

DHCP Client Setup	
<input type="checkbox"/> Physical Address Clone	08-10-17-5e-ae-5c If checked, the Mac address of PC will be updated
MTU	1496
Primary DNS	
Secondary DNS	
<input type="button" value="Apply"/>	

Figure 32

- **Physical Address Clone:** Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work).
- **MTU:** MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Enter your MTU number in the text-box to set the limitation. The recommended size, entered in the Size field, is 1496. You should leave this value in the 1200 to 1500 range.
- **DNS:** Check "DNS" and enter the IP address to specify DNS server for LAN DHCP server.
- Click "Apply" to save these settings with the Router. The System will apply the new settings and start rebooting right away. After reboot, the Wireless Router will enable these settings with the Router.

6.4.2 PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to select PPPoE.

PPPoE Setup	
PPPoE Account	<input type="text" value="account"/>
PPPoE Password	<input type="password" value="••••••••"/>
<input type="checkbox"/> Physical Address Clone	<input type="text" value="08-10-17-5e-ae-5c"/>
MTU	<input type="text" value="1496"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
<input type="radio"/> Connect to Internet automatically (Default) <input type="radio"/> Auto disconnect when idle, time out After <input type="text"/> minutes, if no found the access request then auto-break off! <input checked="" type="radio"/> Connect to Internet manually	
<input type="button" value="Apply"/>	

Figure 33

- **PPPoE Account:** Enter the User Name provided by your ISP for the PPPoE connection
- **PPPoE Password:** Enter the Password provided by your ISP for the PPPoE connection
- **Physical Address Clone:** Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work).
- **MTU:** MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Enter your MTU number in the text-box to set the limitation. The default value of MTU is 1492 and use 1300 while the line condition is bad.
- **DNS:** Check "DNS" and enter the IP address to specify DNS server for LAN DHCP server.
- **Connection Type:** Select your PPPoE connection from these options:
 - Connect to Internet automatically:** This feature will keep your Internet connection always alive. The Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to Auto Connect.
 - Auto disconnect when idle, time out:** If enabled, the router will trigger a PPPoE session for connection to the Internet if any client PC on your WLAN/LAN sends out a request for Internet access. However, the router automatically disconnects the PPPoE session after the WAN connection has been idle for the amount of time you specified in the timeout box. If your

Internet account is billed based on the amount of time of your Internet connection, you probably want to enable this option and enter an idle time value best suitable for your network. To use this option, click the radio button next to Connect on demand.

Connect to Internet manually: The router will connect to Internet while click the "Connect" button on the Web. And the WAN connection will disconnect. If you click "Disconnect" manually from the Web user interface. The router will not auto-connect to the Internet. To use this option, click the radio button next to Connect on demand.

- Click "Apply" to save these settings with the Router. The System will apply the new settings and start rebooting right away. After reboot, the Wireless Router will enable these settings with the Router.

6.4.3 Static IP

If you are required to use a permanent IP address to connect to the Internet, select Static IP.

Static IP Setup	
WAN IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
<input type="checkbox"/> Physical Address Clone	<input type="text" value="08-10-17-5e-a8-5c"/> If checked, the Mac address of PC will be updated
MTU	<input type="text" value="1496"/>
<input type="button" value="Apply"/>	

Figure 34

- **WAN IP Address:** This is the Router's IP address, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.
- **Subnet Mask:** This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.
- **Default Gateway:** Your ISP will provide you with the Gateway Address, which is the ISP server's IP address.
- **Physical Address Clone:** Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet

connection to. Type in this MAC address in this section to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work).

- **MTU:** MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Enter your MTU number in the text-box to set the limitation. The recommended size, entered in the Size field, is 1496. You should leave this value in the 1200 to 1500 range.
- **DNS:** Check "DNS" and enter the IP address to specify DNS server for LAN DHCP server.
- Click "Apply" to save these settings with the Router. The System will apply the new settings and start rebooting right away. After reboot, the Wireless Router will enable these settings with the Router.

6.5 LAN Setup


6.5.1 LAN Setup

The Wireless Broadband Router communicates with the wired/wireless clients through its LAN port. The LAN configuration page allows you to define the private IP address and DHCP server settings over the LAN interface.

