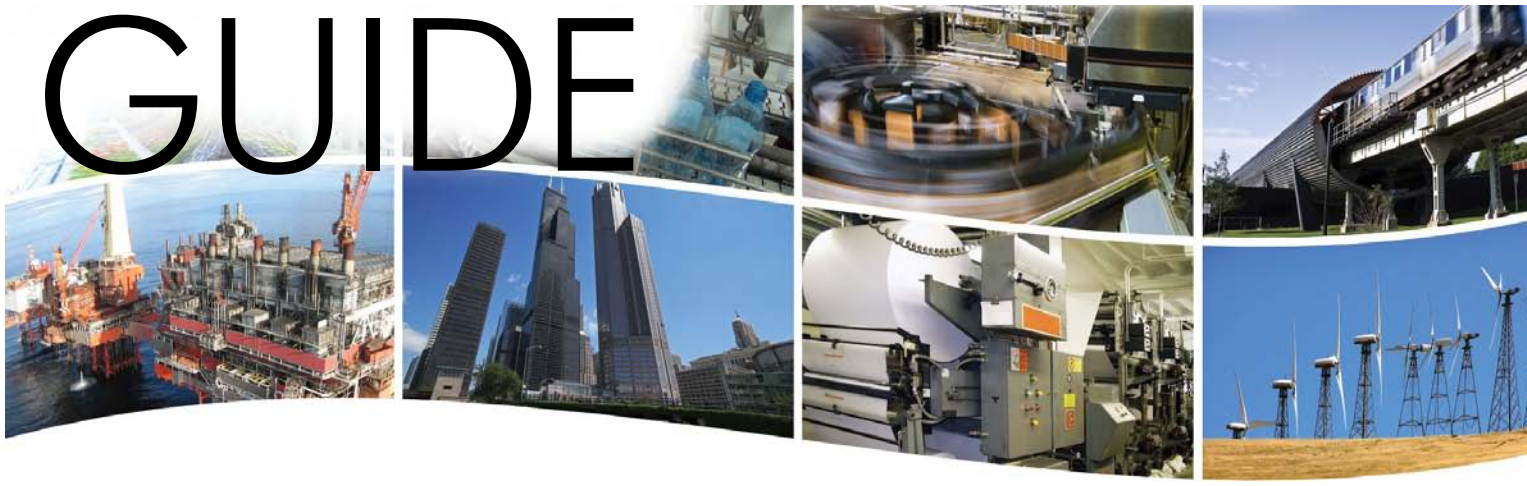
application
GUIDE



EIPR — Skorpion Wired and Wireless IP Routers

The EIPR links two Internet Protocol (IPv4) networks together — passing appropriate traffic while blocking all other traffic. One of the networks is designated the local-area-network (LAN) and the other the wide-area-network (WAN). When the firewall is enabled, communication initiated on the LAN-side passes through the router while WAN-side initiated communication is blocked. The EIPR incorporates an Ethernet switch for multiple LAN-side connections. An external Ethernet cable or DSL modem attached to the WAN-side can be used to connect to the Internet. A USB port allows expansion to wireless networks.

EIPR Skorpion IP Router Features …

- Web page configuration
- 10/100 Mbps WAN port
- 4-port 10/100 Mbps Ethernet LAN switch
- PAT, NAT and Port Forwarding
- NAT Loopback
- Remote Router Access and Whitelist
- Stateful firewall (can be disabled)
- DHCP client (WAN) and DHCP server (LAN)
- Wi-Fi connectivity via USB port
- DIN-rail mounting
- Rugged metal enclosure
- Diagnostic LEDs
- CE Mark, RoHS, UL 508, C22.2 No. 142-M1987
- 24 VAC/VDC powered

EIPR-E

EIPR-E with user-provided Wi-Fi adapter installed

CTRLink®

EIPR — Skorpion IP Router

With a DIN-rail mounting clip, rugged metal enclosure and the ability to be powered from a low-voltage power source, the EIPR is ideal for automation systems.

