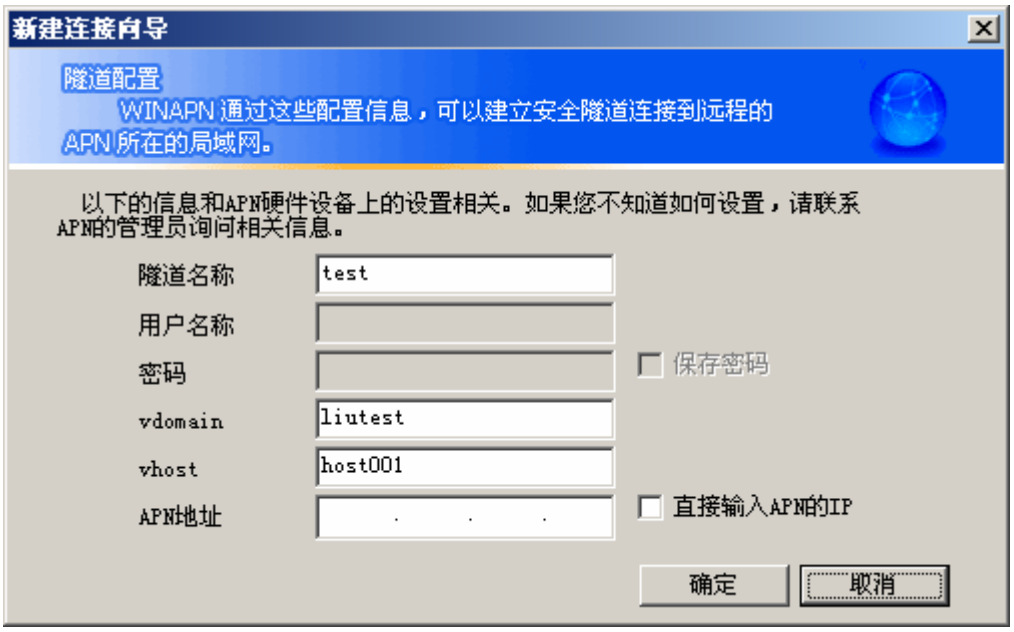
是否无线上网：如果安装客户端的计算机是无线上网的选择这一项。

是否局域网：此选项只有当 APN 端启用网关重定向，且 APN 的公网口和客户端计算机属于同一个网段的时候有效

2.3 隧道

在系统主窗口中选择隧道选项，可以添加、修改以及删除隧道信息，同时能查看隧道连接整个过程的详细日志信息，如下窗口所示：

点击添加按钮，可以添加新的隧道信息，当第一次使用证书版文件模式的客户端时，里面还没有任何隧道信息，用户可以添加一条或者多条隧道，点击添加按钮添加隧道，如下所示：



“隧道名称” 可以根据需要设置便于管理的字符串，比如以 APN GW 设备终端放置的地方的汉语拼音命名。

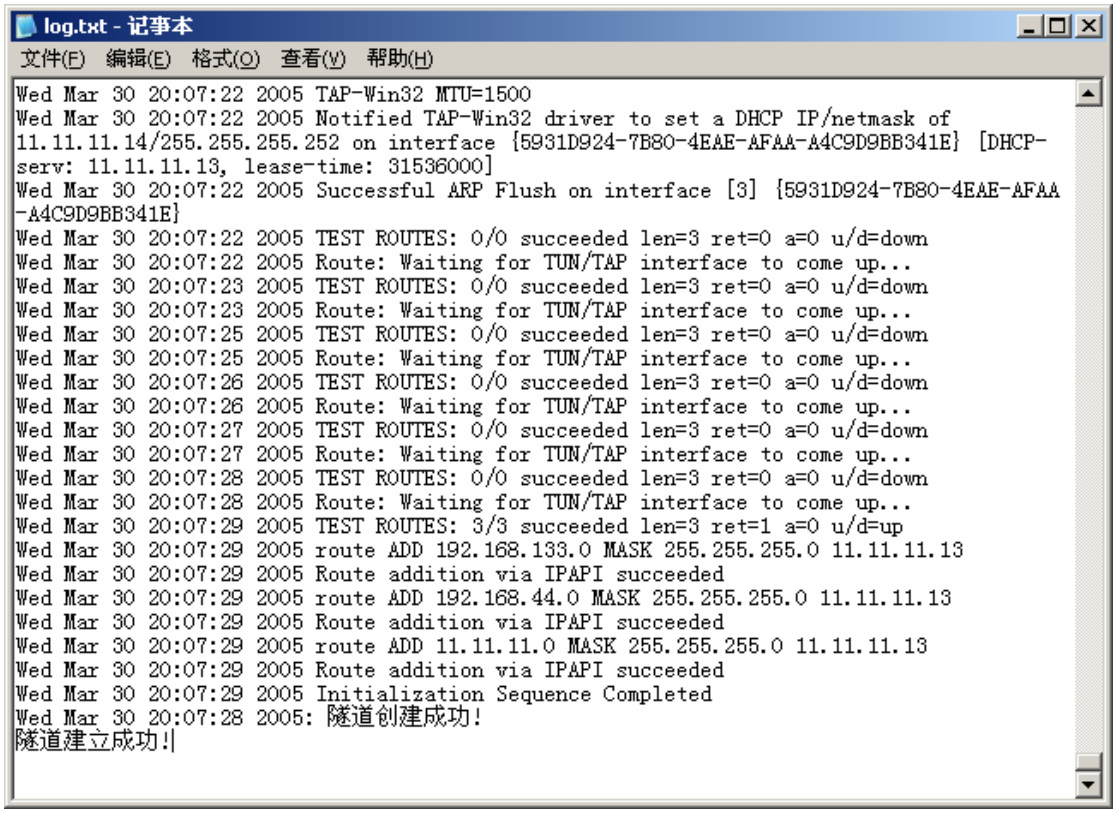
“Vdomain” 要连接的 APN GW 设备终端的组域号。

“Vhost” 要连接的 APN GW 设备终端的节点名。

“APN 地址”即远端ＡＰＮ设备的公网ＩＰ地址，如果远端设备有静态公网ＩＰ，那么可以在建立隧道的时候直接输入远端设备的公网 IP 地址；如果远程设备不是采用静态公网ＩＰ的上网方式，则在输入框中不要输入任何信息。

用户可以有选择的删除整条隧道，以及对某条隧道信息进行修改，操作过程相当简单。

日志功能非常重要，里面记录了所有隧道的连接信息，当连接失败时，可以查看登陆过程的日志，以判断失败原因。当需要向厂家工程师报障时，可向对方提供出错的日志信息。点击日志按钮在弹出的日志信息窗口中，滚动到文件的最后，就可以查看最新的日志信息。



