Dynamic DNS (Domain Name Server)

This free service is very useful when combined with the *Virtual Server* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.

The DynDNS Service works as follows:

1. You must register for the service at http://www.dyndns.org (Registration is free). Your password will be E-mailed to you.
2. After registration, use the "Create New Host" option (at www.dyndns.org) to request your desired Domain name.
3. Enter your data from www.dyndns.org in the Wireless ADSL Router's DDNS screen.
4. The Wireless ADSL Router will then automatically ensure that your current IP Address is recorded at http://www.dyndns.org
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

Dynamic DNS Screen

Select *Advanced* on the main menu, then *Dynamic DNS*, to see a screen like the following:

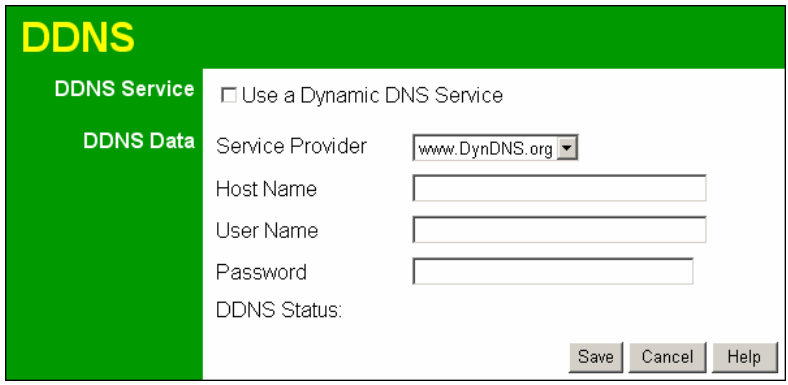

Figure 48: DDNS Screen

Data - Dynamic DNS Screen

DDNS Service	
Use a Dynamic DNS Service	Use this to enable or disable the DDNS feature as required.
DDNS Data	
Service Provider	Select the desired DDNS Service provider.
Host Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
User Name	Enter your Username for the DDNS Service.
Password	Enter your current password for the DDNS Service.
Domain Name	Enter the domain name allocated to you by the DDNS Service. If you

	have more than one name, enter the name you wish to use.
DDNS Status	• This message is returned by the DDNS Server • Normally, this message should be "Update successful" • If the message is "No host", this indicates the host name entered was not allocated to you. You need to connect to DDNS Service provider and correct this problem.

Firewall Rules

The ***Firewall Rules*** screen allows you to define "Firewall Rules" which can allow or prevent certain traffic.

By default:

- All Outgoing traffic is permitted.
- All Incoming traffic is denied.

"Traffic" means incoming connection attempts, not packets.

Because of this default behavior, any **Outgoing** rules will generally **Block** traffic, and **Incoming** rules will generally **Allow** traffic.

Firewall Rules Screen

An example screen is shown below.

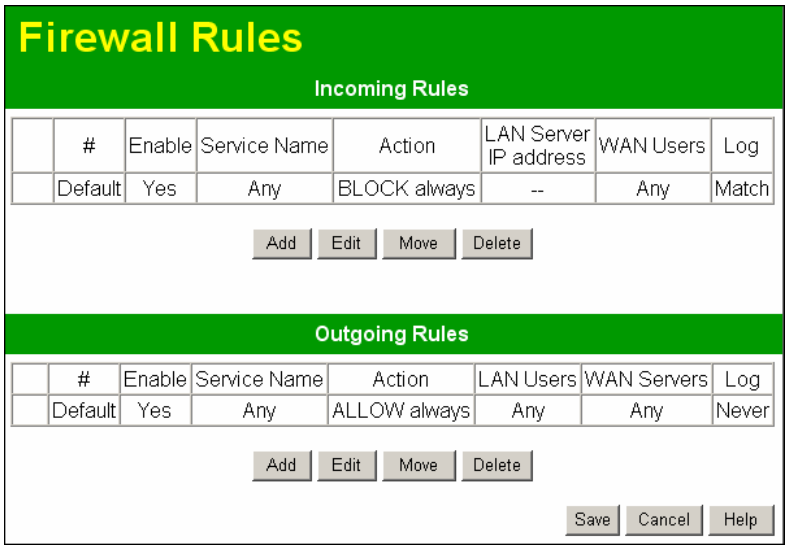

Figure 49 Firewall Screen

Data - Firewall Rules

Incoming Rules	
#	For the default rule, this will display "Default". For rules which you create, this will display a radio button which allows you to select the rule.

Enable	Indicates whether or not the rule is currently enabled. For rules you have added, this column will contain a checkbox, allowing you to easily enable or disable the rule. (Click "Save" after making any changes.)
Service Name	The Service covered by this rule.
Action	The action performed on connections which are covered by this rule.
LAN Server	The PC or Server on your LAN to which traffic covered by this rule will be sent.
WAN Users	The WAN IP address or addresses covered by this rule.
Log	Indicates whether or not connections covered by this rule should be logged.
Buttons	Use the *Add* button to create a new rule. The other buttons - *Edit*, *Move*, or *Delete* - require that a rule be selected first. Use the radio buttons in the left column to select the desired rule.
Outgoing Rules	
#	For the default rule, this will display "Default". For rules which you create, this will display a radio button which allows you to select the rule.
Enable	Indicates whether or not the rule is currently enabled. For rules you have added, this column will contain a checkbox, allowing you to easily enable or disable the rule. (Click "Save" after making any changes.)
Service Name	The Service covered by this rule.
Action	The action performed on connections which are covered by this rule.
LAN Users	The LAN PC or PCs covered by this rule.
WAN Servers	The WAN IP address or addresses covered by this rule.
Log	Indicates whether or not connections covered by this rule should be logged.
Buttons	Use the *Add* button to create a new rule. The other buttons - *Edit*, *Move*, or *Delete* - require that a rule be selected first. Use the radio buttons in the left column to select the desired rule.

Incoming Rules (Inbound Services)

This screen is displayed when the "Add" or "Edit" button for Incoming Rules is clicked.

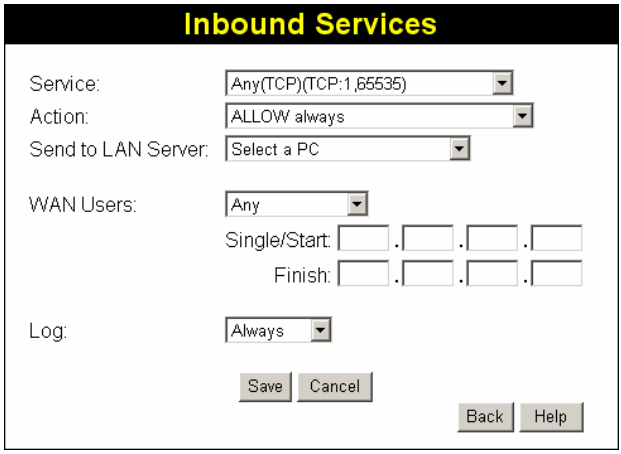

Figure 50: Inbound Services Screen

Data - Incoming Rules Screen

Inbound Services	
Service	Select the desired Service. This determines which packets are covered by this rule. If necessary, you can define a new Service on the "Services" screen, by defining the protocols and port numbers used by the Service.
Action	Select the desired action for packets covered by this rule: • ALLOW always • ALLOW by schedule, otherwise Block • BLOCK always • BLOCK by schedule, otherwise Allow **Note:** • Any inbound traffic which is not allowed by rules you create will be blocked by the Default rule. • BLOCK rules are only useful if the traffic is already covered by an ALLOW rule. (That is, you wish to block a sub-set of traffic which is currently allowed by another rule.) • To define the Schedule used in these selections, use the "Schedule" screen.
Send to LAN Server	Select the PC or Server on your LAN which will receive the inbound traffic covered by this rule.
WAN Users	These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option: • **Any** - All IP addresses are covered by this rule. • **Address range** - If this option is selected, you must enter the desired values in the "Single/Start" and "Finish" fields to determine the address range. • **Single address** - Enter the required address in the "Single/Start"

	fields.
Log	This determines whether packets covered by this rule are logged. Select the desired action. • **Always** - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.) • **Never** - never log traffic considered by this rule, whether it matches or not. • **Match** - Log traffic only it matches this rule. (The action is determined by this rule.) • **Not Match** - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)

Outgoing Rules (Outbound Services)

This screen is displayed when the "Add" or "Edit" button for Outgoing Rules is clicked.

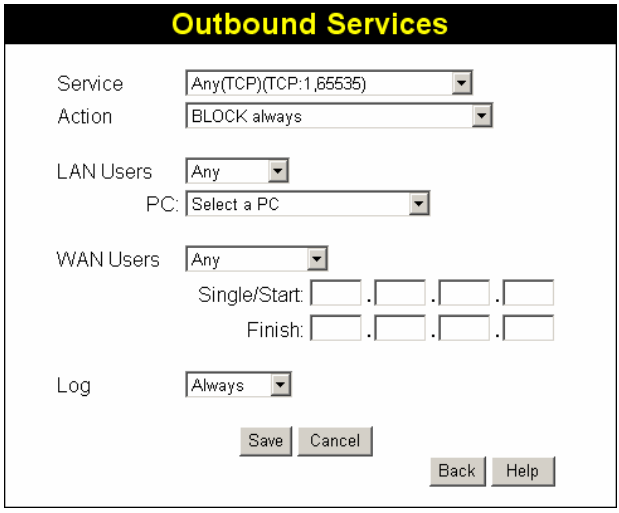

Figure 51: Outbound Services Screen

Data - Outbound Rules Screen

Outbound Services	
Service	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the "Services" menu option
Action	Select the desired action for packets covered by this rule: • BLOCK always • BLOCK by schedule, otherwise Allow • ALLOW always • ALLOW by schedule, otherwise Block **Note:** • Any outbound traffic which is not blocked by rules you create will be allowed by the Default rule.

	• ALLOW rules are only useful if the traffic is already covered by a BLOCK rule. (That is, you wish to allow a subset of traffic which is currently blocked by another rule.) • To define the Schedule used in these selections, use the "Schedule" screen.
LAN Users	Select the desired option to determine which PCs are covered by this rule: • **Any** - All PCs are covered by this rule. • **Single PC** - Only the selected PC is covered by this rule. If selected, you must select the PC. **PC** - If using Single PC above, select the PC or Server on your LAN which will be covered by this rule.
WAN Users	These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option: • **Any** - All IP addresses are covered by this rule. • **Address range** - If this option is selected, you must enter the "Start" and "Finish" fields. • **Single address** - Enter the required address in the "Single/Start" fields.
Log	This determines whether packets covered by this rule are logged. Select the desired action. • **Always** - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.) • **Never** - never log traffic considered by this rule, whether it matches or not. • **Match** - Log traffic only it matches this rule. (The action is determined by this rule.) • **Not Match** - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)

User-defined Services

Services are used when creating Firewall Rules.

If you wish to create a firewall rule, but the required service is not listed in the "Service" list, you can use this feature to define the required service or services. Once created, these services will be listed in the "Service" list, and can be used when creating Firewall Rules.

Figure 52: Add Services Screen

Data - User-defined Services

Services	
Existing Services	This lists any Services you have defined. If you have not defined any Services, this list will be empty. Once you define some services, they will be listed here, and also shown in the Service list used to create Firewall rules. (User-defined services are at the end of the list, after the pre-defined services.)
Add	Use this to open a sub-screen where you can add a new service.
Edit	To modify a service, select it, and then click this button.
Delete	Use this button to delete the selected service. You can delete any services you have defined.

Add/Edit Service

This screen is displayed when the *Add* or *Edit* button on the ***Services*** screen is clicked.

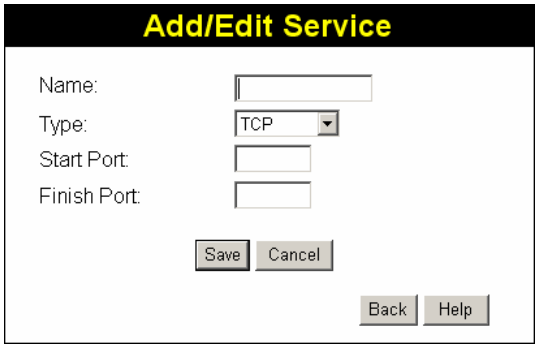

Figure 53 : Add/Edit Service

Data - Add/Edit Service

Services	
Name	If editing, this shows the current name of the Service. If adding a new service, this will be blank, and you should enter a suitable name.
Type	Select the protocol used by the Service.
Start Port	Enter the beginning of the port range used by the Service.
Finish Port	Enter the end of the port range used by the Service.