System IP Setup	
System IP Address	<input type="text" value="192.168.10.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
<input checked="" type="checkbox"/> DHCP Server on	
DHCP IP Pool	192.168.10. <input type="text" value="2"/> - 192.168.10. <input type="text" value="102"/>
<input type="button" value="Apply"/>	

Figure 35

- **IP Address/Subnet Mask:** Enter the IP address and subnet mask for the Wireless Broadband Router LAN port. All local wired/wireless devices communicate with the device through this port. It is also the IP address of the Web-based Configuration Utility. By default, the IP address and subnet mask of the LAN port is 192.168.10.1 and 255.255.255.0 respectively.
- **DHCP Server:** The DHCP server can be ON or OFF in this screen. If you choose to set this device as a DHCP server, then it will assign IP addresses to its clients. The DHCP pool range is also changeable.
- Click "Apply" when you have finished the configuration above. And the wireless router will be automatically restarted if you change the LAN IP address.

 If you change the private IP address and apply the changes, the PC from which you configure the router will lose the communication to the router. To reconnect, you will need to renew the IP address of the PC or change to an IP address compatible with the new LAN port IP address.

6.5.2 DHCP Info

You can View all the pc which connect to the Wireless Router by DHCP here.

DHCP Client Info

ID	IP Address	MAC Address	Status
1	192.168.10.23	8-0-17-14-e5-1c	Manual

Figure 36

6.6 Wireless Settings

The Wireless Broadband Router implements Access Point capability, which connects wireless clients to a wired LAN. It allows wireless stations to access network resources and share the broadband Internet connection.

6.6.1 Basic Wireless Settings

The basic settings for wireless networking are set on this screen.

Basic Setting	
<input checked="" type="checkbox"/> Wireless Status(Enabled/Disabled)	<input type="button" value="Apply"/>
Radio Band	<input type="text" value="802.11b/g"/>
Radio Mode	<input type="text" value="AP"/>
SSID	<input type="text" value="default"/>
Broadcast SSID	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Channel	<input type="text" value="Channel 6"/>
<input type="button" value="Apply"/>	

Figure 37

- **Radio Band:** The default setting is mixed mode [802.11B/G]. If you do not

know or have both 11g and 11b devices in your network, then keep the default in mixed mode. From the drop-down manual, you can select 802.11G if you have only 11G card. If you have only 802.11 B card, then select 802.11B.

- **Radio Mode:** The Router has 3 modes: AP, WDS, AP+WDS
- **SSID:** The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID (default) to a unique name.
- **Channel:** Select the channel used for wireless communication. There are 11 overlapping channels. Channels 1, 6 and 11 are non-overlapping. The default is channel 6.
- Click "Apply" when you have finished the configuration above.
- Please setup authentication and Encryption mode to setup Valid and Safe wireless connection after setting Basic Wireless parameters.

6.6.2 Advanced Wireless Settings

This tab is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

Advanced Setting	
Beacon Interval	<input type="text" value="100"/> (20-1000 ms)
RTS Threshold	<input type="text" value="2347"/> (256-2432)
DTIM Interval	<input type="text" value="1"/> (1-255)
Transmit Rate	<input type="text" value="Auto"/> ▾
Preamble Type	<input checked="" type="radio"/> Long <input type="radio"/> Short <input type="radio"/> Auto
802.11g protection	<input checked="" type="radio"/> CTS <input type="radio"/> RTS/CTS <input type="radio"/> Disabled
<input type="button" value="Apply"/>	

Figure 38

- **Beacon Interval:** This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the wireless router to keep the network synchronized. A beacon includes the wireless LAN service area, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM). The default value is 100.
- **RTS Threshold:** This value should remain at its default setting of 2,347. Should you encounter inconsistent data flow, only minor modifications are recommended.