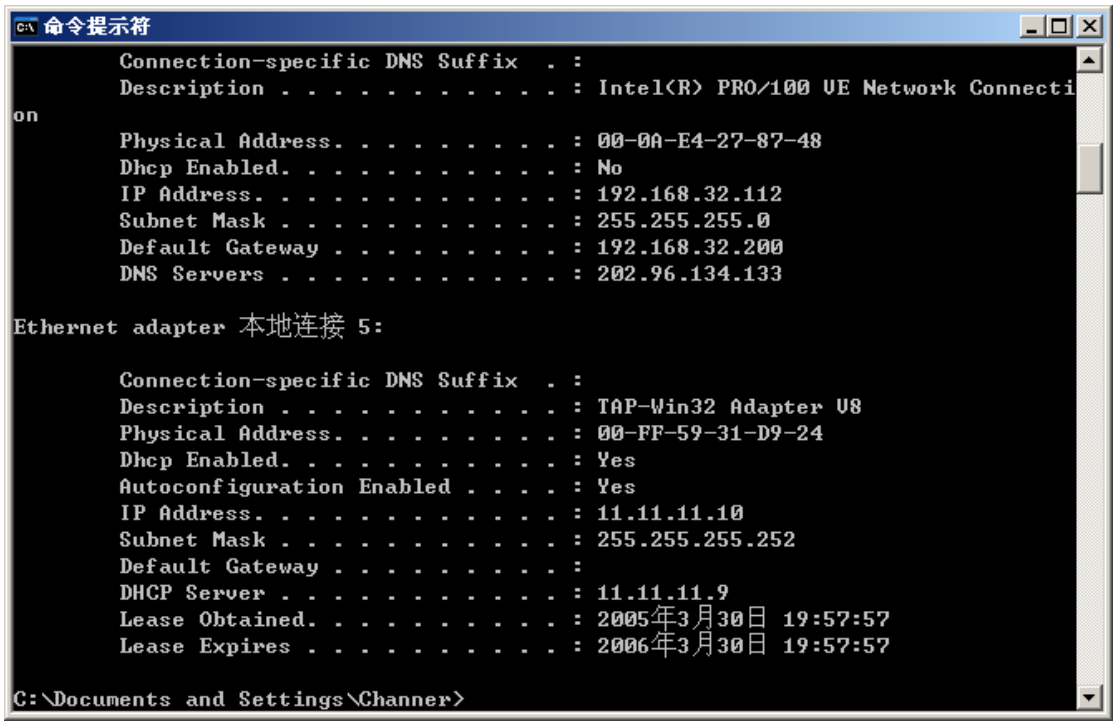
3． 连接服务器

回到软件的第一个界面，在“选择隧道”的右边下拉菜单中选择需要连接的隧道标识，然后点“连接”按钮。

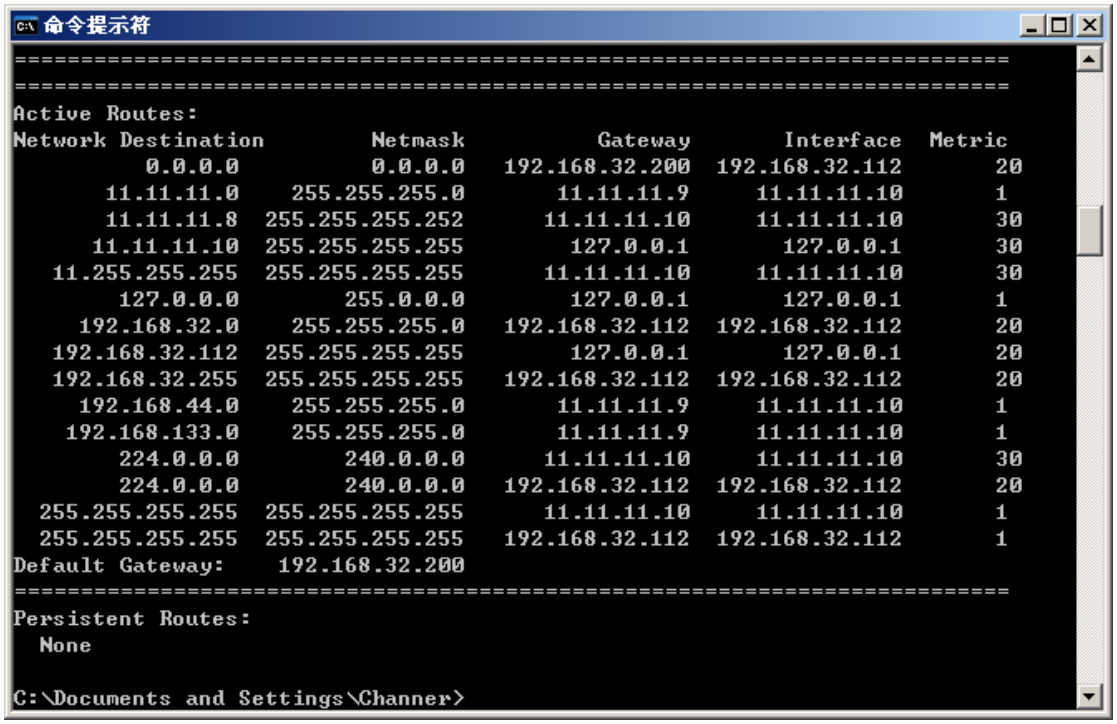
接着开始了连接服务端的过程，如果没有故障的话，可以正常连接到服务端。

4．连接成功后的检查

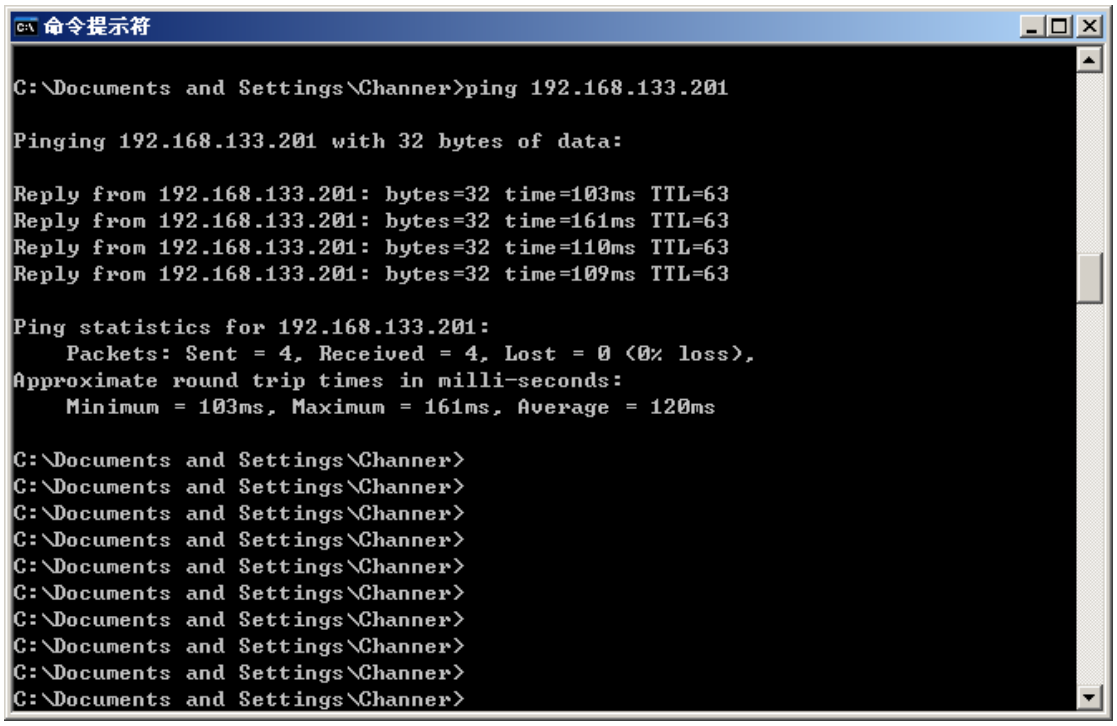
使用 ipconfig 命令查看本地获得的虚拟网口 IP。这个 IP 是服务器端定义的 IP 地址段中的一个。



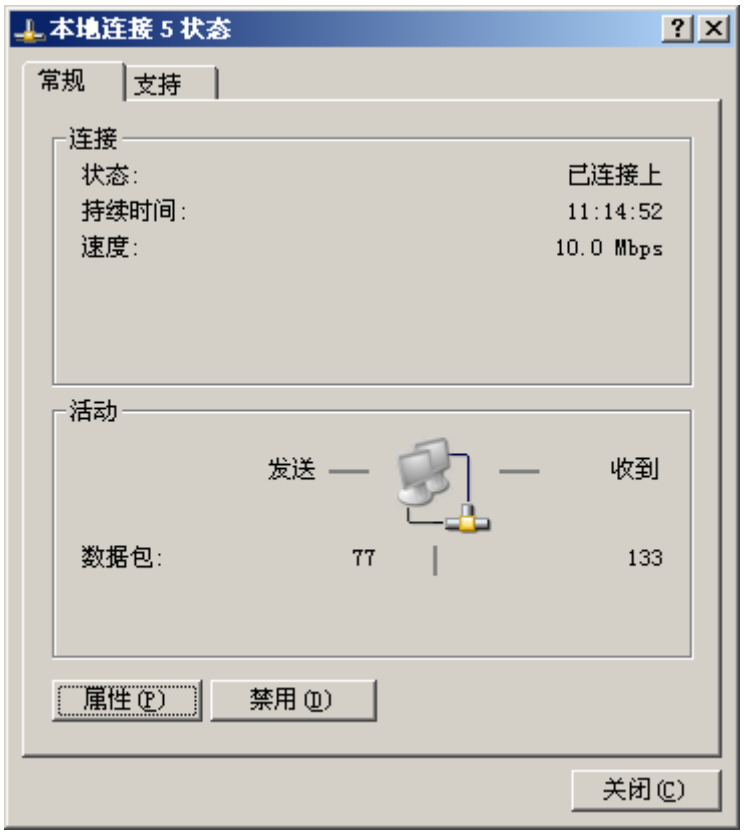
使用 route print 命令查看本地计算机增加的到 APN 内部的静态路由。



使用 ping 命令检查是否跟 APN 内部局域网联通；



检查虚拟网络连接的状态；



四．USB Key 证书客户端使用

1．运行客户端

注意：在运行客户端之前插入 USB Key，并确认 USB KEY 驱动程序正确安装。
点击“开始”→“程序”→ “WINAPN”，开始运行 USB KEY 证书版 WINAPN 客户端。
如果在没有插入 USB KEY 而运行程序的情况下会谈出下面的提出窗口：

如果 USB KEY 客户端软件正常安装并且 USB KEY 正常使用，第一次开始运行客户端软件，为了防止他人通过其他手段获取了 USE KEY 后做非法的事情，系统会提示你输入合法使用 USB KEY 的密码保护口令，如下图所示。

在上图窗口中输入 USB KEY 保护口令，如果选择了保存口令，那么下次再重新登陆时则不用再输入保护口令，如果用户考虑到安全问题，可以不保存口令。刚出厂的 USB KEY 默认密码为 gw1admin，（在后面可以进行修改）输入正确密码后，会弹出下面窗口配置窗口：

2．设置

因为需要连接的通道的信息，VDN 服务器的 Cache 值和证书都已经保存在 USB KEY 上。所以，不象使用文件证书一样，还需要做较多的设置。

2.1 证书

当第一次要运行客户端软件，并且在生成证书的时候，没有把证书的保护口令保存在 USB KEY 里，那么必须首先按上图点击系统按钮，然后选择证书选项：

在此窗口中输入证书的保护口令。提交，如果口令正确下面会显示证书和私钥保护口令匹配的提示，如果口令不正确会显示不匹配的信息。

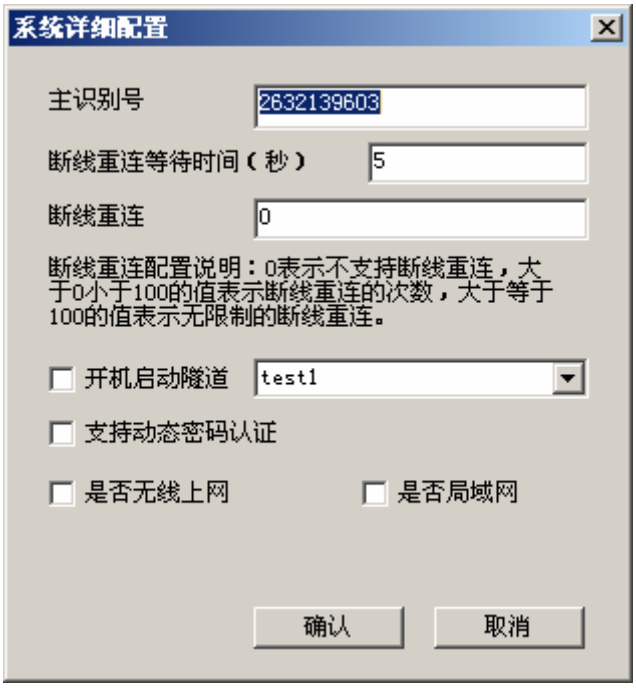
注意从证书的生产时间到证书的使用时间必须有 24 小时的间隔，所以如果还不到这个间隔时间，那么即使你输入的口令是正确的，提示信息依然会显示不匹配的信息。

2.4 USB KEY

在这里可以修改 USB KEY 的保护口令。

2.5 配置

在配置选项中，能看到一些相关的配置信息，点击配置按钮可以重新进行配置。



主识别号：APNGW 终端设备上设置的 VDN 服务器的识别号。缺省为“2362139603”，此缺省识别号为厂家 VDN 服务器的识别号。

注意：

如果客户的终端设备的许可证是由厂家分发的，此主识别号不需要修改。如果客户的终端设备的许可证

是有自有的 VDN 服务模块（GW5000）或者运营商的运营 VDN 平台分发的，需要修改为相对应的主识别号。

断线重连等待时间：当网络断开或者其他原因导致客户端没法连接远端设备的时候，客户端自动去连接远端设备的等待时间，默认为 5 S，此参数可以修改，但如果没有特殊情况不建议修改。

断线重连：0 表示不支持断线重连，大于 0 小于 1 0 0 表示断线后重连的最大次数，大于或者等于 1 0 0 表示无限制的重连，直道隧道建立起来为止。

开机启动隧道：一个 USB KEY 可导入多条隧道的信息，在这里可以选择计算机开机时是否自动连接ＶＰＮ，以及自动连接哪一条ＶＰＮ隧道。

支持动态密码认证：可以选择支持动态协商密码认证。

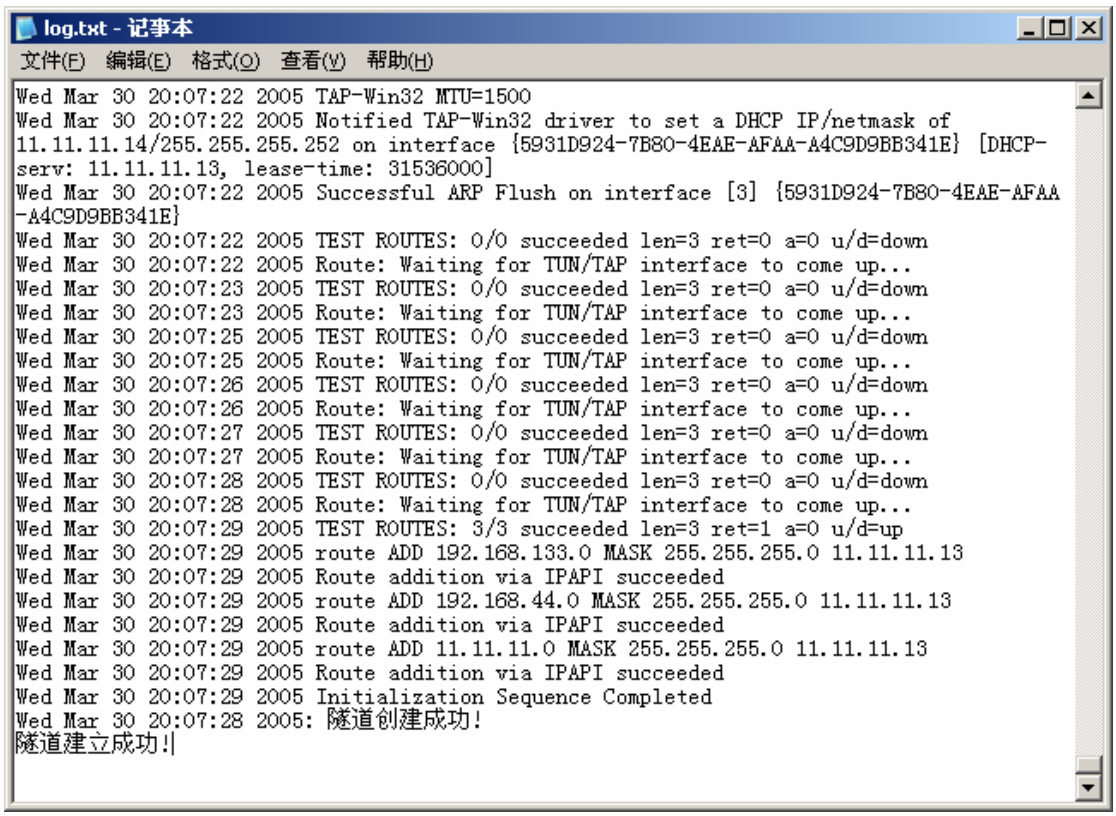
是否无线上网：如果安装客户端的计算机是无线上网的选择这一项。

是否局域网：如果安装客户端的计算机在局域网里面（即此计算机没有公网的情况）选择此项。

2.6 隧道及日志

一个移动客户端只能同时连接一个远端设备，在这里可以看到一些当前所选连接隧道的信息，如 Vdomain 和 Vhost，同时可以选择需要连接的隧道。

日志功能非常重要，里面记录了所有隧道的连接信息，当连接失败时，可以查看登陆过程的日志，以判断失败原因。当需要向厂家工程师报障时，可向对方提供出错的日志信息。点击日志按钮在弹出的日志信息窗口中，滚动到文件的最后，就可以查看最新的日志信息。



