USB 无线网卡

（USB-G31）

产品用户手册

目 录

1.产品介绍

系统需求

安装本产品之前，请确认您具备以下系统配置：

- 搭载Intel Pentium 4或是AMD K7/K8中央处理器的电脑
- 至少64MB的系统内存
- 操作系统为Windows XP/2000/Vista
- 光驱（以安装驱动程序）
- 至少一个USB连接端口（USB2.0版本以下接口会影响此网卡的性能）

产品包装

在您拿到本产品包装盒之后，请马上检查下面所列出的各项标准配件是否齐全：

- ☑ 华硕USB-G31 USB无线网卡
- ☑ USB2.0延长线
- ☑ 驱动程序光碟
- ☑ 快速安装指南

2. 安装步骤

本章将介绍如何安装此无线网卡及驱动程序和应用程序。此无线网卡兼容Windows XP/2000/Vista 操作系统，本指南以在Windows XP 上安装硬件和软件来说明安装的过程。

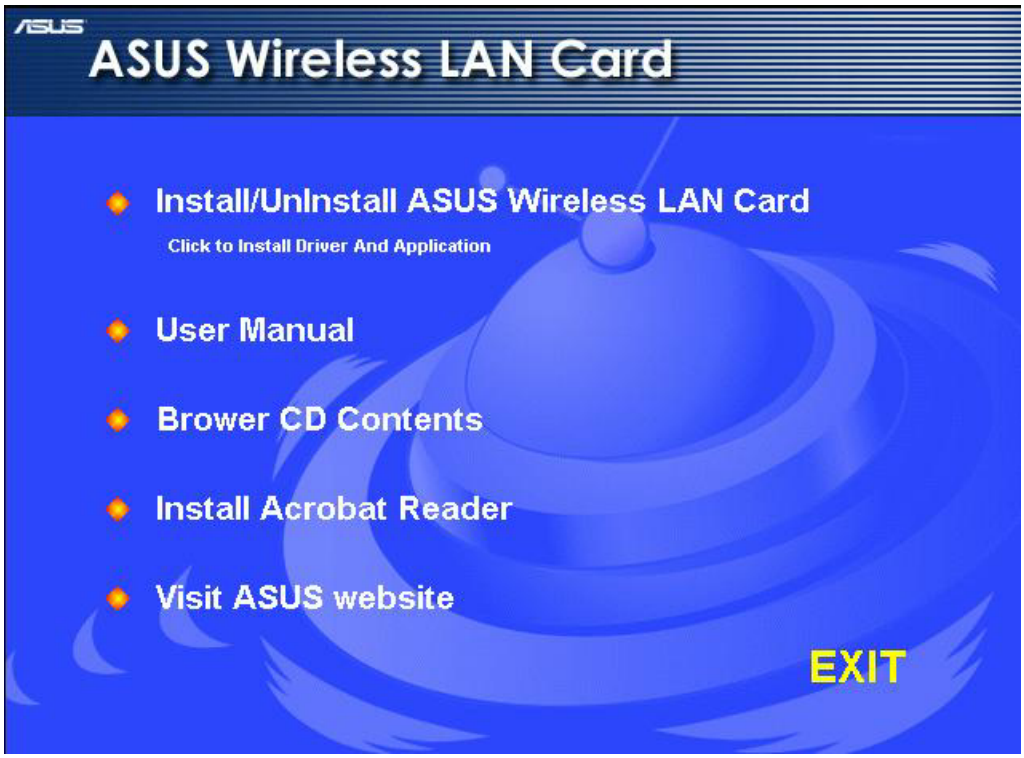
2.1 安装无线网卡

请将此网卡插入主机USB2.0接口。（USB2.0版本以下接口会影响此网卡的性能）

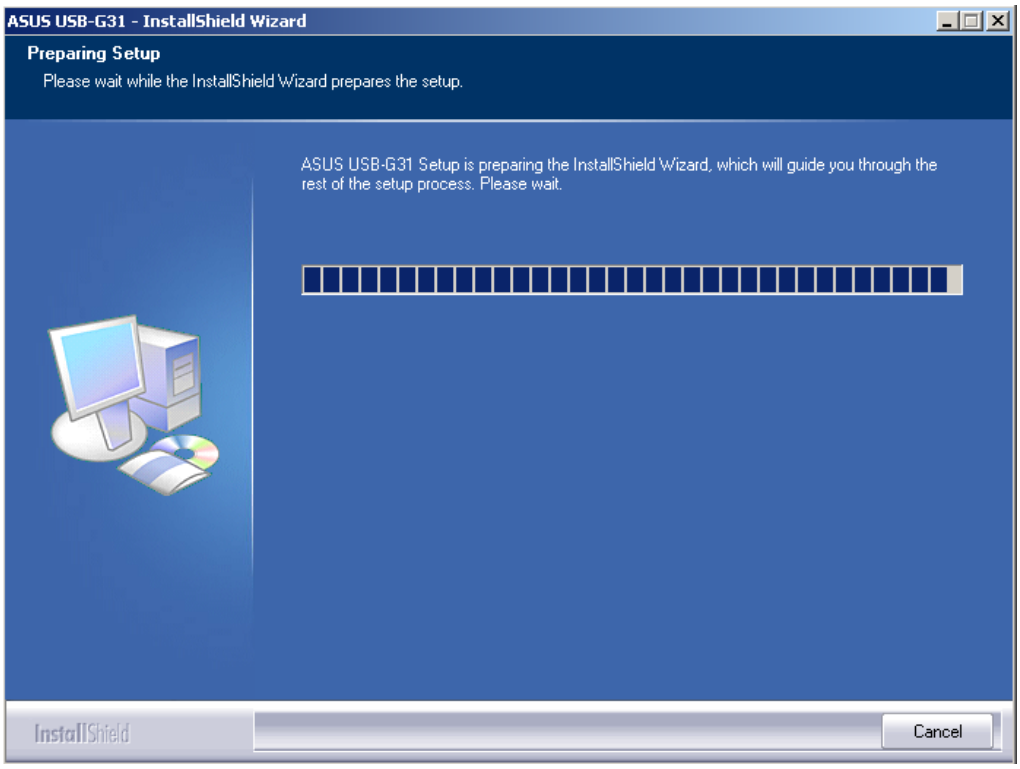
2.2 安装无线网卡驱动程序和应用程序

主机插入网卡后，系统自动搜索到新硬件，并弹出“Found New Hardware Wizard”，点击 Cancel 。

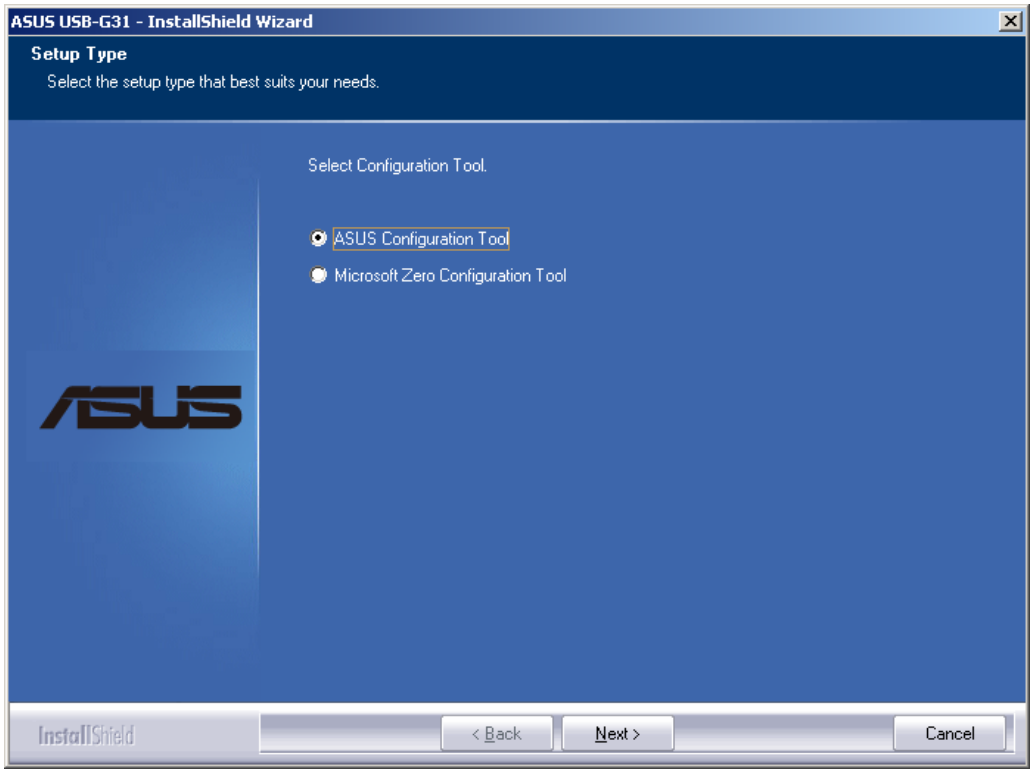
在光驱中放入驱动程序光盘，将自动进入安装向导，如下图所示。选择“Install/Uninstall ASUS Wireless LAN Card ”，可开始进行驱动程序的安装。如果没有自动进入安装向导，请点击光驱，选择浏览驱动光盘内容，双击“ASUS WLAN Setup.exe”图标也可进行驱动程序的安装。



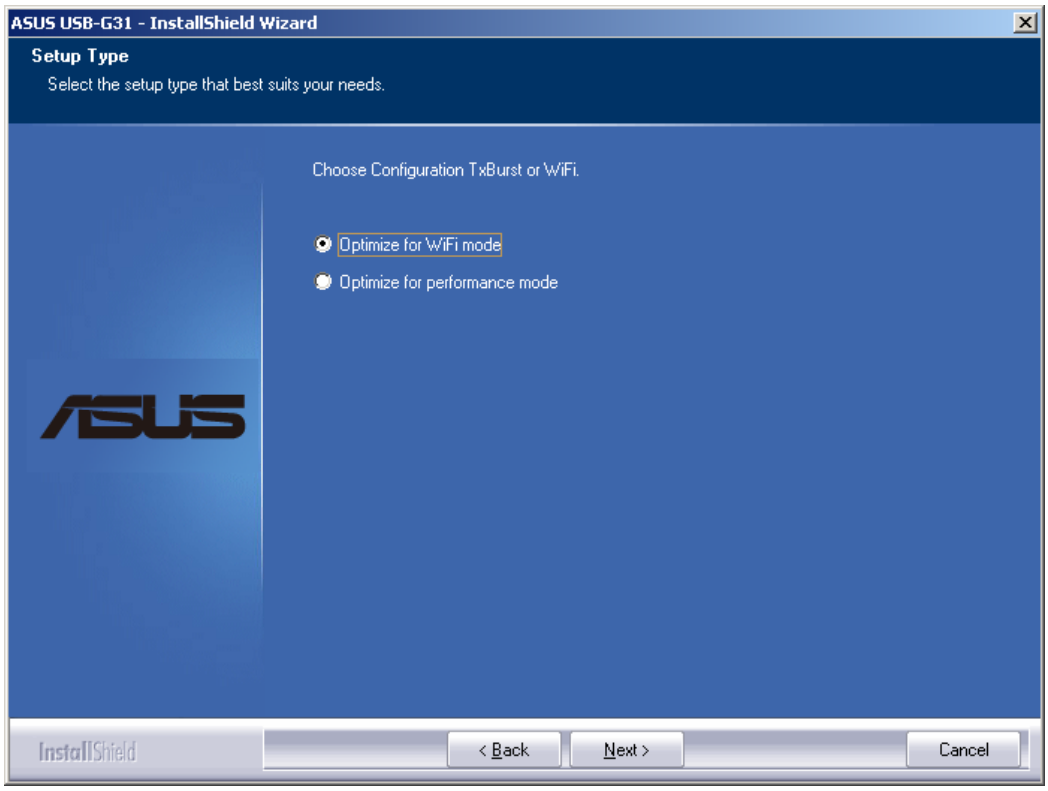
进入准备安装界面。



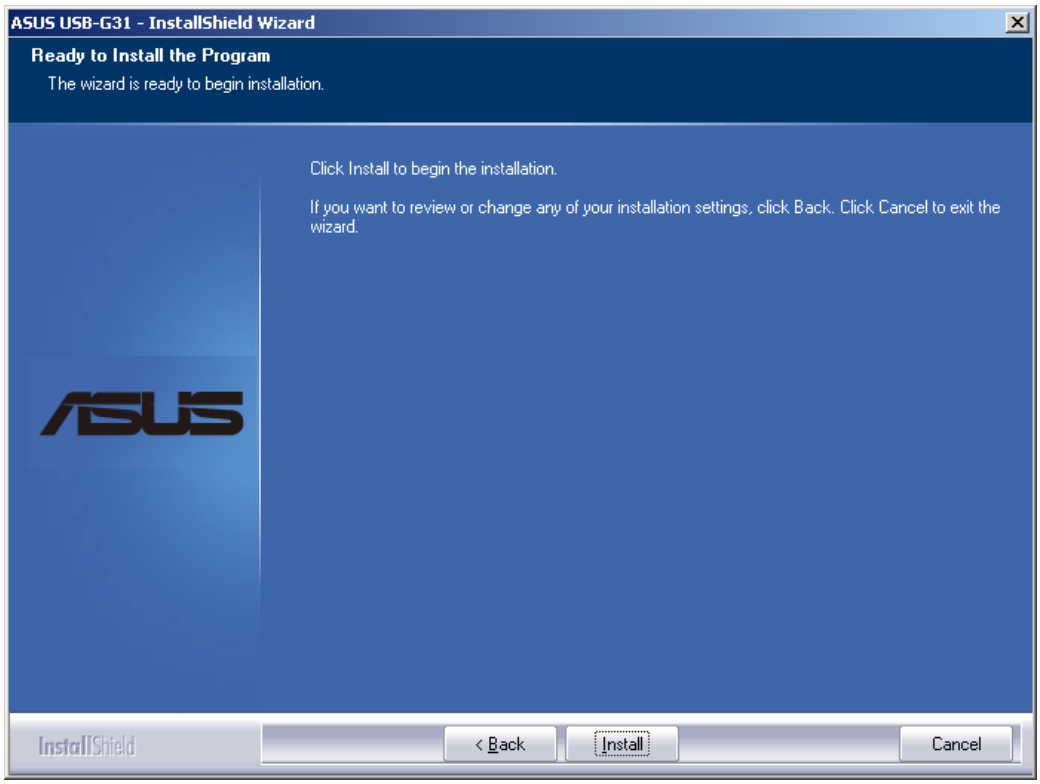
在WinXP和Win2000的平台上，提供了一个“ASUS Configuration Tool”，可对无线网卡进行设置。您可以选择默认配置工具模式。点击“Next”继续安装。



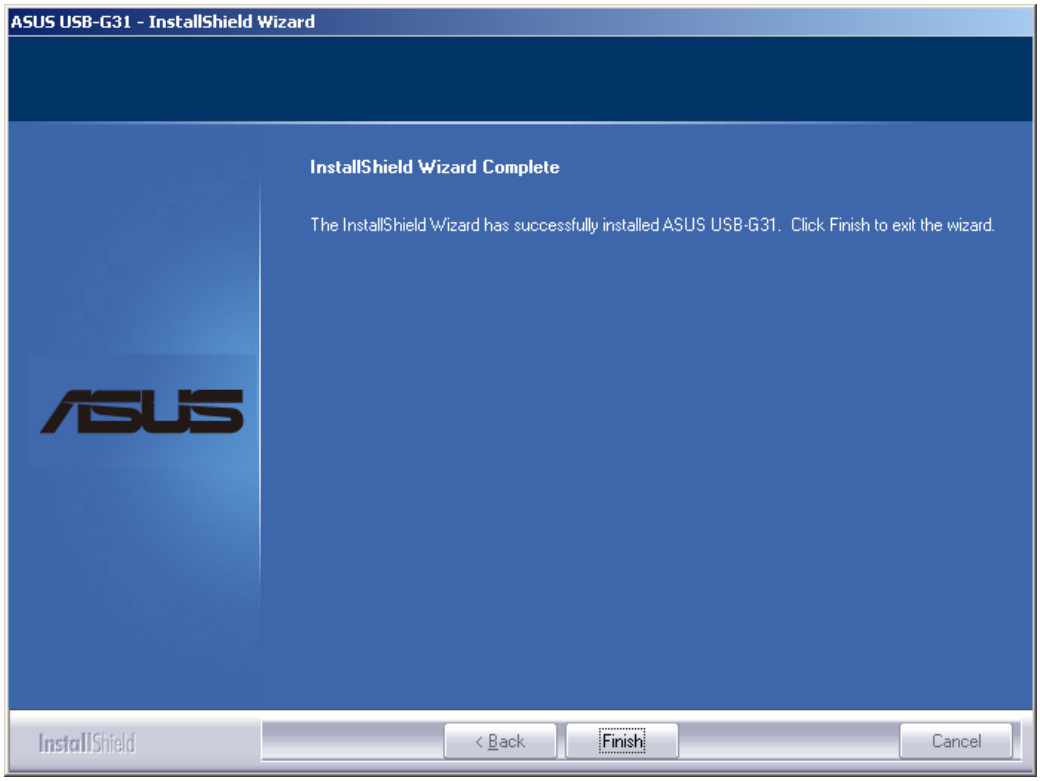
在WinXP和Win2000的平台上，可请根据需求选择是“Optimize for Performance Mode”优化处理突发模式，还是“Optimize for WiFi Mode”优化Wi-Fi模式，使网卡工作在更好的模式下，点击“Next”继续安装。