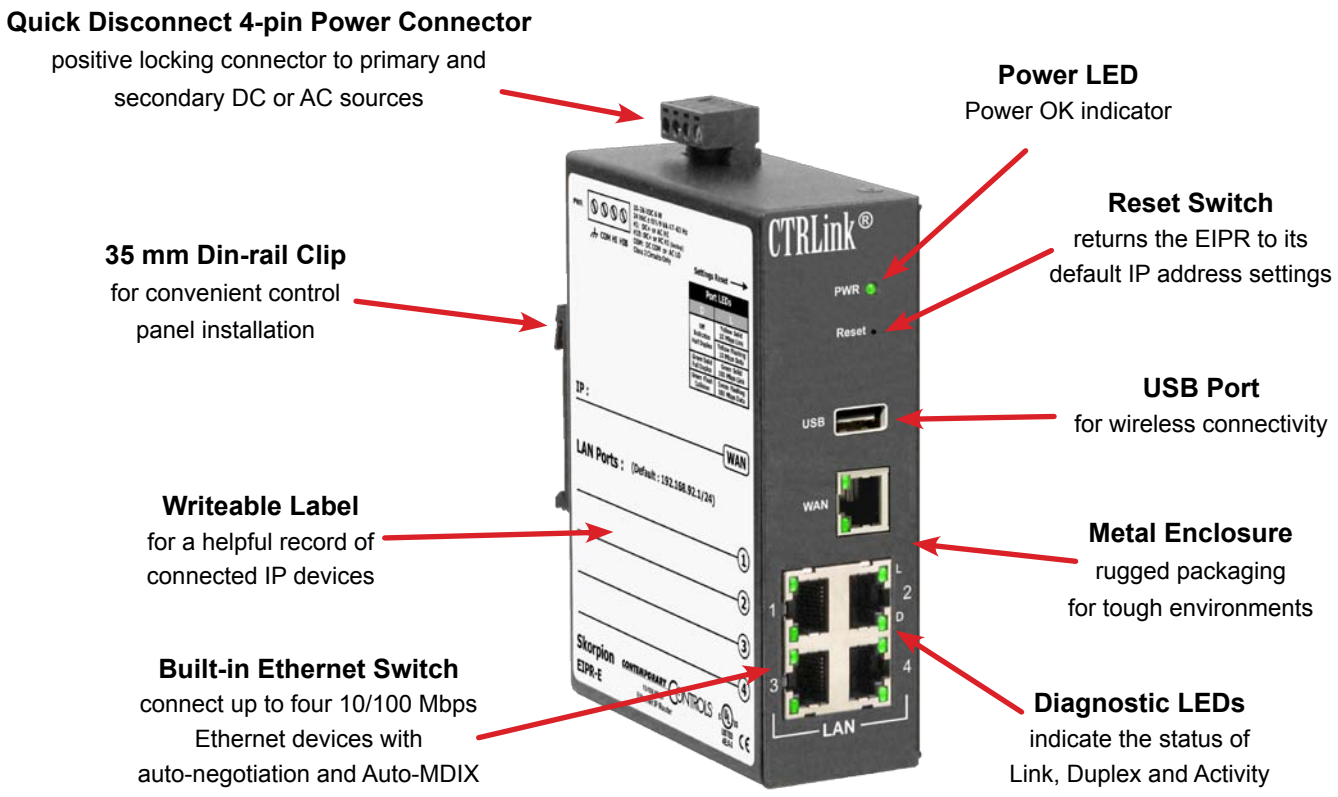
Although the EIPR has some of the same features found in high-end routers, it is simple to install and commission. Configuration is via a web browser.

The lower portion of the router connects the local-area-network or the LAN side. The upper portion of the router connects the wide-area-network or the WAN side. A firewall — which can be disabled by the user — separates the two portions.

In some cases, such as routing between two internal LANs, it may be desirable to disable the firewall.

A firewall controls the passing of messages from one side of router to the other. A stateful firewall makes decisions based upon the structure of the message and who is initiating and who is responding.

After connecting a USB Wi-Fi adapter (IEEE 802.11b, 802.11g, etc.), the EIPR can become a Wi-Fi access point. This will allow Wi-Fi devices to wirelessly communicate with the EIPR and with each other.