Options

This screen allows advanced users to enter or change a number of settings. For normal operation, there is no need to use this screen or change any settings.

An example ***Options*** screen is shown below.

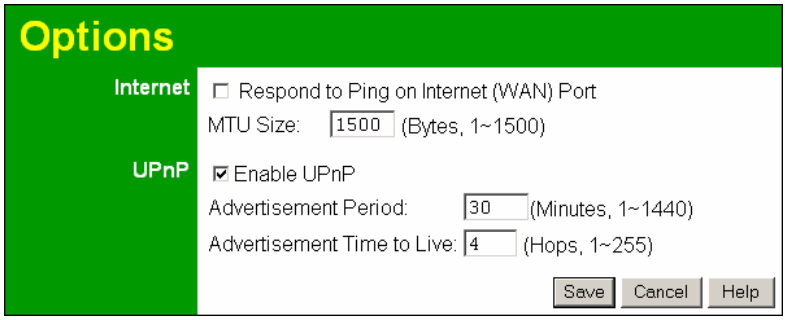

Figure 54: Options Screen

Data - Options Screen

Internet	
Respond to Ping	• If checked, the Wireless Router will repond to Ping (ICMP) packets received from the Internet. • If not checked, Ping (ICMP) packets from the Internet will be ignored. Disabling this option provides a slight increase in security.
MTU Size	Enter a value between 1 and 1500. **Note:** MTU (Maximum Transmission Unit) size should only be changed if advised to do so by Technical Support.
UPnP	
UPnP	• UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is by supported Windows ME, XP, or later. • If Enabled, this device will be visible via UPnP. • If Disabled, this device will not be visible via UPnP.
Advertisement Period	Enter the desired value, in minutes. The valid range is from 1 to 1440.
Advertisement Time to Live	Enter the desired value, in hops. The valid range is from 1 to 255.

Schedule

This Schedule can be used for the Firewall Rules and the URL filter.

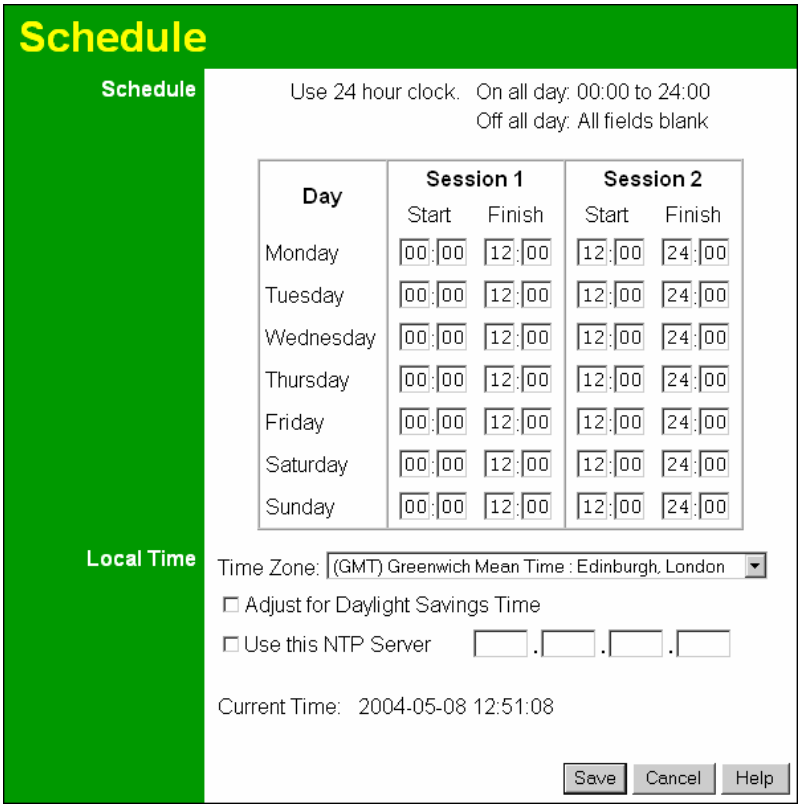

Figure 55: Schedule Screen

Data - Schedule Screen

Schedule	
Day	Each day of the week can scheduled independently.
Session 1 **Session 2**	Two (2) separate sessions or periods can be defined. Session 2 can be left blank if not required.
Start Time	Enter the start using a 24 hr clock.
Finish Time	Enter the finish time using a 24 hr clock.
Local Time	
Time Zone	In order to display your local time correctly, you must select your "Time Zone" from the list.
Adjust for Daylight Savings Time	If your region uses Daylight Savings Time, you must manually check "Adjust for Daylight Savings Time" at the beginning of the adjustment period, and uncheck it at the end of the Daylight Savings period.

Use this NTP Server	If you prefer to use a particular NTP server as the primary server, check the checkbox "Use this NTP Server" and enter the Server's IP address in the fields provided.. If this setting is not enabled, the default NTP Servers are used.
Current Time	This displays the current time on the Wireless ADSL Router.

Virtual Servers

This feature, sometimes called *Port Forwarding*, allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

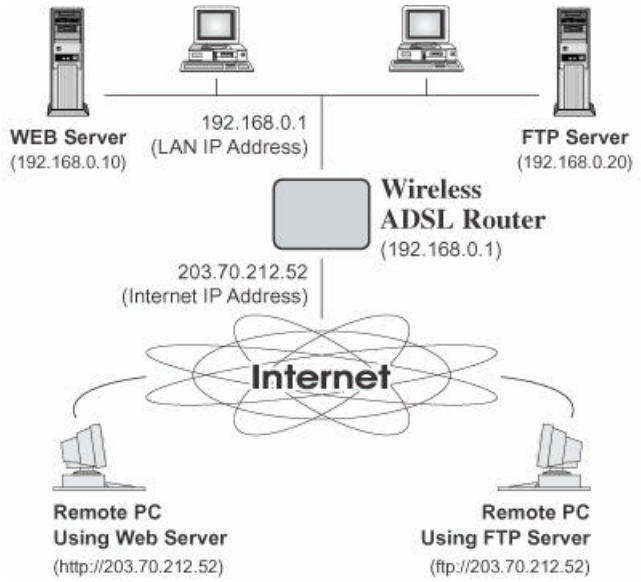

Figure 56: Virtual Servers

IP Address seen by Internet Users

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers.

However, you can use the *DDNS (Dynamic DNS)* feature to allow users to connect to your Virtual Servers using a URL, instead of an IP Address.

Virtual Servers Screen

- The "Virtual Servers" feature allows Internet Users to access PCs on your LAN.
- The PCs must be running the appropriate Server Software.
- For Internet Users, ALL of your Servers have the same IP address. This IP address is allocated by your ISP.
- To make it easier for Internet users to connect to your Servers, you can use the "DDNS" feature. This allows Internet users to connect to your Servers with a URL, rather than an IP address. This technology works even if your ISP allocates dynamic IP addresses (IP address is allocated upon connection, so it may change each time you connect).

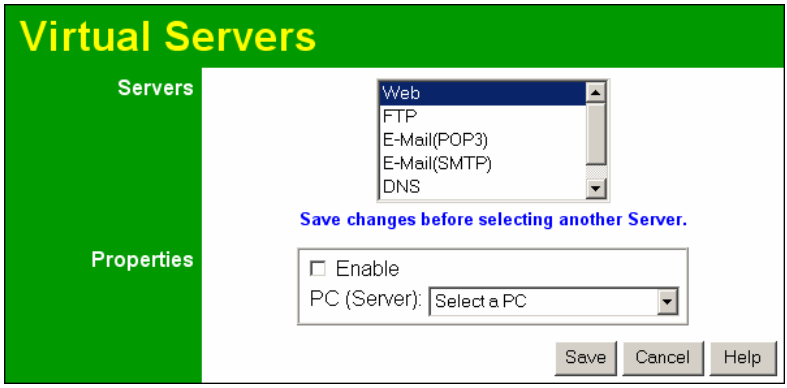

Figure 57: Virtual Servers Screen

Data - Virtual Servers Screen

Servers	
Servers	This lists a number of common Server types. If the desired Server type is not listed, you can create a Firewall Rule to achieve the same effect as the Virtual Server function.
Properties	
Enable	Use this to Enable or Disable support for this Server, as required. If Enabled, you must select the PC to which this traffic will be sent.
PC (Server)	Select the PC for this Server. The PC must be running the appropriate Server software.

For each entry, the PC must be running the appropriate Server software.

If the desired Server type is not listed, you can define your own Servers, using the Firewall Rules.

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the Internet IP Address (the IP Address allocated to you by your ISP).
e.g.

```
http://203.70.212.52
ftp://203.70.212.52
```

It is more convenient if you are using a Fixed IP Address from your ISP, rather than Dynamic. However, you can use the *Dynamic DNS* feature to allow users to connect to your Virtual Servers using a URL, rather than an IP Address.

From the Internet, ALL Virtual Servers have the IP Address allocated by your ISP

VPN Setup

The VPN (Virtual Private Network) feature in the Wireless ADSL Router allows you to create a VPN connection between 2 Wireless ADSL Routers, or a remote PC to establish a VPN connection to the Wireless ADSL Router.

To establish a VPN connection from a remote PC to the Wireless ADSL Router, you need suitable (IPSec) VPN client software on your PC.

For more information about VPNs, please refer to ***Appendix C - About VPNs***.

VPN Policies

A "VPN Policy" contains all the configuration data for a particular VPN connection. Generally, you will have to create one policy for each site you wish to connect to. The remote VPN Gateway (or client) needs to have matching configuration.

- Traffic covered by an enabled policy will automatically be sent via a VPN tunnel. If the VPN tunnel does not exist, it will be created.
- The VPN tunnel is created according to the parameters in the SA (Security Association).
- The remote VPN Endpoint must have a matching SA, or it will refuse the connection.

There are 2 types of VPN Policies:

- **Manual** - All settings (including the keys) for the VPN tunnel are manually input at each end (both VPN Endpoints).
- **Auto** - Some parameters for the VPN tunnel are generated automatically. This requires using the IKE (Internet Key Exchange) protocol to perform negotiations between the 2 VPN Endpoints.

VPN Policies Screen

This screen is displayed when you select **VPN** on the ***Advanced*** menu. It allows you to create, modify and manage your VPN Policies.

If you have not created any policies, the Policy Table will be empty.

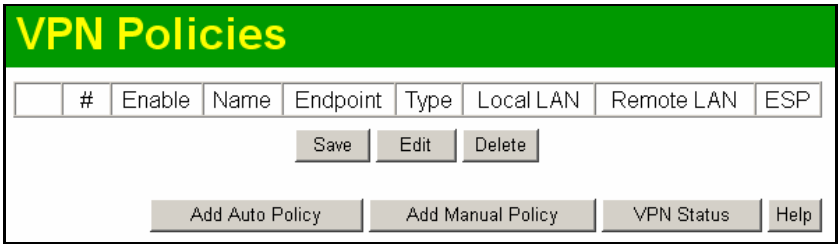

Figure 58: VPN Policies Screen

Data - VPN Policies Screen

Policy Table	The Policy Table contains the following data • **Enable** - Use this checkbox to Enable or Disable a Policy as required. Click "Save" after making any changes. • **Name** - Each policy is given a unique name to identify it. This name is not known to the remote VPN endpoint; it is used only to assist managing your policies. • **Endpoint** - The address of the remote VPN endpoint. • **Type** - The Type is "Auto" or "Manual" as explained above. • **Local LAN** - IP address or subnet on your local LAN. Traffic must be from (or to) these addresses to be covered by this policy. • **Remote LAN** - IP address or subnet on the remote LAN. Traffic must be to (or from) these addresses to be covered by this policy. • **ESP** - ESP (Encapsulating Security Payload) encryption protocol used for the VPN data.
Buttons	
Save	Save any changes to the "Enable" setting for each policy.
Edit	Edit (modify) the selected policy. (Select a policy by clicking on the radio button.)
Delete	Delete the selected policy. (Select a policy by clicking on the radio button.)
Add Auto Policy	Change to the input screen for an "Auto" policy. See the following section for details. When the new policy is saved, it will appear in the bottom row of the Policy Table.

Add Manual Policy	Change to the input screen for an "Manual" policy. See the following section for details. When the new policy is saved, it will appear in the bottom row of the Policy Table.
VPN Status	View details of each current VPN Tunnel (connection) in a sub-window. You also have the option of viewing the VPN Log.

VPN Auto Policy Screen

This screen is displayed when you click the *Add Auto Policy* button on the ***VPN Policies*** screen, or when you edit an existing Auto Policy. It allows you to define or edit an "Auto" VPN policy.