单击“Install”按钮，继续安装并进行相应的文件拷贝。



安装完成，请点击“Finish”结束。

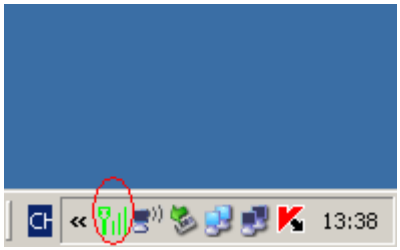


3. WinXP和Win2000下应用程序的使用

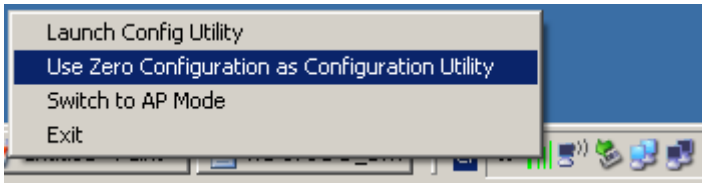
应用程序是管理无线网卡的一个工具，使用应用程序可以查看和修改无线网卡的配置，或监控您的无线网卡的运作状态。 此应用程序仅在WinXP和Win2000操作系统下有效。

3.1 打开应用程序

应用程序开启后，您可以在操作系统托盘看到如下图所示的图标。



右键单击该图标，出现打开应用程序、使用Windows自带程序、切换AP模式、退出四个菜单项。

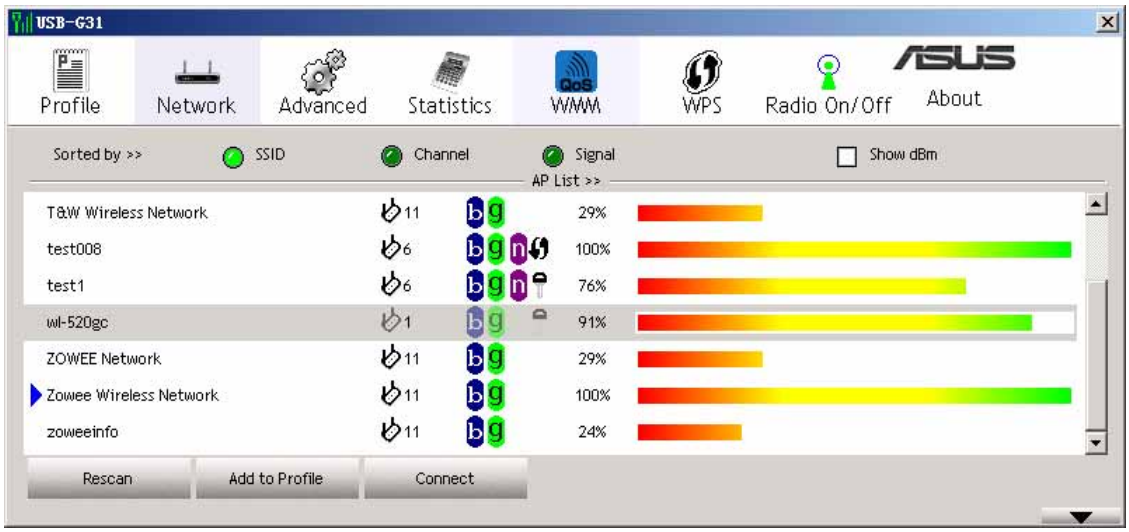


使用Windows自带程序指使用Windows默 认的无线管理程序，而不是ASUS的应用程序，第4 章会讲到使用Windows无线管理程序。

现在选择打开应用程序，出现应用程序主界面。可进行相应的参数设置页面，例如配置页面、无线网络、高级设置，统计信息、WMM、WPS、相关信息等。

3.2 无线网络连接

打开【Network】标签，此页显示了您的无线网卡连接的无线网络的状况。 可以根据需要，按网络名称、信道、信号强度进行排序。



- SSID -- 无线网卡已连接或准备连接的网络名称，上图表示无线网卡已连上SSID为RT2880_ch1的网络。
- BSSID -- 所连接AP 的MAC 地址或Ad Hoc 节点的基础服务设备 (BSS) ID。
- 信道 -- 显示网卡目前的信号频道。这个数字是变化的，因为信号会扫描可用的信道并不断更换。
- 信号强度 -- 显示网卡连接到AP的信号强度，默认用百分比表示，勾选show dbm后，信号强度会用dbm显示。
- 加密 -- 无线网络加密信息。网络中的所有设备都必须使用相同的加密方法来保证通信。

网络模式有两种：基本结构和点对点。

- 基本结构 -- 结构指的是使用AP 建立连接。一旦连接建立，AP 将允许您访问无线局域网和有线局域网（以太网）。若连接是基于结构模式的，信道(Channel) 栏内会显示自动。
- 点对点 -- 点对点指的是不使用AP 直接连接到无线客户端。点对点网络可以快速方便的建立，不需要预先规划，例如，让所有与会者在会议室共享会议内容记录。

无线网络连接步骤

- 重新扫描 -- 让无线网卡重新搜索所有可用设备。如果目前连接质量较低或信号强度较弱，重新搜索可以让网卡连接到信号质量更好的另一设备。这个功能通常需要几秒钟的时间。

- 连接 -- 从网络列表中选择需要连接的设备按钮进行连接。

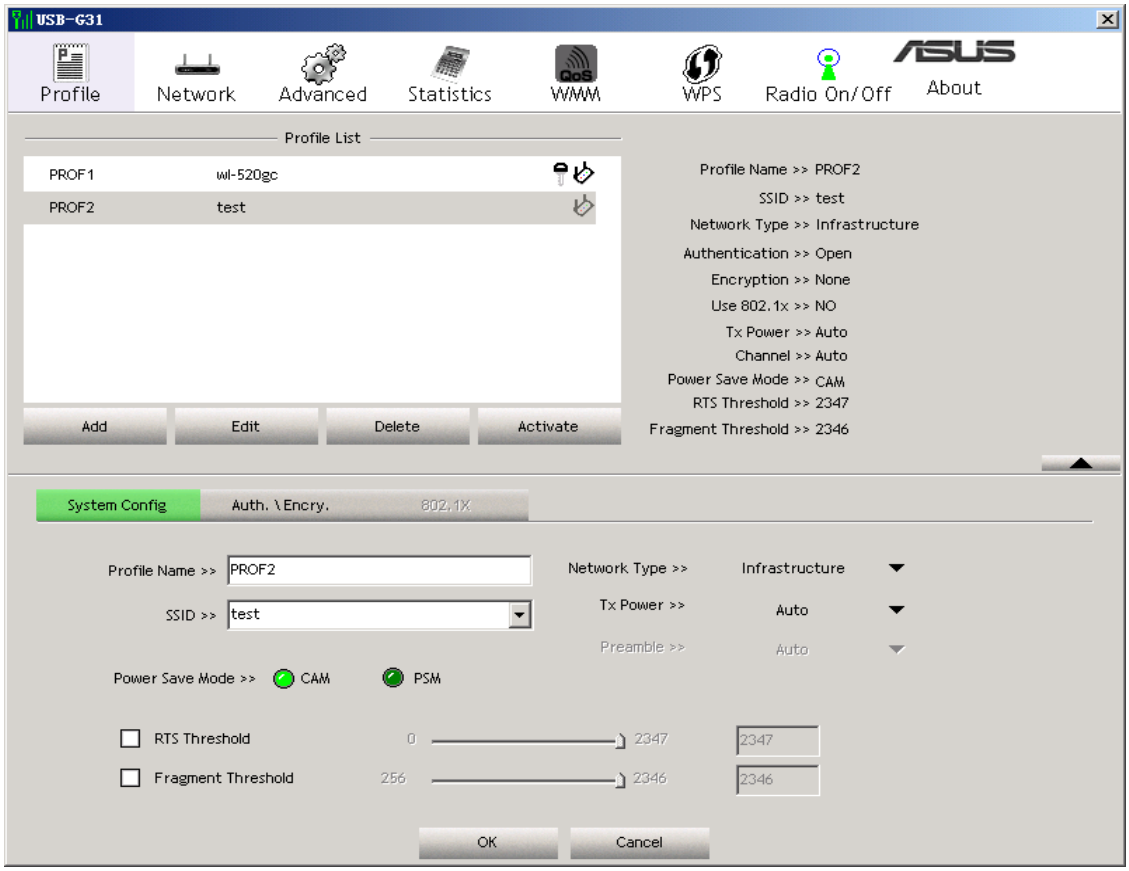
- 加密设置 -- 如果所要连接的设备已设置加密，需选择同所连设备相同的认证和加密方式，并向所连设备管理员获取密匙，并填入对应的密匙输入栏中。

3.3 添加到配置文件

将无线网卡搜索的可用设备的相应信息，与对应的设置保存成一个配置文件，简便以后的重复操作。

例如选择SSID为“wl-520gc”的设备，点击“Add to Profile”，输入保存成配置文件的名称，点击“OK”。在Profile栏可看到如下画面，表示Profile已配置成功。在此菜单中可对此Profile进行编辑、删除。也可在Profile列表中直接激活所要连接的网络设备。

也可以选择“Add”直接添加一个新的Profile文件，可手动输入Profile的名称，设备的SSID。



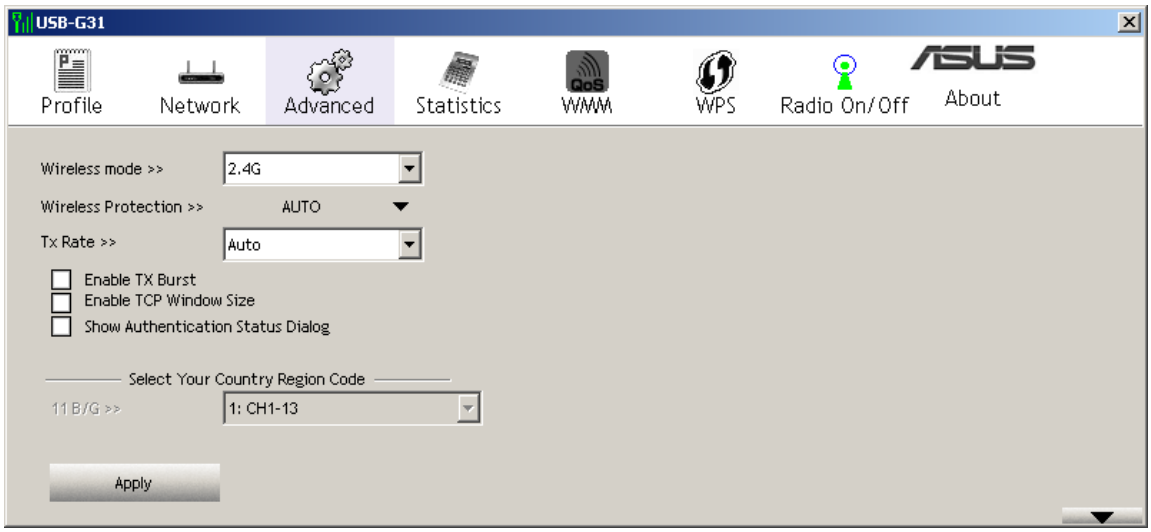
如果所要连接的网络设备有加密，需选择和连接设备相同的认证方式和加密方式，并向所连设备管理员获取密匙，并填入对应的密匙输入栏中。