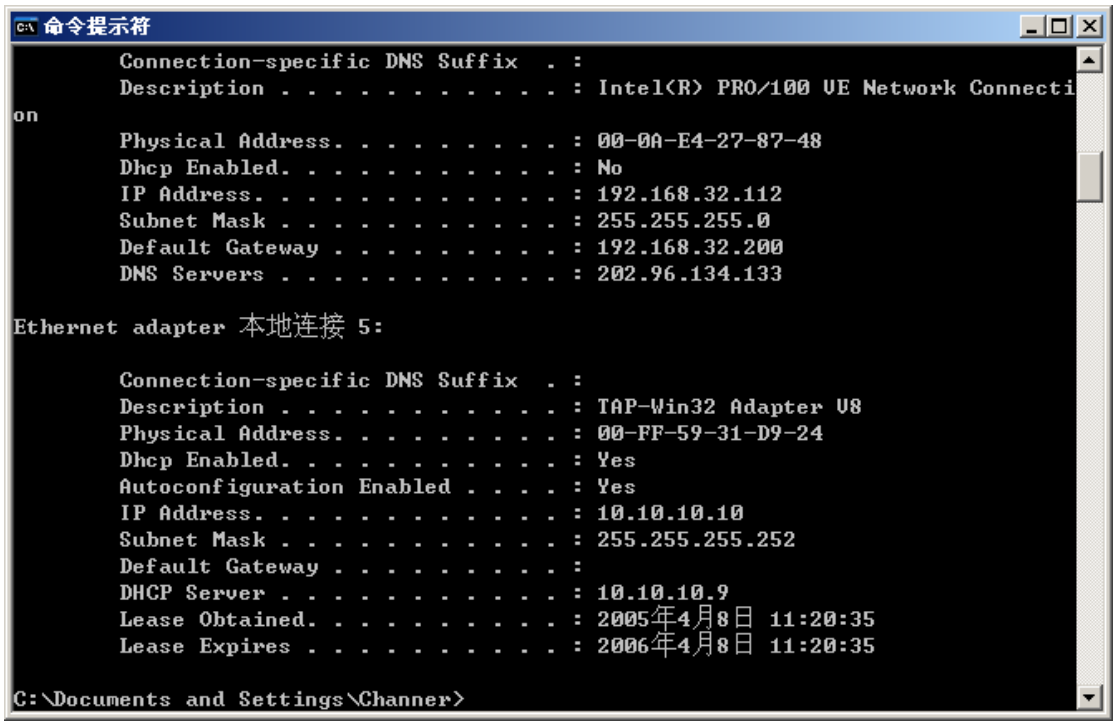
3．连接 APNGW 设备

回到软件的第一个界面，在“选择隧道”的右边下拉菜单中选择需要连接的隧道标识，然后点“连接”按钮。

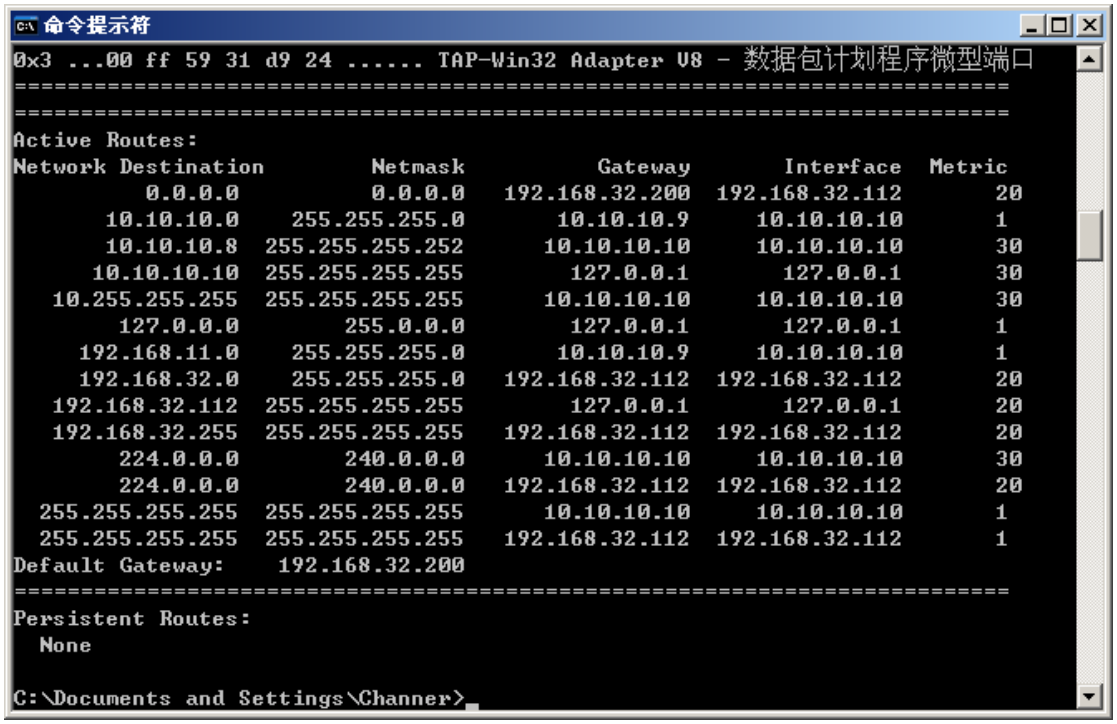
接着开始了连接服务端的过程，如果没有故障的话，可以正常连接到服务端。

4．连接成功后的检查

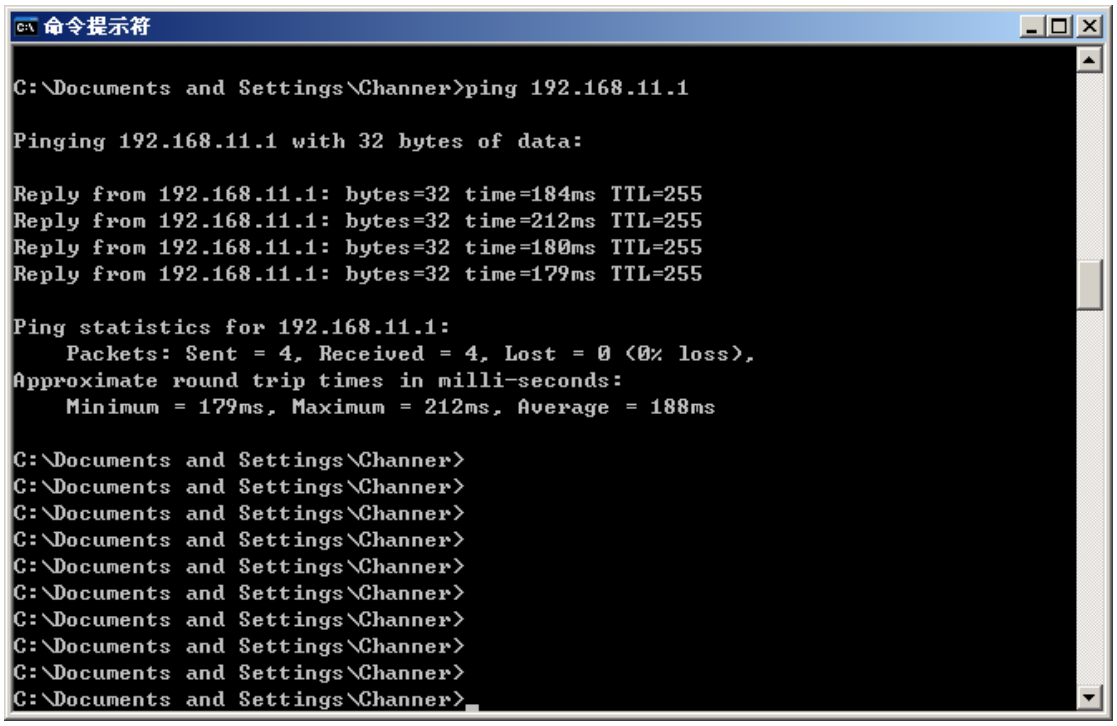
使用 ipconfig 命令查看本地获得的虚拟网口 IP。这个 IP 是服务器端定义的 IP 地址段中的一个。



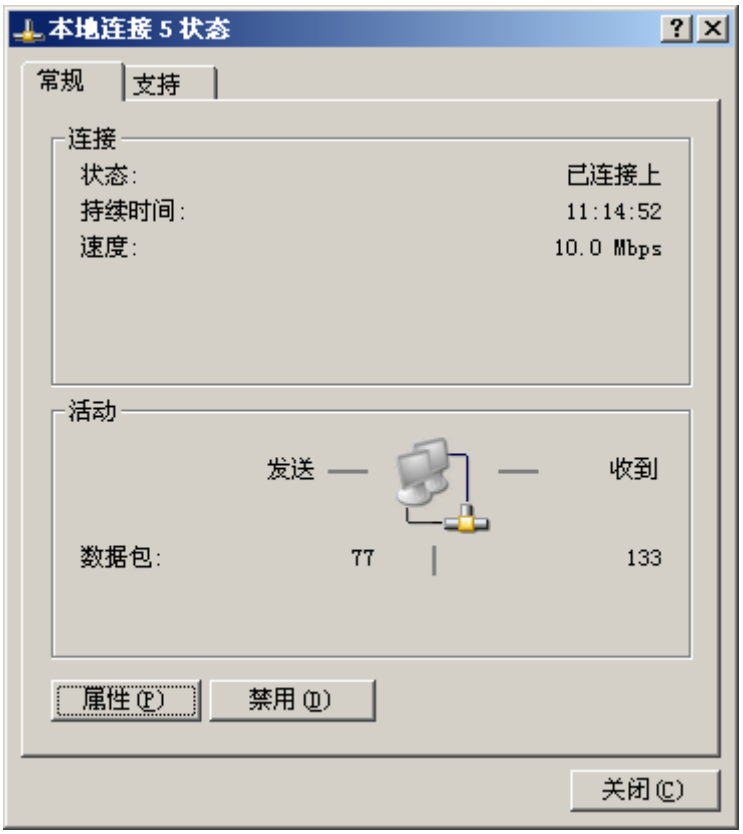
使用 route print 命令查看本地计算机增加的到 APN 内部的静态路由。



