
Basic Setup

Introduction

In the **Basic Setup** group, you can change the administrator password, IP configuration of LAN interface and also local DHCP server, ISDN and Wireless LAN configuration.

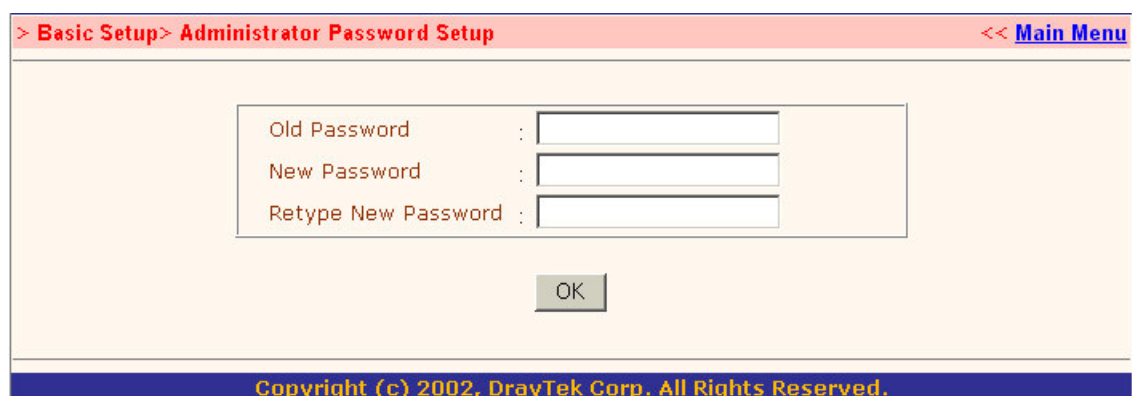


Configuration

- Changing the Administrator Password

For security reasons, we strongly recommend that you set an administrator password for the router. On first setup the router requires no password. If you don't set a password, the router is open and it could be logged into and settings could be changed by any user from the local network or the Internet.

Click **Administrator Password Setup**, the following screen will open.

A screenshot of the "Administrator Password Setup" web form. The title bar at the top reads "> Basic Setup> Administrator Password Setup" in red, with a blue link "<< Main Menu" on the right. The main content area is light yellow and contains three input fields labeled "Old Password", "New Password", and "Retype New Password" in brown text, each followed by a colon and a text box. Below the fields is a grey "OK" button. At the bottom, a dark blue footer bar contains the text "Copyright (c) 2002, DrayTek Corp. All Rights Reserved." in yellow.

Old Password: Enter a current administrator password. If this is the first time to set a password, leave this field blank.

New Password: Enter a new administrator password.

Retype New Password: Type the new password again for confirmation.

Click **OK**.

- Configuring LAN IP Address

There are two sets of IP address settings for the LAN interface. The 1st IP address/netmask is for private users or NAT users, and the 2nd IP address/netmask is for public users. To allow public users requires you to have subscribed to a globally reachable subnet from your ISP.

For example, for some DSL accounts, the ISP will assign a few public IP addresses for your local network usage. You could use one IP address for your router, and the 2nd IP address/netmask should be configured with the public IP address. Other local PCs should set the router IP address as the default gateway. When the DSL connection to the ISP has been established, each local PC will direct route to the Internet. Also, you could use the 1st IP address/netmask to connect to other private users (PCs). These IP addresses of the users will be translated to the 2nd IP address by the router and sent out via the DSL connection.

The screenshot shows a web-based configuration interface for a DrayTek router. The title bar at the top reads "> Basic Setup > Ethernet TCP/IP and DHCP Setup" with a "<< Main Menu" link on the right. The interface is divided into two main sections: "LAN IP Network Configuration" on the left and "DHCP Server Configuration" on the right. In the LAN section, "For NAT Usage" is set to "Enable" (radio button selected), with "1st IP Address" as 192.168.1.1 and "1st Subnet Mask" as 255.255.255.0. "For IP Routing Usage" is set to "Disable" (radio button selected), with "2nd IP Address" as 192.168.2.1 and "2nd Subnet Mask" as 255.255.255.0. A "2nd Subnet DHCP Server" button is located below these fields. The "RIP Protocol Control" is set to "Disable" in a dropdown menu. The DHCP section shows "Enable Server" selected, with "Start IP Address" as 192.168.1.10, "IP Pool Counts" as 50, and "Gateway IP Address" as 192.168.1.1. There are empty fields for "DHCP Server IP Address for Relay Agent", "Primary IP Address", and "Secondary IP Address". A "DNS Server IP Address" section is also present with empty fields. An "OK" button is centered at the bottom of the configuration area. The footer contains the text "Copyright (c) 2002, DrayTek Corp. All Rights Reserved."