An "Auto" VPN policy uses the IKE (Internet Key Protocol) to exchange and negotiate parameters for the IPsec SA (Security Association). Because of this negotiation, it is not necessary for all settings on this VPN Gateway to match the settings on the remote VPN endpoint. Where settings must match, this is indicated.

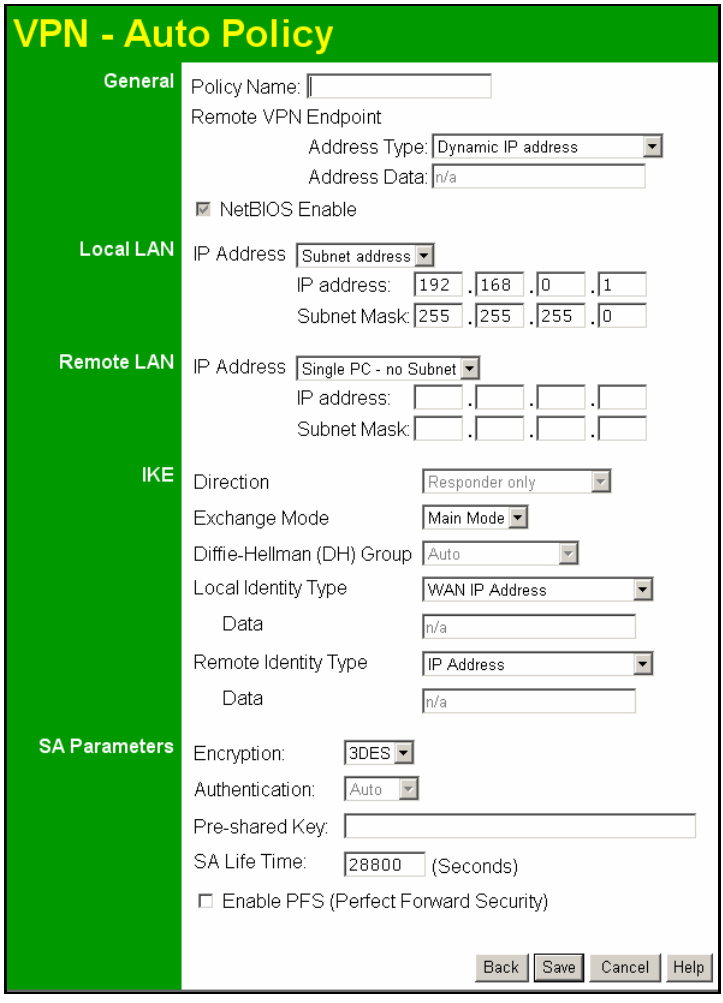

Figure 59: VPN-Auto Policy Screen

Data - VPN-Auto Policy Screen

General	
Policy Name	Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
Remote VPN Endpoint	If the remote endpoint has a dynamic IP address, select "Dynamic IP address". No "Address Data" input is required. Otherwise, select the desired option (IP address or Domain Name) and enter the address of the remote VPN endpoint you wish to connect to. **Note:** The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".
NETBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking.
Local LAN	
Local LAN	This identifies which PCs on your LAN are covered by this policy. For each selection, data must be provided as follows: • Single address Enter an IP address in the "IP address" field. Typically, this setting is used when you wish to make a single Server on your LAN available to remote users. • Subnet address Enter an IP address in the "IP address" field, and the desired network mask in the "Subnet Mask" field. The remote VPN endpoint must have these IP addresses entered as its "Remote" addresses.
Remote LAN	
Remote LAN	This identifies which PCs on the remote LAN are covered by this policy. For each selection, data must be provided as follows: • Single PC - no subnet Select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required. • Single address Enter an IP address in the "IP address" field. This must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN. • Subnet address Enter an IP address in the "IP address" field, and the desired network mask in the "Subnet Mask" field. The remote VPN endpoint must have these IP addresses entered as its "Local" addresses.

IKE	
Direction	This setting is used when determining if the IKE policy matches the current traffic. Select the desired option. • Responder only - Incoming connections are allowed, but outgoing connections will be blocked. • Initiator and Responder - Both incoming and outgoing connections are allowed.
Exchange Mode	IPSec has 2 possibilities - "Main Mode" and "Aggressive Mode". Currently, only "Main Mode" is supported. Ensure the remote VPN endpoint is set to use "Main Mode".
Diffie-Hellman (DH) Group	The Diffie-Hellman algorithm is used when exchanging keys. The DH Group setting determines the number of bit size used in the exchange. This value must match the value used on the remote VPN Gateway.
Local Identity Type	Select the desired option to match the "Remote Identity Type" setting on the remote VPN endpoint. • WAN IP Address - your Internet IP address. • Fully Qualified Domain Name - your domain name. • Fully Qualified User Name - your name, E-mail address, or other ID.
Remote Identity Type	Select the desired option to match the "Local Identity Type" setting on the remote VPN endpoint. • IP Address - The Internet IP address of the remote VPN endpoint. • Fully Qualified Domain Name - the Domain name of the remote VPN endpoint. • Fully Qualified User Name - the name, E-mail address, or other ID of the remote VPN endpoint.
Remote Identity Data	Enter the data for the selection above. (If "IP Address" is selected, no input is required.)
SA Parameters	
Encryption	Encryption Algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN Gateway.
Authentication	Authentication Algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN Gateway.
Pre-shared Key	The key must be entered both here and on the remote VPN Gateway. This method does not require using a CA (Certificate Authority).
SA Life Time	This determines the time interval before the SA (Security Association) expires. (It will automatically be re-established if necessary.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA Life Time. This setting applies to both IKE and IPSec SAs.

IPSec PFS (Perfect Forward Secrecy)	If enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.) This setting applies to both IKE and IPSec SAs. When configuring the remote endpoint to match this setting, you may have to specify the "Key Group" used. For this device, the "Key Group" is the same as the "DH Group" setting in the IKE section.

VPN- Manual Policy Screen

This screen is displayed when you click the *Add Manual Policy* button on the ***VPN Policies*** screen, or when you edit an existing Manual Policy. It allows you to define or edit a "Manual" VPN policy.

An "Manual" VPN policy requires that you enter all data on both VPN endpoints. There is no negotiation between the 2 VPN endpoints.

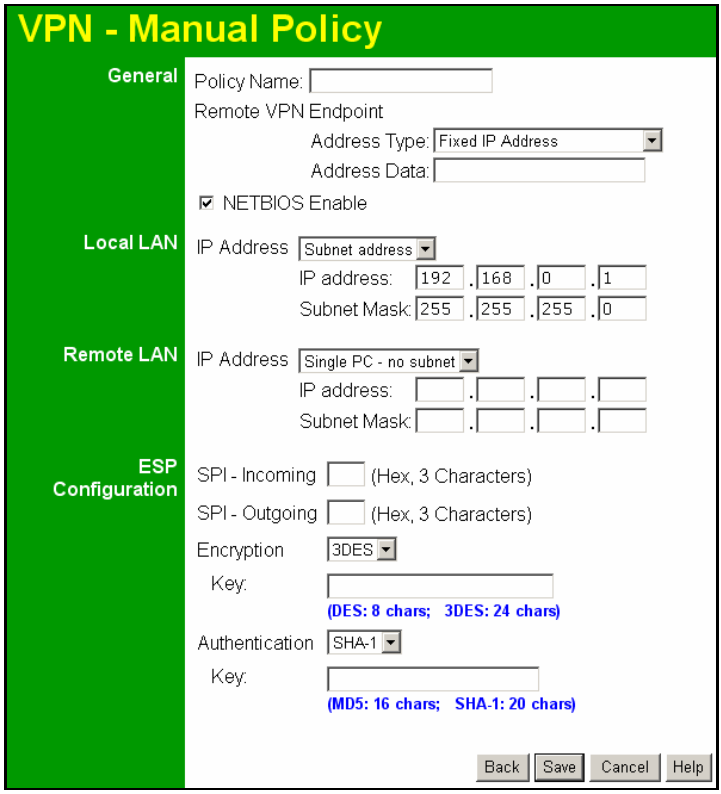

Figure 60: VPN-Manual Policy Screen

Data - VPN-Manual Policy Screen

General	
Policy Name	Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
Remote VPN Endpoint	Select the desired option (IP address or Domain Name) and enter the address of the remote VPN endpoint you wish to connect to. **Note:** The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".
NETBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking.

Local LAN	
Local LAN	This identifies which PCs on your LAN are covered by this policy. For each selection, data must be provided as follows: • Single address Enter an IP address in the "IP address" field. Typically, this setting is used when you wish to make a single Server on your LAN available to remote users. • Subnet address Enter an IP address in the "IP address" field, and the desired network mask in the "Subnet Mask" field. The remote VPN endpoint must have these IP addresses entered as its "Remote" addresses.
Remote LAN	
Remote LAN	This identifies which PCs on the remote LAN are covered by this policy. For each selection, data must be provided as follows: • Single PC - no subnet Select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required. • Single address Enter an IP address in the "IP address" field. This must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN. • Subnet address Enter an IP address in the "IP address" field, and the desired network mask in the "Subnet Mask" field. The remote VPN endpoint must have these IP addresses entered as its "Local" addresses.
ESP Configuration	
SPI	Enter the required SPIs. Each policy must have unique SPIs. These settings must match the remote VPN endpoint. Note that the "in" setting here must match the "out" setting on the remote VPN endpoint, and the "out" setting here must match the "in" setting on the remote VPN endpoint.
Encryption	Select the desired Encryption Algorithm, and enter the key in the field provided. • For DES, the key should be 8 ASCII characters (16 Hex characters). • For 3DES, the key should be 24 ASCII characters (48 Hex characters).
Authentication	Select the desired Authentication Algorithm, and enter the key in the field provided. • For MD5, the key should be 16 ASCII characters (32 Hex characters). • For SHA-1, the key should be 20 ASCII (40 Hex characters).

VPN Status Screen

This screen is displayed when you click the VPN Log button on the VPN Policies screen, or on the Status screen.

This screen allows you to view details of each current VPN Tunnel (connection). If there are no current connections, the status table will be empty.

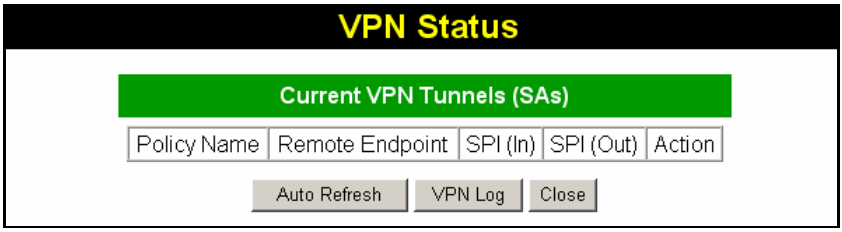

Figure 61: VPN-Status Screen

Data - VPN Status Screen

Tunnel Table	This table contains the following data about each current connection. • **Policy Name** - The name of the policy. When a policy is created, it must be given a unique name to identify it. • **Remote Endpoint** - The address of the remote VPN endpoint. • **SPI (In)** - This is a unique index number to identify the incoming connection. For "Auto" policies, the SPI is automatically generated. For "Manual" policies, the SPI must be entered when the policy is configured. • **SPI (Out)** - This is a unique index number to identify the outgoing connection. For "Auto" policies, the SPI is automatically generated. For "Manual" policies, the SPI must be entered when the policy is configured. • **Action** - This column will contain a button which allows you to break (terminate) the current the VPN connection.
Buttons	
Auto Refresh	Use this to Enable or Disable auto-refresh for this screen. If enabled, the screen will be updated every few seconds. The status bar on the bottom on the screen will indicate if auto-refresh is enabled or disabled.
VPN Log	Click this button to switch to the VPN log screen. The VPN log shows details of each connection as it is created.

Chapter 7
Advanced Administration

This Chapter explains the settings available via the "Administration" section of the menu.

Overview

Normally, it is not necessary to use these screens, or change any settings. These screens and settings are provided to deal with non-standard situations, or to provide additional options for advanced users.

The available settings and features are:

PC Database	This is the list of PCs shown when you select the "DMZ PC" or a "Virtual Server". This database is maintained automatically, but you can add and delete entries for PCs which use a Fixed (Static) IP Address.
Config File	Backup or restore the configuration file for the Wireless ADSL Router. This file contains all the configuration data.
Logging & Email	View or clear all logs, set E-Mailing of log files and alerts.
Diagnostics	Perform a Ping or DNS Lookup.
Remote Admin	Allow settings to be changed from the Internet..
Routing	Only required if your LAN has other Routers or Gateways.
Upgrade Firmware	Upgrade the Firmware (software) installed in your Wireless ADSL Router.