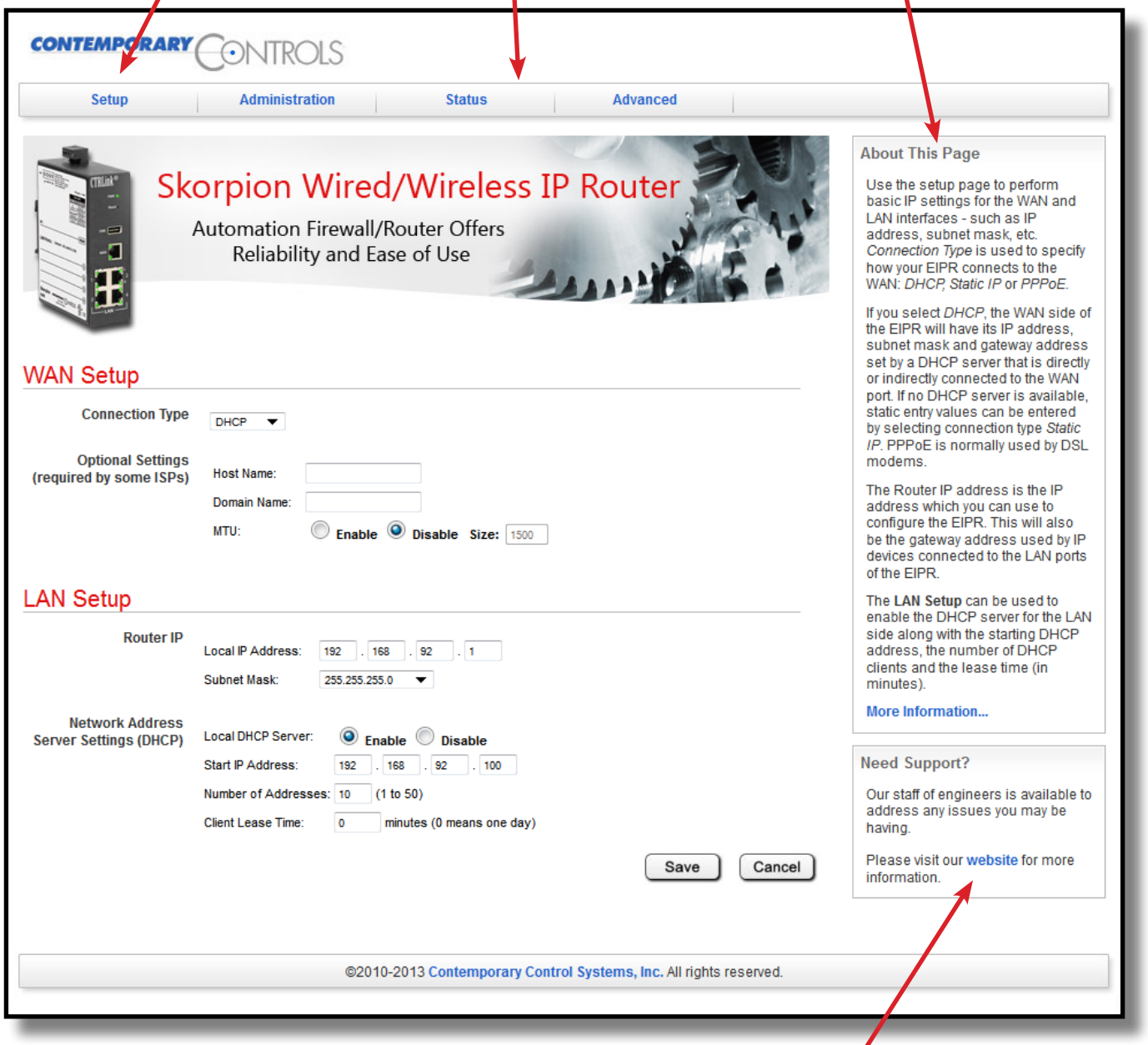


Web Page Configuration

Setup Button
displays the screen shown on this page

Menu Button Bar
provides quick access to all main screens

Resident Help Screens
provide immediate assistance on any feature on any screen



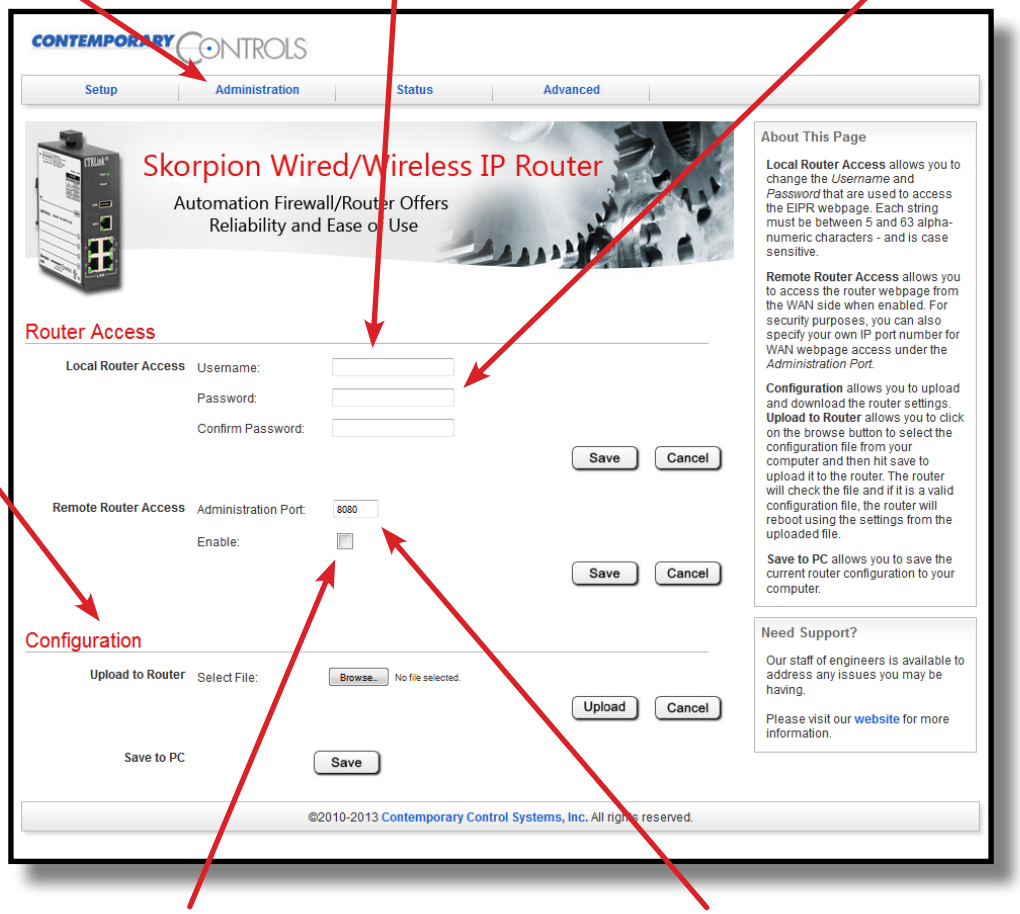
For More Information
each screen has a convenient link to our website

