Help

ROUTER BASICS
1. Check power connection
2. Verify power light status
3. Check connections for networking interface(s)
4. If you are unable to access the router's user interface, please check your computer's network settings - verify that your TCP/IP settings are correct. Check User Guide for more details.
5. Ensure that the latest firmware is installed in the router

Password Settings
Use this menu to restrict management access based on a specific password. By default, there is no password. So please assign a password to the Administrator as soon as possible, and store it in a safe place.
Passwords can contain from 3-12 alphanumeric characters,and are case sensitive.
Idle Time-out - The amount of time of inactivity before the router will automatically close the Administrator session. Set this to zero to disable it.

top

Remote Management
By default, management access is only available to users on your local network. However, you can also manage the router from a remote host by adding the IP address of an administrator to this screen.
top

System Time
Set the time zone for the router and connecting to a Simple Network Time Protocol(SNTP) server allows the router to synchronize the system clock to the global Internet. The synchronized clock in the router is used to recored the system log and control client filtering.
top

LAN Settings
Configure the IP address of the router. To dynamically assign the IP address for client PCs, enable the DHCP Server, set the lease time, and then specify the address range.
Valid IP addresses consist of four numbers, and are separated by periods. The first three fields are the network portion, and can be from 0-255, while the last field is the host portion and can be from 1-254.
top

DHCP Client List
The DHCP client list allows you to see which IPs are offered by this device via IP address, host name, and MAC address.

top

WAN
Specify the WAN connection type required by your Internet Service Provider, then click "Apply Button" to provide detailed configuration parameters for the selected connection type.
top

WAN | Dynamic IP Address
The Host Name is optional, but may be required by some ISPs. The default MAC address is set to the WAN's physical interface on the router. Use this address when registering for Internet service, and do not change it unless required by your ISP, You can use the "Clone MAC Address" button to copy the MAC address of the Ethernet Card installed by your ISP and replace the WAN MAC address with this MAC address.
top

WAN | Static IP
If your Internet Service Provider has assigned a fixed address, enter the assigned address and subnet mask for the router, then enter the gateway address of your ISP.

WAN | PPPoE
Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, by may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the defined Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.
Maximum Idle time - The amount of time of inactivity before disconnecting your PPPoE session. Either set this to zero or enable Auto-reconnect to disable this feature.
Auto-reconnect - If enabled, the router will automatically connect to your ISP after your system is restarted or the connection is dropped.

DNS Settings

Dynamic DNS:

- 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 can also help people to connect to your "DMZ" PC.
- This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change, which makes it difficult to connect to you.
- The Service works as follows:
  1. You must register for the service at http://www.dyndns.org (Registration is free). Your password will be issued by www.dyndns.org
  2. After receiving your password, return to http://www.dyndns.org and use the "Create New Host" option to have your desired Domain name allocated to you.
  3. Enter and save your www.dyndns.org data (username, password, domain name) on this screen.
  4. The Wireless Broadband Router will then automatically ensure that your current IP Address is recorded at http://www.dyndns.org
  5. From the Internet, users will now be able to connect to your Virtual Servers (or DMZ PC) using your Domain name.

DDNS Service

DDNS Service	- You must register and create a new account before using the service. The service is free. - Click this link to connect to the www.dyndns.org Web site. - Your initial password will be E-mailed to you; you can change this. - After registration,use the "Create New Host" option (on the www.dyndns.org Web site) to request your desired Domain name. Note that the domain MUST end with `.dyndns.org`

DDNS Data

DDNS Data	User Name - Enter the Username specified at the www.dyndns.org Web site. Password - Enter your current password for www.dyndns.org

Domain

- Enter the domain name allocated to you by www.dyndns.org
- If you have more than one name, enter the name you wish to use.
- The domain MUST end with `.dyndns.org`

DNS Relay - Domain Name Servers are used to map an IP address to the equivalent domain name (e.g.www.ibm.com). Your ISP should provide the IP address for one or more domain name servers.
top

DNS
Domain Name Servers are used to map an IP address to the equivalent domain name(e.g.www.yahoo.com). Your ISP should provide the IP address for one or more domain name servers.
top

Wireless LAN Settings

SSID - "IEEE 802.11b LAN" is the default setting. All devices on the network must share the same SSID. If you change the default setting, the SSID may be up to 32 characters long. If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier). To communicate, all Wireless stations must use the same SSID/ESSID.
Channel - "11" is the default channel. All devices on the network must share the same channel. Select the Channel you wish to use on your Wireless LAN. If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with different channels to see which is the best.
Authentication - Normally this can be left at the default value of "Automatic". If this fails, select the appropriate value - "Open System" or "Shared Key". Check your Wireless card's documentation to see what method to use.
Wep Mode - "Disable" is the default Encryption. All devices on the network must share the same Encryption.