For NAT Usage: (Default: Always Enable)

1st IP Address: Private IP address for connecting to a local private network (Default: 192.168.1.1).

1st Subnet Mask: Netmask for the local private network (Default: 255.255.255.0/24).

For IP Routing Usage: (Default: Disable)

Enable: Enables the 2nd IP address settings.

Disable: Disables the 2nd IP address settings.

2nd IP Address: Sets a public IP address.

2nd Subnet Mask: Sets a netmask for the public IP address.

RIP Protocol Control:

Disable: Disables RIP packets exchange on LAN interface.

1st Subnet: Sets the 1st subnet to exchange RIP packets with neighbor routers connected to LAN interface.

2nd Subnet: Sets the 2nd subnet to exchange RIP packets with neighbor routers connected to LAN interface.

2nd Subnet DHCP Server: This is for 2nd subnet of Vigor Router.

The screenshot shows a web browser window titled "Router Web Configurator - Microsoft Internet Explorer". The main content area is titled "2nd DHCP Server". It contains the following elements:

- "Start IP Address : " followed by a text input field.
- "IP Pool Counts : " followed by a text input field containing "0" and "(max. 10)".
- A table with three columns: "Index", "Matched MAC Address", and "given IP Address". The table body is empty.
- "MAC Address : " followed by six text input fields separated by colons.
- Four buttons: "Add", "Remove", "Edit", and "Cancel".
- Three buttons at the bottom: "Close", "Clear All", and "OK".

Start IP Address: Sets the start IP address of the IP address pool.

IP Pool Counts: Sets the number of IPs in the IP address pool.

MAC Address: To type the specific MAC Address which could be added on, removed from or edited from the access list above.

ADD: To add a MAC address on the list.

Remove: To remove the selected MAC address on the list.

Edit: To edit the selected MAC address on the list.

Cancel: To cancel the MAC address access control setup.

Close : To close this window.

Clear All: To clean all of configured MAC address on the list.

OK: To save the access control list.

- Configuring DHCP Server

DHCP stands for Dynamic Host Configuration Protocol. It can automatically dispatch related IP settings to any local user configured as a DHCP client.

The screenshot shows a web-based configuration interface for a DHCP server. The title bar at the top reads "> Basic Setup > Ethernet TCP/IP and DHCP Setup" with a "<< Main Menu" link on the right. The interface is divided into two main panels. The left panel, titled "LAN IP Network Configuration", contains settings for NAT Usage (1st IP Address: 192.168.1.1, 1st Subnet Mask: 255.255.255.0), IP Routing Usage (radio buttons for Enable and Disable, with Disable selected; 2nd IP Address: 192.168.2.1, 2nd Subnet Mask: 255.255.255.0), and RIP Protocol Control (a dropdown menu set to Disable). The right panel, titled "DHCP Server Configuration", contains radio buttons for "Enable Server" (selected), "Disable Server", and "Relay Agent". Below these are fields for Start IP Address (192.168.1.10), IP Pool Counts (50), Gateway IP Address (192.168.1.1), DHCP Server IP Address for Relay Agent (blank), and a section for DNS Server IP Address with Primary and Secondary IP Address fields (both blank). An "OK" button is centered at the bottom of the configuration area. A footer bar at the very bottom states "Copyright (c) 2002, DrayTek Corp. All Rights Reserved."

Enable Server: Assign IP to LAN PC automatically.

Disable Server: Assign IP of LAN PC manually.

Relay Agent: Allow PCs on LAN to request IP from other DHCP server.

Start IP Address: Sets the start IP address of the IP address pool.

IP Pool Counts: Sets the number of IPs in the IP address pool.