Secure Login — From Any IP-connected Computer

Administration Button
displays this screen

Default Username is "admin"
Entering a new value is recommended.
Default restored if reset switch is used.

Default Password is "admin"
Entering a new value is recommended.
Default restored if reset switch is used.



Save or Retrieve Configuration

Remote Router Access
Disabled by default. Enable if configuration is desired from a web browser on either LAN side or WAN side.

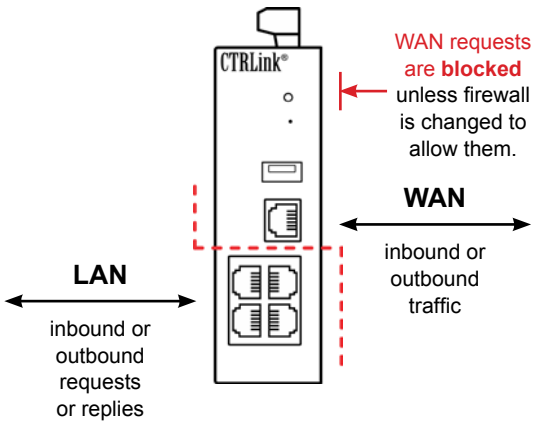
Administration Port
Default setting of 8080 can be changed after Remote Router Access is enabled, but well-known ports are not recommended.

Stateful Firewall — Promotes Secure Communication

The lower part of the router connects the LAN side (the local-area-network). The upper part connects the WAN side (wide-area-network). A firewall (which can be disabled by the user) separates the two parts.