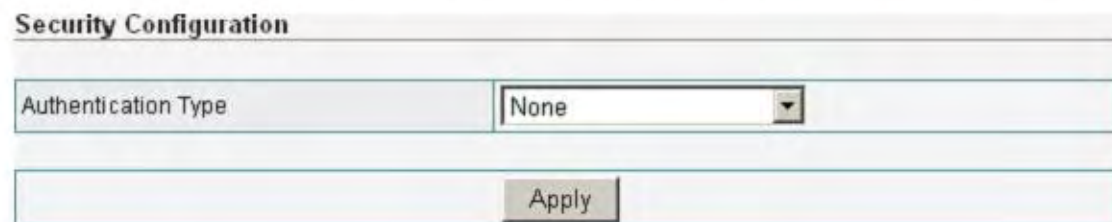
- **DTIM Interval:** This value indicates how often the Access Point sends out a Delivery Traffic Indication Message (DTIM). Lower settings result in more efficient networking, while preventing your PC from dropping into power saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power, but interferes with wireless transmissions.
- **Transmit Rate:** The "Transmit Rate" is the data packets limitation this wireless router can transmit, The wireless router will use the highest possible selected transmission rate to transmit the data packets. The default value is Auto.
- **Preamble Type:** It defines the length of CRC block in the frames during the wireless Communication. "Short Preamble" is suitable for heavy traffic wireless network. "Long Preamble" provides much communication reliability

6.6.3 Wireless Security

This wireless router provides complete wireless LAN security functions; include WEP, WPA with pre-shared key and WPA2 with pre-shared key. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function.

6.6.3.1 None

Transmit data without encryption and authentication. This is the default option.



The screenshot shows a web interface for "Security Configuration". It features a dropdown menu for "Authentication Type" with "None" selected. Below the dropdown is an "Apply" button.

Figure 39

- Click "Apply" when you have selected the "None".



If you select none, any data will be transmitted without Encryption and any station can access the wireless router.

6.6.3.2 WEP

WEP (Wired Equivalent Privacy) is an encryption method used to protect your

wireless data communications. WEP uses a combination of 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission.

Security Configuration

Authentication Type	WEP	
Accessorial Authentication & Encryption	Open System	
WEP		
KEY Length	<input checked="" type="radio"/> 64 bits	<input type="radio"/> 128 bits
WEP Mode	<input checked="" type="radio"/> HEX	
Key 1	<input checked="" type="radio"/> <input type="text"/>	Key format is 10 Hex-Number, every Hex-Number can be 0-9 and A-F
Key 2	<input type="radio"/> <input type="text"/>	
Key 3	<input type="radio"/> <input type="text"/>	
Key 4	<input type="radio"/> <input type="text"/>	
Apply		

Figure 40

- **Open-System:** No authentication is used. But uses WEP encrypt data packets.
- **Share-keys:** Authentication is a process in which the AP validates whether the wireless client is qualified to access the AP's service. You must enable WEP function and define your WEP keys. The keys are used both to authenticate wireless clients and encrypt outgoing data.
- **Auto-Select:** It can detect Wireless Client authentication information, and automatically choose Open-System or Share-Keys mode to communicate with client. When use Auto-Select mode, you must setup WEP keys which are used by authentication system.
- **WEP Length:** Selects 64-bit or 128-bit WEP encryption. Be sure that the key length setting in the AP shall be the same as in wireless clients, or the communication will not work.
- **WEP Mode:** You may select to select ASCII Characters or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.
- **Default Key:** The Key selected here must match the key selected in the client. For example, if you select Key 1 here you have to select Key 1 for the client. The default is 1.
- **Key 1~4:** Enter one to four WEP keys in either ASCII or Hexadecimal format. You can use 64 bits or 128 bits as the encryption algorithm.

Enter one to four WEP keys in either ASCII or Hexadecimal format. You can use 64 bits or 128 bits as the encryption algorithm.

Note that when using Hexadecimal format, only digits 0-9 and letters A-F, a-f

are allowed. Valid key length for each encryption type is as below:

Key Length	HEX Format	ASCII Format
64 Bit	10 hexadecimal digits	5 ASCII characters
128 Bit	26 hexadecimal digits	13 ASCII characters

- Click "Apply" at the bottom of the screen to save the above configurations.

6.6.3.3 WPA Personal

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP and AES to change the encryption key frequently. This can improve security very much.