3.4 连接状态

点击  ，确认无线网卡是否已连接到访问点。可查看Link状态，分配的IP以及Link Speed等信息。

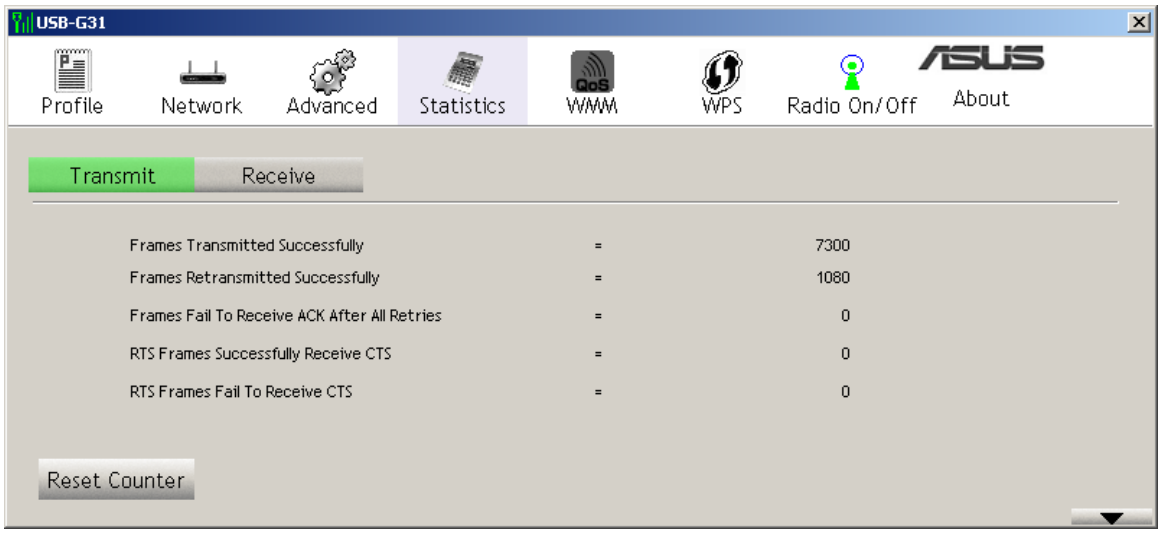
3.5 高级设置

单击【Advanced】标签，出现如下图页面，我们建议您不修改各项目，保持默认设置即可。

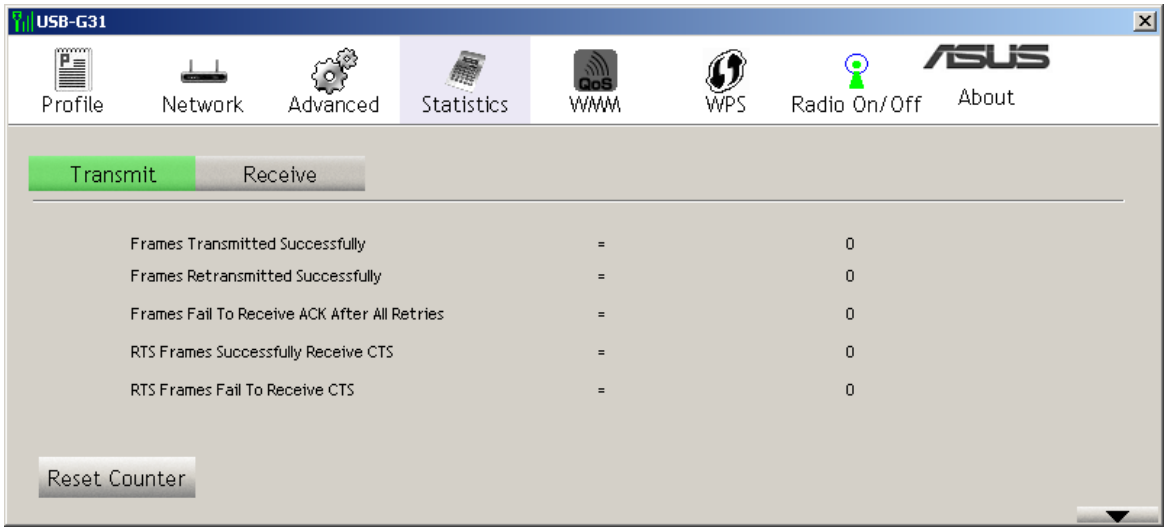


3.6 数据统计

单击【Statistics】标签页，可以看到下图显示信息，显示接收数据的统计情况，单击【Reset Counter】可将各项统计清零。

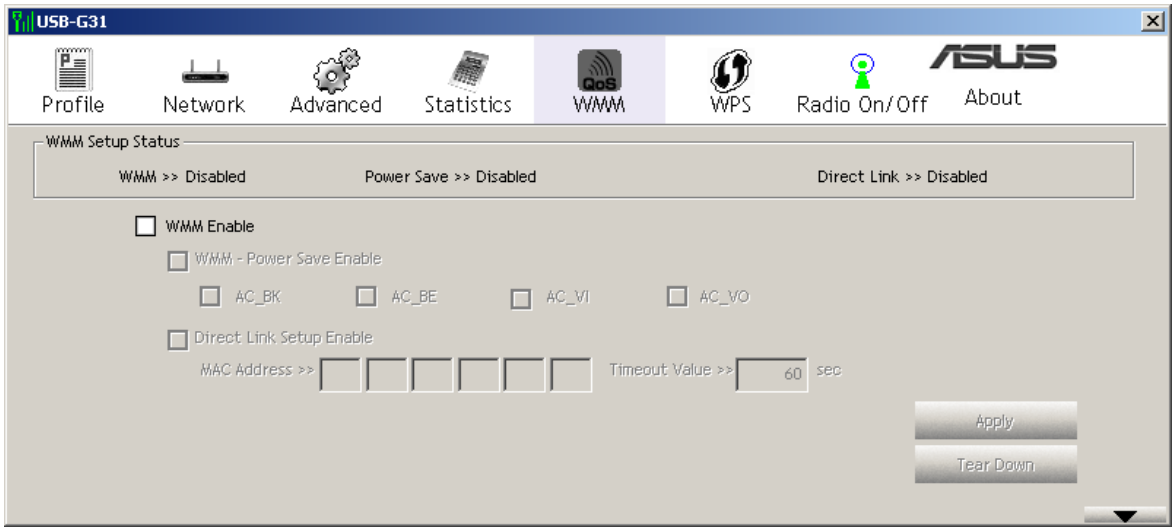


下图信息，显示发送数据的统计情况，单击【Reset Counter】可将各项统计清零。



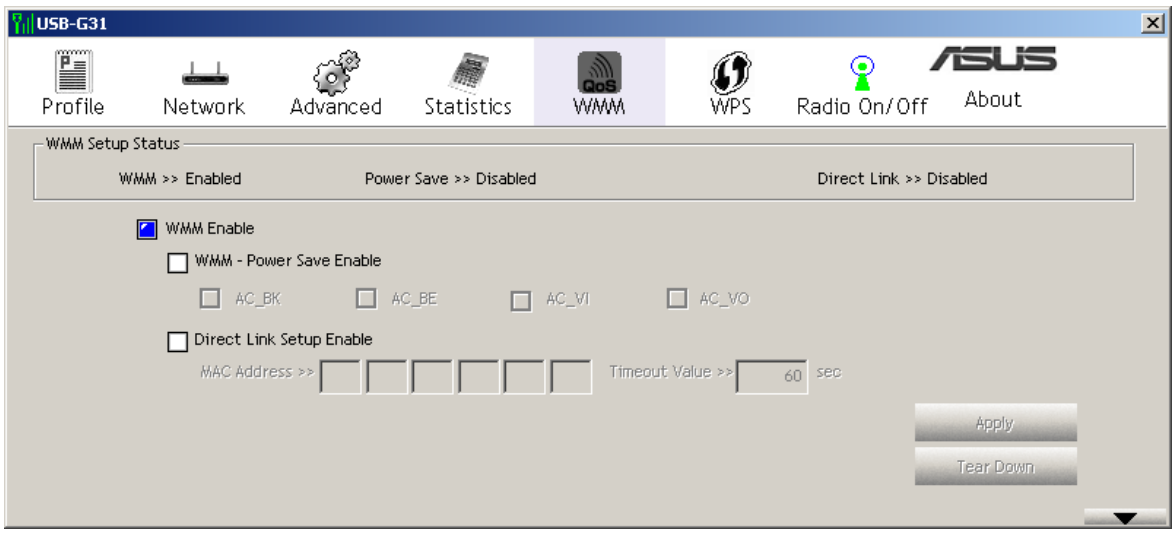
3.7 WMM

点击【WMM】标签页，可以进行相应的设置。包含WMM信息发送优先权设置，启用WMM省电模式，和DLS设置。如下图显示信息。

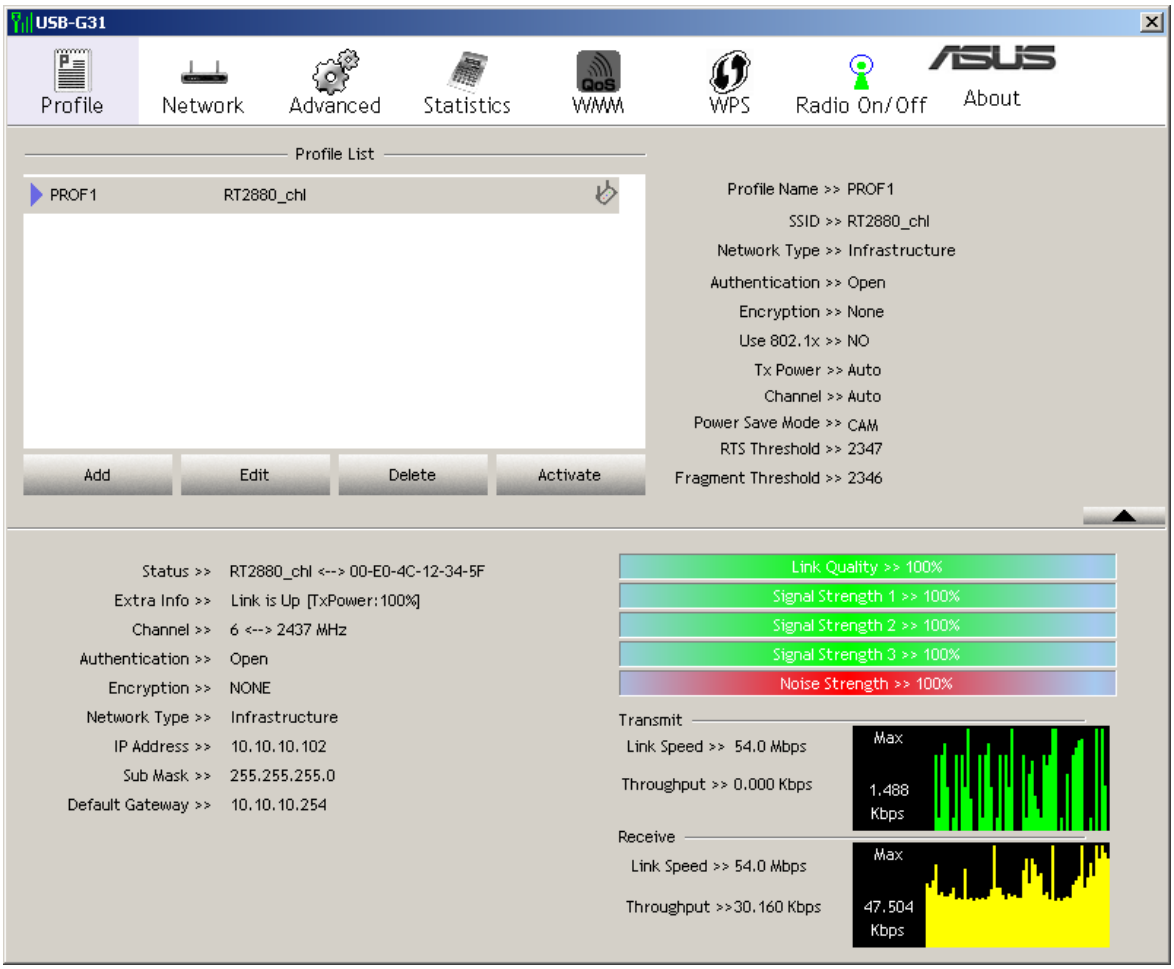


3.7.1 启用WMM: 启用Wi-Fi Multi-media

选择启动“WMM Enable”，如下图所显示

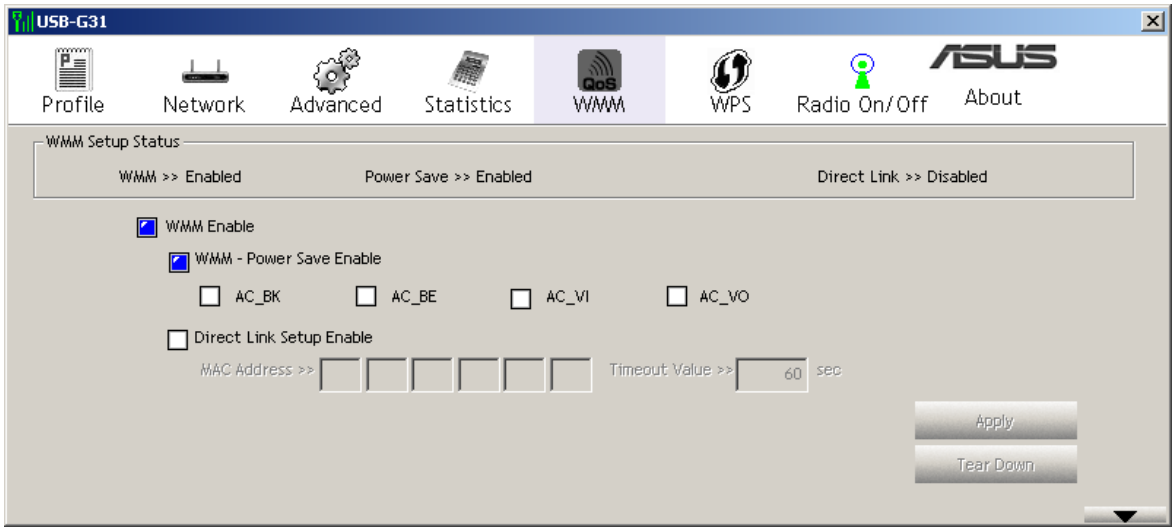


至【Network】功能页面中，将一台有支持WMM的AP，加入配置信息中，设置成功即可在【Profile】功能页面中看到下图。

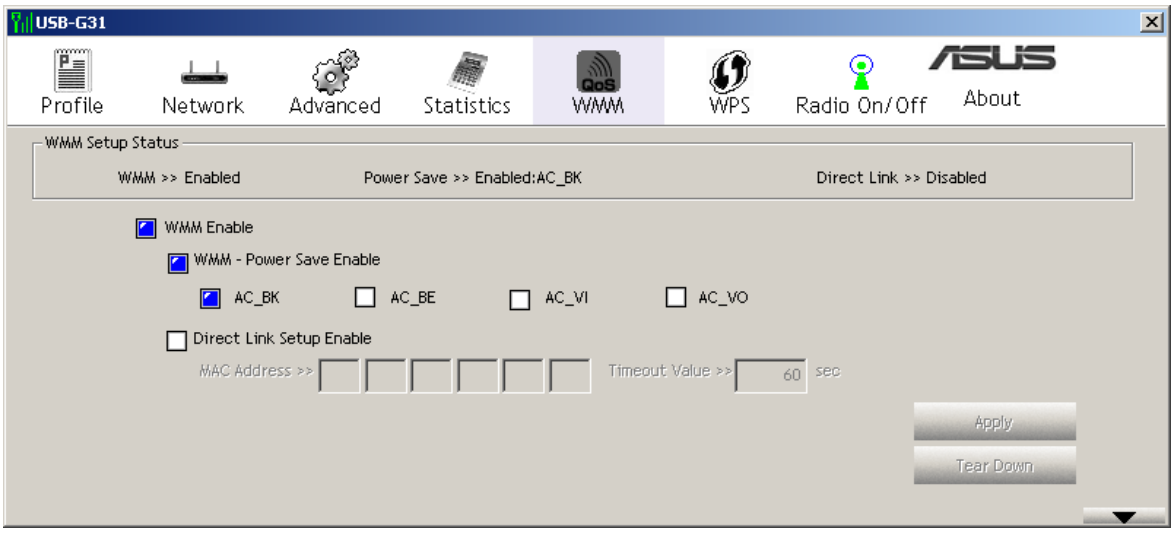


3.7.2 启用省电模式：启用WMM Power Save Mode

选择启动“WMM -Power Save Enable”，如下图所显示

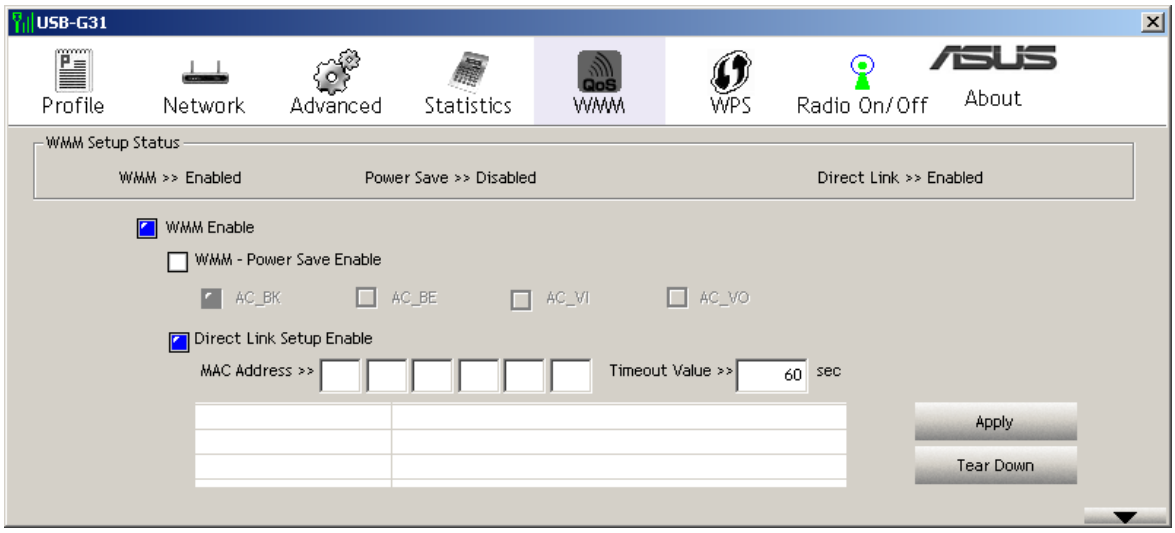


选择启动“AC_BK”，即设置成功。如下图所显示

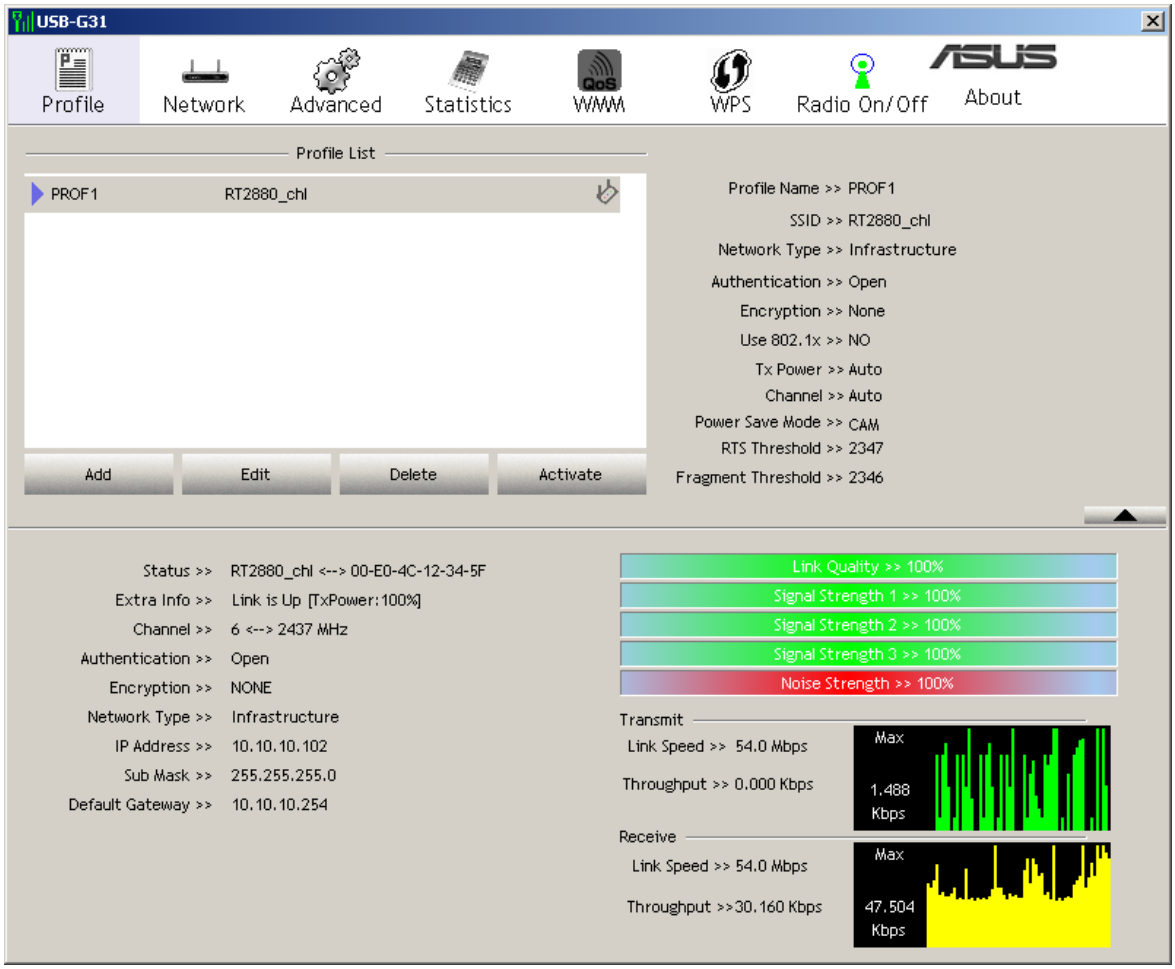


3.7.3 启用直接连接设置：启用DLS (Direct Link Setup)