PC Database

The PC Database is used whenever you need to select a PC (e.g. for the "DMZ" PC).

- It eliminates the need to enter IP addresses.
- Also, you do not need to use fixed IP addresses on your LAN.

However, if you do use a fixed IP address on some devices on your LAN, you should enter details of each such device into the PC database, using the PC Database screen.

PC Database Screen

An example ***PC Database*** screen is shown below.

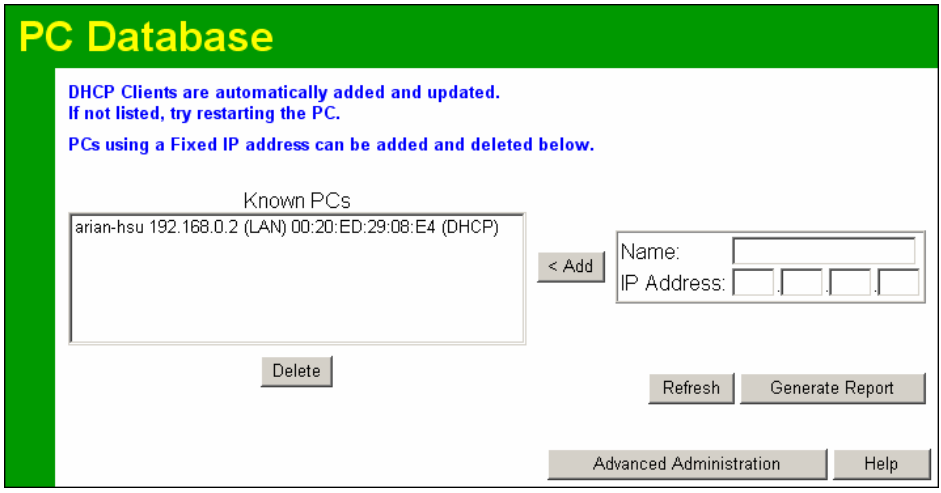

Figure 62: PC Database

- PCs which are "DHCP Clients" are automatically added to the database, and updated as required.
- By default, non-Server versions of Windows act as "DHCP Clients"; this setting is called "Obtain an IP Address automatically".
- The Wireless ADSL Router uses the "Hardware Address" to identify each PC, not the name or IP address. The "Hardware Address" can only change if you change the PC's network card or adapter.
- This system means you do NOT need to use Fixed (static) IP addresses on your LAN. However, you can add PCs using Fixed (static) IP Addresses to the PC database if required.

Data - PC Database Screen

Known PCs	This lists all current entries. Data displayed is *name (IP Address) type*. The "type" indicates whether the PC is connected to the LAN.
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	Enter the IP Address of the PC. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Buttons	
Add	This will add the new PC to the list. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Delete	Delete the selected PC from the list. This should be done in 2 situations: • The PC has been removed from your LAN. • The entry is incorrect.
Refresh	Update the data on screen.
Generate Report	Display a read-only list showing full details of all entries in the PC database.
Advanced Administration	View the Advanced version of the PC database screen - ***PC Database (Admin)***. See below for details.

PC Database - Advanced

This screen is displayed if the "Advanced Administration" button on the ***PC Database*** is clicked. It provides more control than the standard ***PC Database*** screen.

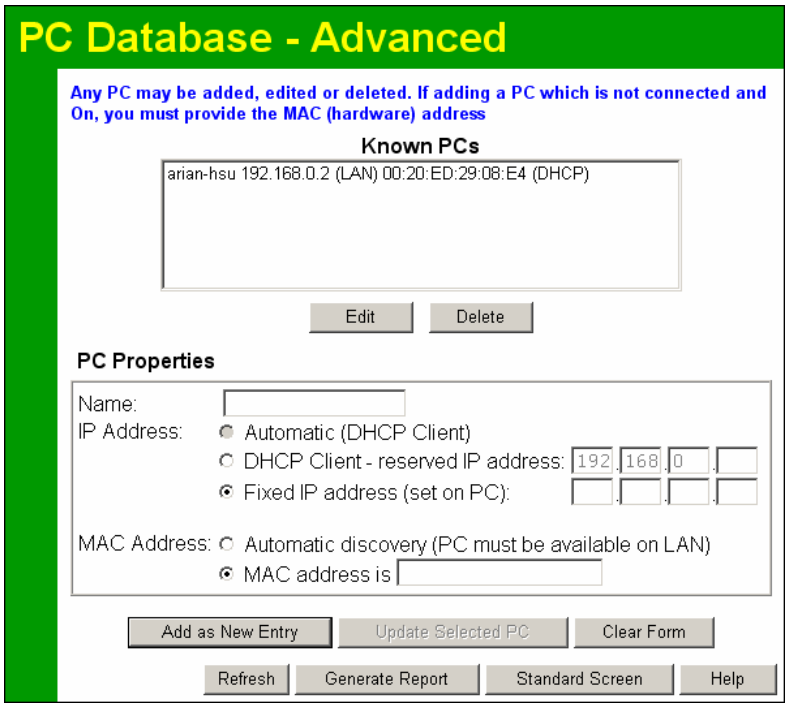

Figure 63: PC Database (Admin)

Data - Advanced PC Database

Known PCs	This lists all current entries. Data displayed is *name (IP Address) type*. The "type" indicates whether the PC is connected to the LAN.
PC Properties	
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	Select the appropriate option: • **Automatic** - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The Wireless ADSL Router will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't. • **DCHP Client - Reserved IP Address** - Select this if the PC is set to be a DCHP client, and you wish to guarantee that the Wireless ADSL Router will always allocate the same IP Address to this PC. Enter the required IP address. • **Fixed IP Address** - Select this if the PC is using a Fixed (Static) IP address. Enter the IP address allocated to the PC. (The PC itself must be configured to use this IP address.)

MAC Address	Select the appropriate option • **Automatic discovery** - Select this to have the Wireless ADSL Router contact the PC and find its MAC address. This is only possible if the PC is connected to the LAN and powered On. • **MAC address is** - Enter the MAC address on the PC. The MAC address is also called the "Hardware Address", "Physical Address", or "Network Adapter Address". The Wireless ADSL Router uses this to provide a unique identifier for each PC. Because of this, the MAC address can NOT be left blank.
Buttons	
Add as New Entry	Add a new PC to the list, using the data in the "Properties" box. If "Automatic discovery" (for MAC address) is selected, the PC will be sent a "ping" to determine its hardware address. This will fail unless the PC is connected to the LAN, and powered on.
Update Selected PC	Update (modify) the selected PC, using the data in the "Properties" box.
Clear Form	Clear the "Properties" box, ready for entering data for a new PC.
Refresh	Update the data on screen.
Generate Report	Display a read-only list showing full details of all entries in the PC database.
Standard Screen	Click this to view the standard ***PC Database*** screen.

Config File

This feature allows you to download the current settings from the Wireless ADSL Router, and save them to a file on your PC.

You can restore a previously-downloaded configuration file to the Wireless ADSL Router, by uploading it to the Wireless ADSL Router.

This screen also allows you to set the Wireless ADSL Router back to its factory default configuration. Any existing settings will be deleted.

An example ***Config File*** screen is shown below.

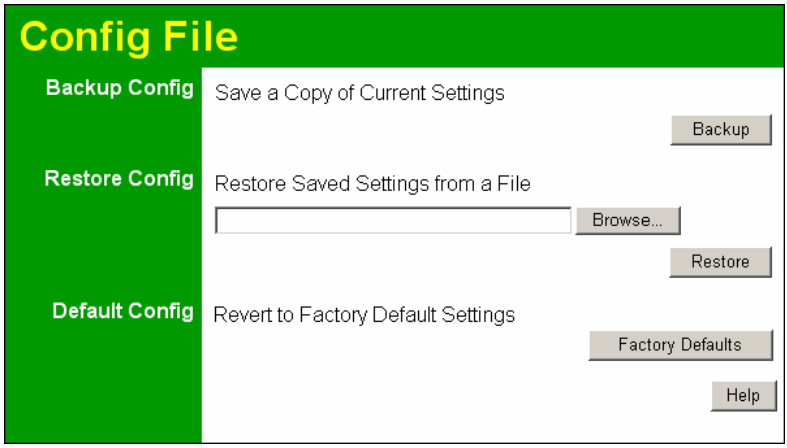

Figure 64: Config File Screen

Data - Config File Screen

Backup Config	Use this to download a copy of the current configuration, and store the file on your PC. Click *Download* to start the download.
Restore Config	This allows you to restore a previously-saved configuration file back to the Wireless ADSL Router. Click *Browse* to select the configuration file, then click *Restore* to upload the configuration file. **WARNING !** Uploading a configuration file will destroy (overwrite) ALL of the existing settings.
Default Config	Clicking the *Factory Defaults* button will reset the Wireless ADSL Router to its factory default settings. **WARNING !** This will delete ALL of the existing settings.

Logging

The Logs record various types of activity on the Wireless ADSL Router. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance.

Since only a limited amount of log data can be stored in the Wireless ADSL Router, log data can also be E-mailed to your PC. Use the ***E-mail*** screen to configure this feature.

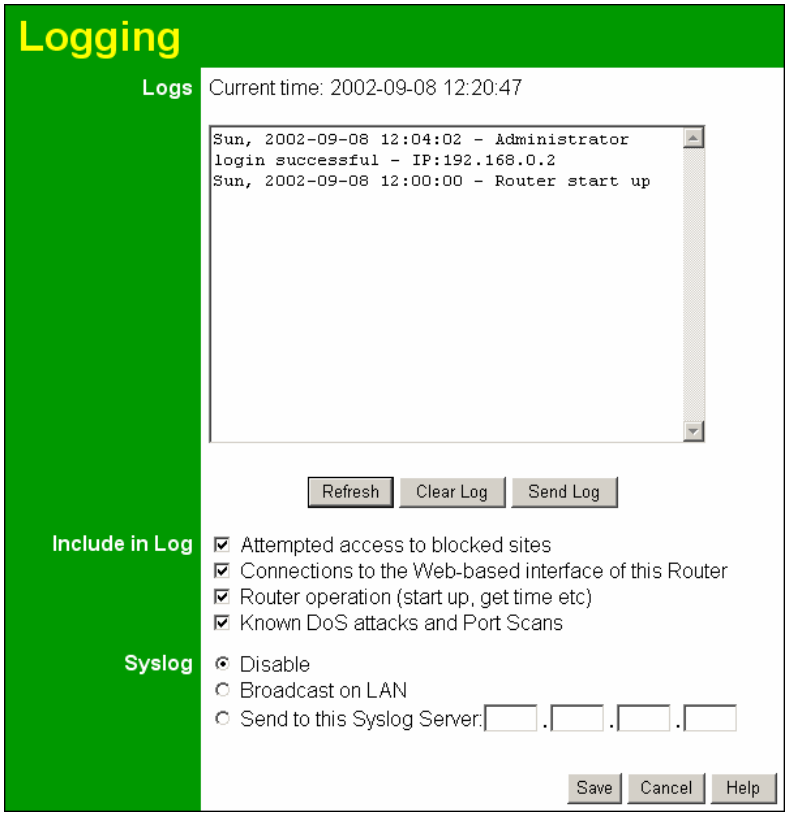

Figure 65: Logging Screen

Data - Logging Screen

Logs	
Current Time	The current time on the Wireless ADSL Router is displayed.
Log Data	Current log data is displayed in this panel.
Buttons	There are three (3) buttons • **Refresh** - Update the log data. • **Clear Log** - Clear the log, and restart it. This makes new messages easier to read. • **Send Log** - E-mail the log immediately. This is only functional if the ***E-mail*** screen has been configured.

Logs	
Include (Checkboxes)	Use these checkboxes to determine which events are included in the log. Checking all options will increase the size of the log, so it is good practice to disable any events which are not really required. • **Attempted access to blocked sites** - If checked, attempted Internet accesses which were blocked are logged. • **Connections to the Web-based interface of this Router** - If checked, this will log connections TO this Router, rather than through this Router to the Internet. • **Router operation** - If checked, other Router operations (not covered by the selections above) will be logged. • **Known DoS attacks and Port Scans** - If checked, Denial of Service attacks, as well as port scans, will be logged.
Syslog	
Disable	Data is not sent to a Syslog Server.
Broadcast on LAN	The Syslog data is broadcast, rather than sent to a specific Syslog server. Use this if your Syslog Server does not have a fixed IP address.
Syslog	If your Syslog server has a fixed IP address, select this option, and enter the IP address of your Syslog server.