Security Configuration

Authentication Type	WPA Personal ▾
Accessorial Authentication & Encryption	TKIP ▾

Pre-Shared Key

Key Format	Please input 8-63 characters
KEY	*****
Rekey Time (sec)	86400
Apply	

Figure 41

- **TKIP:** Temporal Key Integrity Protocol (TKIP) utilizes a stronger encryption algorithm and includes Message Integrity Code (MIC) to provide protection against hackers.
- **AES:** Advanced Encryption System (AES) utilizes a symmetric 128-Bit block data encryption. It's the strongest encryption currently available.
- **WPA Pass Phrase:** The WPA Pass Phrase is used to authenticate and encrypt data transmitted in the wireless network. The input format is in character style and key size should be in the range between 8 and 63 characters.
- **Clear:** If you want to retype again. Just click "Clear" and "WPA Pass Phrase" fields will be cleared.
- **Rekey Time (sec):** Specifies the timer the WPA key must changes. The

change is done automatically between the server and the client. The default value is 86400.

- Click "Apply" at the bottom of the screen to save the above configurations.

6.6.3.4 WPA2 Personal

The WPA2 is a stronger version of WPA. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses AES to change the encryption key frequently. This can improve security very much.

Security Configuration	
Authentication Type	WPA2 Personal ▾
Accessorial Authentication & Encryption	AES ▾
Pre-Shared Key	
Key Format	Please input 8-63 characters
KEY	*****
Rekey Time (sec)	86400
Apply	

Figure 42

- **AES:** Advanced Encryption System (AES) utilizes a symmetric 128-Bit block data encryption. It's the strongest encryption currently available.
- **WPA Pass Phrase:** The WPA Pass Phrase is used to authenticate and encrypt data transmitted in the wireless network. The input format is in character style and key size should be in the range between 8 and 63 characters.
- **Clear:** If you want to retype again. Just click "Clear" and "WPA Pass Phrase" fields will be cleared.
- **Rekey Time (sec):** Specifies the timer the WPA key must changes. The change is done automatically between the server and the client. The default value is 86400.
- Click "Apply" at the bottom of the screen to save the above configurations.

6.6.3.5 WPA&WPA2 Personal

Auto-Select WPA/WPA2 can detect Wireless Client authentication information, and automatically choose WPA or WPA2 mode to communicate with client. Operation is the same as WPA or WPA2.

Security Configuration	
Authentication Type	WPA&WPA2 Personal ▾
Pre-Shared Key	
WPA	<input checked="" type="radio"/> TKIP <input type="radio"/> AES
WPA2	<input checked="" type="radio"/> AES
KEY Mode	Please input 8-63 characters
WPA Pass Phrase	*****
WPA2 Pass Phrase	*****
Rekey Time (sec)	86400
<input type="button" value="Apply"/>	

Figure 43

- Click “Apply” at the bottom of the screen to save the above configurations.

6.6.4 Wireless MAC Filter

This Wireless router has the capability to control the wireless client access based on the MAC address of the wireless client. The user has the flexibility to customize your own control policy based on these options:

Wireless Access Control Configuration		
<input checked="" type="checkbox"/> Enable Wireless Access Control	<input type="button" value="Apply"/>	
<input type="radio"/> Defined items in MAC list are PERMITTED to connect AP, others are DENIED	<input type="button" value="Apply"/>	
<input checked="" type="radio"/> Defined items in MAC list are DENIED to connect AP, others are PERMITTED		
MAC	<input type="text"/> <input type="button" value="Add"/>	
ID	MAC	Delete

Figure 44

- **Enable Wireless Access Control:** To enable Wireless MAC Filter, click the check box. The default is “disable”.
- You can choose a default operation for your factual security or management consideration:
Defined items in MAC list are PERMIT to connect AP, others are DENIED.

Defined items in MAC list are DENIED to connect AP, others are PERMIT.

Click "Apply" when you have selected,

- **MAC:** Enter the MAC Address of a station.
- **Description:** Enter the Comment of station.
- Click "Add". Then this wireless station will be added into the "Current Access Control List" below.
-

ID	MAC	Delete
1	00-CC-00-CC-CC-FF	Delete

Figure 45

- If you want to remove some MAC address from the "Current Access Control List", select the MAC addresses you want to remove in the list and then click "Delete".

6.6.5 Active Clients

You can see the status of all active wireless stations that are connecting to the wireless router.

ID	MAC	Delete
1	00:0a:eb:88:5c:5e	connected

Figure 46

- To see the latest information, click Refresh button.

6.6.6 WDS Set

You can set the wireless Bridge MAC here. The bridge uses to connect between more than 2 routers.