选择启动“Direct Link Setup Enable”，如下图所显示



至【Network】功能中，将一台有支持DLS的AP，加入到配置信息中，设置成功即可在【Profile】功能页面中看到下图所显示。

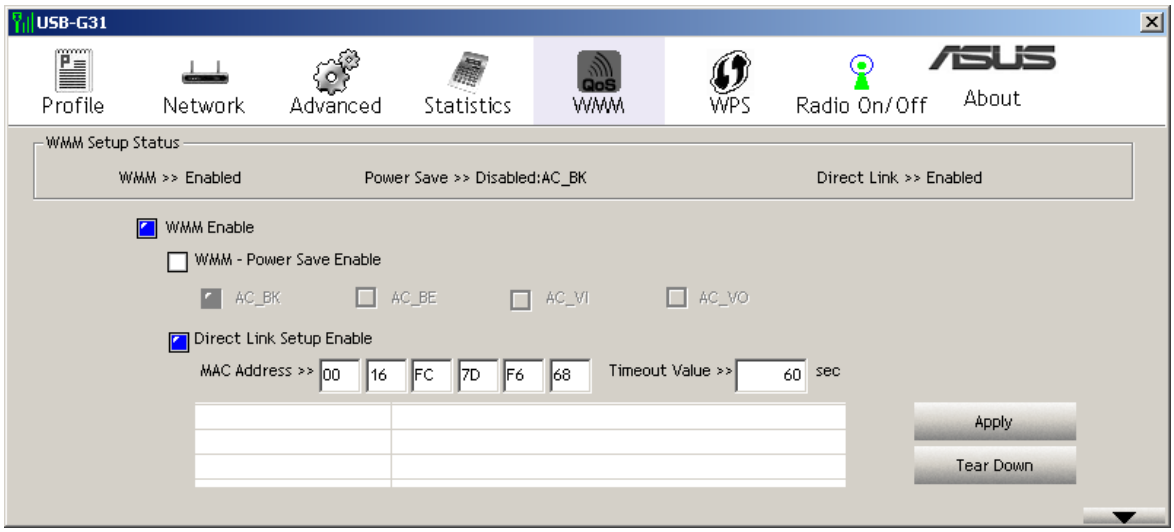


直接连接设置的方式如下：

填入一台STA的MAC地址，此STA必需满足以下条件：

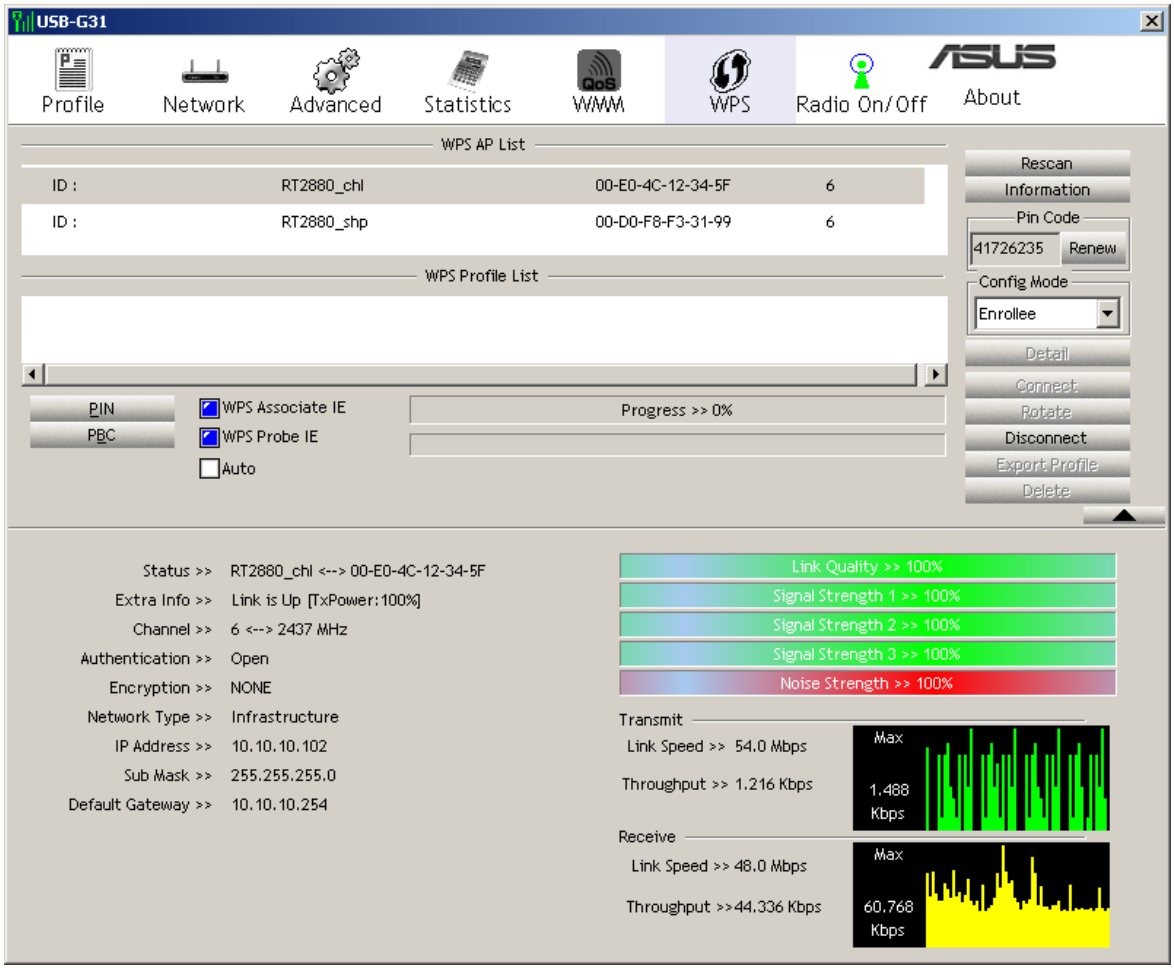
◆ 能和一台支持DLS的AP连接。

◆ 必须启用DLS功能。



3.8 WPS

点击【WPS】标签页面，可以进行相应的设置。WPS分成认证方法、加密方法、连接设置方式、密码ID、选择的受理注册机构、状态、版本、AP的连接安全设置、全域唯一识别码、射频等，如图所示



◆ WPS 设定- 简化 Wi-Fi 网络的规划和配置（ Wi-Fi Protected Setup ）。ASUS的 STA 是一个『登录者』（ Enrollee ）或是一个『受理注册机构』（ Registrar ），使用 PIN 或 PBC 方式，提供联机设定。

◆ WPS 无线网络 - 系统会去扫描带有 WPS IE 的 AP，然后将每个带有 WPS IE 的 AP 信息条列出来，列出的 AP 信息项目依序有：网络名称（SSID）、BSSID、频道、ID（装置密码 ID）、认证、加密。

◆ 重新扫描 - 重新扫描并更新目前所有 AP 的详细资料。

◆ 信息 - 显示所选带有 WPS IE 的 AP 的信息。列出的信息项目依序有：认证、加密、联机设定方式、装置密码 ID、受理注册机构（ Registrar ）、状态、版本、锁定 AP 的联机设定、全域唯一识别码元素、射频频带。其详细介绍如 AP 的 WPS 信息。

◆ Pin 码 - 在使用『PIN 联机设定方式』的时候，一个内部或外部的『受理注册机构』

（Registrar）所属的八个数字。在『受理注册机构』（Registrar）联机设定模式下，使用『PIN 联机设定方式』的时候，会被要求输入一组 PIN 码。ASUS 的 STA 是一个『登录者』（Enrollee）的时候，可以使用『更新』按钮，来重新产生一组 PIN 码。

◆ 联机设定模式 - ASUS的 STA 扮演一个『登录者』（ Enrollee ）或是『受理注册机构』（ Registrar ）的角色。

控制身份证明（ Credentials ）的项目：

◆ 内容：显示所选的身份证明（ Credentials ），有关安全和金钥的信息。

◆ 联机：联机身份证明（Credentials）所属的AP。套用所选择的身份证明（Credentials），如同套用所选择的联机设定。

◆ 轮换：以轮换的方式，联机下一个身份证明（ Credentials ）所属的AP。

◆ 中断联机：停止 WPS 动作，并且中断联机，然后会去联机上一次所套用所选择的联机设定。假如联机设定为空白或是未套用联机设定，则会去联机一台『Open』的AP。

◆ 汇出联机设定：将得到的所有身份证明（ Credentials ）加入联机设定中。

◆ 删除：删除所选择的身份证明（ Credentials ），然后会去联机下一个身份证明（ Credentials ）所属的AP。假如联机设定的表格为空白，则会去联机一台『Open』的AP。

◆ PIN：使用『PIN 联机设定方式』开始或增加一个联机设定。

◆ PBC：使用『PBC 联机设定方式』开始或增加一个联机设定。

◆ 当您按下『PIN』或『PBC』按钮，请不要在两分钟内做任何的重新扫描。如果想要取消这个设定，请重新开始 PIN/PBC 或按下『中断联机』来停止 WPS 动作。

◆ WPS 连结 IE - 在 WPS 联机设定期间，传送一个带有 WPS IE 的连结 IE。对于STA，这是一个可勾取或可不勾取的选项。

◆ WPS 探索 IE - 在 WPS 联机设定期间，传送一个带有 WPS IE 的探索 IE。对于STA，这是一个可勾取或可不勾取的选项。

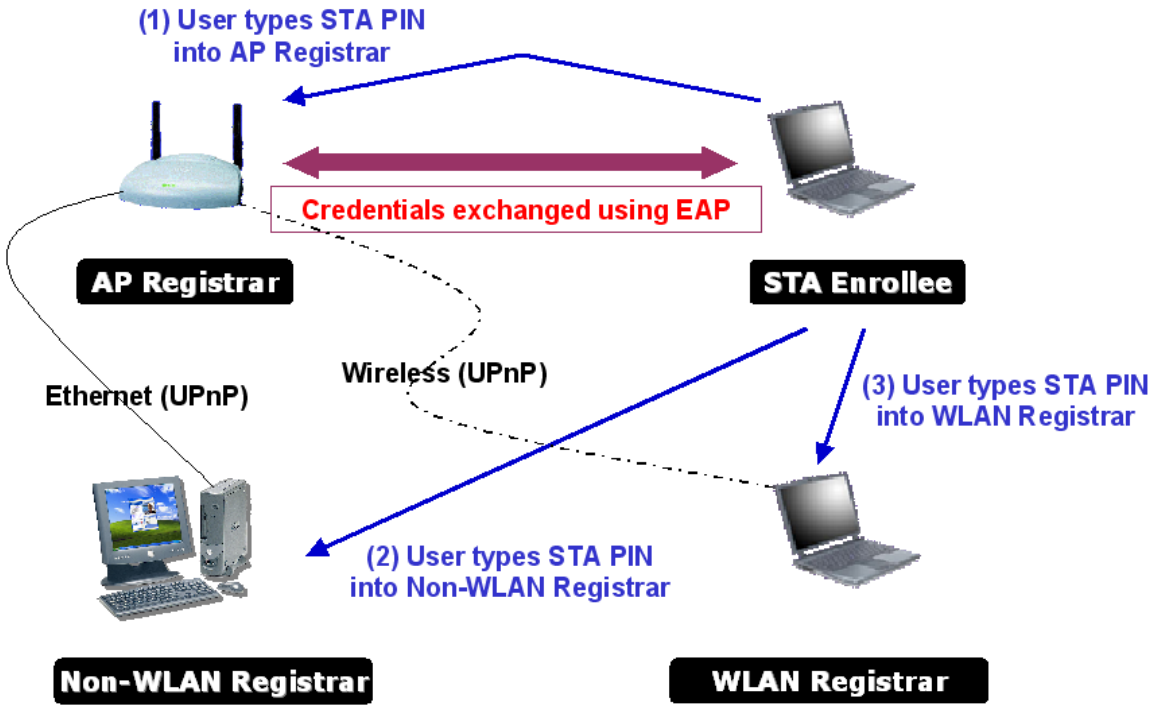
◆ 进度列 - 显示从开始到联机成功状态的进度比例。

◆ 状态列 - 显示现在的 WPS 状态。

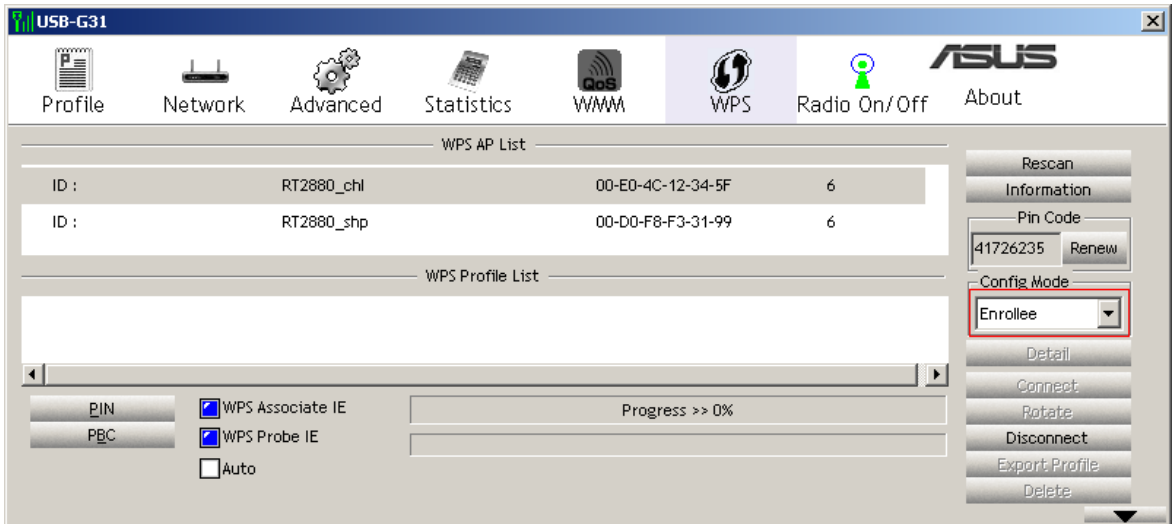
◆ 自动选择 AP - 使用『PIN 联机设定方式』的时候，自动选择一台 AP 开始联机。

3.8.1 使用Pin连接模式进行连接设置

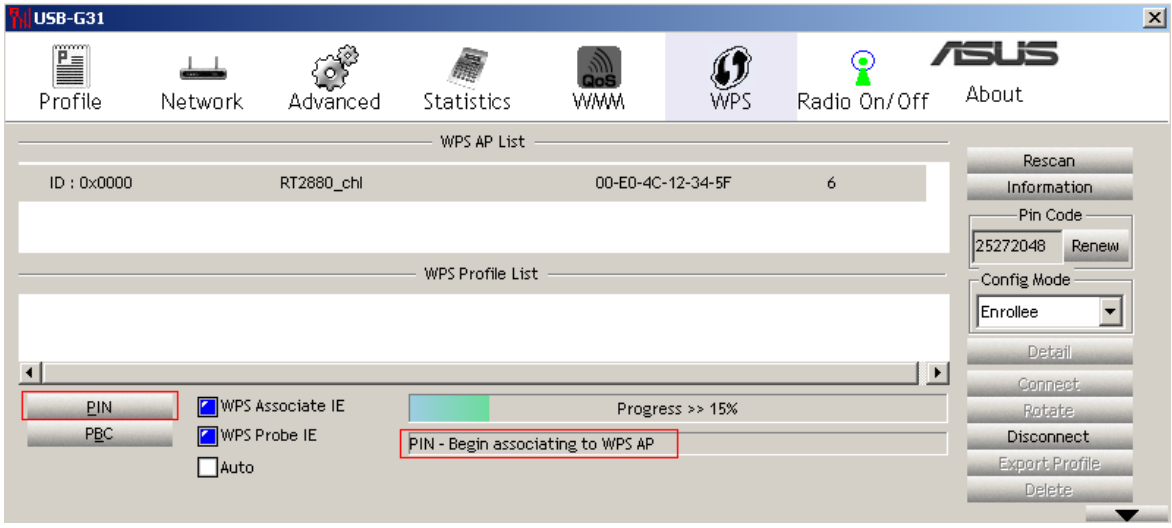
登录者从STA得到一组密码(Pin密码)，将这些密码输入到受理注册机构。在这个连接设置中，『登录者』和『受理注册机构』都必须使用 PIN 连接设置方式。详细设置方法如下图



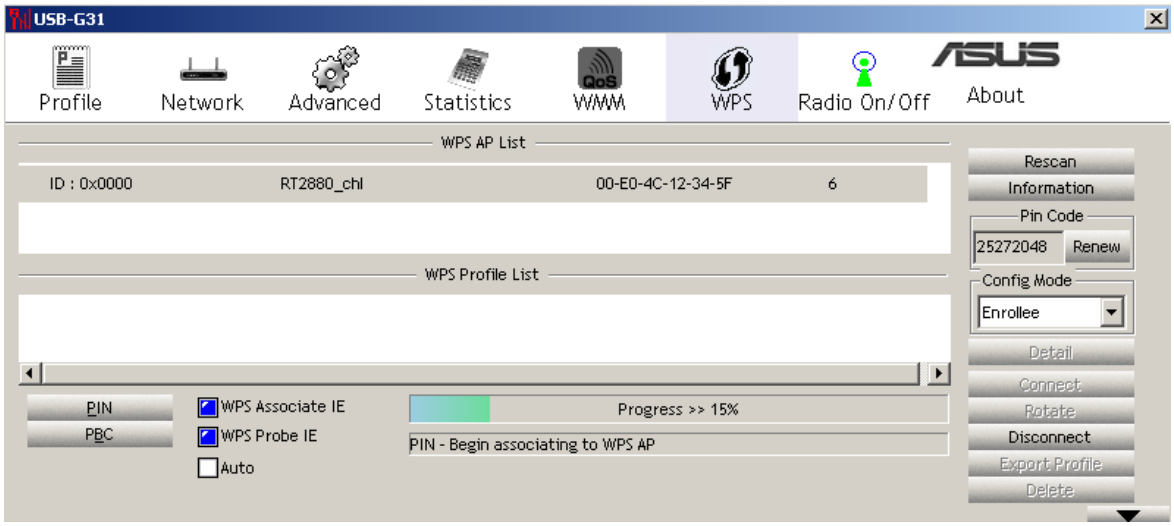
在配置模式中，选择登录者，并“Rescan”更新可使用的AP



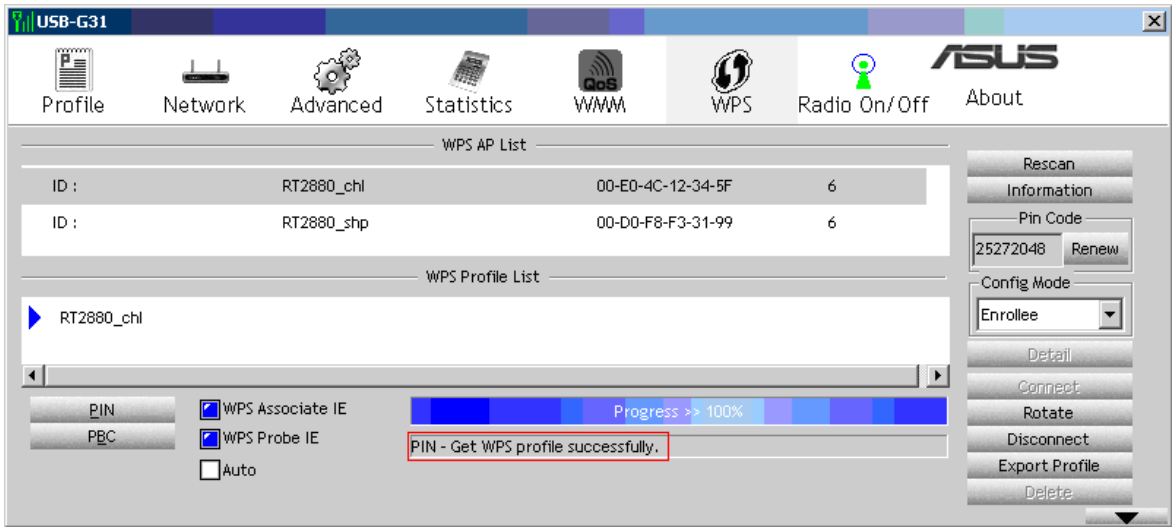
选择一台您想要加入的AP，并点击按钮“PIN”，输入STA提供的PIN码到受理注册机构