E-mail

This screen allows you to E-mail Logs and Alerts. A sample screen is shown below.

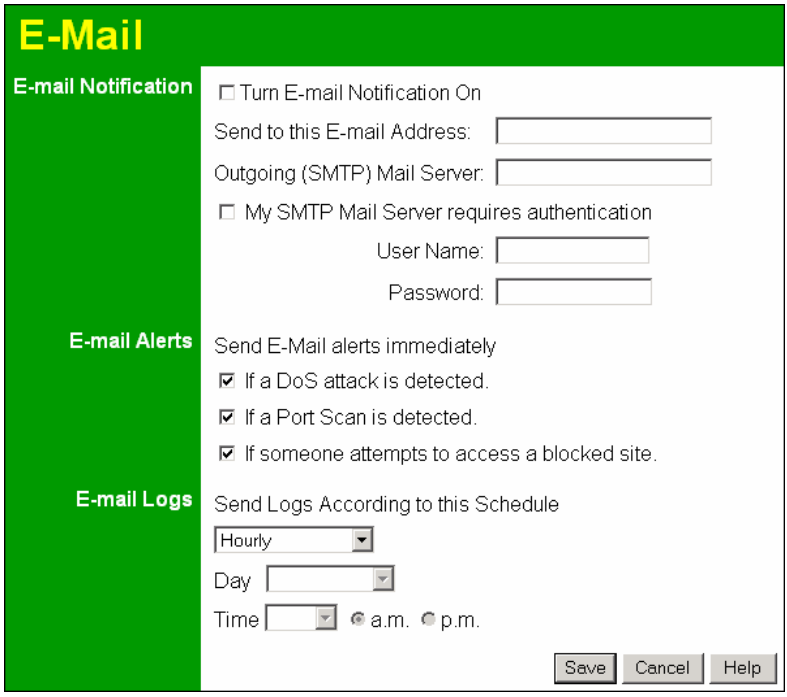

Figure 66: E-mail Screen

Data - E-mail Screen

E-Mail Notification	
Turn E-mail Notification on	Check this box to enable this feature. If enabled, the E-mail address information (below) must be provided.
Send to this E-mail address	Enter the E-mail address the Log is to be sent to. The E-mail will also show this address as the Sender's address.
Outgoing (SMTP) Mail Server	Enter the address or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for outgoing E-mail.
My SMTP Mail Server requires authentication	To stop spanners, many SMTP mail servers require you to log in to send mail. In this case, enable this checkbox, and enter the login information (User name and Password) in the fields below.
User Name	If you have enabled "My SMTP Mail Server requires authentication" above, enter the User Name required to login to your SMTP Server.
Password	If you have enabled "My SMTP Mail Server requires authentication" above, enter the password required to login to your SMTP Server.

E-mail Alerts	
Send E-mail alerts immediately	You can choose to have alerts E-mailed to you, by checking the desired checkboxes. The Broadband ADSL Router can send an immediate alert when it detects a significant security incident such as • A known hacker attack is directed at your IP address • A computer on the Internet scans your IP address for open ports • Someone on your LAN (Local Area Network) tries to visit a blocked site.
E-mail Logs	

Send Logs	Select the desired option for sending the log by E-mail.
	• **Never** (default) - This feature is disabled; Logs are not sent.
	• **When log is full** - The time is not fixed. The log will be sent when the log is full, which will depend on the volume of traffic.
	• **Hourly, Daily, Weekly...** - The log is sent on the interval specified.
	  • If **Daily** is selected, the log is sent at the time specified. Select the time of day you wish the E-mail to be sent.
	  • If **Weekly** is selected, the log is sent once per week, on the specified day, at the specified time. Select the day and the time of day you wish the E-mail to be sent.
	Note:
	If the log is full before the time specified to send it, it will be sent regardless of the day and time specified.

Diagnostics

This screen allows you to perform a "Ping" or a "DNS lookup". These activities can be useful in solving network problems.

An example ***Network Diagnostics*** screen is shown below.

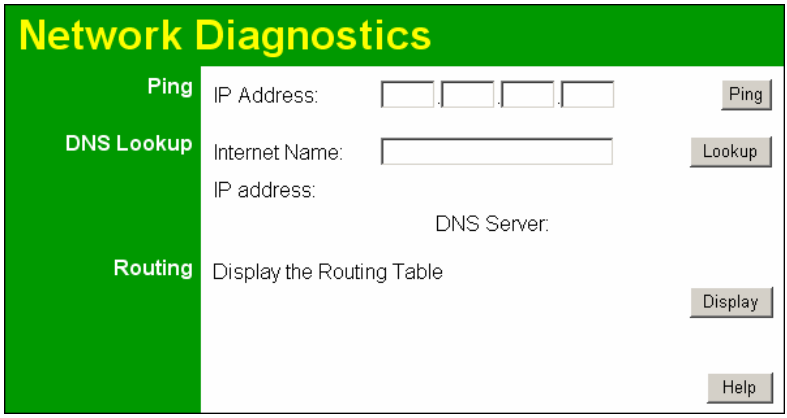

Figure 67: Network Diagnostics Screen

Data - Network Diagnostics Screen

Ping	
Ping this IP Address	Enter the IP address you wish to ping. The IP address can be on your LAN, or on the Internet. Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.
Ping Button	After entering the IP address, click this button to start the "Ping" procedure. The results will be displayed in the *Ping Results* pane.
DNS Lookup	
Internet name	Enter the Domain name or URL for which you want a DNS (Domain Name Server) lookup. Note that if the address in on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.
Lookup Button	After entering the Domain name/URL, click this button to start the "DNS Lookup" procedure.
Routing	
Display	Click this button to display the internal routing table. This information can be used by Technical Support and other staff who understand Routing Tables.

Remote Administration

If enabled, this feature allows you to manage the Wireless ADSL Router via the Internet.

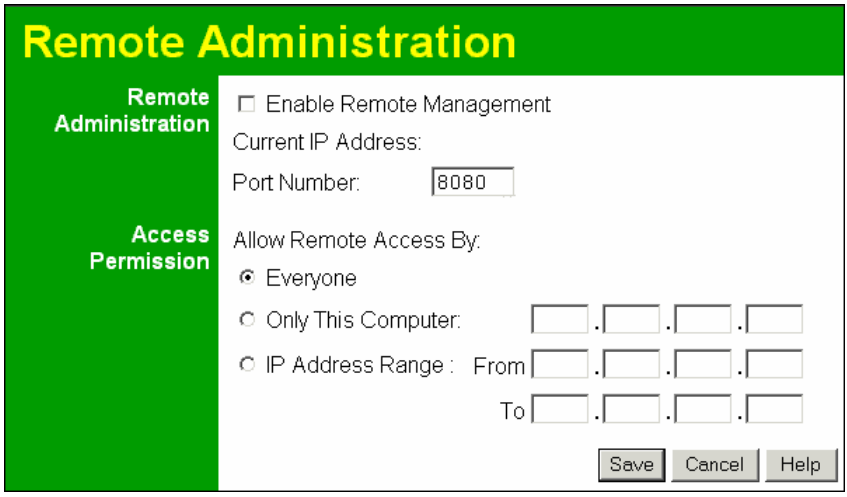

Figure 68: Remote Administration Screen

Data - Remote Administration Screen

Remote Administration	
Enable Remote Management	Check to allow administration/management via the Internet. (To connect, see below). If Disabled, this device will ignore Administration connection attempts from the Internet.
Current IP Address	This is the current address you will use when accessing this device from the Internet. To connect, see details and an example below.
Port Number	Enter a port number between 1 and 65535. The default for HTTP (Web) connections is port 80, but using port 80 will prevent the use of a Web "Virtual Server" on your LAN. So using a different port number is recommended. The default value is 8080. The port number must be specified in your Browser when you connect. See the following section for details.
Access Permission	
Allow Remote Access	Select the desired option. • **Everyone** - allow access by everyone on the Internet. • **Only This Computer** - allow access by only one IP address. Enter the desired IP address. • **IP Address Range** - allow access from a range of IP addresses on the Internet. Enter a beginning and ending IP address to define the allowed range. For security, you should restrict access to as few external IP addresses as practical.

To connect from a remote PC via the Internet

1. Ensure your Internet connection is established, and start your Web Browser.
2. In the "Address" bar, enter "HTTP://" followed by the Internet IP Address of the Wireless ADSL Router. If the port number is not 80, the port number is also required. (After the IP Address, enter ":" followed by the port number.)
   e.g.

   ```
   HTTP://123.123.123.123:8080
   ```

   This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.
3. You will then be prompted for the login name and password for this device.

Routing

Overview

- If you don't have other Routers or Gateways on your LAN, you can ignore the "Routing" page completely.
- If the Wireless ADSL Router is only acting as a Gateway for the local LAN segment, ignore the "Routing" page even if your LAN has other Routers.
- If your LAN has a standard Router (e.g. Cisco) on your LAN, and the Wireless ADSL Router is to act as a Gateway for all LAN segments, enable RIP (Routing Information Protocol) and ignore the Static Routing table.
- If your LAN has other Gateways and Routers, and you wish to control which LAN segments use each Gateway, do NOT enable RIP (Routing Information Protocol). Configure the Static Routing table instead. (You also need to configure the other Routers.)
- If using Windows 2000 Data center Server as a software Router, enable RIP on the Wireless ADSL Router, and ensure the following Windows 2000 settings are correct:
  - Open *Routing and Remote Access*
  - In the console tree, select *Routing and Remote Access , [server name], IP Routing, RIP*
  - In the "Details" pane, right-click the interface you want to configure for RIP version 2, and then click "Properties".
  - On the "General" tab, set *Outgoing packet protocol* to "RIP version 2 broadcast", and *Incoming packet protocol* to "RIP version 1 and 2".

Routing Screen

The routing table is accessed by the *Routing* link on the *Administration* menu.

Using this Screen

Generally, you will use either RIP (Routing Information Protocol) OR the Static Routing Table, as explained above, although is it possible to use both methods simultaneously.

Static Routing Table

- If RIP is not used, an entry in the routing table is required for each LAN segment on your Network, other than the segment to which this device is attached.
- The other Routers must also be configured. See *Configuring Other Routers on your LAN* later in this chapter for further details and an example.

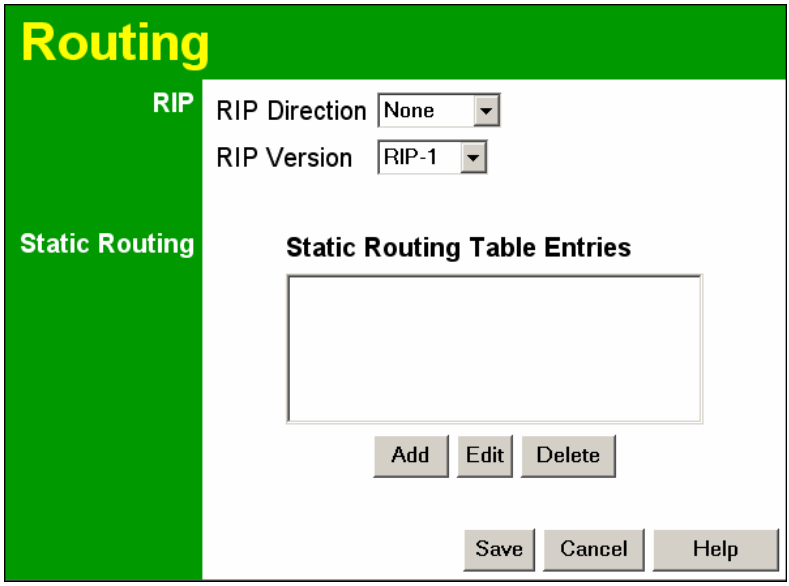

Figure 69: Routing Screen

Data - Routing Screen

RIP	
RIP Direction	Select the desired RIP Direction.
RIP Version	Choose the RIP Version for the Server.
Static Routing	
Static Routing Table Entries	This list shows all entries in the Routing Table. • This area shows details of the selected item in the list. • Change any the properties as required, then click the "Edit" button to save the changes to the selected entry.
Buttons	
Add	Add a new entry to the Static Routing table, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.
Edit	Update the current Static Routing Table entry, using the data shown in the table area on screen.
Delete	Delete the current Static Routing Table entry.
Save	Save the RIP setting. This has no effect on the Static Routing Table.

Configuring Other Routers on your LAN

It is essential that all IP packets for devices not on the local LAN be passed to the Wireless ADSL Router, so that they can be forwarded to the external LAN, WAN, or Internet. To achieve this, the local LAN must be configured to use the Wireless ADSL Router as the *Default Route* or *Default Gateway*.