Wireless Bridge Configuration		
Wireless Bridge MAC	<input type="text"/>	Add
Current Wireless Bridge Information		
No	MAC	Delete
Refresh		

Figure 47

6.7 Routing

If the Router is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network.

Routing Table Management

Type	Target	Mask	Gateway
NET ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/>			

ID	Type	Target	Mask	Gateway	Delete
1	NET	10.0.0.0	255.255.255.0	192.168.10.8	<input type="button" value="Delete"/>

Figure 48

- **Type / Target / Mask / Gateway:** Fill in these fields required by this Static Routing function.
- **Add:** Fill in the all of the setting to be added and then click "Add". Then this Special Application setting will be added into the "Current Routing Table" below.
- **Current Routing Table:** This display shows the valid routing paths in Broadband Router. User can view the information about current routing paths
- If you want to remove some route entries from the "Current Routing Table", select the Route entry you want to remove in the table and then click "Delete".

6.8 NAT

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP.

6.8.1 DMZ Host Setup

If you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to

a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

DMZ Host Setup		
<input checked="" type="checkbox"/> DMZ	192.168.10.11	Apply

Figure 49

- DMZ : Enable/disable DMZ
- DMZ Host: Input the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above, you need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.
- Click "Apply" at the bottom of the screen to save the DMZ configurations.



If there is a conflict between the Virtual Server and the DMZ setting, then Virtual Server function will have priority over the DMZ function.

6.8.2 FTP Private Port

FTP private port enables user to setup FTP server which is not using the standard port 21.

FTP Private Port		
<input checked="" type="checkbox"/> Port Number	1025	Apply

Figure 50

- Check port number and enter the number and then press the "Apply" button to setup Private FTP port. The default Value is 1025.

6.8.3 Virtual Server Setup

Use the Virtual Server function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN

Port) to a particular LAN private IP address and its service port number.

Virtual Server Setup

Rule Name	FTP
Internal Server IP Address	192.168.10.6
Protocol	TCP
External Port	21
Internal Port	21
Add	

Figure 51

- **Rule Name:** You can enter whatever you want. It's just a string.
- **Internal Server IP:** Enter the host IP address to which the packet will be forwarded. The virtual server can be set easily by setting the internal server IP address only. You need to give your LAN PC clients a fixed/static IP address for Virtual Server to work properly.
- **Protocol:** Chose TCP/UDP type for the packet you want to forward. If the rule existed in predefined virtual server rule, you can choose the rule.
- **External Port:** Enter the port number (The value's range is 1 to 65535) from which the packet will be on WAN.
- **Internal Port:** Enter the port number to which the packet will be forwarded on LAN
- Press "Add" button after enter the all fields to add the rule.
- Check to select the rule and press "Delete" to delete the rule.

ID	Rule Name	Internal IP	Protocol	External Port	Internal Port	Delete
1	FTP	192.168.10.6	TCP	21	21	Delete

Figure 52

The diagram below demonstrates one of the ways you can use the Virtual Server function. Use the Virtual Server when you want the FTP server located in your private LAN to be accessible to Internet users. The configuration below means that any request coming from the Internet to access your web server will be translated to your LAN's FTP server (192.168.10.6). Note: For the virtual server to work properly Internet/remote users must know your global IP address.