使用 ping 命令检查是否跟 APN 内部局域网联通；



检查虚拟网络连接的状态；



五．在线升级

奥联公司的研发人员对产品的功能一直在不断完善和增加，通过在线升级功能，你可以非常方便的连接到我们公司的升级服务器，对软件客户端进行升级。选择在线升级选项可以看到当前软件客户端的版本号及相关信息，如下图所示：

点击在线升级按钮可以进行对软件的升级。如下图，点击下一步进行对升级的查询。

连接到服务器查询后可知软件是否需要更新，如下所示：

从上图中可以看出通过对升级服务器的查询发现有新的软件版本，点击更新，以后的升级过程则无需进行人工进行操作即可完成。

第三章 证书管理员使用指南

本章描述了证书管理员所需要做的工作和注意事项，适合使用证书版本的管理员。

一、概述

如果使用证书版本的 WINAPN，每个公司应设定唯一的一名证书管理员。负责导入或分发、管理所有用户的证书。

随机的 CD 中提供了一个证书管理程序，可以协助管理员完成证书管理工作。

二、安装证书管理软件

系统要求：

- 操作系统：Windows 2000/Windows XP/Windows 2003
- 系统配置：CD-ROM（用于安装程序），USB 接口（用于生成 USB Key）

管理员在进行证书发放与管理前，需要安装 winapn 证书管理软件。

将附件中所带的光盘插入光驱，打开光盘中的 WINAPN CERTMAN 目录，运行该目录中的 setup.exe 文件，根据安装向导提示进行，直到将此程序正确安装到你的电脑上。

如果从互联网或者其他方式得到此客户端安装包，请解压后运行目录中的 setup.exe。

三、证书发放与管理

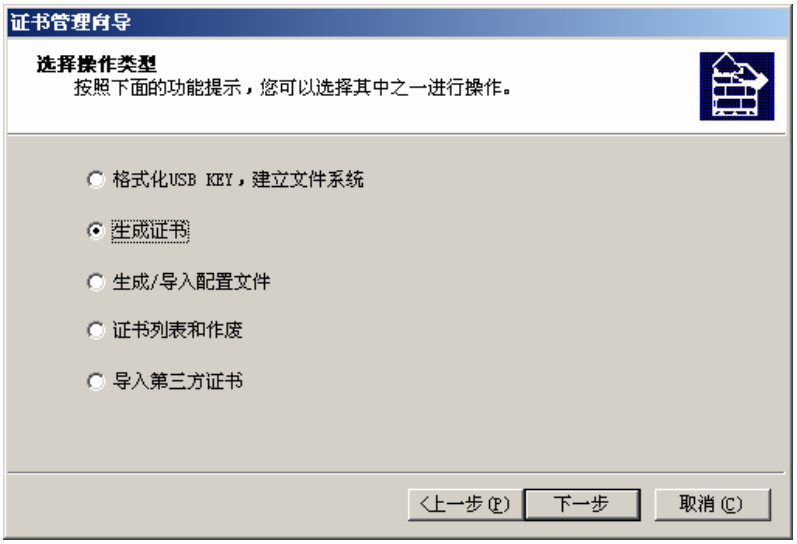
如果是首次使用，管理员需要使用证书管理软件生成根证书（root 证书），然后使用此根证书为 APNGW 终端设备和 WINAPN 客户端签发用户证书。