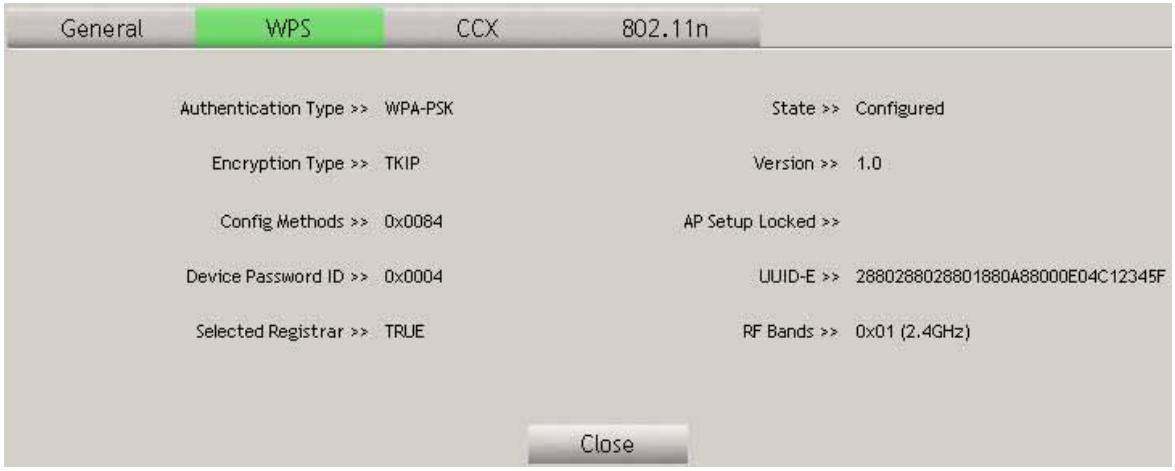
假如您使用共享因特网联机来当做外部的受理注册机构，在 STA 端必须先开始『PIN 联机』，然后必须在微软的受理注册机构中找出 WPS 的装置名称和MAC地址，接着在微软的受理注册机构中加入一个新的装置和输入 STA 的 Pin 码。设置成功如下图



联机设置得到一组或更多组的身份证明（ Credentials ）。成功联机如图所显示内容



联机设置成功的详细内容如图所显示



◆ 如果第一个身份证明（Credentials）是有效并且存在的，系统将会连上第一个身份证明（Credentials）的 AP。相反地，系统会自动连上下一个身份证明（Credentials）的 AP。

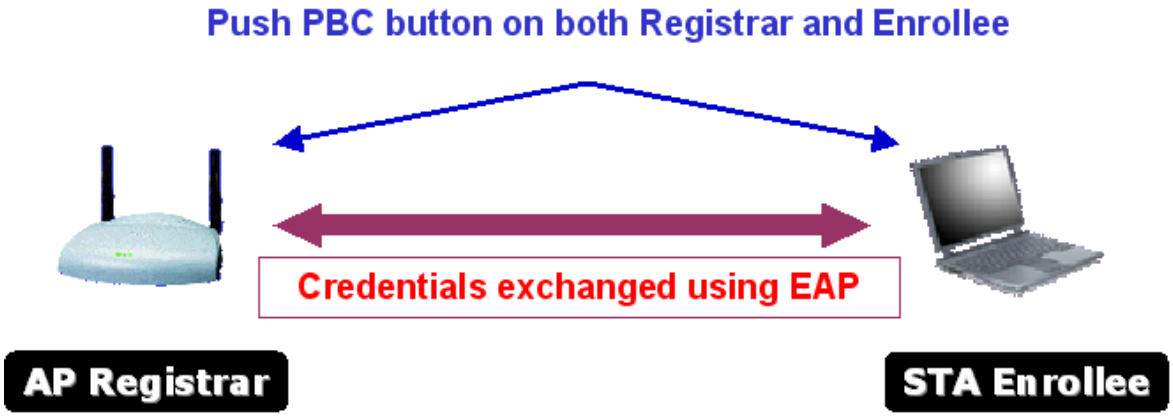
◆ 您也可以按下『Rotate』的按钮，指示轮换联机下一个身份证明（Credentials）的 AP。

3.8.2 使用PBC连接模式进行连接设置

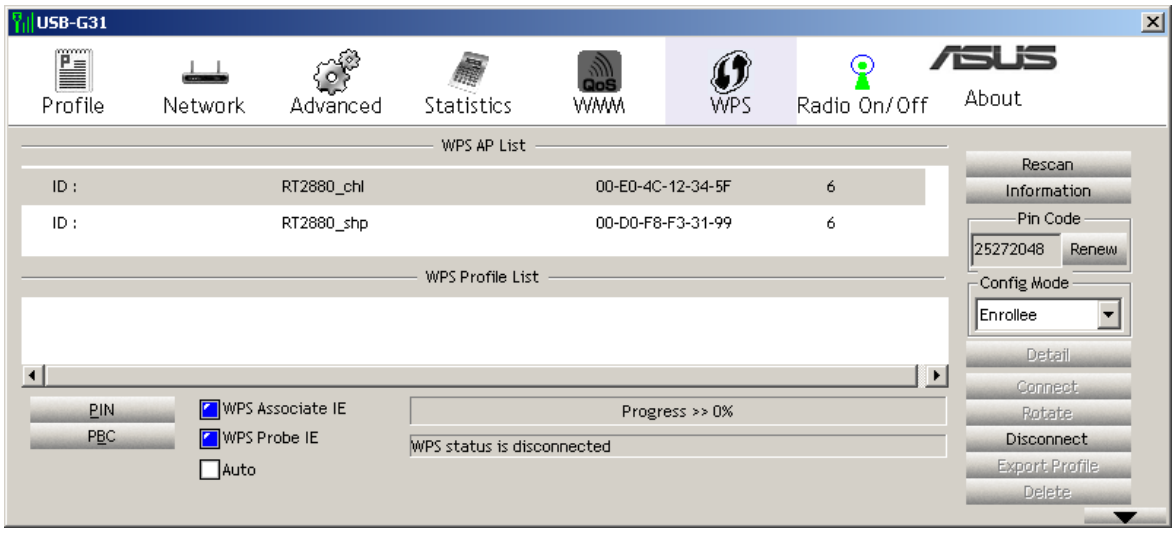
PBC 联机设置方式要求『登录者』和『受理注册机构』两者需在二分钟内按下『PBC』按钮，其称为这二分钟为『漫游时间』。在 PBC 联机设定方式中，只能有一个受理注册机构被扫描到，它带有 ID 为 0x0004，然后『登录者』立即执行注册协议。

如果『登录者』发现有二台以上的『受理注册机构』，则它会取消这次扫描的联机，然后继续扫描直到超过二分钟。

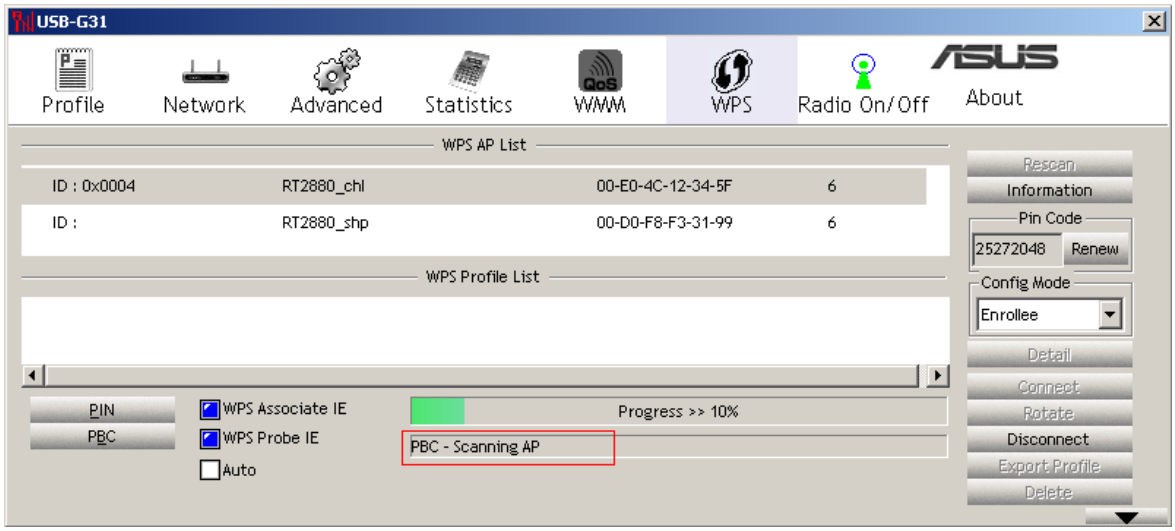
在按下『PBC』按钮和欲联机的 AP 之前，确定所有其它的 AP 都不是 PBC 的联机设置方式，或者使用 PBC 联机设定方式的 AP 都已经超过所属的『漫游时间』。



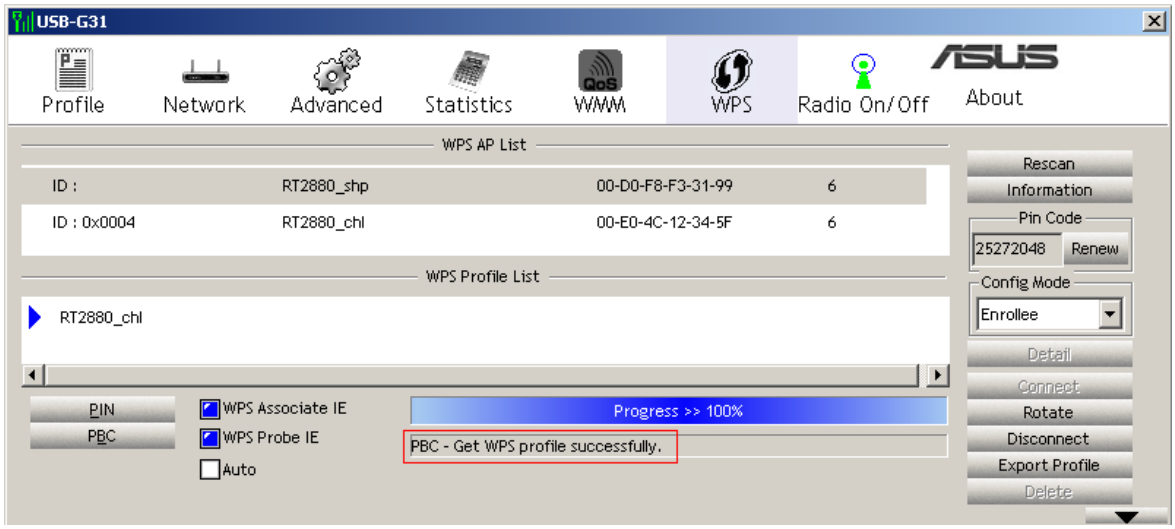
在配置模式中，选择登录者。并按下按钮“PBC”开始联机



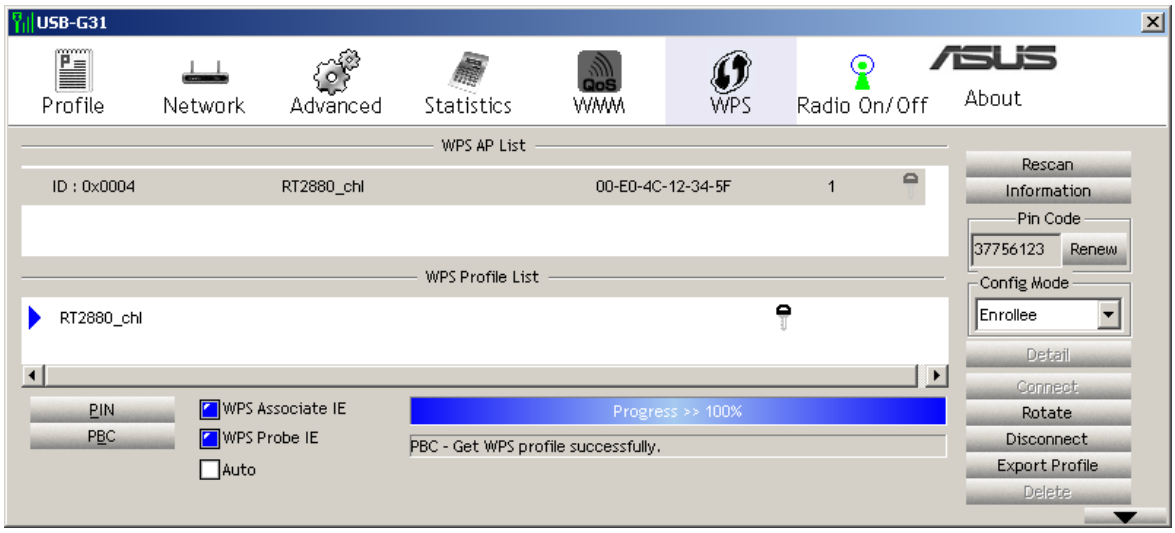
选择一台AP进行PBC连接，如下图



确定此AP拥有有效WPS功能，如下图所示

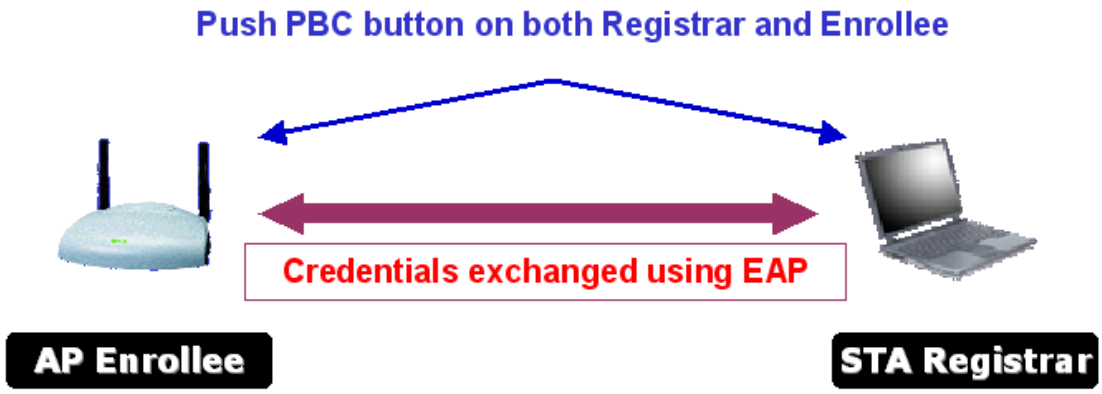


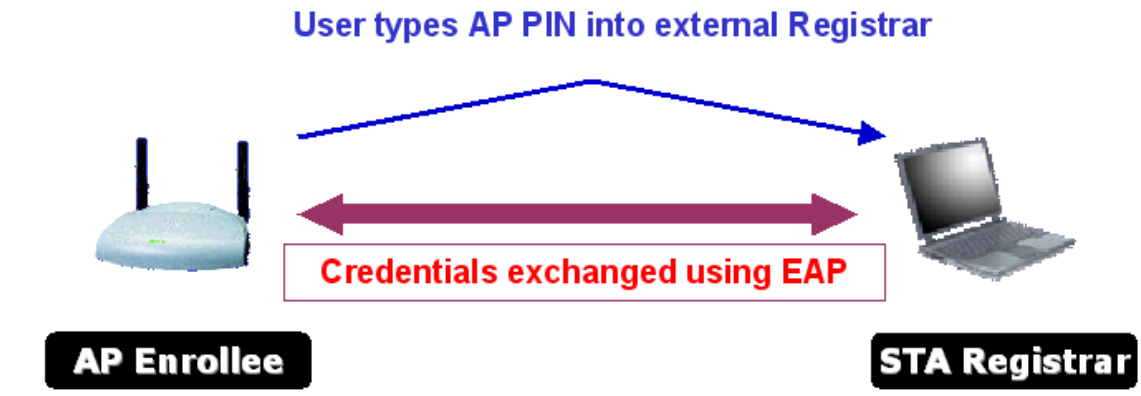
联机设置得到一组或更多组的身份证明（ Credentials ）。成功联机如图所显示内容