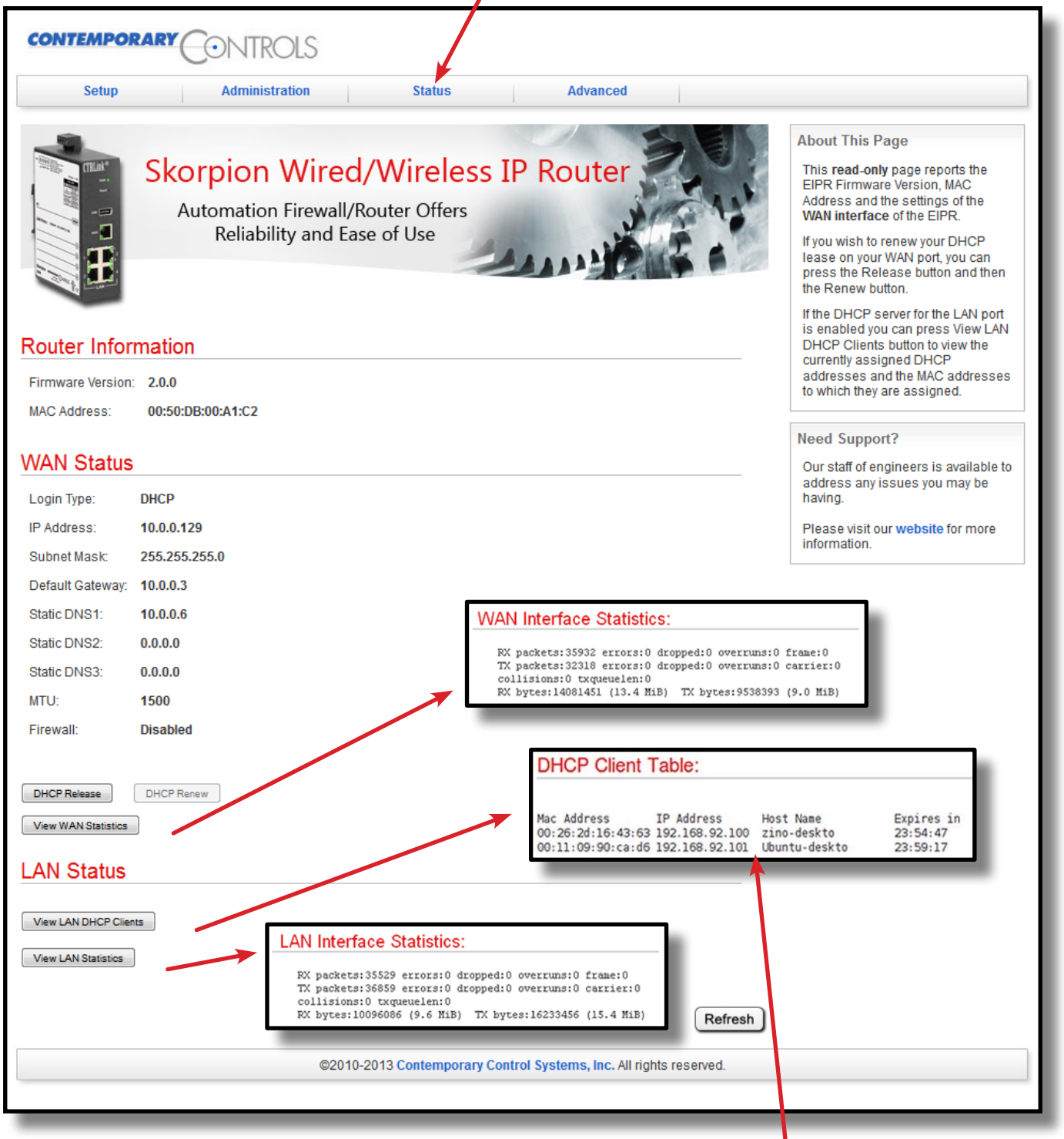
A firewall controls the passing of messages from one side of a router to the other. A *stateful firewall* acts on the structure of the message and who is initiating and who is responding.

Originating requests from the LAN side and corresponding responses from the WAN side ***pass through*** the firewall. But traffic originating from the WAN side is ***blocked*** from the LAN side ***unless*** the firewall is adjusted to allow it. This protects the LAN side from unauthorised WAN access. **NOTE:** Wi-Fi is part of the LAN.