步骤如下：

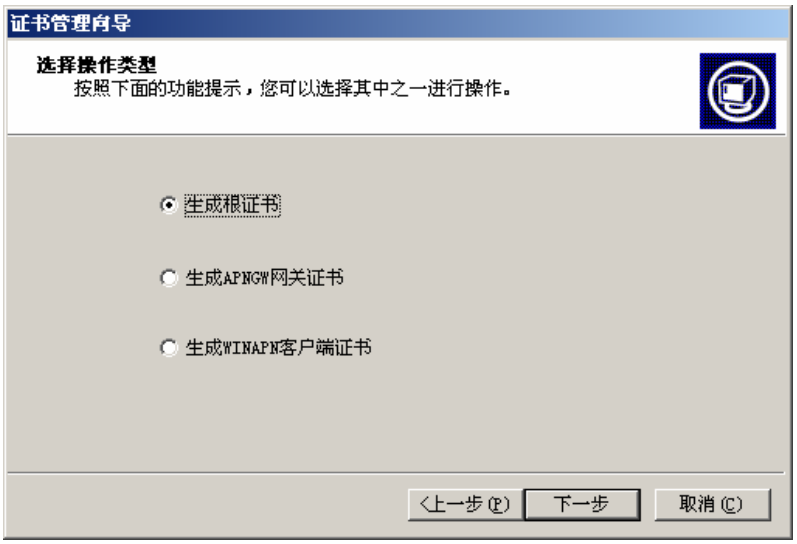
1．生成根证书

运行“开始”—>“程序”—>“winapn 证书管理软件”—>“CertManager”。

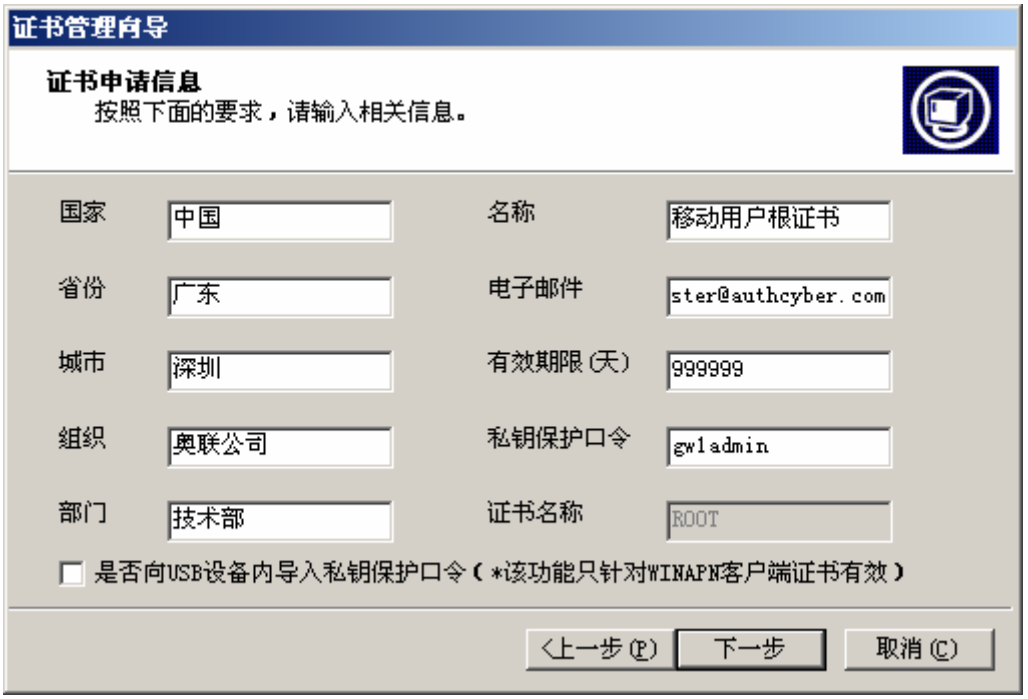
在弹出的向导窗口中选择“生成证书”选项，然后点击“下一步”，如下图：



选择“生成根证书”，点击“下一步”，如下图：



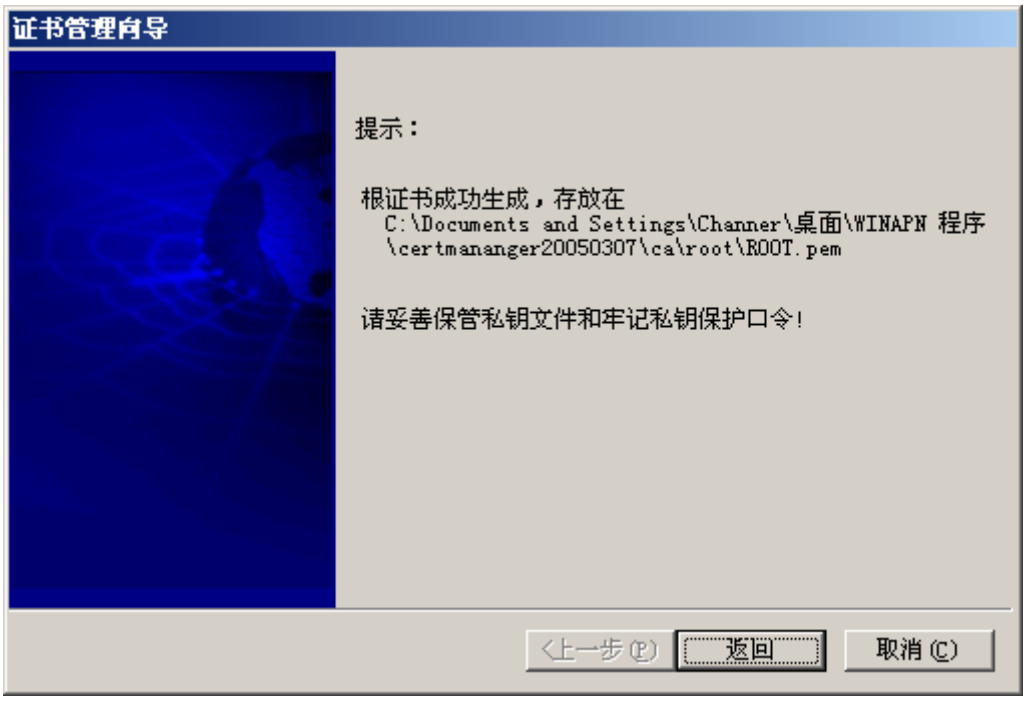
在“证书申请信息”中填入相应信息，然后点击“下一步，如下图：



注意：在“有效期限”栏目中填入根证书的有效天数，根证书的有效期是发放根证书后 24 小时生效。

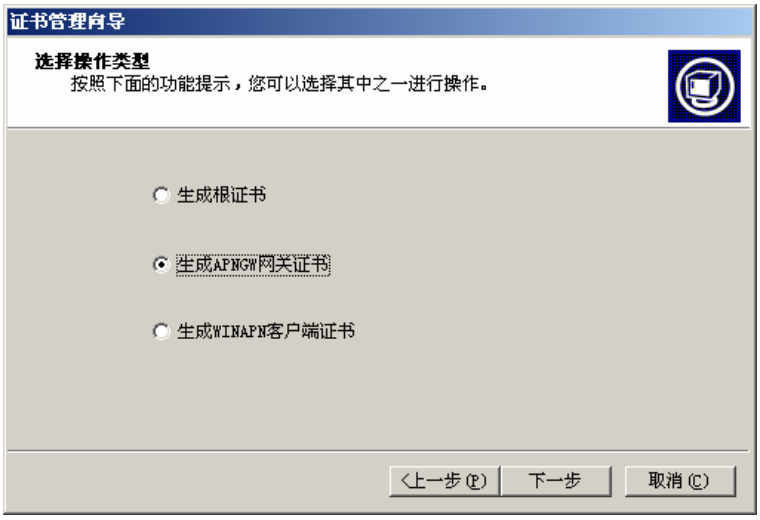
向导最后提示根证书已经生成，并且提示了存放的目录。

因为以后所有的用户证书都需要根据此根证书来签发，所以，一定要把此文件备份到安全的地方！并且牢记根证书的私钥保护口令。

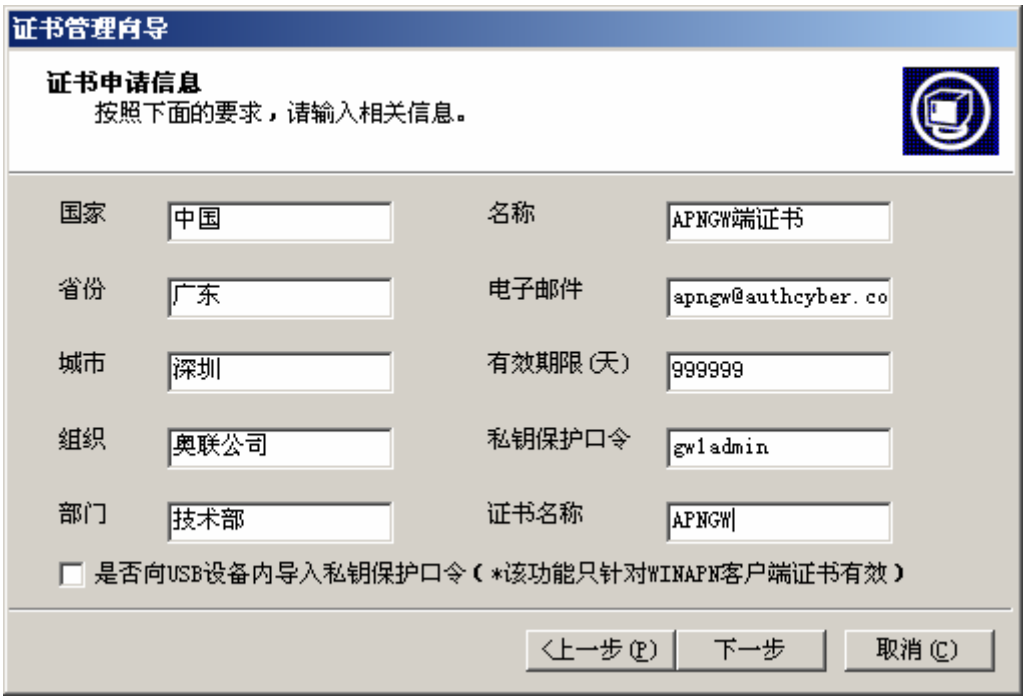


2．生成终端设备证书

在接着的向导窗口中选择“生成 APNGW 网关证书”选项，然后点击“下一步”，如下图：



在“证书申请信息”中填入相应信息，然后点击“下一步，如下图：

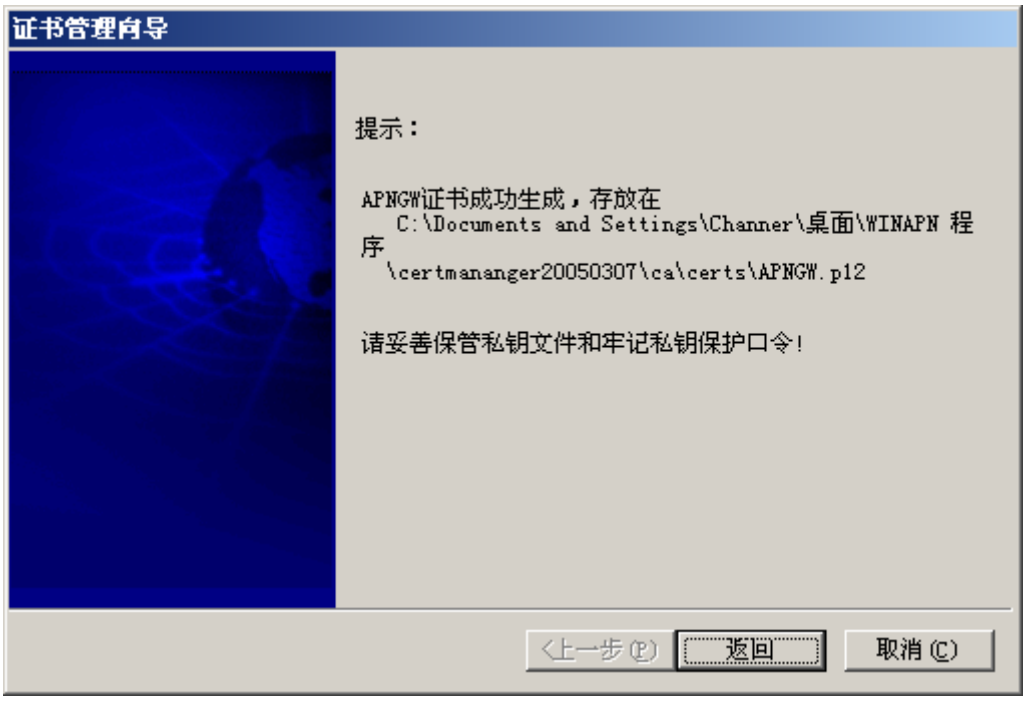


注意：在“有效期限”栏目中填入终端证书的有效天数，证书的有效期是在发放证书后 24 小时生效。并且请注意修改“证书名称”（应该区别与根证书的“root“）

提示输入“根证书”的保护口令，如下图所示：

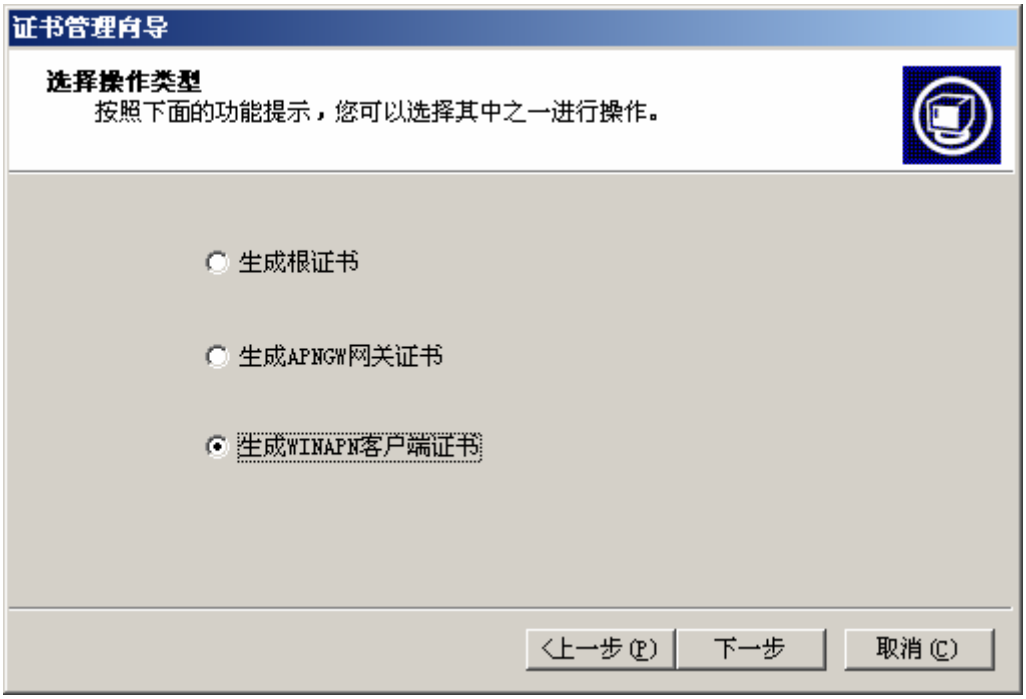
输入“根证书”保护口令，按“确定”后，向导最后提示证书已经生成，并且提示了存放的目录。

请牢记此证书的私钥保护口令。

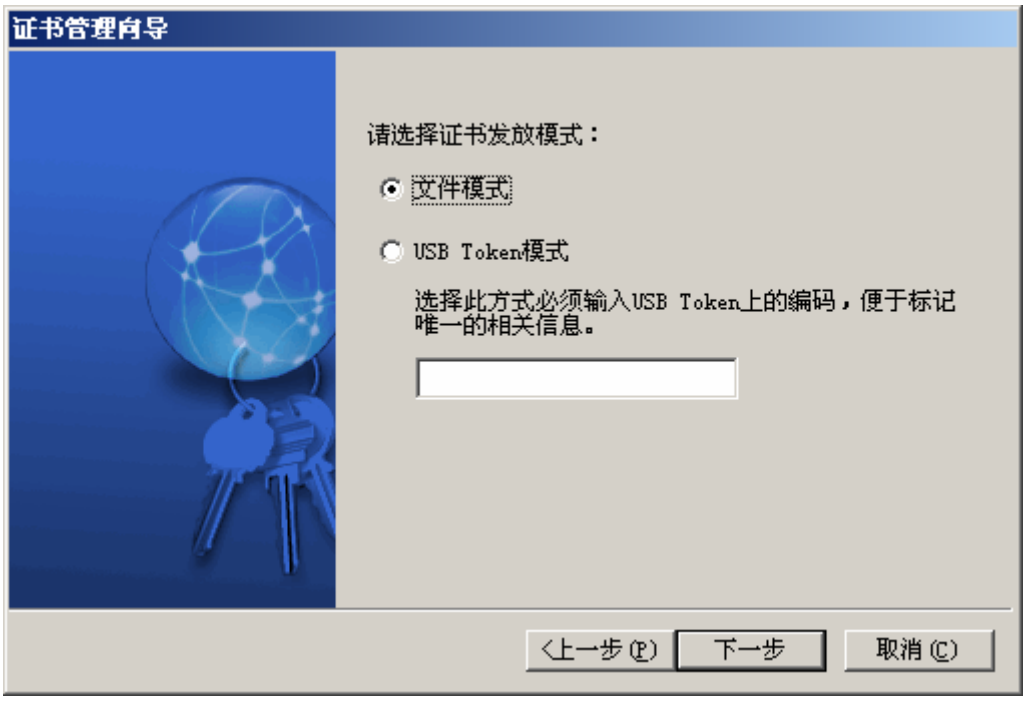


3．生成客户端证书

在接着的向导窗口中选择“生成 WINAPN 客户端证书”选项，然后点击“下一步”，如下图：

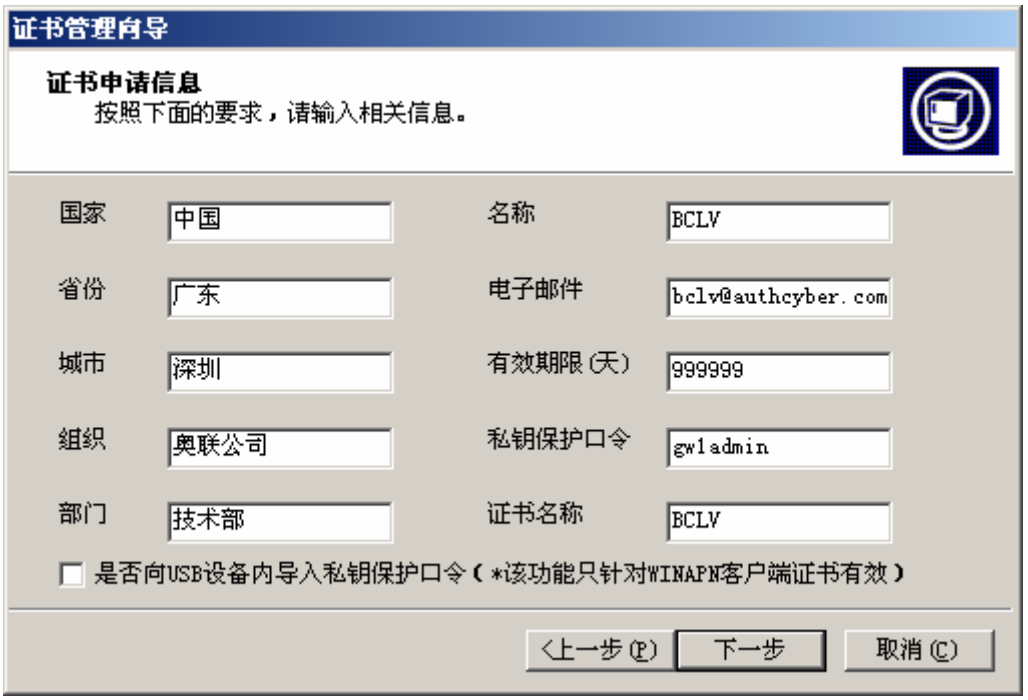


在“选择证书发放模式”中，根据实际情况选择“文件模式”还是“USB Token 模式”。如果是“USB Token”模式，请输入输入“USB Token”上的唯一编号。完成后按“下一步”，如下图所示：



