

第 3 章 无线局域网设定

3.1 介绍

近年来，无线通讯市场正以难以想象的速度在增长，无线组网方式完全摒弃了复杂的传统网络布线，用户可以根据自己的需求，配置“混合”类型（包括无线和有线）的网络环境。在无线环境中，所有的无线器件都是可移动的，便携的。

Vigor2900VG路由器配有一个符合IEEE 802.11g标准的无线接口，能够提供达到 54Mbps的传输速度。此无线接口在与原有的旧 802.11b标准兼容的情况下，还能提供高速无线传输以及高度的灵活性。

在本章节中，我们将详细介绍基本设定中的无线局域网设定部分。

基本设定 > 无线局域网设定

基本设定

- [快速设定向导](#)
- [系统管理员密码设定](#)
- [局域网TCP/IP与DHCP设定](#)
- [无线局域网设定](#)

3.2 配置

无线局域网设定

点击无线局域网设定按键，您将会看到下图中的显示页面。



DrayTek Vigor2900V Series Broadband Security VoIP Router

基本设定 > 无线局域网设定

无线局域网 (WLAN) 信息

MAC地址:	00-11-09-bf-c6-4d
频率区域:	
固件版本:	v1.0.6.7.04.2

详细设定

- >> [一般设定](#)
- >> [安全性设定](#)
- >> [接入控制](#)
- >> [接入者列表](#)

Copyright (c) 2004, DrayTek Corp. All Rights Reserved.

页面中，您可以看到无线局域网的信息，包括**MAC地址**，**频率区域**，**固件版本**以及无线网络的**详细设定**部分。详细设定区域则由**一般设定**、**安全性设定**、**接入控制**以及**接入者列表**组成。

3.2.1 一般设定

点击**一般设定**，您将会进入一个新窗口，在此您可以设定**SSID**以及无线频道等相关配置。

无线局域网设定

一般设定 (IEEE 802.11)

☐ 启用无线局域网

模式：

混合模式 (11b+11g)

计划任务 (1-15)

SSID：

频道：

☐ 隐藏SSID

☐ Long Preamble

SSID：

无线局域网服务集ID。

隐藏SSID：

在监听无线讯号时，扫描工具无法读到SSID。

频道：

选择无线局域网的频道。

Long Preamble

仅在使用旧式802.11b装置且遭遇连线问题时才须启用本功能，否则本功能将使效能降低。

启用无线局域网：勾选此单选框，即开启无线局域网。

模式：选择合适的无线模式。在下拉菜单中，您可以看到我们所支持的**混合模式(11b+11g)**、**仅 11g**以及**仅 11b**，三种无线模式。

相较于旧的 802.11b 标准，802.11g 采用了不同的 OFDM 调制技术，因此可以提供更加高速的传输速度。而且 802.11g 还能够与 802.11b 的 WIFI 系统互相连通，保证了向下兼容。

传输速度 (理想状况)：

802.11b 11Mbps

802.11g 54Mbps

而鉴于目前市场上仍然存在很多只支持 802.11b 标准的无线器件，我们提供了一个**混合模式**的选项。

但请您注意，此环境中 802.11g 设备的传输速度会受到影响而降低。

计划任务：您可以配置路由器的无线功能仅在某些特定时段工作，总共可以设置四个时段。默认情况下，路由器的无线功能没有时限。您可以到 **> 高级设定 > 拨号计划任务设定** 配置相关计划任务。

SSID：SSID是Service Set Identification（服务集标识）的简称。它是用来标识某个网络的一个字符串，也就是俗称的网络ID。对于同一网络中的所有用户来说，它的SSID必须都是一样的。此外，SSID是区分大小写的，而且最大只能输入 32 个字符。Vigor的默认SSID为**default**。为安全着想，您最好自己重新定义一个独有的SSID，而不要用默认的。