Gateway IP Address: Sets the gateway IP address for the DHCP server. Usually, it should be same as 1st IP address when the router works as a default gateway.

DNS Server IP Address: (Default: None).

DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user friendly name into it's equivalent IP address.

Primary IP Address: Sets the IP address of the primary DNS server.

Secondary IP Address: Sets the IP address of the secondary DNS server.

Note: If both the Primary IP and Secondary IP Address fields are left blank, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache. If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

- Configuring the ISDN Interface (VigorX/i and VigorW/Gi only)

This setup page is present in the VigorX/i and VigorW/Gi.

> Basic Setup > ISDN Setup [<< Main Menu](#)

<p>ISDN Port <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Country Code : International</p> <p>Own Number : </p> <p>"Own Number" means that the router will tell the remote end the ISDN number when it's placing an outgoing call.</p> <p>MSN numbers for the router</p> <p>1. : </p> <p>2. : </p> <p>3. : </p> <p>"MSN Numbers" means that the router is able to accept number-matched incoming calls. In addition, MSN service should be supported by the local ISDN network provider.</p>	<p>Blocked MSN numbers for the router</p> <p>1. : </p> <p>2. : </p> <p>3. : </p> <p>4. : </p> <p>5. : </p>
--	--

OK

ISDN Port: Click **Enable** to turn on the ISDN port, **Disable** to turn off.

Country Code: For proper operation on your local ISDN network you should set the correct country code.

Own Number: Sets your ISDN number. If the field has been configured, every outgoing call will carry the number to the called user.

MSN Numbers for the Router: **MSN Numbers** means that the router is able to accept number-matched incoming calls. In addition, MSN service should be supported by local ISDN network provider. The router provides three MSN number fields. Note that MSN services must be subscribed for from your local telecom.

By default, MSN function is disabled. Leave the MSN number fields blank, under which all incoming calls will be accepted without number-matching.

- Configuring the Wireless LAN Interface (VigorG)

The VigorG are equipped with a wireless LAN interface compliant with the 11Mbps IEEE 802.11b and 54Mbps IEEE802.11g protocols. The features of wireless LAN capability enable high mobility of several simultaneous users accessing all LAN facilities just like on a wired LAN as well as Internet and WAN access.

The screenshot shows the 'Wireless LAN Setup' page. At the top, there is a breadcrumb trail: '> Basic Setup > Wireless LAN Setup' and a link '<< Main Menu'. Below this, the 'Wireless LAN Infomation' section displays the MAC Address as '00-04-e2-87-f9-f3' and the Frequency Domain as 'Europe'. A '<< Back' link is present. The 'Detailed Settings' section contains three links: '>> General Settings', '>> Security Settings', and '>> Access Control'.

The Frequency Domain is set as Europe and the MAC address will show as above.

Click **General Settings**, you could configure the SSID and wireless channel.

The screenshot shows the 'General Settings' page for the Wireless LAN interface. The breadcrumb trail is '> Basic Setup > Wireless LAN Setup > General Settings' with a '<< Main Menu' link. The title is 'General Setting (IEEE 802.11)' with a '<< Back' link. The 'Enable Wireless LAN' checkbox is checked. The 'Mode' is set to 'Mixed(11b+11g)'. There are four empty input boxes for 'Scheduler (1-15)'. The 'SSID' is 'Draytek' and the 'Channel' is 'Channel 1, 2412MHz'. The 'Hide SSID' checkbox is unchecked. At the bottom, there is an explanation: 'SSID : wireless LAN Service Set ID.' and 'Hide SSID : the scanning tool can't read the SSID when sniffing radio.'

Mode: In Mixed(11b+11g) mode, the radio can support both IEEE802.11b and IEEE802.11g protocols simultaneously. In 11g-only mode, the radio only supports IEEE802.11g protocol. In 11b-only mode, the radio only supports IEEE802.11b protocol.

Scheduler: You can set wireless device to work at some time interval only. There are 4 intervals you can choose : schedule1, schedule2, schedule3, and schedule4. The default setting is always working. You can set the schedule under **Advanced Setup >> Call Schedule Setup**.

SSID (Service Set Identification): You should set the SSID same as your notebook wireless card to allow the client PCs to access the network via the wireless LAN interface. The default SSID is "default".