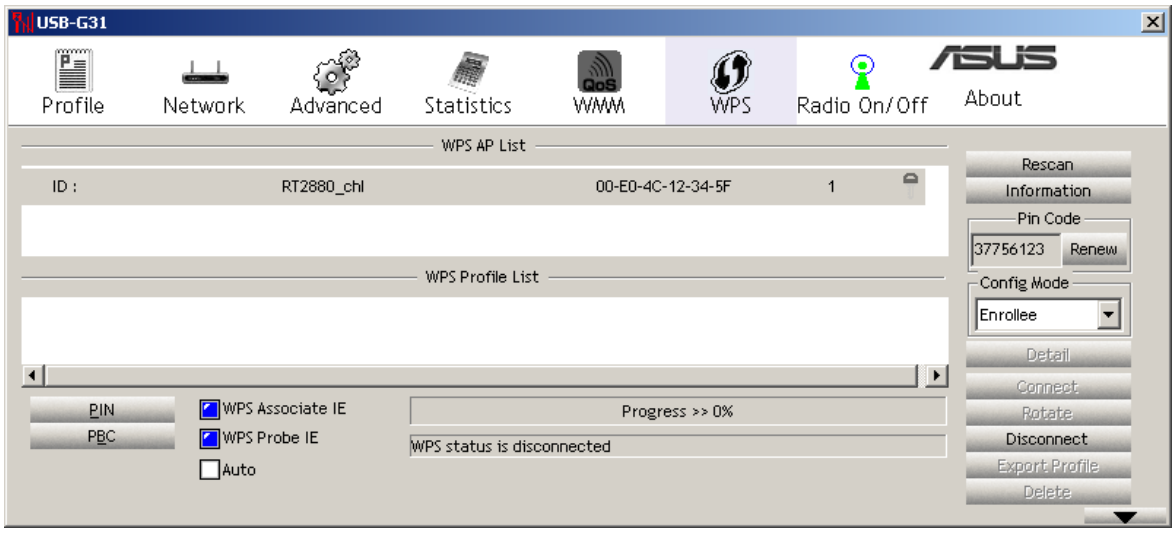
3.8.3 使用PIN或者PBC连接模式进行连接一台AP 或者一台网络

使用PIN或者PBC连接模式进行连接一台AP 或者一台网络的事例图

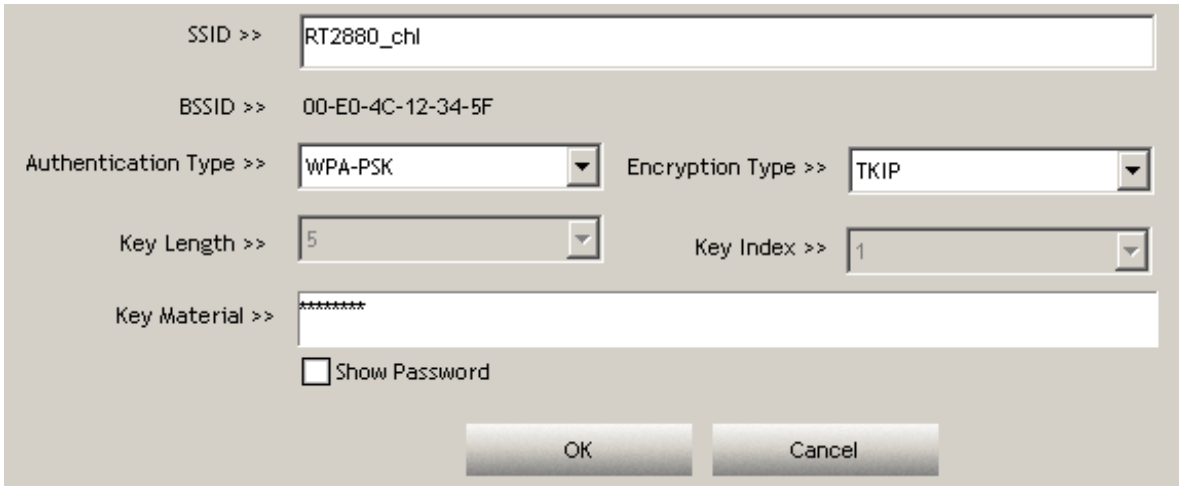




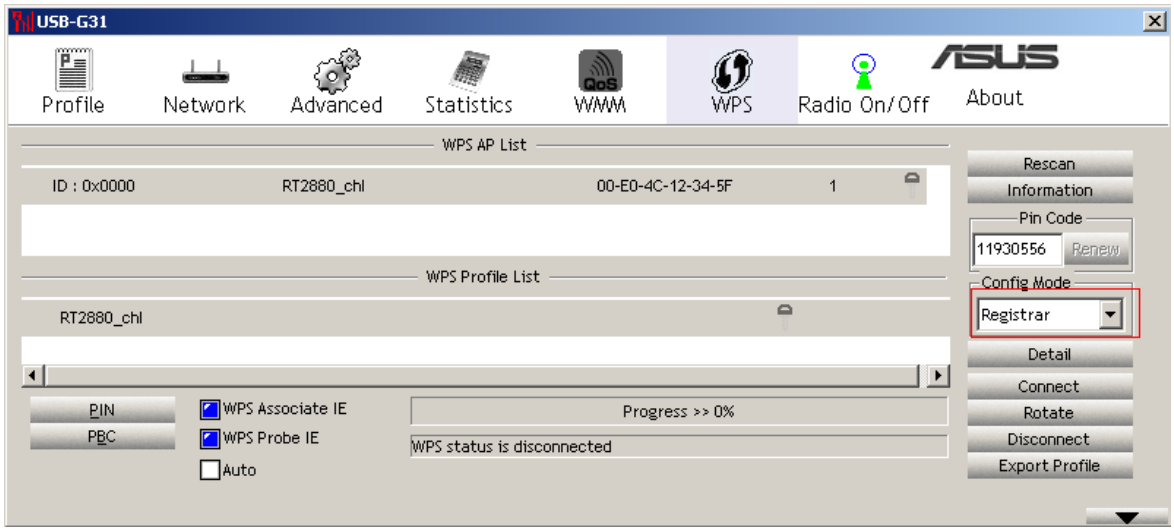
在配置模式中，选择受理注册机构，如图



在如果需要更改 SSID、认证方法、加密方法和密钥，请按下『Detail』按钮，手动更改其内容。

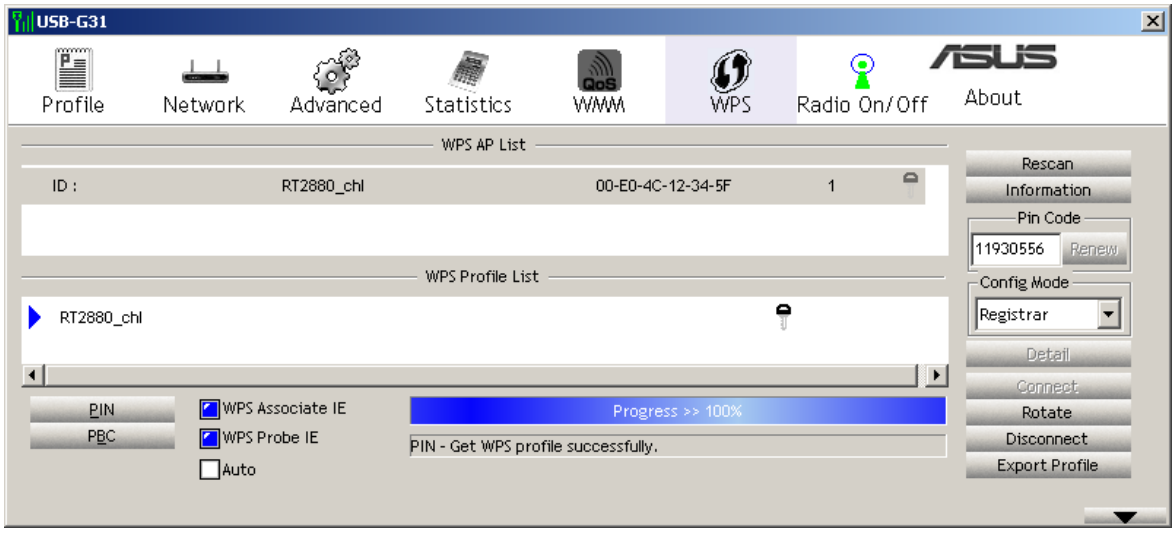


如果使用『PIN 联机设置方式』，请输入『登录者』的 PIN 码。



开始一个『PIN 联机设定』或『PBC 联机设定』。接下来的设置，如同3.7.1(登录者模式 PIN 设置)或3.7.2(登录者模式 PBC 设置)。

如果『登录者』在执行 WPS 之前，已经联机设定，则身份证明（Credentials）被更新成『登录者』的设定；否则在注册成功后，『登录者』使用新的参数重新联机设定，然后 STA 『受理注册机构』将会使用新的参数和 AP 做联机。如图



『WPS』-『PIN - xxx』详细设置如下：

一个成功的 PIN 联机设置：

Start PIN connection - SSID -> Begin associating to WPS AP -> Associated to WPS AP -> Sending EAPOL-Start -> Sending EAP-Rsp (ID) -> Receive M1 -> Sending M2 -> Receive M3 -> Sending M4 -> Receive M5 -> Sending M6 -> Receive M7 -> Sending M8 -> Receive EAP-Rsp (Done) -> Sending EAP Rsp (ACK) -> Configured -> WPS status is disconnected -> WPS status is connected successfully-SSID

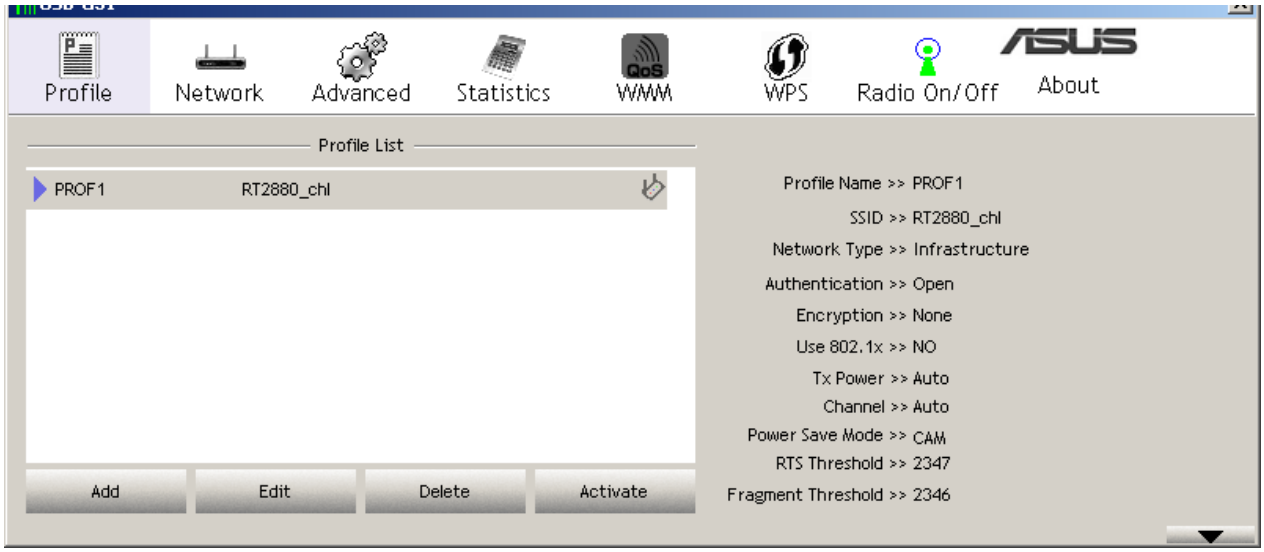
『WPS』-『PBC - xxx』详细设置如下：

一个成功的 PBC 联机设置：

Start PBC connection -> Scanning AP -> Begin associating to WPS AP -> Associated to WPS AP -> Sending EAPOL-Start -> Sending EAP-Rsp (ID) -> Receive M1 -> Sending M2 -> Receive M3 -> Sending M4 -> Receive M5 -> Sending M6 -> Receive M7 -> Sending M8 -> Receive EAP Rsp (Done) -> Sending EAP-Rsp (ACK) -> Configured -> WPS status is disconnected -> WPS status is connected successfully-SSID

3.9 配置文件

【Profile】页面保存了您对各个无线网络的配置或者对同一网络的不同配置。



◆ 删除 -- 删去不用的配置文件。

◆ 编辑 -- 用来修改无线网络配置。

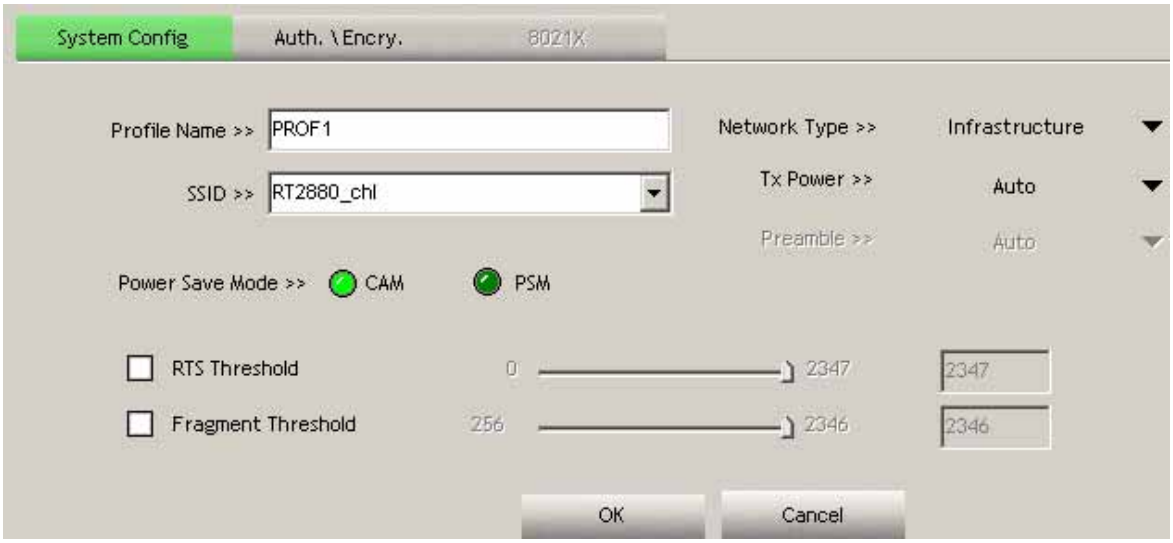
◆ 激活 -- 在多个配置文件中选择适用于当前网络的配置。

◆ 新增 -- 用来增加新的配置。

【System Config】

RTS 阈值 --RTS/CTS (Request to Send/Clear to Send) 功能用于将无线基站之间的冲突到降至最小。当RTS/CTS启动时，路由器会重复发出数据帧直到另一个RTS/CTS握手完成。您可通过设置特定的封包大小上限值来启动 RTS/CTS 功能。建议您使用默认值(2347)。

帧阈值 -- 帧阈值用来将 802.11 帧分成更小的片段（段），并将他们独立地送至目的地。您可以指定封包大小的上限值来开启分割功能。如果无线网络中存在大量冲突，您可以设置不同的上限值来进行试验，以增加帧传输的可靠性。对于一般的使用，建议使用默认值(2346)。



【Auth.\Encry.】

这个页面允许您进行无线网卡的加密和身份验证设置。

对于无线环境中的数据安全，IEEE 802.11 规定了WEP（有线等效加密）协议以保证传输的保密性。WEP 采用密钥来加密或解密数据包。加密过程打乱了帧的顺序以避免对他人泄露。WPA/WPA2 则是改进的

802.11 安全系统 ，克服了WEP 协议的缺陷。 身份验证模式 由于无线网络不存在精确的边界，无线网络用户需要补充特定的

设置来提供安全措施。本标签页中的认证方式提供了不同的保护等级，如开放，共享密钥，WPA，WPA-PSK，WPA2，WPA2-PSK。

◆ 开放 –选择这个选项使网络运行于开放系统模式，不使用任何认证法则。开放式基站和 AP 可以相互认证，即使存在 WEP 密钥，也不需要验证。

◆ 共享密钥- 选择这个选项使网络运行于共享密钥模式。在共享密钥认证系统中，需要进行四步帧交换来确定基站是否与 AP 采用同样的 WEP 密钥。

◆ WPA-PSK/ WPA2-PSK - 选择这个选项来允许在结构模式下使用 WPA Pre-Shared 密钥。它允许您在客户端和 AP 之间使用 WPA-PSK/WPA2-PSK 加密方式。

◆ WPA/ WPA2 – 网络使用 IEEE 802.1x 认证方式。这种方式用于 RADIUS（Remote Access Dial-in User Service，远程拨入用户服务）环境。RADIUS 环境支持多种扩展认证协议（EAP），包括 PEAP,TLS/Smart Card, TTLS。

数据加密

在开放和共享密钥认证模式下，加密类型的选项有禁用和WEP。在WPA, WPA-PSK, WPA2 和 WPA2-PSK 认证模式下，支持 TemporalKey Integrity Protocol (TKIP) 加密和 Advanced Encryption Standard (AES) 加密。

◆ 禁用 -- 禁用加密功能。

◆ WEP --WEP 密钥是在数据无线传输之前进行加密。您只能与使用相同 WEP 密钥的无线设备进行通信。

◆ TKIP --TKIP 使用比 WEP 更严格的加密法则。它也是采用既有的 WLAN 算法来实现加密。TKIP 会在加密密钥确定后校验安全设置。

◆ AES --AES 是一种对称的 128 位块加密技术，可同时工作于网络中多个层。

WPA共享密钥

这个选项只有当您选择了 WPA-PSK 或WPA2-PSK 认证模式时才可以启用。在【数据加密】区域选择“TKIP”或“AES”加密模式以开始加密过程。注意：这里需要输入8-64个字母。

