information SHEET

EIPR-E Help Screens

The EIPR-E has convenient Help Screens that are resident within the device. However, some users may also enjoy the convenience of all Help Screen information gathered into one searchable document. Such is the purpose of this Information Sheet.

System Configuration (Setup Tab)

Use the setup page to perform basic IP settings for the WAN and LAN interfaces — such as IP address, subnet mask, etc. *Connection Type* is used to specify how your EIPR connects to the WAN: *DHCP, Static IP, PPPoE* or *PPTP*. If required, you can also set optional items like Host Name, Domain Name and MTU. Host Name will be used in your DHCP requests and Domain Name will be used by the EIPR DHCP server.

If you select *DHCP*, the WAN side of the EIPR will have its IP address, subnet mask and gateway address set by a DHCP server that is directly or indirectly connected to the WAN port. If no DHCP server is available, static entry values can be entered by selecting connection type *Static IP.* PPPoE is normally used by DSL modems. Follow the instructions provided by the DSL provider when configuring the *PPPoE* connection settings.

The Router IP address is the IP address which you can use to configure the EIPR. This will also be the gateway address used by IP devices connected to the LAN ports of the EIPR.

The **LAN Setup** can be used to enable the DHCP server for the LAN side along with the starting DHCP address, the number of DHCP clients and the lease time (in minutes). Only one DHCP server should be used in a LAN, so use caution when enabling DHCP. Set the EIPR's DHCP server addresses to be in the same subnet as the EIPR's IP address.

Upload Firmware (Setup Tab)

Firmware allows you to upload new firmware to the EIPR.

Click on the **Browse...** button to select the firmware file from your computer, then press **Upload**.

NOTE: The firmware filename should not be changed and used as is provided by Contemporary Controls.

CTRLink®

Administration Tab

Local Router Access allows you to change the Username and Password that are used to access the EIPR webpage. Each string must be between 5 and 63 alpha-numeric characters — and is case sensitive.

Remote Router Access allows you to access the router webpage from the WAN side when enabled. For security purposes, you can also specify your own IP port number for WAN webpage access under the Administration Port.

Configuration allows you to upload and download the router settings. Upload to Router allows you to click on the browse button to select the configuration file from your computer and then hit save to upload it to the router. The router will check the file and if it is a valid configuration file, the router will reboot using the settings from the uploaded file.

Save to PC allows you to save the current router configuration to your computer.

Status Tab

This **read-only** page reports the EIPR Firmware Version, MAC Address and the settings of the **WAN interface** of the EIPR.

If you wish to renew your DHCP lease on your WAN port, you can press the Release button and then the Renew button.

If the DHCP server for the LAN port is enabled you can press View LAN DHCP Clients button to view the currently assigned DHCP addresses and the MAC addresses to which they are assigned.

Advanced Tab

The firewall within the EIPR can be disabled on this page. It is enabled by default. When the firewall is disabled ALL requests from the WAN network will be transmitted to the LAN network of the EIPR. When enabled the firewall will block requests from the WAN network. It is recommended that you enable the firewall when connecting the EIPR to the Internet. Disabling the firewall can be useful when interconnecting two private networks.

Port Range Forwarding (Advanced Tab)

Port Range Forwarding allows an IP port range from one network to be used in another network. The firewall within the EIPR will block all communications originated on the WAN side. To pass certain messages through the firewall, use port range forwarding. In the *WAN IP Port*, enter the *Start* and *End* WAN IP port number corresponding to the range to be forwarded — then select the IP protocols to be forwarded: *TCP, UDP* or *Both*. Next enter the IP address of the computer on the LAN side which will receive these messages. Selecting Enabled will cause the EIPR to utilize the entry.

NAT Loopback provides the ability to have a request originating from an EIPR LAN side device using the WAN IP address redirect back to an internal device as indicated by the port range forwarding entries. For example, this can be used to create a hyperlink using the WAN IP address that can work from either of the LAN side or the WAN side of the EIPR.

Port Forwarding (Advanced Tab)

Port Forwarding allows an IP port from one network to be used in another network. It is sometimes called port mapping. The firewall within the EIPR will block all communications originated on the WAN side. To pass certain messages through the firewall, use port forwarding. In the *WAN IP Port* box, enter the WAN IP port number to be forwarded — then select the IP protocols to be forwarded: *TCP, UDP* or *Both*. Next enter the IP address of the computer on the LAN side which will receive these messages and the IP port (*LAN IP Port*) to which the messages will be addressed. Selecting Enable will cause the EIPR to utilize the entry.

NAT Loopback provides the ability to have a request originating from an EIPR LAN side device using the WAN IP address redirect back to an internal device as indicated by the port forwarding entries. For example, this can be used to create a hyperlink using the WAN IP address that can work from either of the LAN side or the WAN side of the EIPR.

NAT (Advanced Tab)

NAT (Network Address Translation) is used to pass data from one IP address in one network to another IP address on a another network. Thus, the EIPR translates a WAN-side IP address to a specific LAN-side IP address. The firewall within the EIPR will block all communications originated on the WAN side — unless you specify exceptions. Enter the LAN device address in the NAT *LAN IP Address* boxes. In the *WAN IP Address* boxes, enter the address you want it to "appear as" on the WAN side. For example, if you want LAN device 192.168.1.2 to appear on the WAN network as 1.2.3.4 then put 192.168.1.2 in the *LAN IP Address* boxes and 1.2.3.4 in the *WAN IP Address* boxes — then enable this entry.

Firewall (Advanced Tab)

The firewall within the EIPR can be disabled on this page. It is enabled by default. When the firewall is disabled ALL requests from the WAN network will be transmitted to the LAN network of the EIPR. When enabled the firewall will block requests from the WAN network. It is recommended that you enable the firewall when connecting the EIPR to the Internet. Disabling the firewall can be useful when interconnecting two private networks.

Allowlist (Advanced Tab)

When port forwarding or port range forwarding is enabled any WAN connected device can originate a conversation to LAN side connected devices when using the enabled port ranges. Also any WAN connected device can configure the router if remote router access is enabled. An Allowlist is used to limit the WAN connected devices which can use the port forwarding, port range forwarding and remote router access feature. The Allowlist feature does not affect IP conversations initiated on the LAN network.

Wi-Fi (Advanced Tab)

This page allows you to configure the settings for the Wireless. You can enable Wi-Fi, setup the SSID string, enable/disable the SSID broadcast, select the channel and the security mode.

Three security modes are available: WEP, WPA Personal (WPA-PSK) and WPA2 Personal (WPA2-PSK). WEP has 64-bit and 128-bit key length and the user can enter the shared key in HEX or ASCII format. 64-bit WEP key length uses 5 ASCII characters or 10 HEX characters. 128-bit WEP requires 13 ASCII characters or 26 HEX characters. WPA and WPA2 require 8 to 63 characters for the shared key and can support AES or TKIP encryption. The Group Key Update Interval specifies the time interval for rekeying Groupwise Transient Key GTK (broadcast/multicast encryption keys) in seconds. This should usually be left at the default value.

Please note: WEP is less secure and should be used as the last option. Please use WPA2 with AES whenever possible. WPA with TKIP is provided for compatibility with older devices that don't support WPA2.