Local Router

The local router is the Router installed on the same LAN segment as the Wireless ADSL Router. This router requires that the *Default Route* is the Wireless ADSL Router itself. Typically, routers have a special entry for the *Default Route*. It should be configured as follows.

Destination IP Address	Normally 0.0.0.0, but check your router documentation.
Network Mask	Normally 0.0.0.0, but check your router documentation.
Gateway IP Address	The IP Address of the Wireless ADSL Router.
Metric	1

Other Routers on the Local LAN

Other routers on the local LAN must use the Wireless ADSL Router's *Local Router* as the *Default Route*. The entries will be the same as the Wireless ADSL Router's local router, with the exception of the *Gateway IP Address*.

- For a router with a direct connection to the Wireless ADSL Router's local Router, the *Gateway IP Address* is the address of the Wireless ADSL Router's local router.
- For routers which must forward packets to another router before reaching the Wireless ADSL Router's local router, the *Gateway IP Address* is the address of the intermediate router.

Static Routing - Example

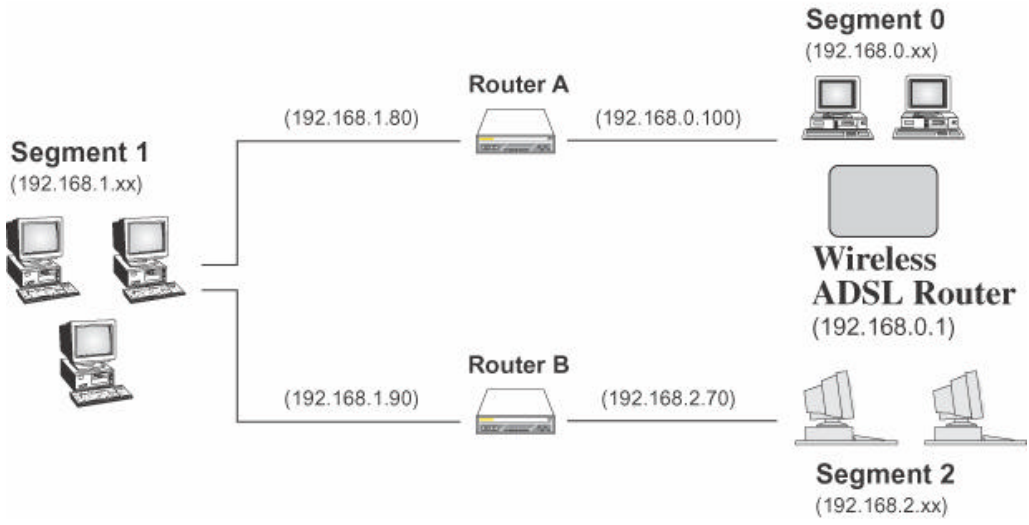

Figure 70: Routing Example

For the Wireless ADSL Router's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the Wireless ADSL Router requires 2 entries as follows.

Entry 1 (Segment 1)	
Destination IP Address	192.168.1.0
Network Mask	255.255.255.0 (Standard Class C)

Gateway IP Address	192.168.0.100 (Wireless ADSL Router's local Router)
Metric	2
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100
Metric	3

For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.0.1 (Wireless ADSL Router's IP Address)

For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 (Wireless ADSL Router's local router)

Upgrade Firmware

The firmware (software) in the Wireless ADSL Router can be upgraded using your Web Browser.

You must first download the upgrade file, then select *Upgrade Firmware* on the *Administration* menu. You will see a screen like the following.

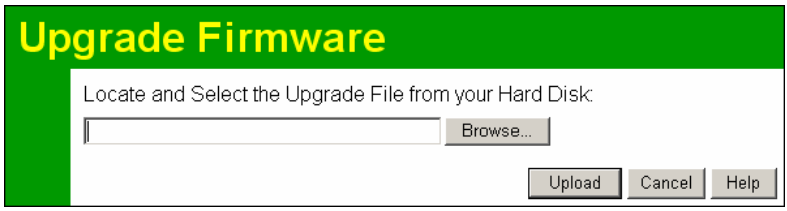

Figure 71: Router Upgrade Screen

To perform the Firmware Upgrade:

1. Click the *Browse* button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the *Upgrade File* field.
3. Click the *Upload* button to commence the firmware upgrade.

The Wireless ADSL Router is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the Wireless ADSL Router will be lost.

Chapter 8
Modem Mode

This Chapter explains configuration and operation when in "Modem" or "Bridge" mode..

Overview

There are two modes available on the ***Mode*** screen.

- **Router** - Both the ADSL Modem and the Router features are operational. In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless and LAN users.
- **Modem** - Only the ADSL Modem component is operational. All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point.

This Chapter describes operation while in **Modem Mode**, also called **Bridge Mode**.

Management Connections

When this device restarts in Modem mode, the IP address does not change, but the DHCP server is disabled. However, your PC will usually retain the IP address provided by the DHCP Server, so the connection will be automatically re-established. You then need to ensure that the IP address of this modem is suitable for your LAN.

- You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point.
- This Modem/AP must be a valid device on your LAN, to allow management connections. You must assign a (fixed) IP address which is within the address range used on your LAN, but not within the address range used by your DHCP server.

When you connect in future, just connect normally, using the IP address you assigned.

1. Start your WEB browser.
2. In the *Address* box, enter "HTTP://" and the current IP Address of the Wireless ADSL Modem, as in this example, which uses the Wireless ADSL Modem's default IP Address:

   `HTTP://192.168.0.1`
3. When prompted for the User name and Password, enter `admin` for the user name, and the current password, as set on the password screen. (The password is the same regardless of the mode.)

Home Screen

If in Modem mode, the home screen will look like the example below.

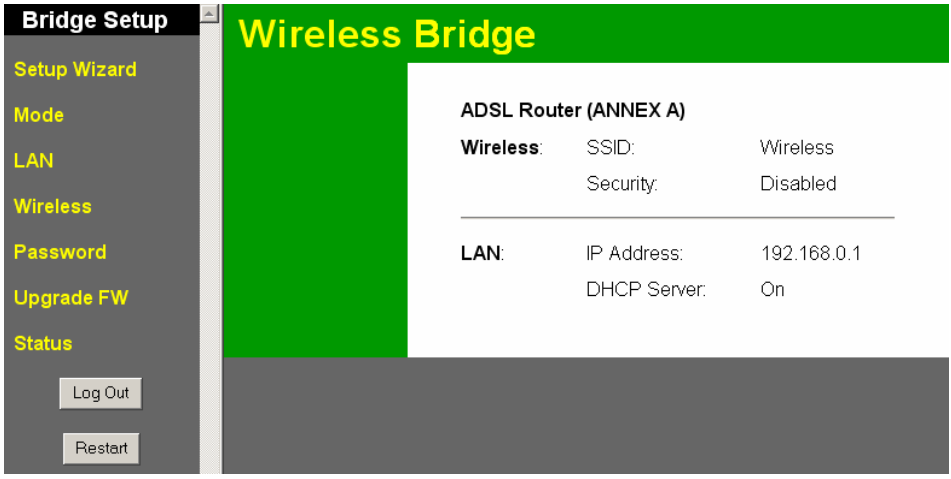

Figure 72: Home Screen - Modem Mode

Note that the menu has changed, many of the options in Router mode are not available. The screens available are:

- **Mode** - change back to Router mode, if desired.
- **LAN** - set IP address, mask and gateway. This is the same as in Router mode, except that the DHCP server is not available while in Modem mode.
- **Wireless** - this screen, and related sub-screens, is the same as in Router mode.
- **Password** - this screen is the same as in Router mode.
- **Upgrade Firmware** - this screen is the same as in Router mode.
- **Status** - displays current settings and status. See the following section for details.

Mode Screen

This screen is change back to Router mode, if desired.

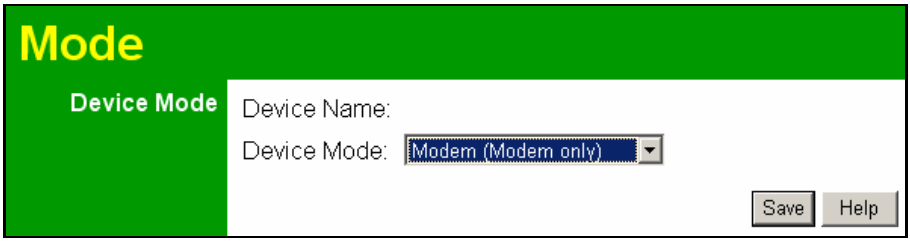

Figure 73: Mode Screen

Data - Mode Screen

Device Name	This field displays the current name of this device.
Device Mode	Select the desired device mode for the router: • **Router** - Both the ADSL Modem and the Router features are operational. In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless and LAN users. • **Modem** - Only the ADSL Modem component is operational. All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point. This mode is also called ***Bridge Mode***. After changing the mode, this device will restart, which will take a few seconds. The menu will also change, depending on the mode you are in.

Operation

Operation is automatic and transparent.

- Wireless clients can connect to the Access Point if they have the correct SSID and security, but they must obtain an IP address from the DHCP Server on your LAN.
- The modem will act like any other ADSL modem. No routing will be performed, and no client login will be done. If a client login is required, it must be performed by your Router/Gateway or by software on your PC.

Status Screen

In Modem mode, the Status screen looks like the example below.

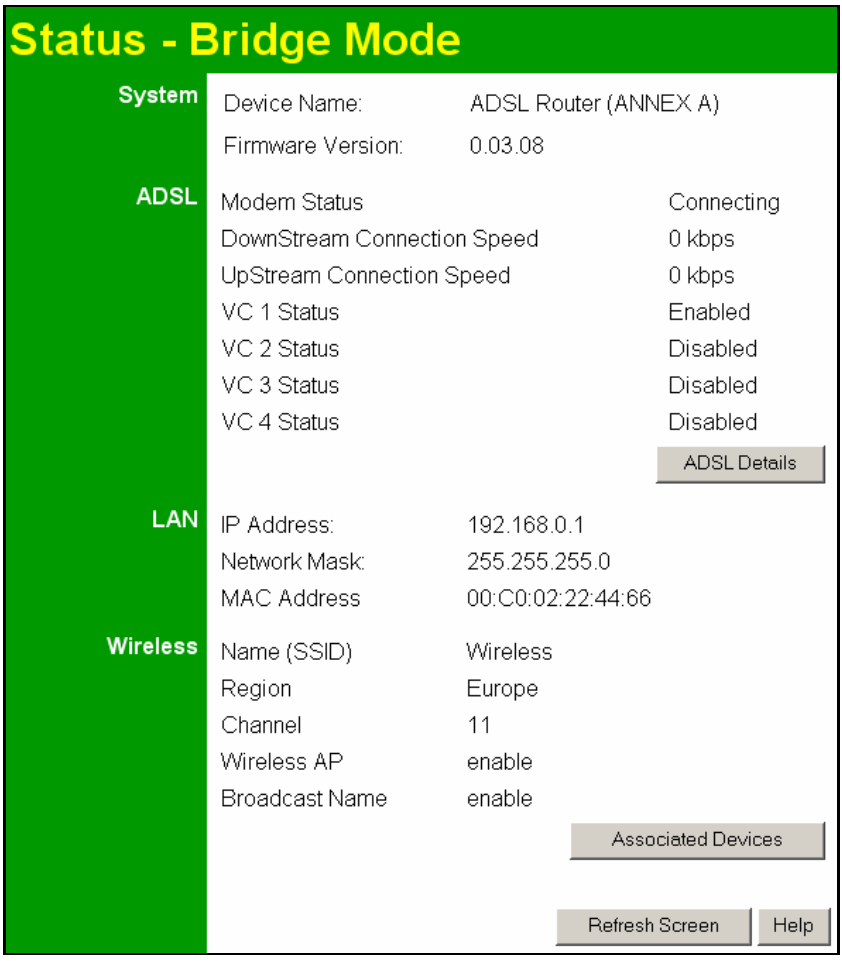

Figure 74: Status Screen - Bridge Mode

Data - Status Screen (Bridge Mode)

System	
Device Name	The current name of the Router. This name is also the "hostname" for users with an "@Home" type connection.
Firmware Version	The version of the current firmware installed.
ADSL	
Modem Status	This indicates the status of the ADSL modem component.
DownStream Connection Speed	Displays the speed for the DownStream Connection.
UpStream Connection Speed	If connected, displays the speed for the Up Stream (upload) ADSL Connection.