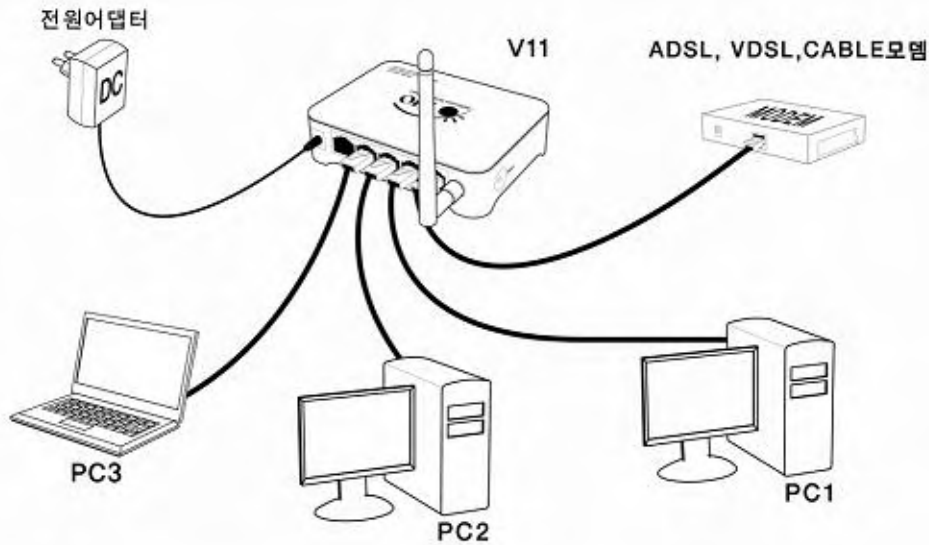


Figure 53

6.8.4 Port Trigger

Port Trigger set the port you want used for some special use.

Port Triggering	
Predefined Trigger Rules	Select one of the predefined rules ▾
Rule Name	<input type="text"/>
Trigger Protocol	TCP ▾
Trigger Port	<input type="text"/> - <input type="text"/>
Forward Protocol	TCP ▾
Forward Port	<input type="text"/>
Add	

Figure 54

- **Rule Name:** You can enter whatever you want. It's just a string.
- **Trigger Protocol:** Chose TCP/UDP type for the packet you want to trigger. If the rule existed in predefined virtual server rule, you can choose the rule.
- **Trigger Port:** Enter the port number (The value's range is 1 to 65535) from which the packet will be on WAN.
- **Forward Protocol:** Chose TCP/UDP type for the packet you want to forward. If the rule existed in predefined virtual server rule, you can choose the rule.
- **Forward Port:** Enter the port number to which the packet will be

- forwarded on LAN
- Press "Add" button after enter the all fields to add the rule.
- Check to select the rule and press "Delete" to delete the rule.

ID	Rule Name	Trigger Condition	Forward Condition	Delete
1	WarCraft	tcp:6112	tcp:6112	<input type="button" value="Delete"/>

Figure 55

6.9 Fire Wall

The Wireless Broadband Router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common Internet attacks.

6.9.1 MAC Filtering

This Wireless router has the capability to control the wired client access based on the MAC address of the wired client. The user has the flexibility to customize your own control policy based on these options:

MAC Filtering Configuration			
Status	The current status is enabled		<input type="button" value="Stop"/>
<input checked="" type="checkbox"/>	If checked, the undefined item in MAC Address list is allowed to access Internet; Unchecked means reverse		<input type="button" value="Apply"/>
MAC Address	<input type="text" value="00-CC-33-00-CC-CC"/>	<input type="text" value="Permit"/>	<input type="button" value="Add"/>

Figure 56

- **Enable MAC Filtering:** To enable MAC Filtering, click the check box. The default is "disable".
- You can choose a default operation for your factual security or management consideration:
 - Defined items in MAC list are DENIED to access internet, others are PERMIT
 - Defined items in MAC list are PERMIT to access internet, others are DENIED
 Click "Apply" when you have selected,
- **MAC:** Enter the MAC Address of a station.
- **Description:** Enter the Comment of station.
- Click "Add". Then this wired station will be added into the "Current Access Control List" below.

ID	MAC Address	Rule	Delete
1	0-cc-33-0-cc-cc	Permit	<input type="button" value="Delete"/>

Figure 57

- If you want to remove some MAC address from the "Current Access Control List ", select the MAC address you want to remove in the list and then click "Delete ".

6.9.2 Access Control

If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.).This is the place to set that configuration. Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.

Connection Filtering Configuration

Status	The current status is enabled	<input type="button" value="Stop"/>
<input checked="" type="checkbox"/> If checked, the undefined item in IP Address list is allowed to access Internet;Unchecked means reverse		<input type="button" value="Apply"/>
Rule Name	<input type="text" value="test"/>	
Source IP Address	192.168.10. <input type="text" value="11"/> - 192.168.10. <input type="text" value="12"/>	
Protocol	<input type="text" value="TCP"/>	
Destination Port	<input type="text" value="80"/> - <input type="text" value="80"/>	
status	<input type="text" value="Permit"/>	
Days To Block	<input type="checkbox"/> Everyday <input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	
Times To Block	<input type="checkbox"/> All Day <input type="text" value="00:00"/> - <input type="text" value="00:00"/>	
<input type="button" value="Add"/>		

Figure 58

Enable Access Control: To filter the outgoing packets for security or management consideration by IP Address, either permitting or blocking access, Enable Access Control is checked.