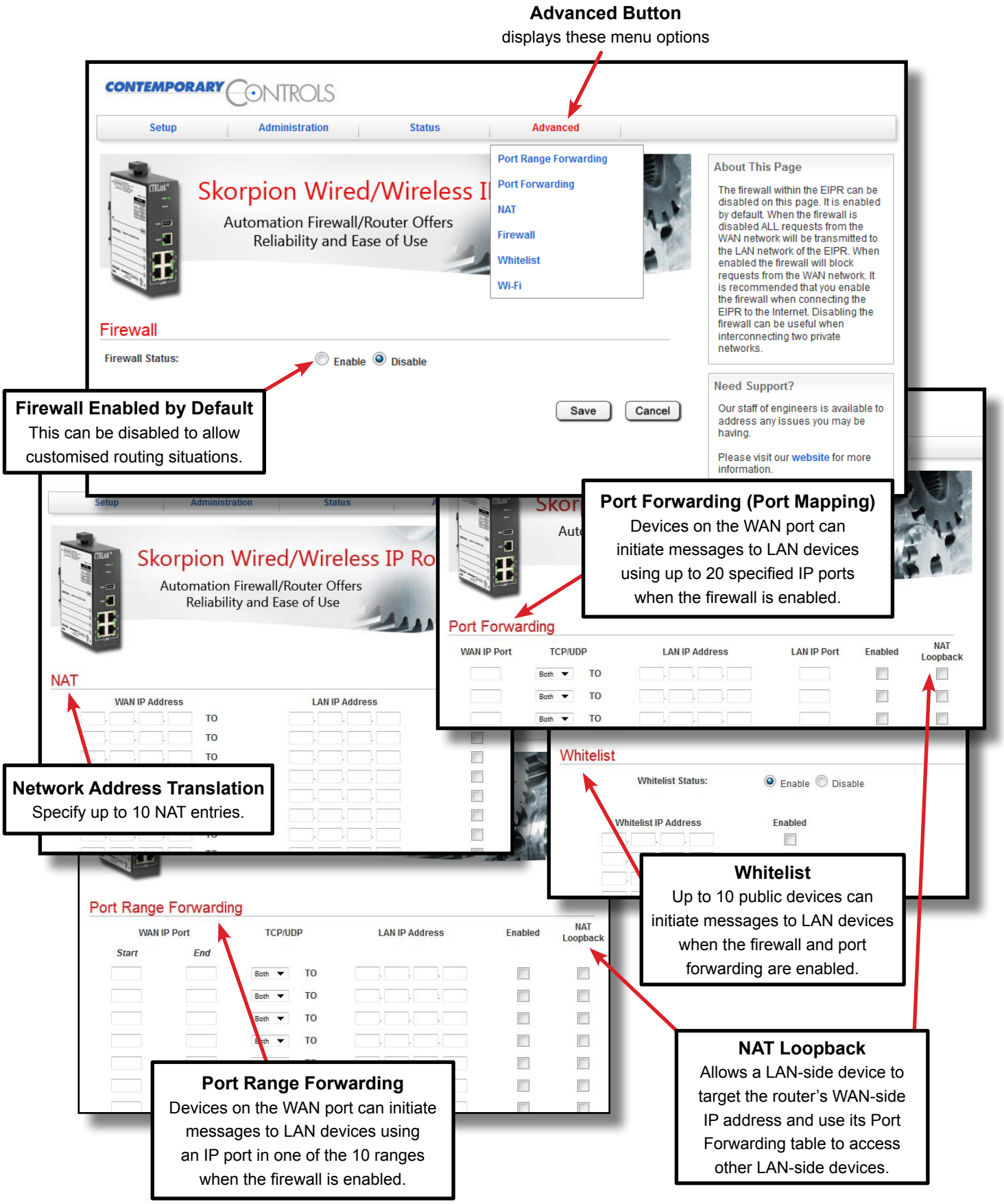
Status and Configuration Report — Just a Click Away

Status Button
displays the screen shown on this page



If the EIPR is enabled as a DHCP Server,
clicking the View LAN DHCP Clients button brings up another window to view the status of the LAN devices being served.

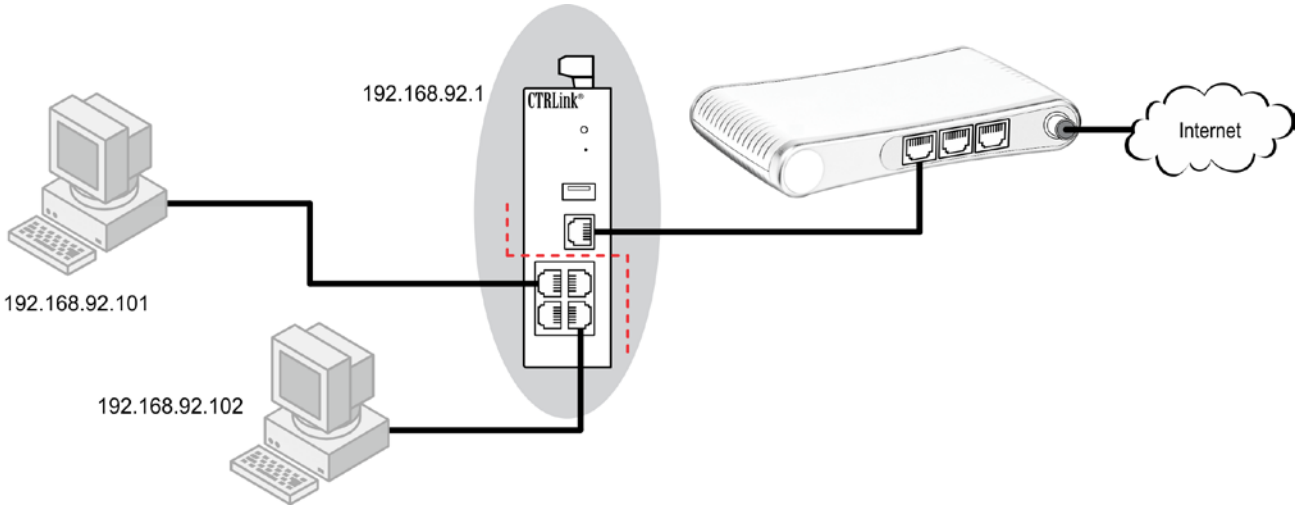
Advanced Features — for Demanding Situations