频道：选择一个合适的无线频道。所有在无线网络中的用户都必须要在同一个频道内进行通讯。Vigor默认使用频道 6。

隐藏SSID：启用此功能，本来应被路由器广播的SSID信息将会被隐藏起来。
默认情况下，这个选项是开启的。

Long Preamble：启用此功能，是为了与旧式的 802.11b装置更好的兼容，但是这会影响到无线的效能。

3.2.2 安全性设定

为了保护无线封包不被那些不受欢迎的任侦听或窃取到，我们采用WEP和WPA两种安全方式。

WEP是Wired Equivalent Privacy（有线对等保密）的缩写。它是在IEEE 802.11b标准中定义的，用于无线网络的一种安全协议，也是最基本的保密措施。WEP通过密钥（四个预设密钥中的任意一个）来加密无线电波中的数据帧，以达到安全的目的。路由器和客户端都必须使用同一个密钥。

WPA是Wi-Fi Protected Access（Wi-Fi保护访问）的缩写。实际上，作为802.11i标准的一个子集，当初在开发的时候，只是将它作为一个过渡标准，在802.11i标准完成后将自动废止。不管怎样，相较于WEP，WPA要安全多了。

它使用临时密钥完整性协议（TKIP: Temporal Key Integrity Protocol）为加密引入了新的机制，并且采用可扩展认证协议（EAP: Extensible Authentication Protocol）、消息完整性校验（MIC: Message Integrity Check）以及 802.1x，作为认证机制。这些都大大的提高了WPA的安全性能。

点击**安全性设定**，进入新页面配置WEP和WPA安全设定。

安全性设定

模式: WEP 或 WPA/PSK

设定 **RADIUS 服务器** 若启用了 802.1x。

WPA:

加密模式: TKIP

预共享密钥 (PSK) *****

键入 8~63 个 ASCII 字符或以 "0x" 为首后接 64 个十六进位字符，例如 "cfgs01a2..." 或 "0x655abcd..."。

WEP:

加密模式: 64 位

使用 WEP 密钥

☐ 密钥1: *****

☒ 密钥2: *****

☐ 密钥3: *****

☐ 密钥4: *****

关于 64 位 WEP 密钥
键入 5 个 ASCII 字符或开头为 "0x" 的 10 个十六进位数字，
如 "AB312" 或 "0x4142333132"。

关于 128 位 WEP 密钥
键入 13 个 ASCII 字符或开头为 "0x" 的 26 个十六进位数字，
如 "AB312" 或 "01234567890x4142333132"。

模式: 有多种安全模式可供选择。您可以点击下拉菜单选择合适的模式。

• **停用:** 停用加密机制。

• **仅 WEP:** 要求客户端只能使用提供的 WEP 密钥无线接入。

• **仅 WEP/802.1x:** 要求客户端只能使用通过 802.1x 机制动态生成的 WEP 密钥无线接入。

• **WEP 或 WPA/PSK:** 客户端可以同时使用提供的 WEP 密钥，以及由 WPA-PSK 定期生成地动态密钥来无线接入。

• **WEP/802.1x 或 WPA/802.1x:** 客户端可以同时使用 802.1x 机制生成地 WEP

密钥以及 WPA 动态密钥来无线接入。

- 仅 **WPA/PSK**: 客户端只能采用 WPA-PSK 定期生成的动态密钥来无线接入。

- 仅 **WPA/802.1x**: 客户端只能采用由 802.1x 机制生成的动态密钥来无线接入。

注意: 若选择选择了 **WEP/802.1x** 或 **WPA/802.1x**, 仅 **WEP/802.1x** 以及仅 **WPA/802.1x** 等模式, 您还应该去配置 **RADIUS 服务器** 的相关设定。

而且, Vigor 路由器目前只支持 **EAP-TLS**, 而非 **PEAP**。因此无论您在配置 **RADIUS 服务器** 还是客户端, 都必须选择“**智能卡或其他证书**”, 而非“**受保护的 EAP (PEAP)**”。