You can choose a default operation for your factual security or management consideration:

The Undefined items beside the Rule list are PERMIT to access internet

DENIED to access internet.

The Undefined items beside the Rule list are DENIED to access internet
DENIED to access internet.

Rule Name: Enter the rule name which you want, it is just only a string.

Source IP: Enter the IP address of a station which is you want to setting.

Predefined Applications: Chose the Predefined rule in the list to be allowed or forbade accessing Internet.

Protocol & Port: Chose protocol type (TCP/UDP) and enter the single port number or the port range to allow or forbid.

Action: You can choose the rule is be allowed or forbade accessing Internet.

Rule Name	Source IP	Protocol	Dest Port	Days	Times	Rule	Delete
test	192.168.10.11- 192.168.10.12	TCP	80	Mon Wed Sun	All Day	Permit	Delete

Figure 59

6.9.3 URL Filtering

URL (Uniform Resource Locator – e.g. an address in the form of <http://www.abcde.com> or <http://www.example.com>) filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.

URL Filtering Configuration

Note: You can use wildcards(* and ?), "*" is the multi-letters, "?" is a letter; For example: *.*sex*. * express that all URL with "sex" will be blocked!

Input Filtering Keyword

Figure 60

- **Enable URL Filtering:** To enable or disable URL Filter feature. Enable URL Filtering is checked.
- You can choose a default operation for your factual security or management consideration:
 - Predefined URLs/Keywords in list are BLOCKED, others are PERMITTED.
 - Predefined URLs/Keywords in list are PERMITTED, others are BLOCKED.
- **URLs/Keywords:** Enter the specified URL site for security or management consideration by URLs/Keywords, either permitting or blocking access.

ID	Filtering Keyword	Delete
1	*.example.com	Delete

Figure 61

- Press "Delete" button to delete a rule after select a rule.

6.10 DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers.

DDNS Setup	
* Sign up www.dyndns.org first.(Free)	
DynDNS Operation	<input type="radio"/> Start <input checked="" type="radio"/> Stop
User ID	<input type="text"/>
Password	<input type="text"/>
Host Name	<input type="text"/>
Information	close!
<input type="button" value="Apply"/> <input type="button" value="Reconnect"/>	

Figure 62

- **User ID/Password/Host Name:** Enter your registered domain name and your username and password for this service.
- **Information:** The status of the DDNS service connection is displayed here. To see the latest DDNS status, click Refresh button.

6.11 MISC


6.11.1 Login ID & Password Setup

In factory setting, the default password is "N/A", and that for user is also password. You can change the default password to ensure that someone cannot adjust your settings without your permission. Every time you change your password, please record the password and keep it at a safe place.

Login ID & Password Setup	
Login name is "admin"	
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 63

- New Password. Enter your new password.
- Confirmed New Password: Enter your new password again for verification purposes.
- Click "Apply" at the bottom of the screen to change the password.

 If you forget your password, you'll have to reset the router to the factory default (Password is "N/A") with the reset button (see router's front panel).

6.11.2 Remote Mgmt

This feature allows you to manage the Router from a remote location, via the Internet. To enable this feature, check the "Management Port" checkbox, and click the Apply button.

Remote Mgmt		
<input type="checkbox"/> Management Port	<input type="text" value="8080"/>	<input type="button" value="Apply"/>

Figure 64

- Management Port: Enter the port number.
- Click "Apply" at the bottom of the screen to change the Management Port.

When you want to access the web-based management from a remote site, enter `http://WAN IP Address:8080`. (e.g: <http://192.168.10.1:8080>).

`http://192.168.10.1:8080`

Figure 65

6.11.3 WAN Link Status & Setup

WAN Link Status & Setup			
WAN Link Status	Disconnect	WAN Link Setup	<input type="button" value="Apply"/>
		<input type="text" value="Auto"/>	

Figure 66

6.11.4 Restore Default / Restart System

Restore Default / Restart System	
<input type="button" value="Restore Default"/>	<input type="button" value="Restart System"/>

Figure 67

Restore Default / Restart System

Restore the Router's configuration to its factory default settings. Restore Factory Defaults. To clear all of the Router's settings and reset them to its factory defaults.