Application #1 — A Cable Modem Connection to the Internet

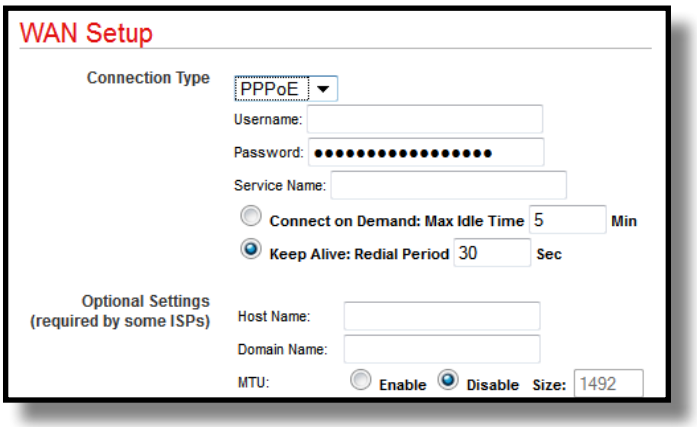
In the WAN Setup, the default Connection Type is *DHCP* — where a DHCP server on the WAN side will automatically assign an IP address, subnet mask, default gateway address and one or more DNS addresses to the WAN side of the IP router. Some cable modems have DHCP server functionality.

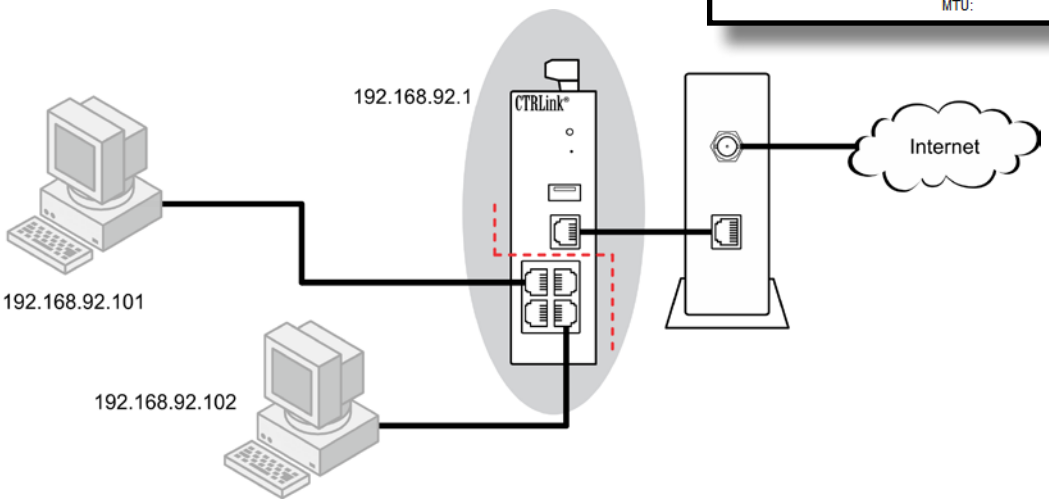
If a DHCP server is unavailable on the WAN network, you must make static IP entries for the WAN side of the router. Enter the IP address, subnet mask, default gateway address and one or more DNS addresses when using the Static IP option.



Application #2 — A DSL Modem Connection to the Internet

With DSL modems, the PPPoE protocol must be selected — and a username and password provided. Once a connection is established, the ISP furnishes all the needed WAN IP address assignments.