密钥设置

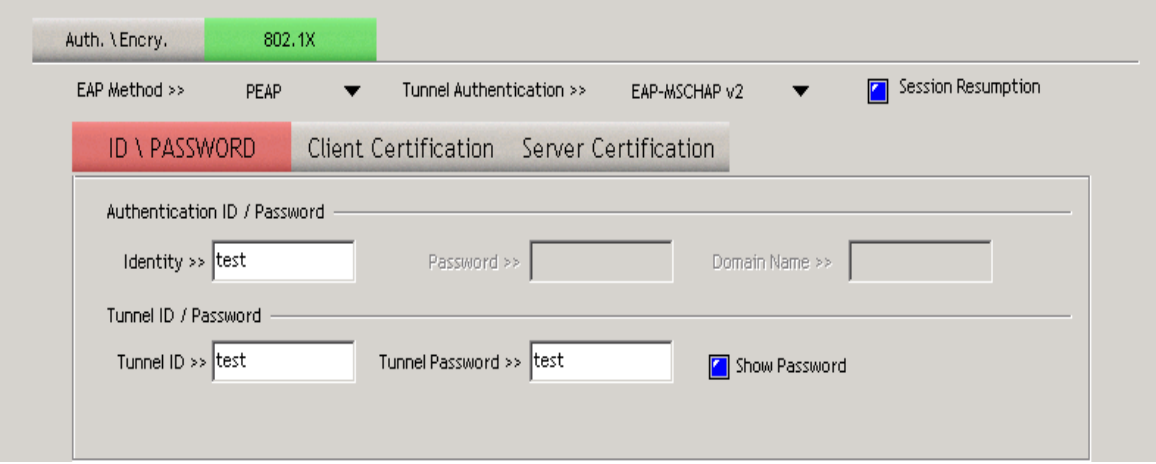
这个选项只有在【数据加密】区域选择了WEP的情况下才可以设置。WEP密钥是一串64位（5个字节）或128位（13个字节）16进制的数字，用来加密和解密数据包。

显示密钥

选择此项时，您设置的密钥会以明文显示出来。

【802.1x设置】

当您在身份验证模式中选择“WPA”或“WPA2”，可以设置本项目，如果您选择了“开放”和“共享密钥”，也可以单击“使用802.1x验证”，从而设置802.1x。



验证方式包括：

◆ PEAP --PEAP (Protected Extensible Authentication Protocol) 认证是 EAP （ Extensible Authentication Protocol）的一个版本。EAP 保证了位于网络操作中心的无线客户端和服务器的相互认证。

◆ TLS/Smart Card -- TLS (Transport Layer Security，传输层安 全协议) 认证是用来创建一个加密渠道并获得服务器端的认证，类似于使用 SSL(Secure Sockets Layer)协议的网页服务器认证。这个方法采用数字证书来检查客户端和服务器的身份。

◆ TTLS --TTLS 认证使用证书来验证服务器身份，同时保留了类似 TLS 的安全属性，例如相互认证和会话 WEP 密钥的共享机密。

◆ EAP-FAST：透过安全信道的延伸验证通讯协议。在与 Cisco 兼容的延伸功能版本 3 (CCX v.3) 中，Cisco 为 EAP-FAST (透过安全信道的延伸验证通讯协议) 增加了支持，该协议使用受保护的存取身分证明 (PAC) 在客户端和服务器间建立验证的通道。彼此验证并不使用凭证，而是利用某种『受保护的存取身分证明』(PAC) 的方法来达成，这种方法可以让验证服务器进行动态管理。『受保护的存取身分证明』(PAC) 可以利用手动或自动的方式提供 (一次分配) 到客户端。手动分配可以透过磁盘或安全网络配送方法传递到客户端。自动分配是透过空中无线传送的频带内配送。针对 Tunnel 验证部份，目前只提供『Generic Token Card』验证方式。

◆ MD5-Challenge：讯息摘要 5。MD5 是提供基本等级 EAP 支持的一种 EAP 验证类型，它只适合作为单向的验证；无线客户端与网络之间没有共同的验证。

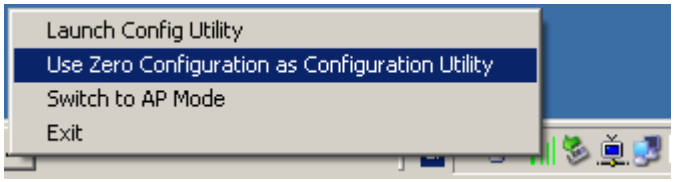
◆ Session Resumption：讯号中断重新连接后，可设定去减少重新连接时的封包，可加强中断后再连接的速度。共有 2 种方式可选择，『Disabled』和『Enabled』。

Tunnel 验证 ：

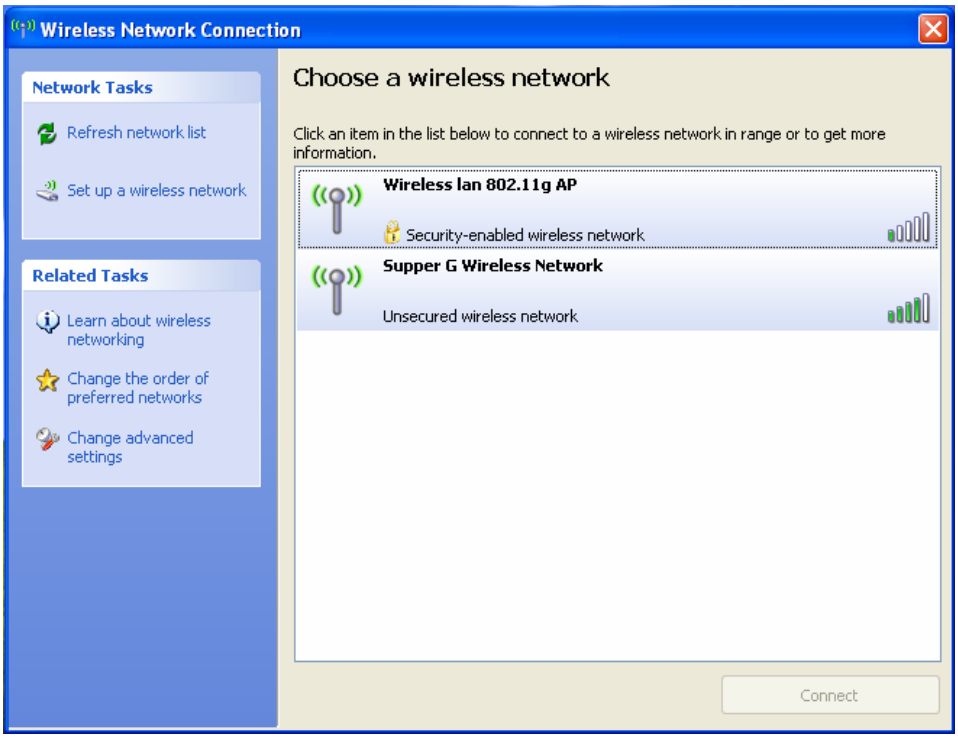
◆ Tunnel 协定：隧道验证，依照验证方式的不同目前分有，『EAP-MSCHAP v2』、『EAP-TLS/Smart card』、『Generic Token Card』、『CHAP』、『MS-CHAP』、『MS-CHAP-V2』、『PAP』、『EAP-MD5』。

4. 应用程式的Zero配置模式

右键单击系统托盘的应用程序，选择“Use Zero Configuration as configuration Utility”，即可使用Windows 无线网络设置功能。如果选择“Use ASUS Configuration as configuration Utility ”，则使用ASUS配置程序，如下图。

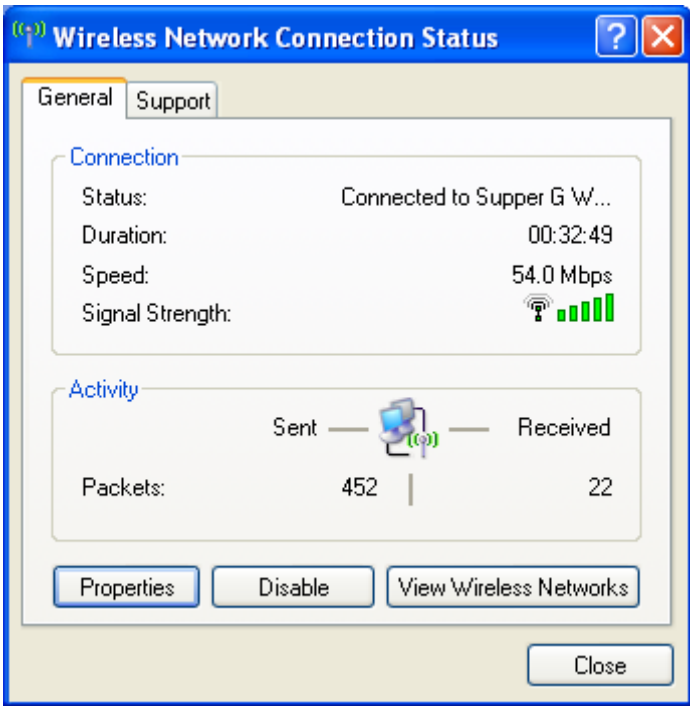


在任务栏双击无线网络图标，查看无线网络，选择要连接的网络并点击“Connect”。



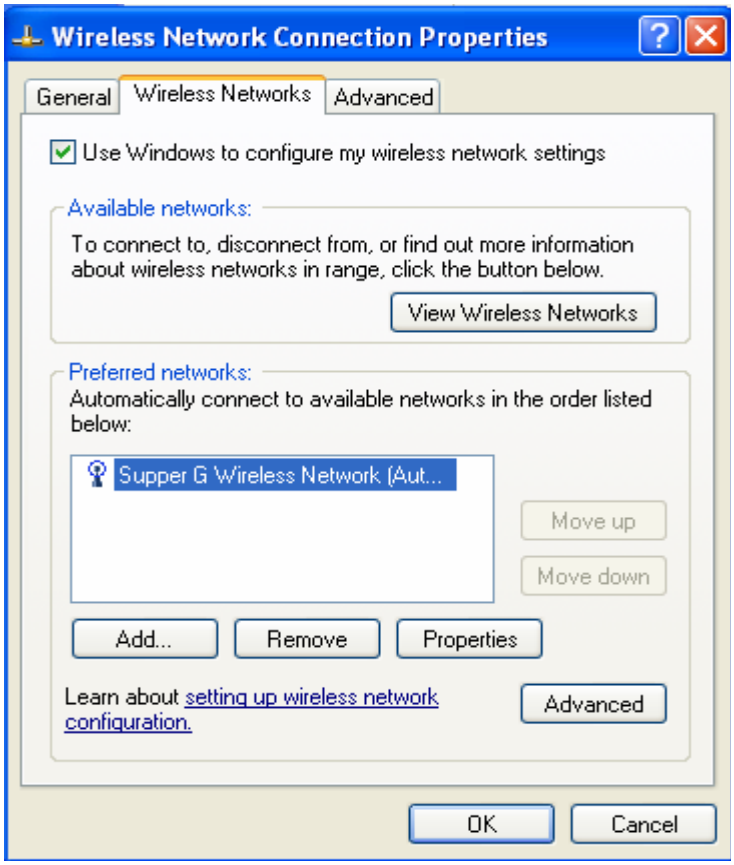
若您的无线路由器进行了加密，将会弹出窗口提示您输入密钥。请输入密钥并点击“Connect”，连接完成。

要设置无线连接属性，在系统托盘右击无线图标，选择“Status”， 打开【Wireless Network Connection Status】页面。

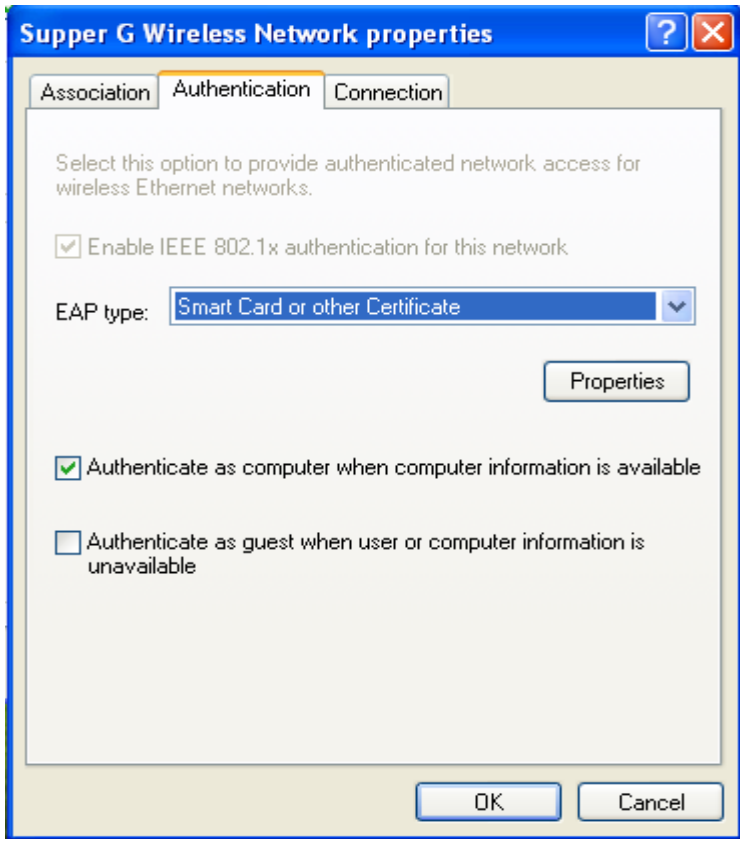


【General】页面显示了、连接时间、速率和信号强度。信号强度用绿色的线条表示，5条表示信号良好，1条表示信号极差

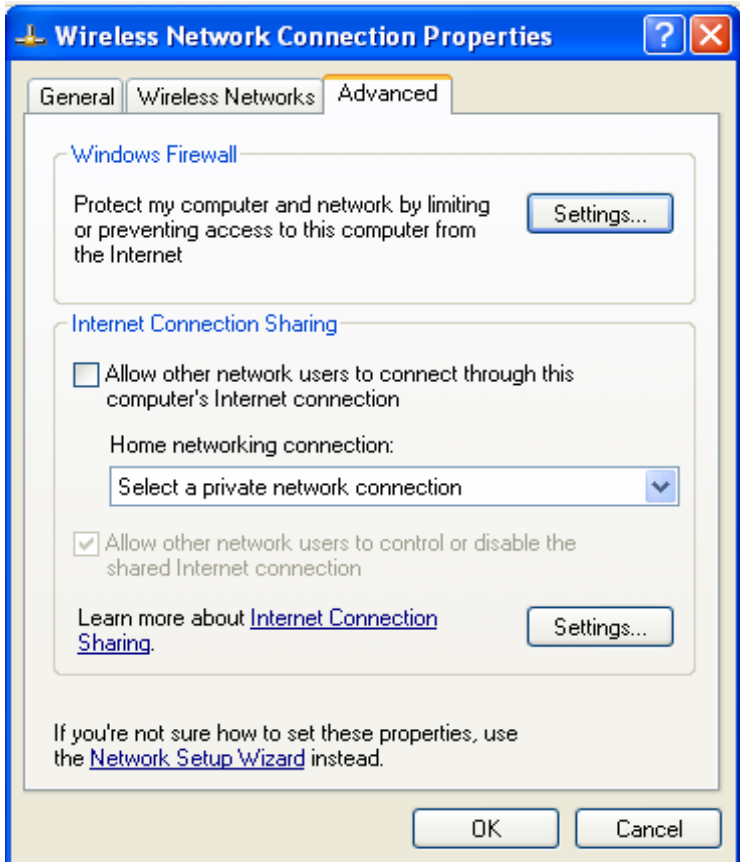
【View Wireless Network】标签页以显示首选网络。使用 “Add” 按钮来添加可用网络的“SSID”，若有多个可用网络,可通过“Move up”和“Move down”按钮来设置连接的优先顺序。带有信号的发射塔图标表示当前连接的AP。点击“Properties”可以设置无线连接的验证方式。



【Authertication】页允许您添加安全设置。您可以参考Windows 帮助以获得更多信息。



【Advance】页面允许您设置防火墙和共享。您可以参考Windows帮助以获得更多信息。

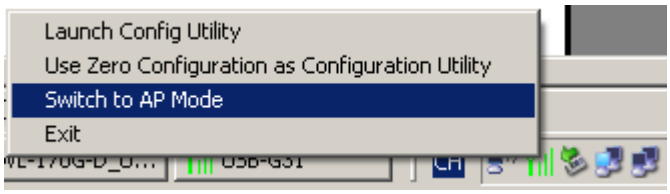


5. Soft AP 功能

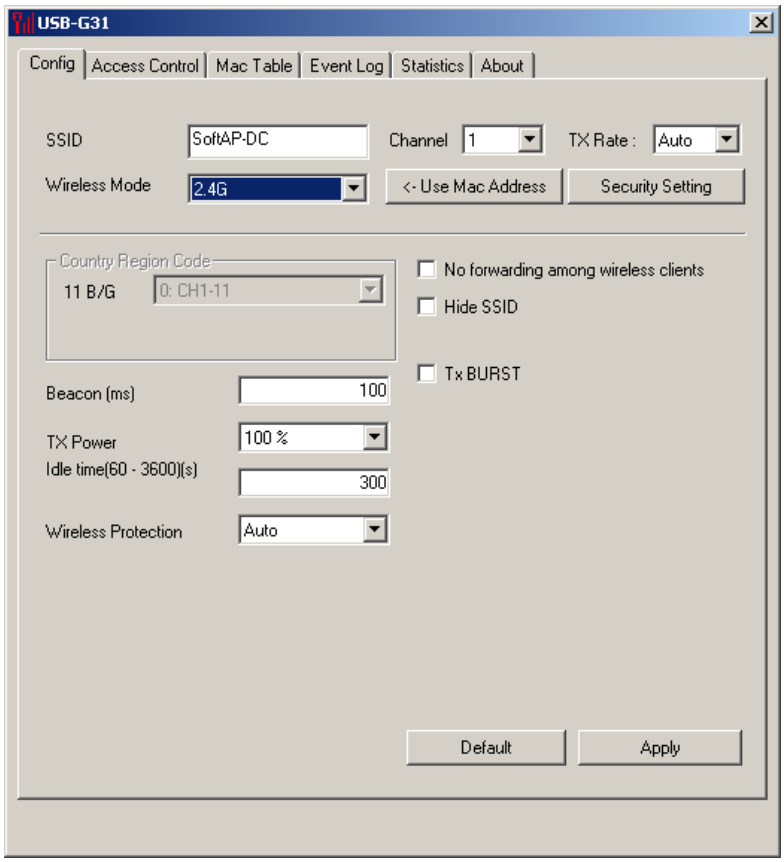
本无线网卡具有工作站和Soft AP 两种模式。启用Soft AP 模式后，网卡将成为一个AP(访问点)，从而可接受无线设备的访问接入。注意：本无线网卡仅支持在Windows XP和Win2000环境时才具有Soft AP功能，本指南以在Windows XP为例来说明Soft AP的使用方法。