VC 1 Status **VC 2 Status** **VC 3 Status** **VC 4 Status**	For each VC (Virtual Circuit), the current status is displayed. This will be either "Enabled" or "Disabled".
ADSL Details	Click this button to open a sub-window and view the details of each VC (Virtual Circuit).
LAN	
IP Address	The IP Address of the Wireless ADSL Router.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
MAC Address	This shows the MAC Address for the Wireless ADSL Router, as seen on the LAN interface.
Wireless	
Name (SSID)	If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier).
Region	The current region, as set on the Wireless screen.
Channel	This shows the Channel currently used, as set on the Wireless screen.
Wireless AP	This indicates whether or not the Wireless Access Point feature is enabled.
Broadcast Name	This indicates whether or not the SSID is Broadcast. This setting is on the Wireless screen.
Associated Devices	Clicking this will generate a list of all devices currently using the Access Point.
Buttons	
ADSL Details	View the details of each VC (Virtual Circuit).
Associated Devices	Clicking this will generate a list of all devices currently using the Access Point.
Refresh Screen	Update the data displayed on screen.

Appendix A
Troubleshooting

This Appendix covers the most likely problems and their solutions.

Overview

This chapter covers some common problems that may be encountered while using the Wireless ADSL Router and some possible solutions to them. If you follow the suggested steps and the Wireless ADSL Router still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: **Can't connect to the Wireless ADSL Router to configure it.**

Solution 1: Check the following:

- The Wireless ADSL Router is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the Wireless ADSL Router are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the Wireless ADSL Router's default IP Address of 192.168.0.1. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless ADSL Router.
  In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1: **When I enter a URL or IP address I get a time out error.**

Solution 1: A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.
- If the PCs are configured correctly, but still not working, check the Wireless ADSL Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- Check the Wireless ADSL Router's status screen to see if it is working correctly.

Problem 2: **Some applications do not run properly when using the Wireless ADSL Router.**

Solution 2: The Wireless ADSL Router processes the data passing through it, so it is not transparent.

For incoming connections, you must use the Virtual Server or Firewall Rules to specify the PC which will receive the incoming traffic.

You can also use the *DMZ* function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

Wireless Access

Problem 1: **My PC can't locate the Wireless Access Point.**

Solution 1: Check the following.

- Your PC is set to *Infrastructure Mode*. (Access Points are always in *Infrastructure Mode*)
- The SSID on your PC and the Wireless Access Point are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the Wireless ADSL Router must have the same setting for WEP. The default setting for the Wireless ADSL Router is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled on the Wireless ADSL Router, your PC must have WEP enabled, and the key must match.
- If the Wireless ADSL Router's *Wireless* screen is set to *Allow Trusted PCs only*, then each of your Wireless stations must have been designated as "Trusted", or the Wireless station will be blocked.
- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless ADSL Router.
  Remember that the connection range can be as little as 100 feet in poor environments.

Problem 2: **Wireless connection speed is very slow.**

Solution 2: The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:

- Wireless ADSL Router location.
  Try adjusting the location and orientation of the Wireless ADSL Router.
- Wireless Channel
  If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference
  Other devices may be causing interference. You can experiment by switching other devices Off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding
  Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Wireless ADSL Router.

Appendix B
About Wireless LANs

This Appendix provides some background information about using Wireless LANs (WLANs).

Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.

Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.

BSS/ESS

BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

ESS

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. In fact, to reduce interference, it is recommended that adjacent Access Points SHOULD use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called **Roaming**. (Access Points do not have or require Roaming capabilities.)

Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channel are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted.

This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WEP	Off, 64 Bit, 128 Bit
Key	For 64 Bit encryption, the Key value must match. For 128 Bit encryption, the Key value must match
WEP Authentication	Open System or Shared Key.

WPA-PSK

WPA-PSK is another standard for encrypting data before it is transmitted. This is a later standard than WEP (Wired Equivalent Privacy), and provides greater security for your data. Data is encrypted using a 256Bit key which is automatically generated and changed often.

If all your Wireless stations support WPA-PSK, you should use this instead of WEP.

If WPA-PSK is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WPA PSK (Pre-shared Key)	Enter the same value on every station and the AP. The PSK must be from 8 to 63 characters in length. The 256Bit key used for the actual encryption is derived from this key.
Encryption	The same encryption method must be used. The most common encryption method is TKIP. Another widely-supported method is AES.

Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

Mode	On client Wireless Stations, the mode must be set to "Infrastructure". (The Access Point is always in "Infrastructure" mode.)
SSID (ESSID)	Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to. Alternatively, the SSID can be set to "any" or null (blank) to allow connection to any Access Point.
Wireless Security	The Wireless Stations and the Access Point must use the same settings for Wireless security. (None, WEP, WPA-PSK). **WEP:** If WEP is used, the Key size (64Bit, 128Bit), Key value, and Authentication settings must be the same on the Wireless Stations and the Access Point. **WPA-PSK:** If WPA-PSK is used, all Wireless Stations must be set to use WPA-PSK, and have the same Pre-shared Key and encryption system. For **Ad-hoc networks** (no Access Point), all Wireless stations must use the same security settings.

Appendix C
About VPNs

Overview

A VPN (Virtual Private Network) provides a secure connection between 2 points, over an insecure network - typically the Internet. This secure connection is called a **VPN Tunnel**.

There are many standards and protocols for VPNs. The standard implemented in the Wireless ADSL Router is **IPSec**.

IPSec

IPSec is a near-ubiquitous VPN security standard, designed for use with TCP/IP networks. It works at the packet level, and authenticates and encrypts all packets traveling over the VPN Tunnel. Thus, it does not matter what applications are used on your PC. Any application can use the VPN like any other network connection.

IPsec VPNs exchange information through logical connections called **SA**s (Security Associations). An SA is simply a definition of the protocols, algorithms and keys used between the two VPN devices (endpoints).

Each IPsec VPN has two SAs - one in each direction. If **IKE** (Internet Key Exchange) is used to generate and exchange keys, there are also SA's for the IKE connection as well as the IPsec connection.

There are two security modes possible with IPSec:

- **Transport Mode** - the payload (data) part of the packet is encapsulated through encryption but the IP header remains in the clear (unchanged).

  The Wireless ADSL Router does NOT support Transport Mode.

- **Tunnel Mode** - everything is encapsulated, including the original IP header, and a new IP header is generated. Only the new header in the clear (i.e. not protected). This system provides enhanced security.

  The Wireless ADSL Router always uses Tunnel Mode.

IKE

IKE (Internet Key Exchange) is an optional, but widely used, component of IPsec. IKE provides a method of negotiating and generating the keys and IDs required by IPSec. If using IKE, only a single key is required to be provided during configuration. Also, IKE supports using **Certificates** (provided by CAs - Certification Authorities) to authenticate the identify of the remote user or gateway.

If IKE is NOT used, then all keys and IDs (SPIs) must be entered manually, and Certificates can NOT be used. This is called a "Manual Key Exchange".

When using IKE, there are 2 phases to creating the VPN tunnel:

- **Phase I** is the negotiation and establishment up of the IKE connection.
- **Phase II** is the negotiation and establishment up of the IPsec connection.

Because the IKE and IPsec connections are separate, they have different SAs (security associations).

Policies

VPN configuration settings are stored in **Policies**.

Note that different vendors use different terms. Generally, the terms "VPN Policy", "IPSec Policy", and "IPSec Proposal" have the same meaning. However, some vendors separate IKE Policies (Phase 1 parameters) from IPSec Policies (Phase 2 parameters).

For the Wireless ADSL Router; each VPN policy contains both Phase 1 and Phase 2 parameters (if IKE is used). Each policy defines:

- The address of the remote VPN endpoint
- The traffic which is allowed to use the VPN connection.
- The parameters (settings) for the IPsec SA (Security Association)
- If IKE is used, the parameters (settings) for the IKE SA (Security Association)

Generally, you will need at least one (1) VPN Policy for each remote site for which you wish to establish VPN connections.

It is possible, and sometimes necessary, to have multiple Policies for the same remote site. However, you should only Enable one (1) policy at a time.

VPN Configuration

The general rule is that each endpoint must have matching Policies, as follows:

VPN Endpoint address	Each VPN endpoint must be configured to initiate or accept connections to the remote VPN client or Gateway. Usually, this requires having a fixed Internet IP address. However, it is possible for a VPN Gateway to accept incoming connections from a remote client where the client's IP address is not known in advance.
Local & Remote LAN definition	This determines which outgoing traffic will cause a VPN connection to be established, and which incoming traffic will be accepted. Each endpoint must be configured to pass and accept the desired traffic from the remote endpoint. If connecting 2 LANs, this requires that: • Each endpoint must be aware of the IP addresses used on the other endpoint. • The 2 LANs MUST use different IP address ranges.
IKE parameters	If using IKE (recommended), the IKE parameters must match (except for the SA lifetime, which can be different).
IPsec parameters	The IPsec parameters at each endpoint must match.

Common VPN Situations

VPN Pass-through

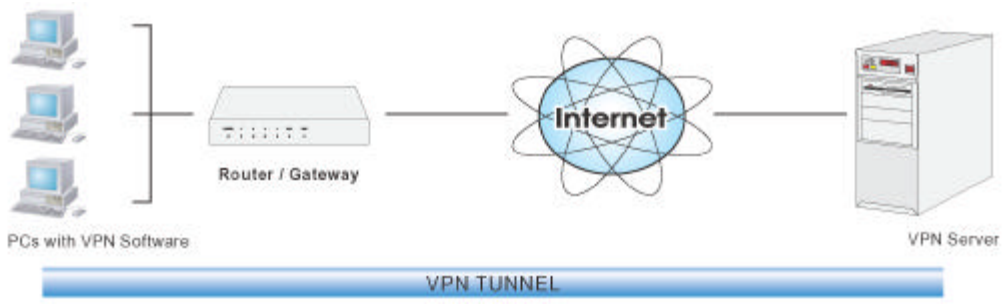

Figure 75: VPN Pass-through

Here, a PC on the LAN behind the Router/Gateway is using VPN software, but the Router/Gateway is NOT acting as a VPN endpoint. It is only allowing the VPN connection.

- The PC software can use any VPN protocol supported by the remote VPN.
- The remote VPN Server must support client PCs which are behind a NAT router, and so have an IP address which is not valid on the Internet.
- The Router/Gateway requires no VPN configuration, since it is not acting as a VPN end-point.

Client PC to VPN Gateway

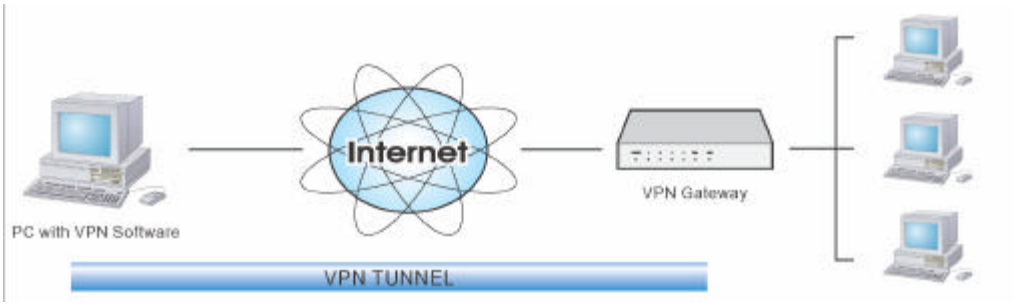

Figure 76: Client PC to VPN Server

In this situation, the PC must run appropriate VPN client software in order to connect, via the Internet, to the Wireless ADSL Router or other VPN Gateway. Once connected, the client PC has the same access to LAN resources as PCs on the local LAN (unless restricted by the network administrator).

- IPsec is not the only protocol which can be used in this situation, but the Wireless ADSL Router supports IPsec ONLY.
- Windows 2000 and Windows XP include an IPsec VPN client program. However, configuration of this client program for use with the Wireless ADSL Router is very complex and beyond the scope of this document.