"Disable" (default) - data is NOT encrypted before being transmitted.

"64 Bit Encryption " - data is encrypted, using the default key, before being transmitted. The receiving station must be set to use 64 Bit Encryption, and have the same Key value in the same position in its key table. Otherwise, it will not be able to decrypt the data.

"128 Bit Encryption " - data is encrypted, using the default key, before being transmitted. The receiving station must be set to use 128 Bit Encryption, and have the same Key value in the same position in its key table. Otherwise, it will not be able to decrypt the data.

WEP Key - The encryption key is a password that allows access to a network which uses data encryption. The input format for this key can be set here.

ASCII characters: The encryption key is input as ASCII characters (alphanumeric characters or symbols).
Hexadecimal digits: The encryption key is input as hexadecimal digits (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f).

Passphrase - Use this to generate a set of key values from a phrase.

1. Select the desired key option (64 Bit or 128 Bit)
2. Enter the desired phrase
3. Click the "Generate Keys" button.
4. The screen will refresh with the key values inserted.
5. Save the data.

Key #(1,2,3,4) - This table is used when Encrypting and Decrypting data. All stations, including this Access Point, always transmit data encrypted using their default key. The key number (1, 2, 3, 4) is also transmitted. The receiving station will use the key number (1, 2, 3, 4) to determine which key value to use for decryption. If the key value does not match the transmitting station, decryption will fail. The easiest way to ensure there are no problems is to have

every Station, including the Access Point, use the same key table (all entries identical).
Default Key - select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only.
top

802.1X

IEEE 802.1x is a port based authentication protocol. It can be used in *any* scenario where one can abstract out the notion of a port. It requires entitie(s) to play three roles in the authentication process: that of an supplicant, an authenticator and an authentication server. The diagram below shows the basic scenario.
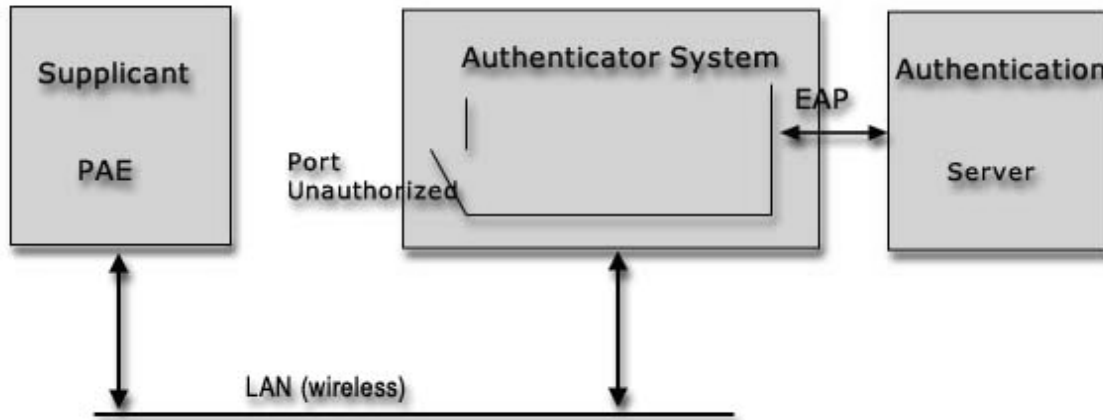
A Port Access Entity (PAE) is an entity that has access or is capable of gaining or controlling access to some port which offers some services. When applied to IEEE 802.11, the Access Point acts as an authenticator, while a wireless station (laptop etc) is the supplicant which is authenticated by the RADIUS server (Authentication Server).

RADIUS - A protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

Wep Key Distribution - A feature of IEEE 802.1x. It provides automatic/dynamic Wep key distribution mechanism.
top

NAT
Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses.
top

UPnP
UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is supported by Windows ME, XP, or later.
top

Virtual DMZ Host - If you have a client PC that cannot run Internet application properly from behind the NAT firewall or after configuring the Special Applications function, then you can open the client up to unrestricted two-way Internet access.
Enter the IP address of a DMZ host to this screen. Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks, so only use this option as a last resort.
top

Virtual Server
If you configure the router as a virtual server, remote users accessing services such as Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP address. In other words, depending on the requested service (TCP/UDP port number), the router redirects the external service request to the appropriate server.