Channel: To select a wireless channel for VigorG. The default channel is 6.

Hide SSID: To check it to hide SSID when the wireless clients sniffing radio.

- Configuring the Security of Wireless LAN Interface (VigorG)

Security Settings << Back

Mode : None

Set up [RADIUS Server](#) if 802.1x is enabled.

WPA:

Pre-Shared Key(PSK)

Type 32 ASCII character or 64 Hexadecimal digits leading by "0x", for example "ab1234..." or "0x982acf313..."

WEP:

Encryption Mode: 64-Bit

Use WEP Key

☐ Key 1 :

☐ Key 2 :

☐ Key 3 :

☐ Key 4 :

Mode:

To improve the security and privacy of your wireless data packets one of the following encryption feature can be used.

- **Disable:** Turn off the encryption mechanism.
- **WEP Only:** Accepts only WEP clients and the encryption key should be entered in WEP Key.
- **WEP/802.1x Only:** Accepts only WEP clients and the encryption key is got dynamically through 802.1x.
- **WEP or WPA/PSK:** Accepts WEP and WPA clients simultaneously and the encryption key should be entered in WEP Key and PSK respectively.
- **WEP/802.1x or WPA/802.1x:** Accepts WEP and WPA clients simultaneously and the encryption key is got dynamically through 802.1x.
- **WPA/PSK Only:** Accepts only WPA clients and the encryption key should be entered in PSK.
- **WPA/802.1x Only:** Accepts only WPA clients and the encryption key is got dynamically through 802.1x.

Note: You should also set RADIUS Server if **WEP/802.1x Only**, **WEP/802.1x or WPA/802.1x** or **WPA/802.1x Only** mode is selected.

WPA Encryption:

The WPA encrypts each frame transmitted from the radio using the pre-shared key (PSK) entered from this panel or a key got dynamically through 802.1x.

Pre-Shared Key (PSK): Either 32 ASCII characters or 64 Hexadecimal digits leading by 0x can be entered. For example "0123456789ABCD...." or "0x321253abcde.....".

WEP Encryption:

The WEP encrypts each frame transmitted from the radio using one of the keys entered from this panel. WEP encryption can be enabled by selecting 64 bits or 128 bits from pull down menu. There are 4 key sets can be entered and only one key can be selected. The key can be entered by ASCII or Hexadecimal.

Disable: Turns off the WEP encryption mechanism.

WEP 64 Bit: For 64bits WEP key, either 5 ASCII characters or 10 hexadecimal digits leading by **0x** can be entered. For example **ABCDE** or **0x4142434445**.

WEP 128 Bit: For 128bits 13 ASCII characters or 26 hexadecimal digits leading by **0x** can be entered. For example, **ABCDEFGHIJKLM** or **0x4142434445464748494A4B4C4D**.

- Configuring the Access Control of Wireless LAN Interface (VigorG)

For additional security of wireless access, the **Access Control** allows you to restrict the network access rights by the wireless LAN MAC address of client. Only the valid MAC address which has been configured can allow to access the wireless LAN interface.

The screenshot shows the 'Access Control' configuration page. At the top, a breadcrumb trail reads '> Basic Setup > Wireless LAN Setup > Access Control' and a '<< Main Menu' link is on the right. The page title is 'Access Control' with a '<< Back' link. A checkbox labeled 'Enable Access Control' is present. Below it is a table with two columns: 'Index' and 'MAC Address'. The table is currently empty. Under the table, there is a 'MAC Address :' label followed by six input boxes separated by colons. Below these are four buttons: 'Add', 'Remove', 'Edit', and 'Cancel'. A 'Note :' section states: 'Add or remove the wireless user's MAC address to accept or deny the access to the network.' At the bottom are 'Clear All' and 'OK' buttons.

Enable Access Control: To check the **Enable Access Control** to enable the MAC Address access control feature.

MAC Address: To type the specific MAC Address which could be added on, removed from or edited from the access list above.

ADD: To add a MAC address on the list.

Remove: To remove the selected MAC address on the list.

Edit: To edit the selected MAC address on the list.

Cancel: To cancel the MAC address access control setup.

Clear All: To clean all of configured MAC address on the list.

OK: To save the access control list.