Connecting 2 LANs via VPN

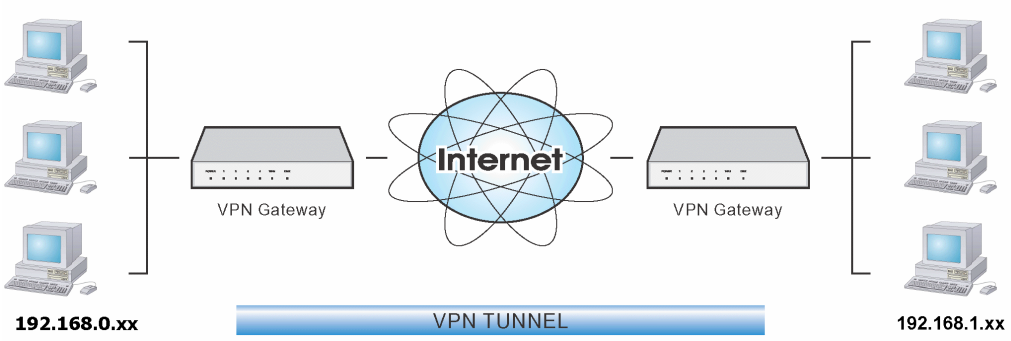

Figure 77: Connecting 2 VPN Gateways

This allows two (2) LANs to be connected. PCs on each endpoint gain secure access to the remote LAN.

- The 2 LANs MUST use different IP address ranges.
- The VPN Policies at each end determine when a VPN tunnel will be established, and what systems on the remote LAN can be accessed once the VPN connection is established.
- It is possible to have simultaneous VPN connections to many remote sites.

VPN Example

In this example, 2 LANs are connected via VPN. Each end has a Wireless ADSL Router.

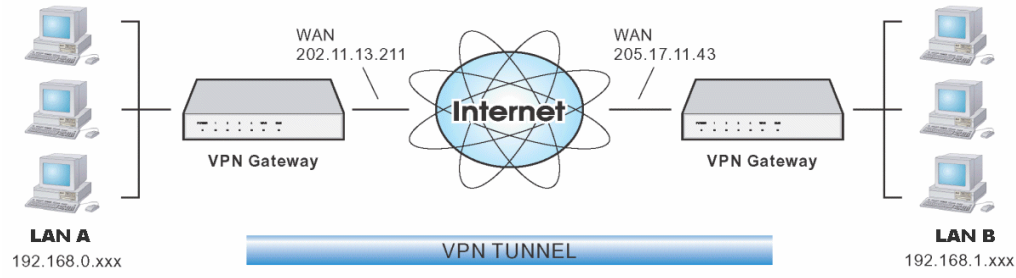

Figure 78: Connecting 2 Wireless ADSL Routers

Note

- The LANs MUST use different IP address ranges.
- Both endpoints have fixed WAN (Internet) IP addresses.
- This example uses an "Auto" policy, using IKE

Configuration Settings - Gateway A

Gateway A should be configured as shown below.

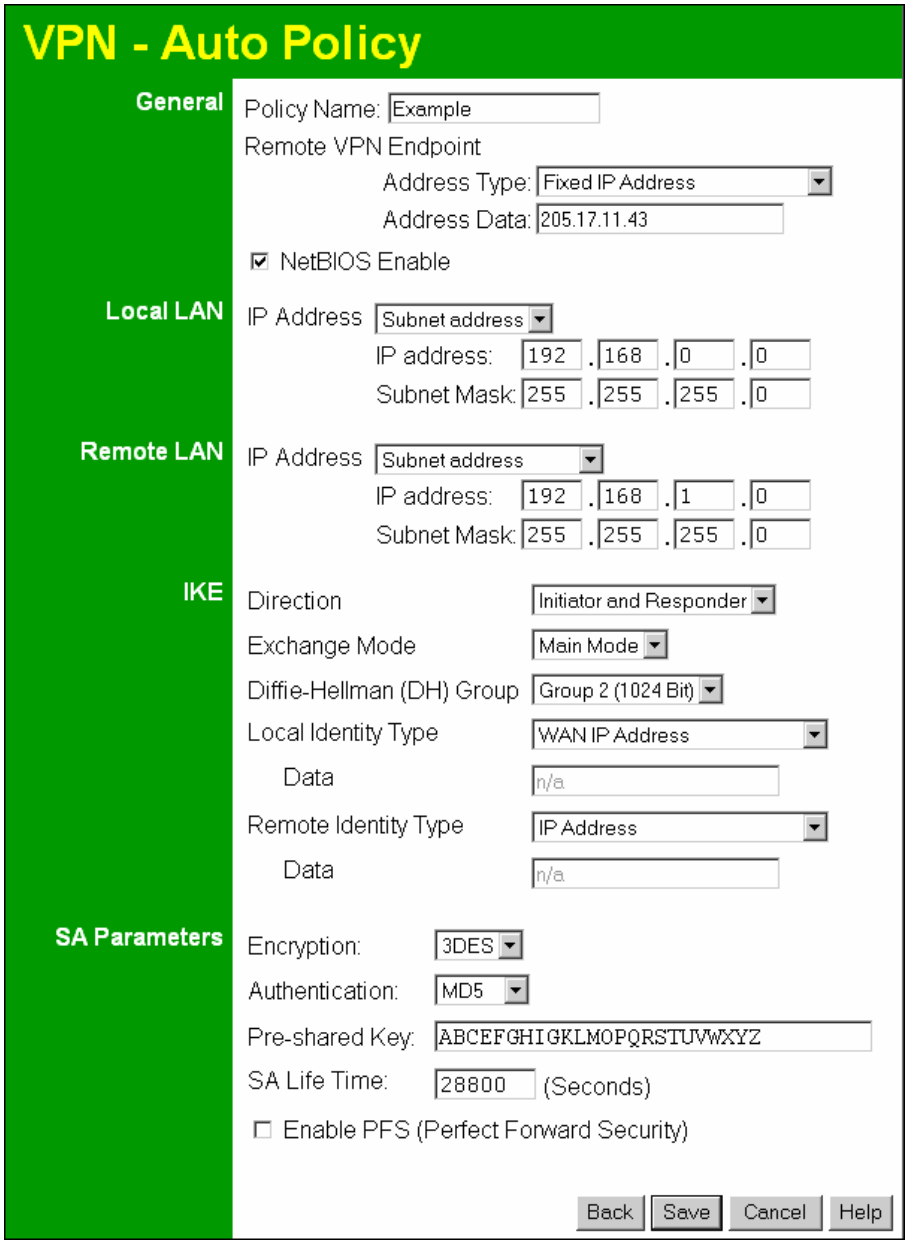

Figure 79: Gateway A Configuration

Configuration Settings - Gateway B

Gateway B should be configured as shown below.

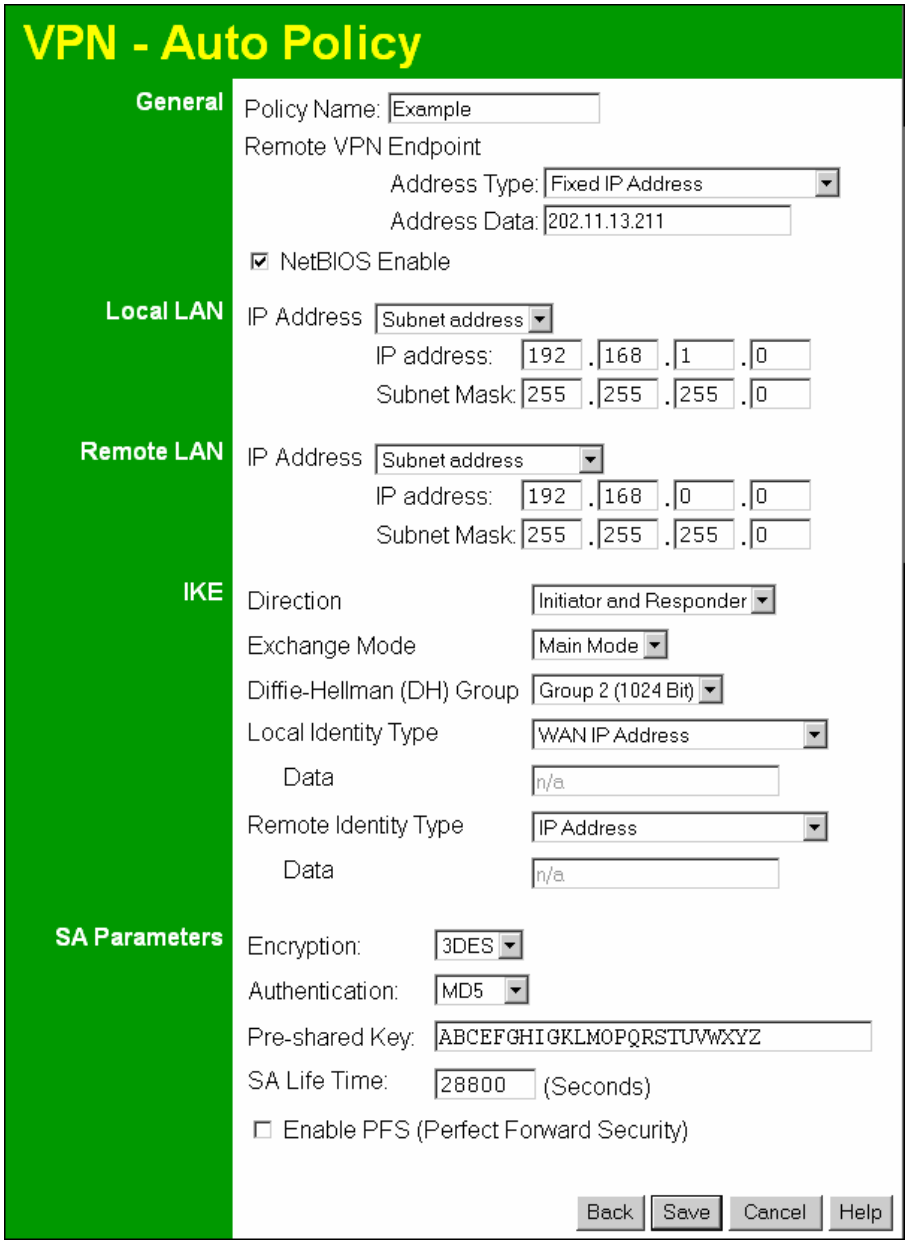

Figure 80: Gateway B Configuration

Settings

Setting	LAN A Gateway	LAN B Gateway	Notes
Policy Name	Example	Example	Name does not affect operation. Select a meaningful name.
Remote VPN Endpoint	Fixed IP Address 205.17.11.43	Fixed IP Address 202.11.13.211	Other endpoint's WAN (Internet) IP address.

NetBIOS	Enable	Enable	Disable if not required.
Local LAN IP address Mask	192.168.0.0 255.255.255.0	192.168.1.0 255.255.255.0	Local Address subnet. Use a more restrictive definition if possible.
Remote LAN IP address Mask	192.168.1.0 255.255.255.0	192.168.0.0 255.255.255.0	Remote Address subnet. Use a more restrictive definition if possible.
IKE			
Direction	Initiator & re-sponder	Initiator & re-sponder	Does not have to match. Either endpoint can block 1 direction.
Exchange mode	Main Mode	Main Mode	Must match
DH Group	Group 2 (1024 bit)	Group 2 (1024 bit)	Must match
Local Identity	IP address	IP address	IP address is the most common ID method
Remote Identity	WAN IP address	WAN IP address	IP address is the most common ID method
SA Parameters			
Encryption	3DES	3DES	Must match.
Authentication	MD5	MD5	Must match
Pre-shared Key	xxxxxxxx	xxxxxxxxx	Must match; use any string.
SA Life time	28800	28800	Does not have to match. Shorter period will be used.
PFS	Disabled	Disabled	Must match

Note:

Some VPN Gateways or programs let you specify the following settings separately for IKE and IPSec. For this device, the same settings are used for both IKE and IPSec.

- Authentication
- Encryption
- SA Lifetime

Also, IPSec allows for "AH Authentication", using MD5 or SHA-1. For this device, "AH Authentication" is always DISABLED.

Appendix D
Specifications

Multi-Function Wireless ADSL Router

Model	Wireless ADSL Router
ADSL Interface	T1.413, G.DMT, G.lite, multi-mode
Dimensions	189mm(W) * 122mm(D) * 33mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	4 * 10/100BaseT (RJ45) LAN connection 1 * RJ11 for ADSL line
LEDs	12
Power Adapter	12 V DC External

Wireless Interface

Standards	IEEE802.11b, IEEE802.11g WLAN,
Frequency	2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Channels	Maximum 14 Channels, depending on regulatory authorities
Modulation	CCK, DQPSK, DBPSK, OFDM/CCK
Data Rate	Up to 54 Mbps
Security	WEP 64Bit, WPA 128Bit, WPA-PSK, MAC address checking
Output Power	13dBm (typical)
Receiver Sensitivity	-80dBm Min.

Regulatory Approvals

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Approval

CE Standards

This product complies with the 99/5/EEC directives, including the following safety and EMC standards:

- EN300328-2
- EN301489-1/-17
- EN60950

CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.