WPA 加密: WPA 通过 WPA-PSK 定期生成的动态密钥或者 802.1x 机制定期生成的密钥, 对在无线电波中传输的数据帧进行加密。

- 预共享密钥 (PSK):** 输入一个长度为 8~63 个 ASCII 字符的 WPA 预共享密钥。例如, 0123456789ABCD

WEP 加密:

- 64 位:** 64 位 WEP 密钥, 请在文字框内输入长度为 5 个 ASCII 字符, 或者以“0x”开头的 10 个十六进制数字的密钥。例如, ABCDE 或者 0x4142434445

- 128 位:** 128 位 WEP 密钥, 请在文字框内输入长度为 13 个 ASCII 字符, 或者以“0x”开头的 26 个十六进制数字的密钥。例如, ABCDEFGHIJKLM 或者 0x4142434445464748494A4B4C4D

注意:

1. 128 为 WEP 密钥较 64 位更为安全, 不过传输速度有所下降, 因为它会引入更多的编码/解码动作。请注意所有的无线装置都必须使用一样长度的同一个 WEP。

2. 这里您可以预设四个密钥, 但是在每次使用的时候, 您只能选取其一。

3. 若您选择 **WEP** 或 **WPA/PSK**, 密钥的编号会固定在“2”, 请您注意在客户端也选取相同编号的密钥。

在配置完后，请点击 **OK** 保存设定。

3.2.3 接入控制设定

基本上每个无线设备（网卡或者AP）都有一个独一无二的硬件地址，即所谓的MAC地址。通过**接入控制**功能，您可以过滤无线客户端的MAC地址来限制它们。这样，只有被允许的合法MAC地址才有资格接入无线网络。

点击**详细设定**部分中的**接入控制**，进入新的配置页面，如下图所示。您将可以编辑输入相关的客户MAC地址，以控制它们的接入。

接入控制

☒ 启用接入控制

索引	须使用VPN	MAC地址
1		00 : 0C : 10 : 2C : 1B : 01

MAC地址：
[] : [] : [] : [] : [] : []

☐ 必须在WLAN上使用VPN联网

WLAN的VPN服务器IP地址 [] . [] . [] . []

附注：
添加或移除无线网络用户的MAC地址以允许或拒绝其接入网络。

启用接入控制：勾选启用接入控制以开启此功能。

MAC地址：输入被允许接入的客户端的MAC地址。

添加：添加一个MAC地址到列表中。

移除：从列表中删除一个MAC地址。

编辑：编辑存在于列表中的某个MAC地址。

取消：放弃本次设置。

如何获取无线客户端的MAC地址呢？

无线局域网设定

以Window XP为例，请到系统的**开始菜单**中，选择**运行**，键入**cmd**，并确定。在弹出的命令行提示符中键入 **ipconfig/all**，就会显示出无线网卡的MAC地址了。