重要：如果选择 USB Token 模式时，必须插入已经成功格式化和生成了文件系统的 USB Token。请参考下一节。

在“证书申请信息”中填入相应信息，然后点击“下一步，如下图：

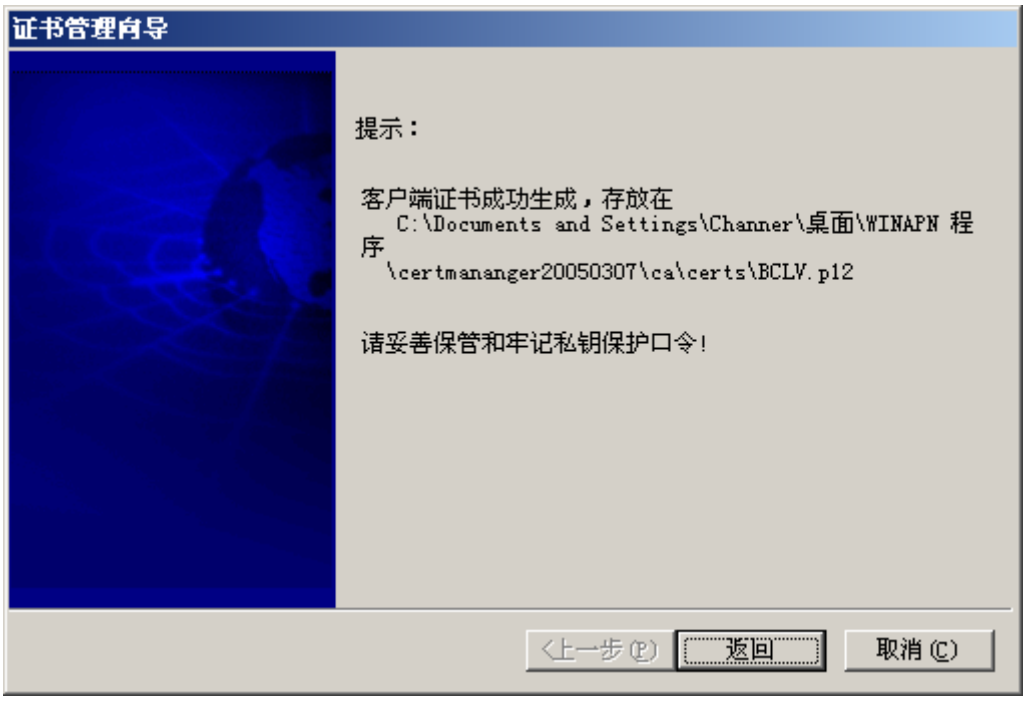


注意：在“有效期限”栏目中填入客户端证书的有效天数，证书的有效期是在发放证书后 24 小时生效。并且请注意修改“证书名称”，建议以使用者名称命名，如“BCLV”。

如果是 USB Token 模式，而且用户要求在使用客户端时，不输入证书的密码，而仅仅输入 USB Token 的密码，请选择“是否向 USB 设备内导入私匙保护口令”，这样，程序就会把此证书的私钥保护口令记录到 USB 中，用户在使用的过程中不需要输入。

提示输入“根证书”的保护口令，如下图所示：

输入“根证书”保护口令，按“确定”后，向导最后提示证书已经生成，并且提示了存放的目录。请牢记此证书的私钥保护口令。



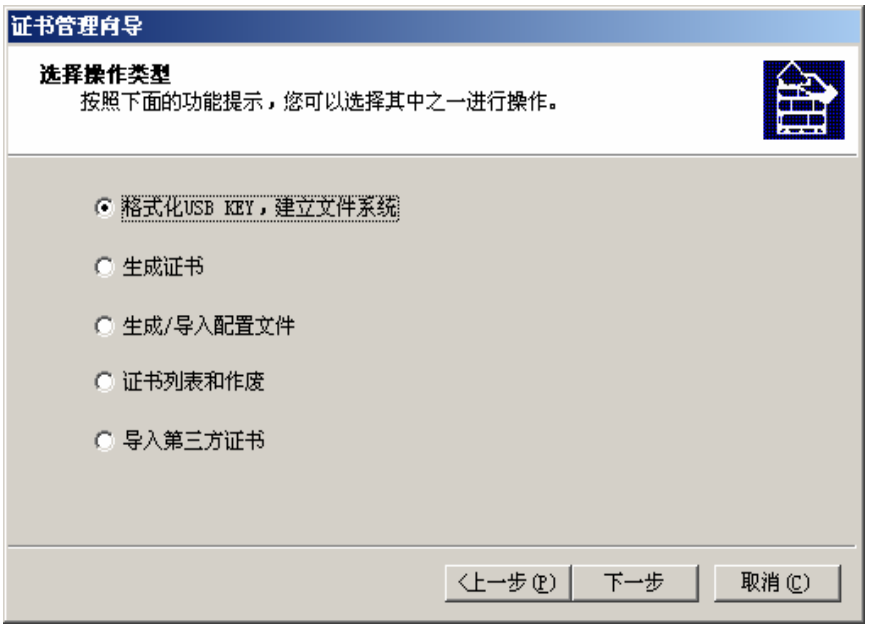
4．格式化 USB Key 和建立文件系统

重要：选择了 USB Token 模式时，必须先对 USB Key 进行格式化和建立文件系统，才能进行下面的写入配置文件的操作。

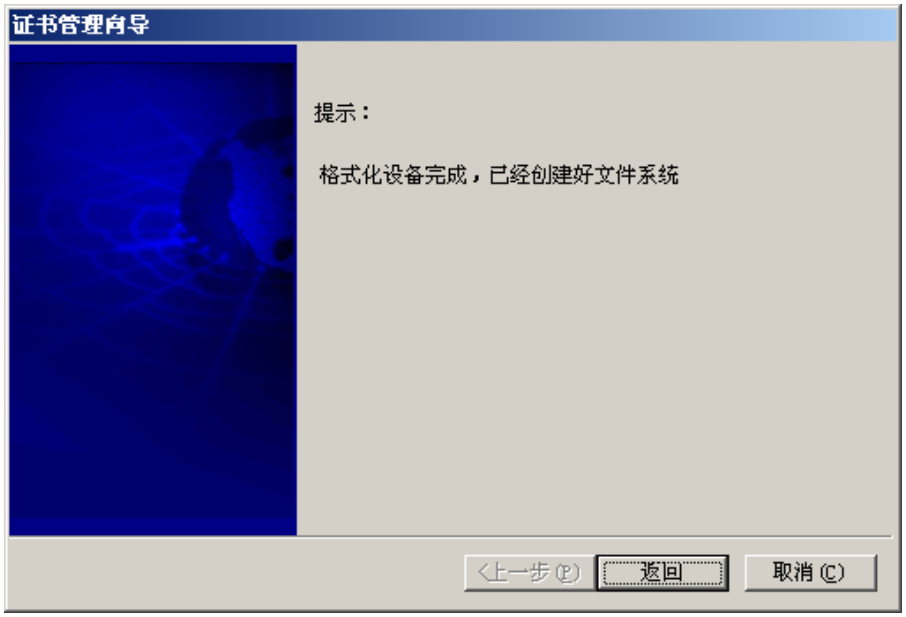
格式化前的准备－安装 USB Key 的驱动：

将 USB KEY 附件中所带的光盘插入光驱中，进入“驱动安装程序”目录，运行该目录中的 InstallDriver.exe，按照安装向导完成 USB KEY 驱动程序的安装。