Example:

ID	Mapping Ports	Server IP	Enable	Comment
1	80	192.168.2.20	✓	Web Server
2	21	192.168.2.21	✓	FTP Server
3	23	192.168.2.23	✓	Telnet Server

top

Special Application
Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections,-specify the port normally associated with an application in the "Trigger Port" field,select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

Example:

ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624	UDP	MSN Game Zone
2	28800	UDP	2300-2400, 47624	TCP	MSN Game Zone
3	6112	UDP	6112	UDP	Battle.net

top

Security

The router provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).

Intrusion Detect - This function explicitly enables/disables the IDS(Intrusion Detection Service)portion of the Firewall. You must enable IDS if you want to activate the settings specified in the firewall IDS.

Discard PING WAN - When this feature is enabled, hosts on the WAN cannot ping the router.

Remote Management - By default, management access is only available to users on your local network. However, you can also manage the router from a remote host by adding the IP address of an administrator to this screen.

MAC Control - You can block certain client PCs accessing the Internet based on MAC address.
top

Access Control
You can filter Internet access for local clients based on IP addresses, application types, (i.e., HTTP port), and time of day.

Content Filter - Filter the Http contents which contain the texts user want to block.
URL Filter - Filter the DNS queries by the URLs user inputted.
top

IGMP
The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for an Internet computer

to report its multicast group membership to adjacent routers. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. Multicasting can be used for such applications as updating the address books of mobile computer users in the field, sending out company newsletters to a distribution list, and "broadcasting" high-bandwidth programs of streaming media to an audience that has "tuned in" by setting up a multicast group membership.
top

Routing

Routing Information Protocol(RIP) is a distance-vector protocol that uses hop count as its metric. RIP is widely used for routing traffic in the global Internet and is an interior gateway protocol (IGP).The original incarnation of RIP was the Xerox protocol, GWINFO. RIP itself evolved as an Internet routing protocol, and other protocol suites use modified versions of RIP.
The latest enhancement to RIP is the specification RIP 2. RIP2 allows more information to be included in RIP packets and provides a simple authentication mechanism.

Static Routing

Static Routing Table Entries	This list shows all entries in the Routing Table. • The "Properties" area shows details of the selected item in the list. • Change any the properties as required, then click the "Update" button to save the changes to the selected entry.
Properties	• **Destination IP Address** - The network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of the Destination IP Address. The 4th (last) field can be left at 0. • **Network Mask** - The Network Mask for the remote LAN segment. For class "C" networks, the default mask is 255.255.255.0 • **Gateway IP Address** - The IP Address of the Gateway or Router which the Wireless Broadband Router must use to communicate with the destination above. (**NOT** the router attached to the remote segment.) • **Metric** - The number of "hops" (routers) to pass through to reach the remote LAN segment. The shortest path will be used. The default value is 1.

top

System Logs
System Log - Displays any events on the router.

Configuration Tools
Restore Factory Defaults - Reset the settings of this device to the factory default values.
Backup Settings - Save the settings of this device to a file.
Restore Settings - Restore the settings of this device to the backup settings.
top

GLOSSARY OF TERMS
top

DHCP Dynamic Host Configuration Protocol. This protocol automatically configures the TCP/IP settings of every computer on your home network.
top

DNS Server Address DNS stands for Domain Name System, which allows Internet host computers to have a domain name (such as www.yahoo.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps

a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing " www.yahoo.com" into your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.
top

DSL Modem DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.
top

Ethernet A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 100 million bits per second (Mbps).
top

IP Address IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies an single, unique Internet computer host. Example: 192.34.45.8.
top

ISP Gateway Address (see ISP for definition). The ISP Gateway Address is an IP address for the Internet router located at the ISP's office. This address is required only when using a cable or DSL modem.
top

ISP Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.
top

LAN Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.
top

MAC Address MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network.
top

NAT Network Address Translation. This process allows all of the computers on your home network to use one IP address. The NAT capability of the router, allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.
Network Address Translation can be used to give multiple users access to the Internet with a single user account, or to map the local address for an IP server(such as Web or FTP) to a public address. This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network. NAT must be enabled to provide multi-user access to the Internet or to use the Virtual Server function.
top

PPPoE Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of secure data transmission originally created for dial-up connections. PPPoE is for Ethernet connections.
top

Subnet Mask A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet.
top

TCP/IP Transmission Control Protocol/Internet Protocol. This is the standard protocol for data transmission over the Internet.
top

WAN Specify the WAN connection type required by your Internet Service Provider, then click "Apply" to provide detailed configuration parameters for the selected connection type. Specify one of the first five options to configure a WAN connection through the RJ-45 port.
top