Clean All: 清除列表中的所有MAC地址。

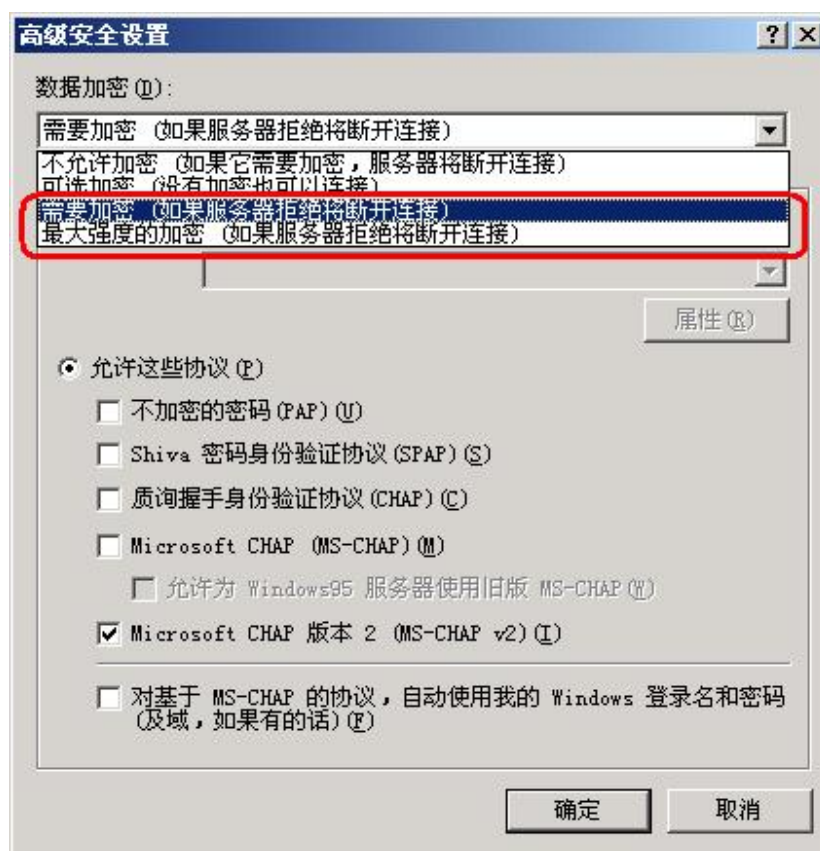
OK: 保存对MAC接入控制所做的设定。

WLAN的VPN服务器地址: 输入提供给WLAN连接的VPN服务器地址。

此功能是用于VPN（PPTP/L2TP/L2TP over IPsec） over Wireless LAN的构建。也就是，将无线数据帧封装然，后通过一个加密的VPN隧道进行传输。您若开启了WEP/WPA+VPN over WLAN，就相当于为无线接入提供一个双重安全保证。关于此功能的实际应用，附在CD中的文档会有说明。

注意: 在应用VPN over WLAN的时候，您必须要选择经过数据加密的VPN隧道类型。比如PPTP的无加密方式或者L2TP，您就不可以在这里使用。

以PPTP为例，若您在配置XP自带的VPN拨号软件时，您就必须选择“需要加密”或“最大强度的加密”。



3.3 接入者列表

点击接入者列表，进入列表页面。

接入者列表

状态

MAC地址

更新

状态码:

C: 已连线。

B: 受到接入控制功能的封锁。

N: 正在建立新连线。

F: 无法通过802.1X或WPA认证。

X: 正在执行802.1X。

W: 正在WPA认证。

附注:

当一个节点成功连接到路由器后,它有可能在不通知路由器的情况下关闭。在这种情况下,它仍然会显示在列表中,直到连接过期。

添加到接入控制:

客户端的MAC地址

:

:

:

:

:

Back

Add

这个页面可以显示出所有与路由器相联系的无线基站。您可以点击**更新**以获取无线基站的最新连接信息，包括他们的**MAC地址**和连接状态。

您还可以点选**接入者列表**中的某个指定的**MAC地址**，然后点击**添加**，这样可以把它添加到**接入控制**中，以控制它们的连接。当然，您还可以直接在**客户端的MAC地址**中编辑**MAC地址**，然后添加到**接入控制**中。

附：应用范围

1. 简化网络的铺设

对于一个拥有较多网络设备的地方，相信所有人都会对屋里一地的网线感到头痛。而选择无线网络，则可大大简化了整个网络的铺设过程，不用打墙钻洞，更不用到处铺那麻烦的“绊马锁”了。

2. 提供灵活的网络接入

尤其适用于那些，由于工作关系，经常需要外出的人。比方说销售人员，为方便起见，公司为他们每人都配备了一台笔记本电脑。但是每当他们回到公司想要获取数据库内的资料时，还得重新铺设一根网线，并且对笔记本的网络配置重新设定。

此时，若有了无线网络，随时打开笔记本，即可随时接入网络，不用再浪费精力在那些繁琐的网线配置上了。

3. 有线网络不可达

有时我们会碰到一些很恼人的情况：公司部门分布在办公楼的上下层；家中刚刚电脑距离路由器，隔了两间屋子，等等。此时，铺设网线不是不实际，就是不划算。

这些情况下，无线网络无疑是最好的选择。