5.1启用Soft AP模式

网卡配置软件启动后，您可以在操作系统托盘看到如下图所示的图标 



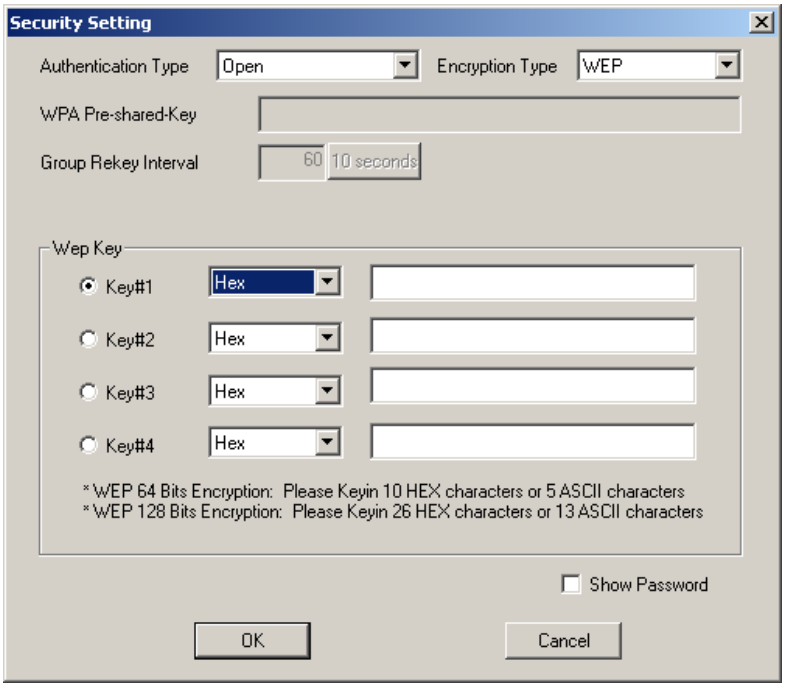
右键单击该图标，出现如右图的弹出式菜单。点击“Switch to AP Mode”菜单项，即会弹出如下图的Soft AP 配置软件。



5.2 Configuration Page

如上图。通过该配置页面，可以设置无线网络名称、模式、信道、身份验证等基本的配置。

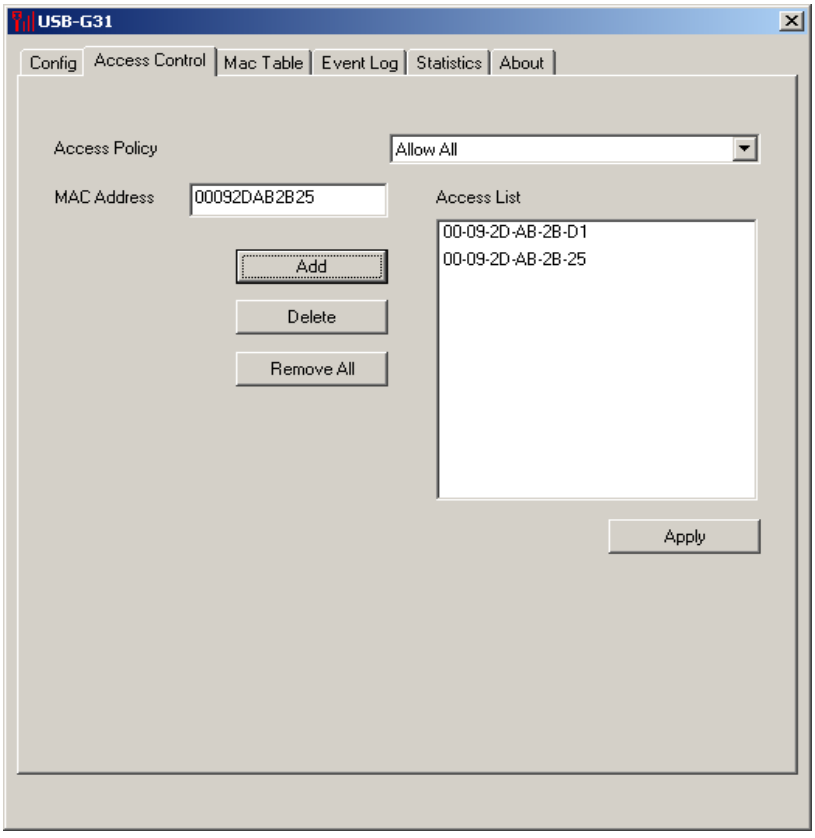
点击“Security Setting”按钮，可以进行无线通信的各种安全设置，如下图。 可选择各种认证类型和加密类型。例如WEP 64与WEP128加密。



5.3 Access Control

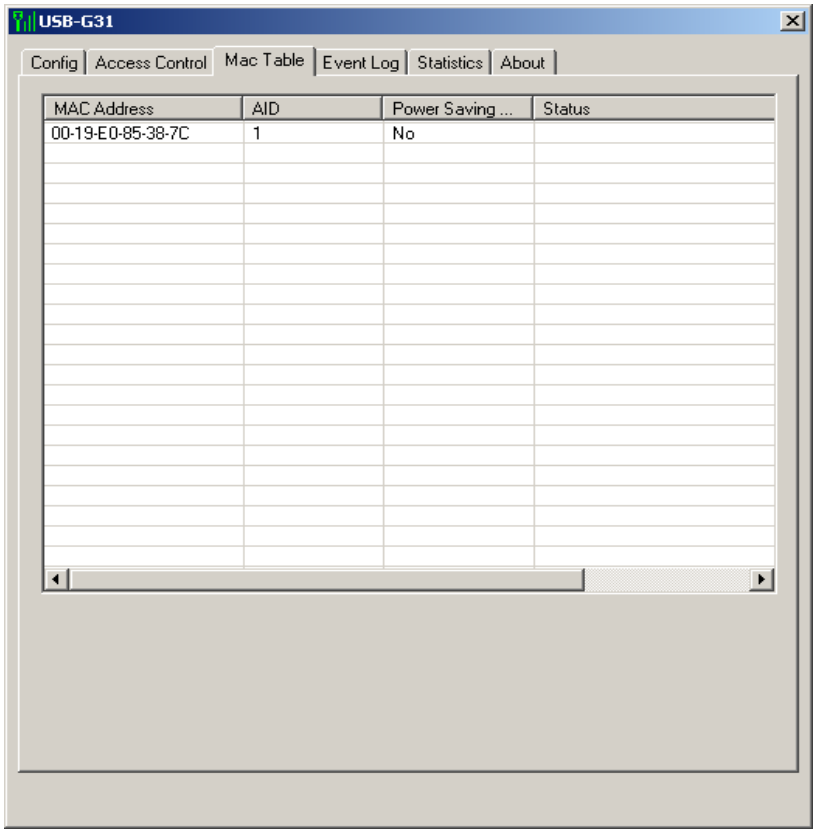
如下图。通过该页面，可以选择启用MAC控制功能。

MAC控制功能包括“允许所有”和“拒绝所有”。编辑完MAC 地址访问列表后，将只有或仅仅允许访问列表中的MAC 访问本Soft AP。



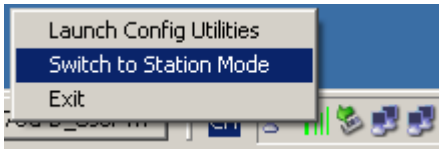
5.4 MAC

该页面显示已经接入本AP 的无线设备的信息。



5.5 切换到工作站模式

如下图，网卡在Soft AP 模式时，右键点击配置软件托盘图标，在弹出式菜单中选择“Switch to Station Mode”菜单项，将会使网卡切换为工作站模式,并且弹出工作站模式的配置软件界面。



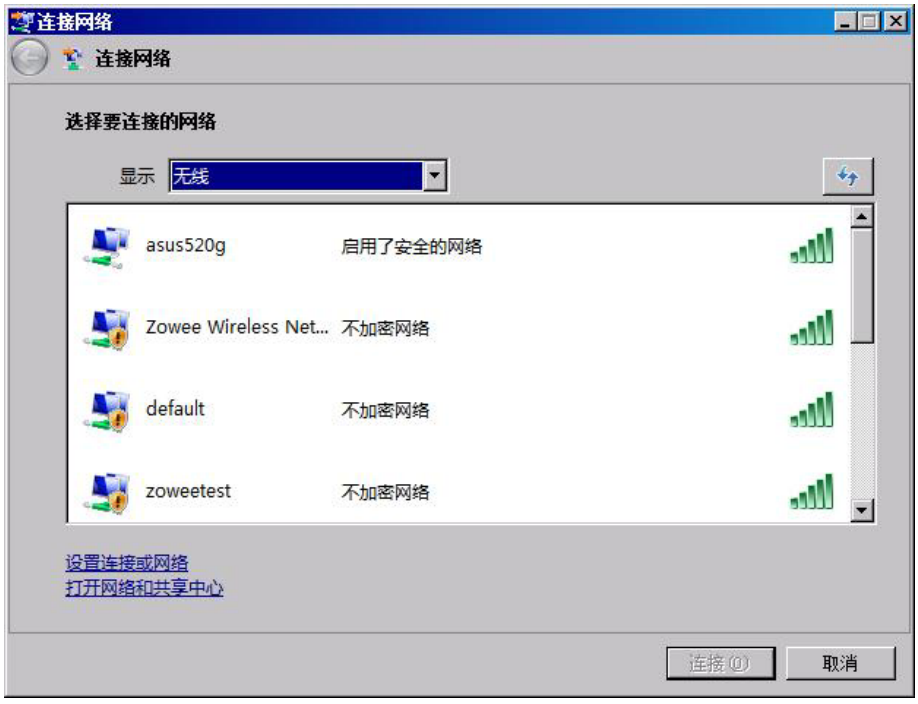
6. Vista系统下无线USB网卡的使用

Vista系统下有自带的无线网络管理程序，使用管理程序可以查看和进行无线网络的连接，或监控您的无线网卡的运作状态。在使用无线USB网卡连接网络时，请确认您已安装了无线网卡，并成功安装了无线网卡的驱动。

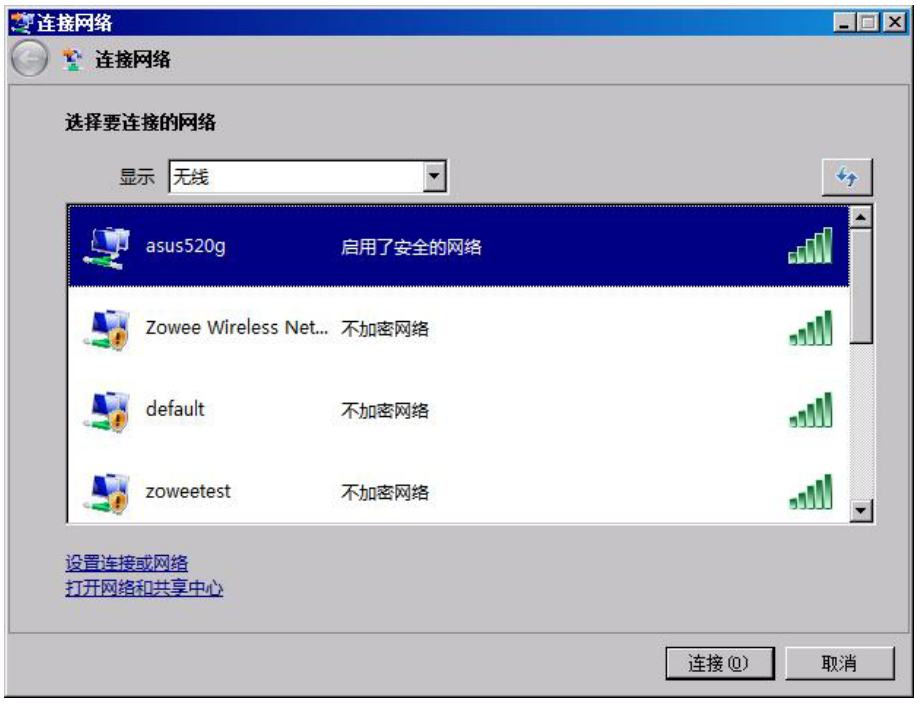
您可以在操作系统托盘看到如右图所示的图标。

单击红色方框选择的图标，出现如下画所示画面。

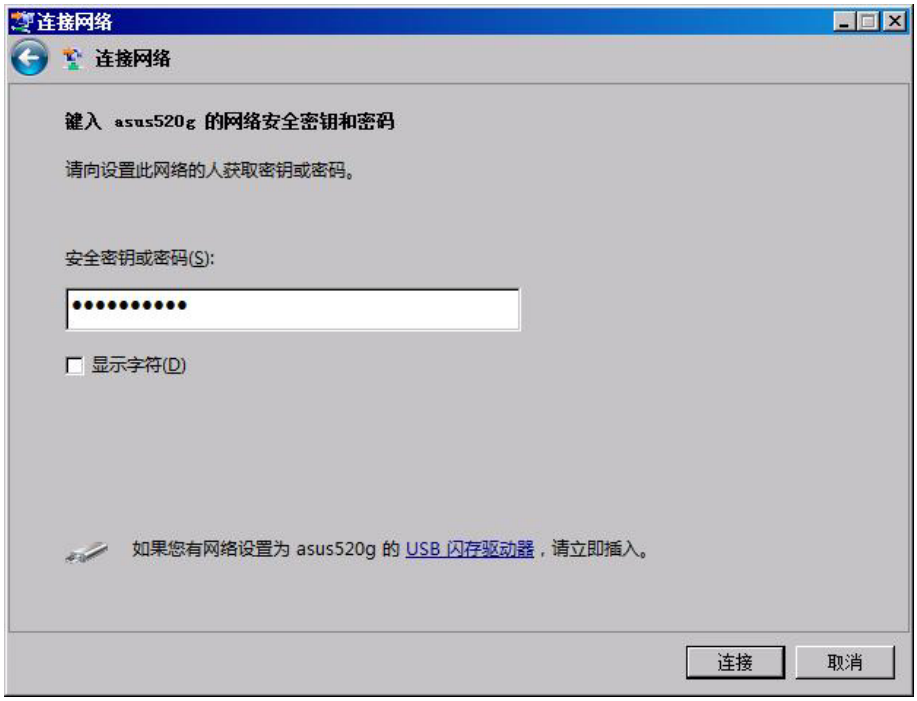
单击“连接到网络”，显示选择“无线 ”出现如下画所示画面。



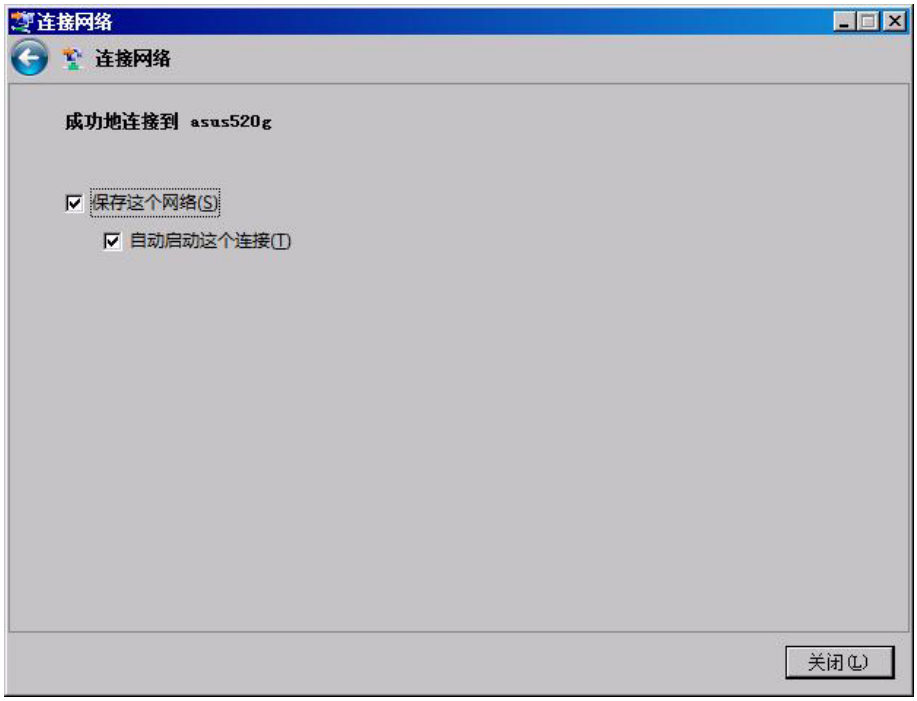
我们以连接到“asus520g”为例进行说明。



选择“asus520g”，单击连接出现如下画所示画面。



根据从所连网络设备管理员获取的密钥，填入对应的密钥输入栏中。如果所要连接的网络设备没有加密，可直接跳到下一步。



连接成功后显示如下图标。

查看无线连接，如下图所示“asus520g”已为“已连接”状态。可断开此无线网络，同样的方法，连接到其它的无线设备。