在“证书管理向导”中选择“格式化 USB Key，建立文件系统”，点击“下一步”，如下图所示：



完成格式化和建立文件系统过程，如下图所示：

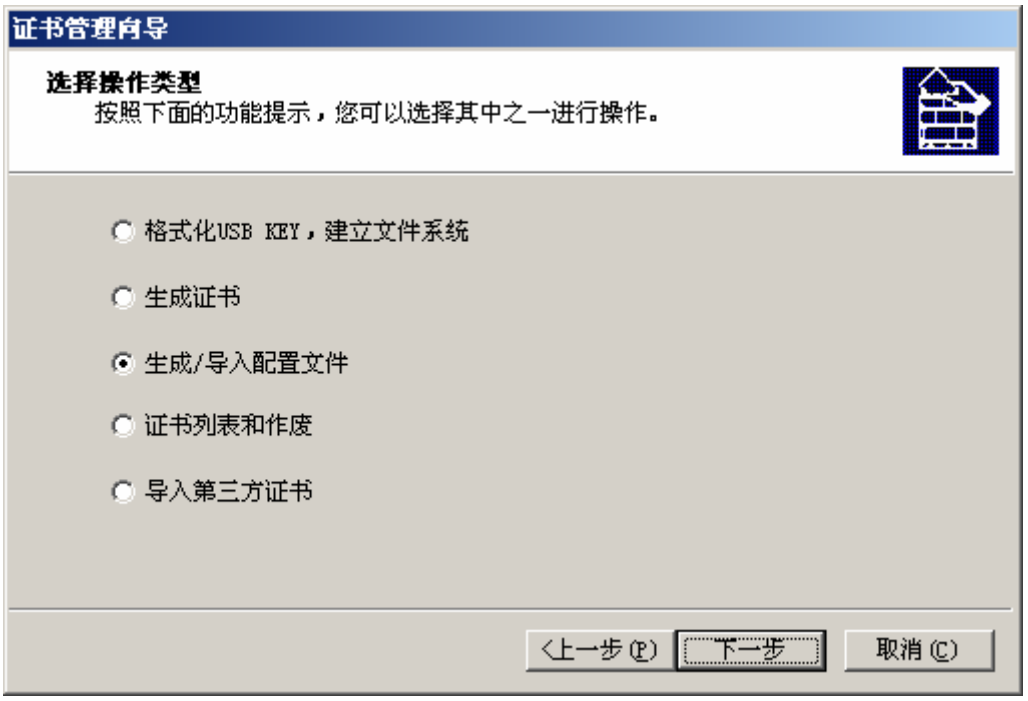


注意：USB Key 格式化完成后，会产生一个缺省的 Key 密码：“gw1admin”。此密码在管理工具中不能修改，但使用软件客户端时可修改。

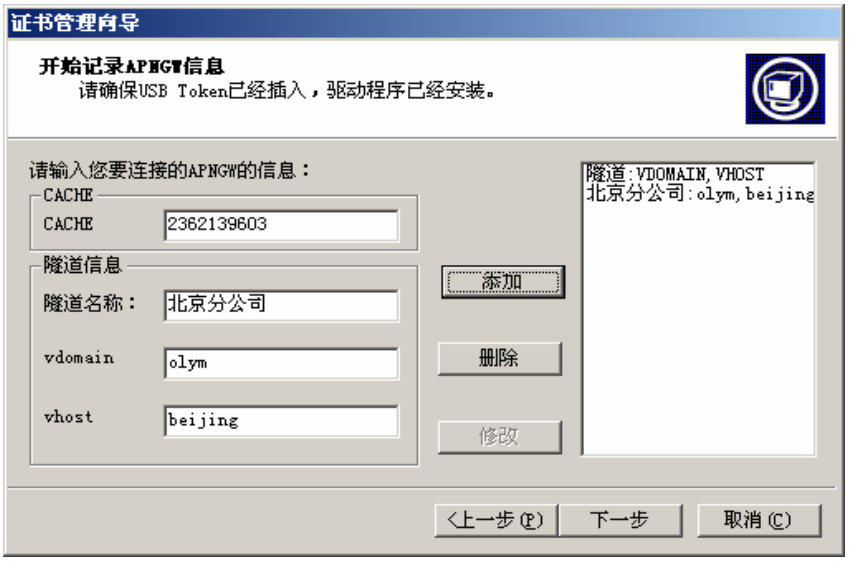
5．生成配置文件

重要：选择了 USB Token 模式，需要将证书写入 USB Tokey 时，才需要生成配置文件。

在“证书管理向导”中选择“生成／导入配置文件”，点击“下一步”，如下图所示：

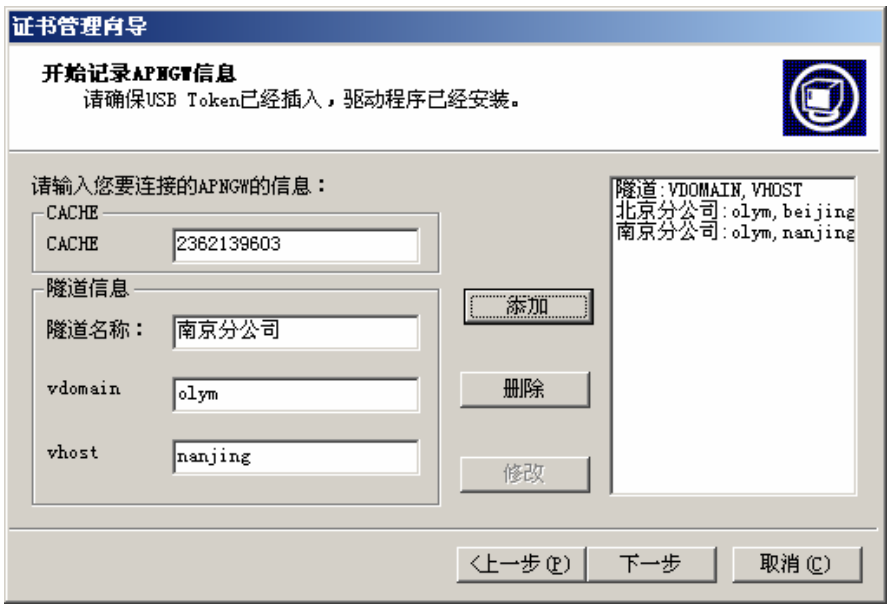


在接下来的窗口中输入连接 APNGW 终端设备所需要的信息，如下图所示：



- cache 值：APN 设备的主机识别号（查看“WEB 管理界面”—>“虚拟专网”）
- 隧道名称：可以给定一个容易理解的名称，比如上海办事处，北京市场部等等
- VDOMAIN：需要连接的终端设备的组域号（“查看 WEB 管理界面”—>“虚拟专网”）
- VHOST：需要连接的终端设备的节点名（“查看 WEB 管理界面”—>“虚拟专网”）

输入完成后，按“添加”按钮。用户可以根据实际情况添加多条隧道信息。



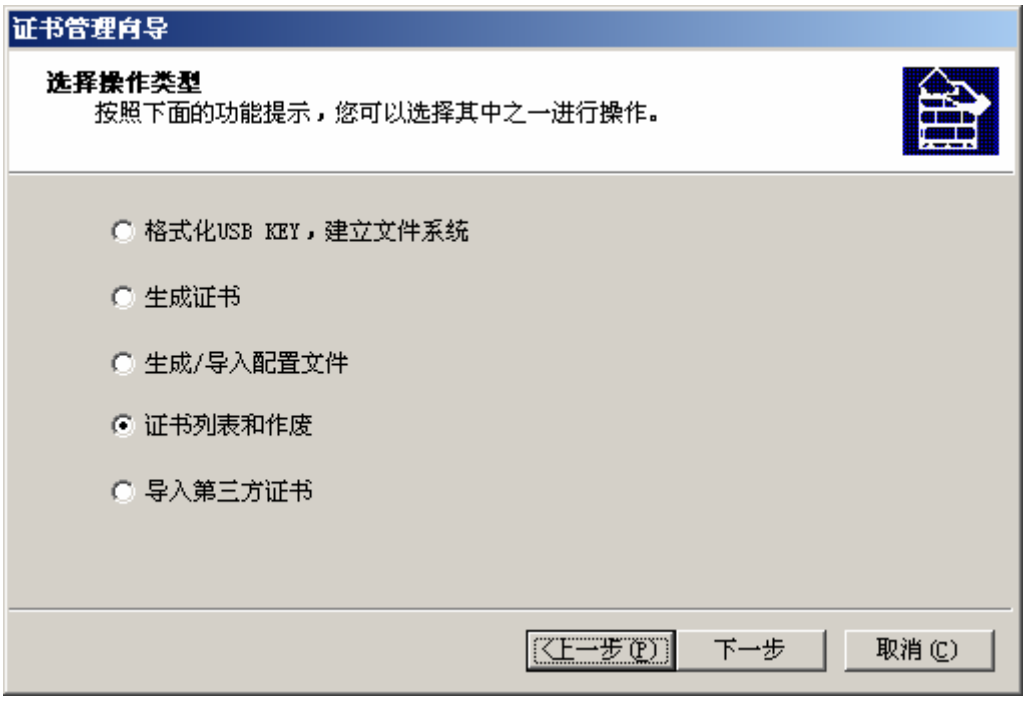
添加完隧道信息后，点击“下一步”

6．证书列表与作废

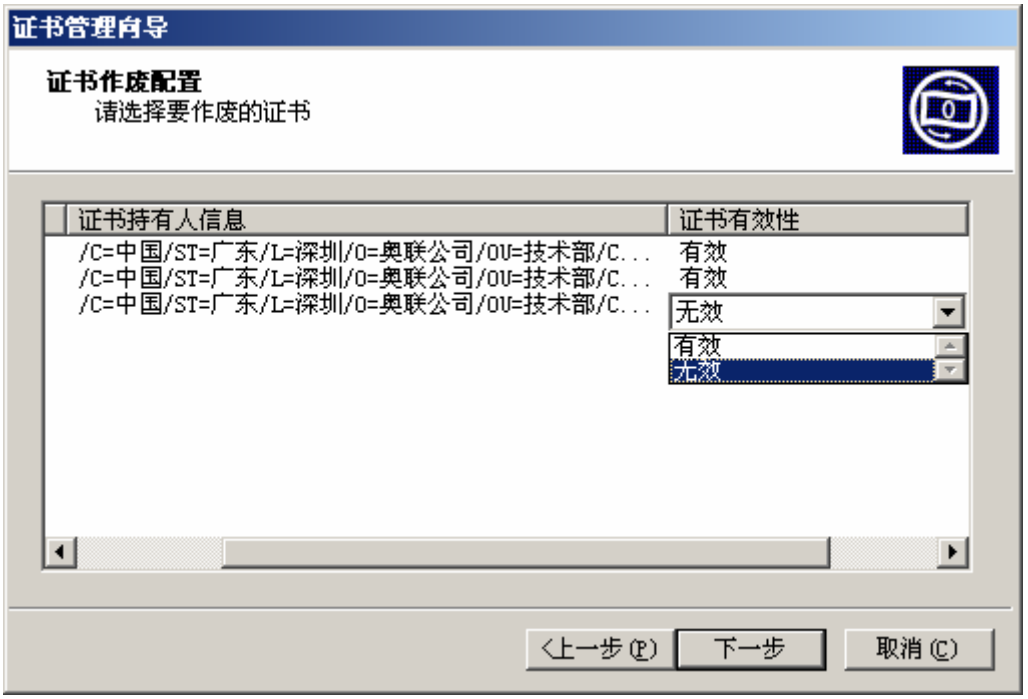
重要：管理员必须生成 CRL 证书，并且配置到 APN GW 终端上，终端上的服务才能正常启动。

如果使用者不慎丢失 USB KEY，为防止获得此 USB Key 的非授权人员强行破解 USB Key 的密码后连接 APN GW 终端设备，管理员必须生成新的 CRL 证书，然后应用在 APN GW 服务端上，作废此 USB Key 所包含的证书。