- Click the Restore Default button. Router will restart automatically.

Restart System

Click "Restart System" button to reboot router.

REBOOT
Please wait a few seconds.The router is rebooting.....

Figure 68

6.11.5 Firmware Upgrade

Upgrade the Broadband router's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Firmware Upgrade	
Current Version:	APR-M14H-V1.00B1-U12EN-OEM, 2006.02.27.22:25.
New Firmware File:	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Apply"/>

Figure 69

Appendix I : Troubleshooting

1. I cannot access the Web-based Configuration Utility from the Ethernet computer used to configure the router.

- Check that the LAN LED is on. If the LED is not on, verify that the cable for the LAN connection is firmly connected.
- Check whether the computer resides on the same subnet with the router's LAN IP address.
- If the computer acts as a DHCP client, check whether the computer has been assigned an IP address from the DHCP server. If not, you will need to renew the IP address.
- Use the ping command to ping the router's LAN IP address to verify the connection.
- Make sure your browser is not configured to use a proxy server.
- Check that the IP address you entered is correct. If the router's LAN IP address has been changed, you should enter the reassigned IP address instead.

2. I forget Password (Reset the Router without Login)

- Plug out the power of the Router.
- Use a pencil to press and hold the default button on the back panel of the Router. Plug in the power of the Router.
- Press and hold the default button wait for a few seconds until the CPU LED indicator stays green.
- Reboot the AP.
- After the above those steps, the manufacture's parameters will be restored in the Router. The default password is N/A.

3. I have some problems related to Connection with Cable Modem please follow the following steps to check the problems:

- Check whether the DSL modem works well or the signal is stable. Normally there will be some indicator lights on the modem, users can check whether the signal is ok or the modem works well from those lights. If not, please contact the ISP.
- Check the front panel of the Router, there are also some indicator lights there. When the physical connection is correct, the Power light and the CPU light should be solid; the WAN light should be blinking. If you use your computer, the corresponding LAN port light should be blinking too. If not,

- please check whether the cables work or not.
- Repeat the steps in WAN Setup Connect with Internet through DSL Modem.

4. I can browse the router's Web-based Configuration Utility but cannot access the Internet.

- Check if the WAN LED is ON. If not, verify that the physical connection between the router and the DSL/Cable modem is firmly connected. Also ensure the DSL/Cable modem is working properly.
- If WAN LED is ON, open the System Overview page of the Web configuration utility and check the status group to see if the router's WAN port has successfully obtained an IP address.
- Make sure you are using the connection method (Dynamic IP Address, PPPoE, or Static IP) as required by the ISP. Also ensure you have entered the correct settings provided by the ISP.
- For cable users, if your ISP requires a registered Ethernet card MAC address, make sure you have cloned the network adapter's MAC address to the WAN port of the router. (See the MAC Address field in WAN Setup.)

5. My wireless client cannot communicate with another Ethernet computer.

- Ensure the wireless adapter functions properly. You may open the Device Manager in Windows to see if the adapter is properly installed.
- Make sure the wireless client uses the same SSID and security settings (if enabled) as the Wireless Broadband Router.
- Ensure that the wireless adapter's TCP/IP settings are correct as required by your network administrator.
- If you are using a 802.11b wireless adapter, and check that the 802.11G Mode item in Wireless Basic Setting page, is not configured to use 802.11G Performance.
- Use the ping command to verify that the wireless client is able to communicate with the router's LAN port and with the remote computer. If the wireless client can successfully ping the router's LAN port but fails to ping the remote computer, then verify the TCP/IP settings of the remote computer.

 **Service Call**
1588-1696

 **SDT**
Information Technology
5-63, Hyochang-Dong, Yongsan-Gu
SEOUL, KOREA, Zip 140-120
Tel : 82-2-714-5083
Fax : 82-2-712-3977
www.SDT.co.kr

 **SDT**
Service Center
6-31, Singea-Dong, Yongsan-Gu
SEOUL, KOREA, Zip 140-090
Tel : 82-2-718-1696
Fax : 82-2-718-1698
www.ZIO.ne.kr