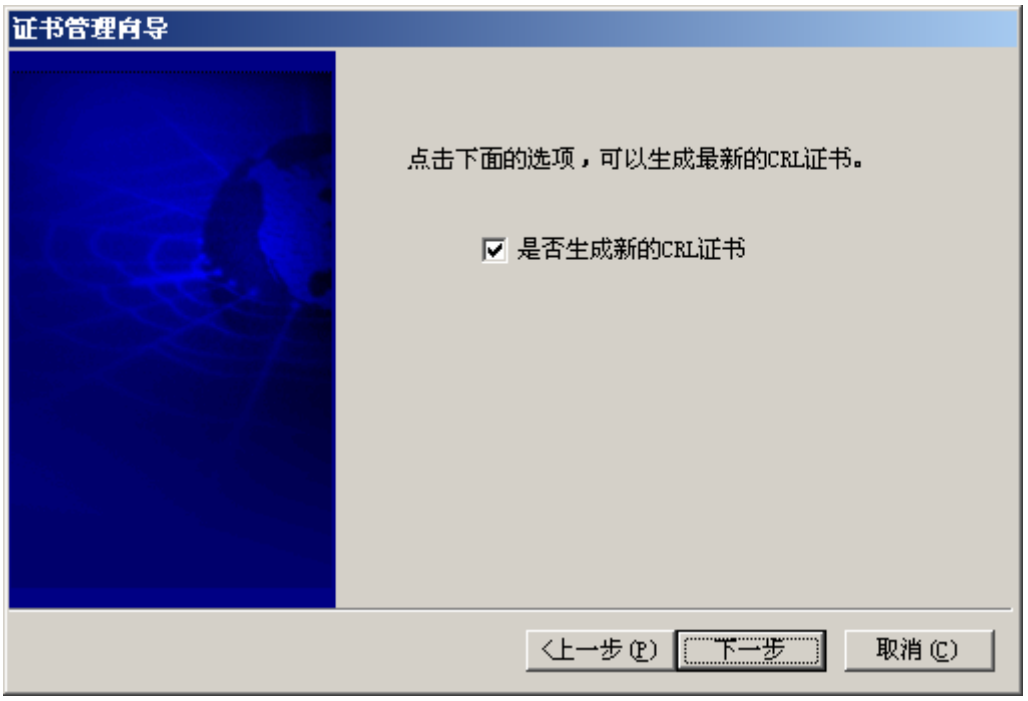
在“证书管理向导”中选择“证书列表与作废”，点击“下一步”，如下图所示：



选中需要作废的证书，在“证书有效性”一栏的列表框中选择“无效”，如下图所示：



完成后，点击“下一步”，提示是否生成新的 CRL 证书，如下图所示：

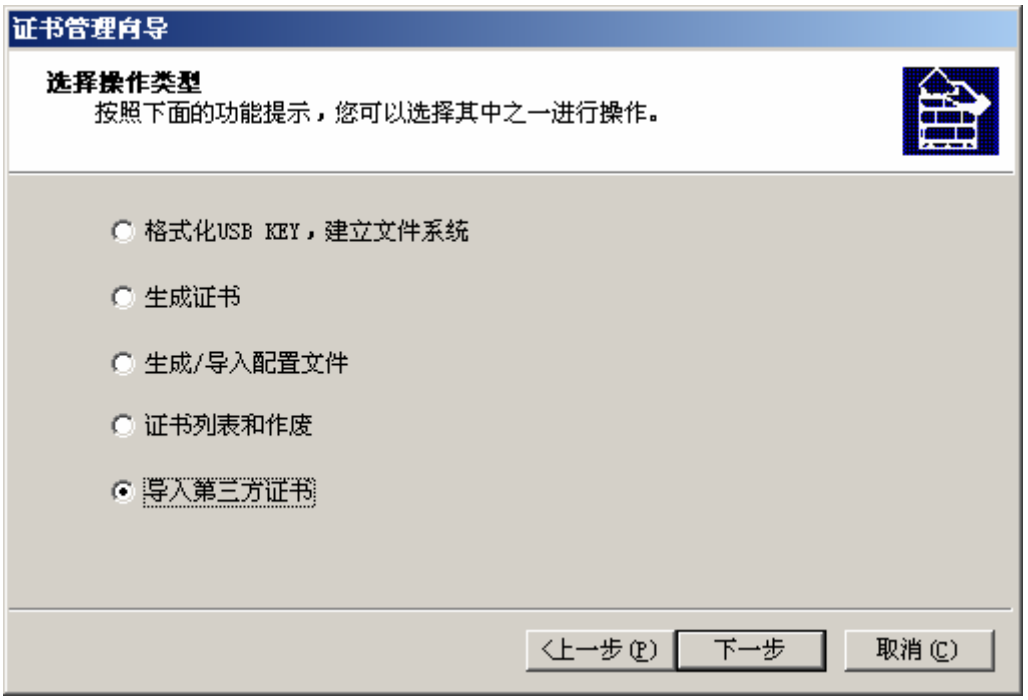


选中“是否生成新的 CRL 证书”，按“下一步”，按提示输入根证书的私匙保护密码，按“确定”后，向导最后提示 CRL 证书已经生成，并且提示了存放的目录。

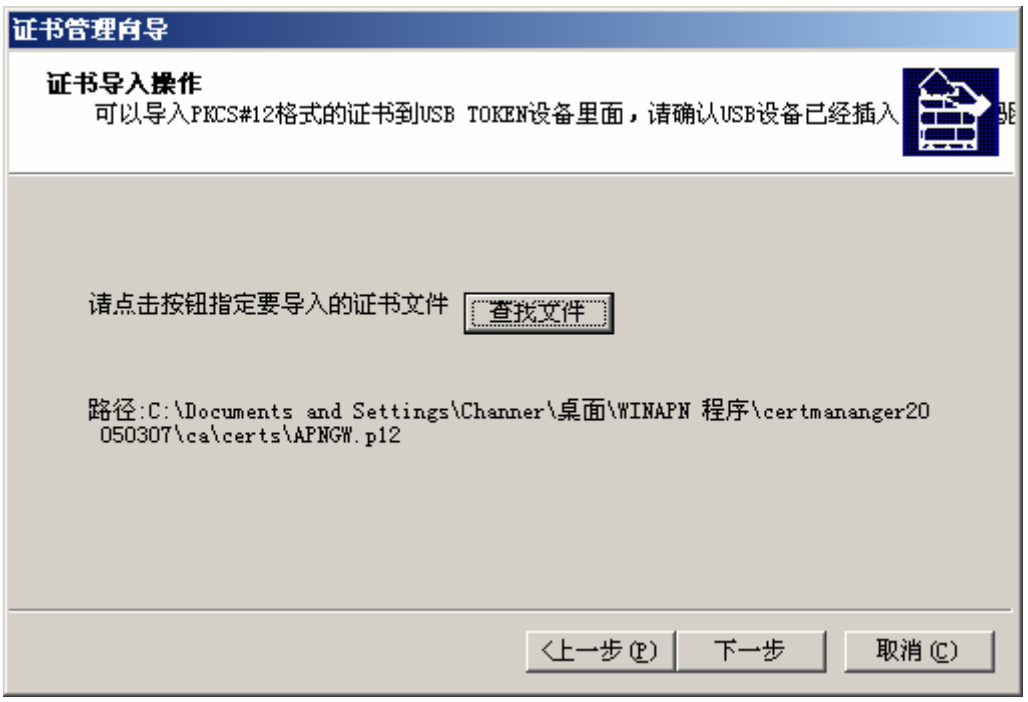
7．使用第三方证书

重要：只支持导入 PKCS #12 格式的证书。如果不是此格式，请使用第三方工具转换为 PKCS #12 格式。同时，APNGW 设备端也需要使用此第三方发放的证书。

在“证书管理向导”中选择“导入第三方证书”，点击“下一步”，如下图所示：



在“证书导入操作中”，选择“查找文件”按钮，然后选择第三方发放的证书文件，完成后，点击“下一步”，如下图所示：



如果正确插入了 USB Token，会提示正式已经导入到 USB Token 的提示。如下图。

注意：USB Tokey 必须先格式化。导入证书后，必须继续进行生成和导入配置文件的处理。

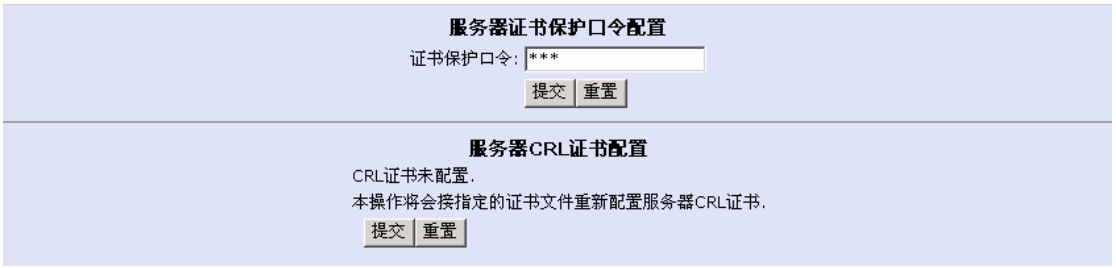
四．APNGW 设备服务端配置

1．选用“证书认证模式”

当前“APN 移动用户”支持“PSK 认证模式”和“证书认证模式”两种，必须先选用“证书认证模式”。通过 IE 浏览器进入 APN 终端的 web 管理页面，进入“虚拟专网”→“APN 移动用户”，在“隧道认证方式”中，通过“编辑”功能，选用“证书认证模式”。如下图所示：

2．启用服务端

选中“服务器管理”，按“提交”按钮。进入服务端管理页面如下：



- 启动 WINAPN 服务程序

选中 “启动 WINAPN 服务”，然后按“提交”按钮。

■ Winapn 服务器设置

1) 服务器 IP 地址设置：

需要规划一段移动用户使用的 IP 地址段，缺省的是 10.10.10.0/24。 用户可以规划使用其他网段。

规划好使用的网段后，按“提交”按钮，如下图所示。

注意：WINAPN 服务使用的地址段不能与 APN 设备的内网口地址相同，也不能与其它互连的节点内网段地址相同。

2) 静态分配 IP 地址设置：

默认情况下此处为空。一般情况下，证书版的客户端连接进来是由 APN 动态分配一个 IP，此 IP 的 IP 段跟上面设置的服务器 IP 段相同。如果想要做到静态地给移动客户端分配 IP 的话，则需要在此指定静态 IP 的 IP 段，这必须与服务器 IP、其他总部或者分支节点在不同 IP 段内。至于如何具体的指定每一个移动客户端的 IP，我们后面会谈到。

3) 服务器端口设置：

该端口为 winapn 客户端接入将使用的端口，为默认为 udp5000，允许更改为其他的 udp 端口，比如 5001，另外 winapn 客户端接入的时候将使用到另外一个 udp8500 的端口，该端口不允许修改，即 APN 上的 udp8500 端口将长期被占用。

4) 压缩传送：

该选项为 winapn 客户端接入到 APN 后，之间传输的数据是否压缩的选项，在 APN 端为非 56Kmodem 拨号的情况下不推荐使用，因为进行压缩要耗用 CPU 较多的时钟。

5) 重定向网关：

该选项如果启用，则当 winapn 客户端连接上来后，该客户端的计算机的默认网关将变为以上所设置的服务器 IP 地址

6) WINS、DNS 服务器 IP 地址：

若填写了该信息，则接入的客户端的计算机的 WINS 和 DNS 的首选服务器将变为所设置的服务器 IP

7) 纪录调试信息程度：

范围在 0~9，程度越强，纪录的信息就越细致。

默认为 4，不建议客户对该值进行修改。若不希望有 WINAPN 的相关日志信息的输出，可设置该值为 0。

■ 服务器证书配置

重要：在进行服务器证书配置时，需要将证书管理软件所分发的或者第三方证书机构分发的 APN GW 设备端的证书保存在本地计算机。

“服务器证书配置”下面的“提交”按钮。进入服务器证书配置页面。按“浏览”按钮，选择 APN GW 设备端的证书，然后按“提交”按钮。

■ 服务器证书保护口令配置

空格中输入生成终端设备证书时的私钥保护口令，然后按“提交”按钮。

■ 服务器 CRL 证书配置

重要：在进行服务器 CRL 证书配置时，需要将证书管理软件所分发的或者第三方证书机构分发的 CRL 证书保存在本地计算机。CRL 证书为 PEM 格式。

“服务器 CRL 证书配置”下面的“提交”按钮。进入服务器 CRL 证书配置页面。按“浏览”按钮，选择 CRL

证书，然后按“提交”按钮。

3．访问控制策略

选中“访问控制策略”，按“提交”按钮。进入可信任用户访问设置页面。

■ 缺省策略

缺省设置中，允许所有的通过同一个根证书签名的证书接入。并且不设置黑名单。如下图所示。

简单的说，除了 CRL 证书中指定不生效的证书外，其他的都可以接入。

■ 只允许指定的证书用户接入

将可信任用户访问设置的缺省规则删除，然后增加指定的证书信息。如下图所示。

也可以使用“*”号来匹配所有。如下图所示。

上图所示的规则代表“Olymtech”的“Tech”的所有证书用户都可以访问。

注意：录入这些信息应该跟生成证书时所填写的信息是一致的；同时生成证书时不能使用中文，所以上面输入信息也不能使用中文。

■ 允许大部分人而禁止指定的证书用户接入

在“可信任用户访问设置”中设置所有证书用户可访问的规则（缺省规则），然后在“黑名单设置”中增加指定的不允许访问的用户证书。如下图所示。

■ 固定移动用户的 IP 地址

在“用户 IP 地址配置”中，点击“添加”开始设置，所属 IP 段是我们在前面提到过“服务器设置”中的“静态分配 IP 地址设置”里有说明；而具体的主机地址，必须遵循“4n+2”法则，如下图“10.10.10.18”中的“18”=“4*4+2”，如此类推。


APN test002@pengbo - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹 媒体
地址(D) http://192.168.133.2/cgi-bin/apnget.cgi?langu=1
链接
Google 最新!
系统管理
网络接口
虚拟专网
防 火 墙
带宽管理
流量监控
主机服务
日志审计
APN GW200
许可证号
专网特性
RP:定点检查汇报
隧道信息
手动隧道配置
APN 移动用户
子网共享管理
可信任用户访问设置
最大在线人数 5
公司 部门 名称 电子邮件名称 编辑
* * * *
删除
添加
黑名单设置
公司 部门 名称 电子邮件名称 编辑
添加
用户IP地址配置
用户指定的IP地址必须属于10.10.20.0/255.255.255.0
用户名称 IP地址 编辑
syh 10.10.20.18
删除
添 加
IP规则，IP地址的最后一位必须满足4n+2,n>=1这个条件
完毕
Internet