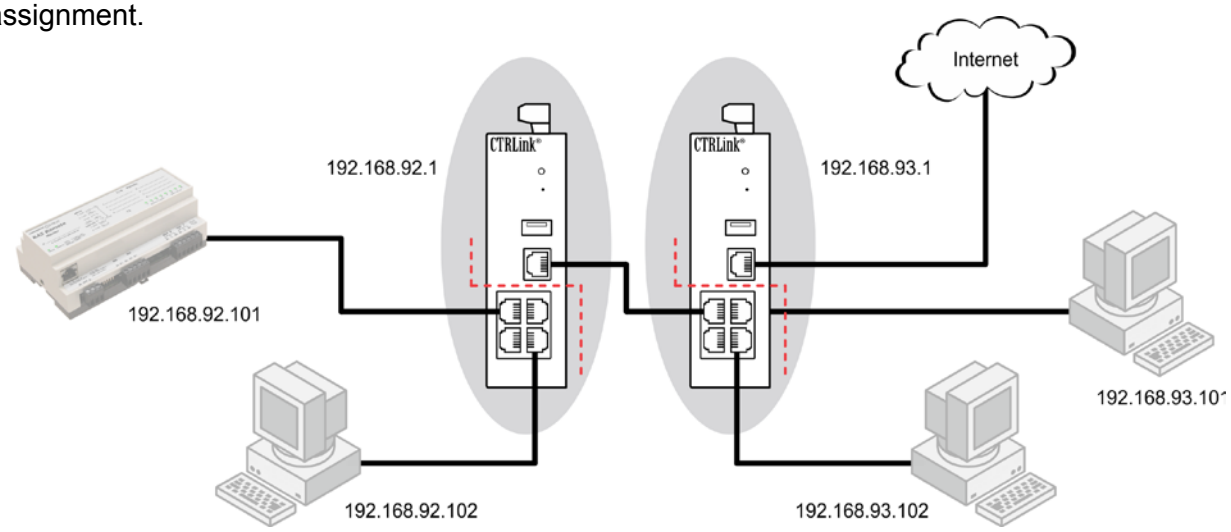




Application #3 — Cascaded Routers for Additional Isolation

For increased security and isolation, IP routers can be cascaded. Make sure that each LAN-side subnet address is unique when cascading IP routers. The left-most IP router can have its WAN-side IP address assigned using DHCP client or by using static IP address assignment.

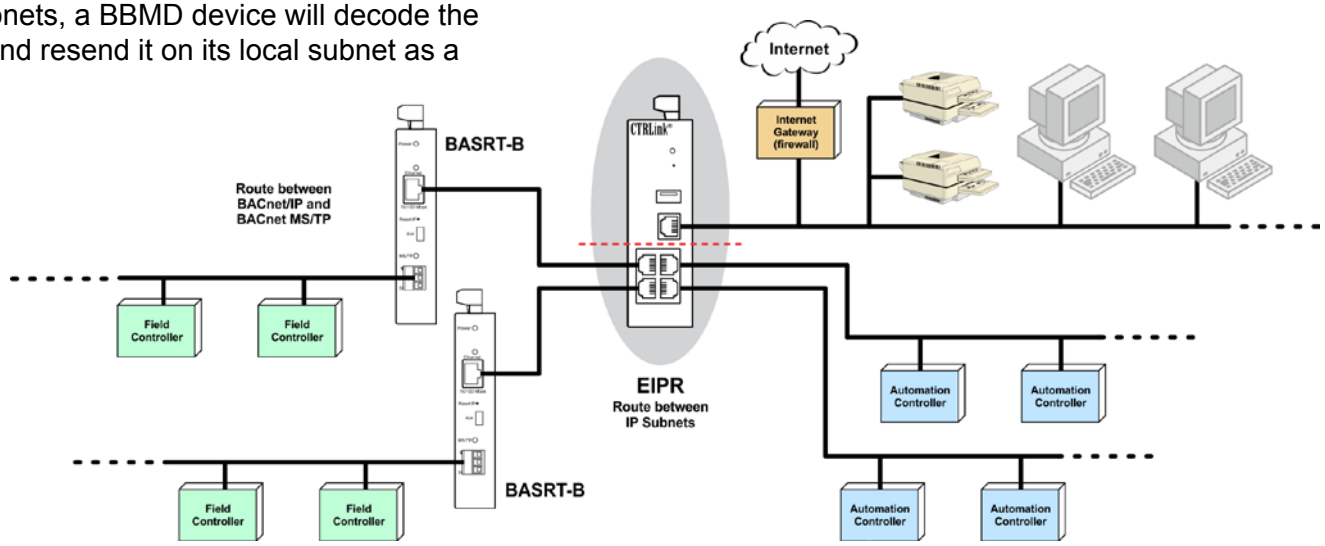
The illustration shows a pair of EIPR routers, but the right-most router could also be some other type of router — perhaps one already existing in the business system — because the EIPR supports standard Internet protocols.



Application #4 — Limiting BACnet Traffic

When attaching BACnet devices to IP networks it is possible that the IP network has been sub-netted through the use of IP routers. Most IP routers will not pass broadcast messages which are crucial to BACnet's operation. The solution is to incorporate BACnet/IP Broadcast Management Device (BBMD) functionality within the BACnet internetwork.

The BBMD concept requires that a broadcast message originating on one subnet be encapsulated into a directed message and sent to all remote subnets since these directed messages will pass through IP routers. Once the encapsulated messages are received on the remote subnets, a BBMD device will decode the message and resend it on its local subnet as a broadcast message. Therefore it would appear that a BBMD device must be present on each subnet in order to provide this encoding and decoding function. However, this is not the case if all the BACnet/IP devices support Foreign Device Registration (FDR). At a minimum, one BBMD device is required to be located on one of the subnets with FDR devices registering to this one BBMD. This is what is shown in the example with a BAS Router providing BBMD functionality while allowing for foreign devices registration. Notice that connecting to a BACnet MS/TP network is an option.

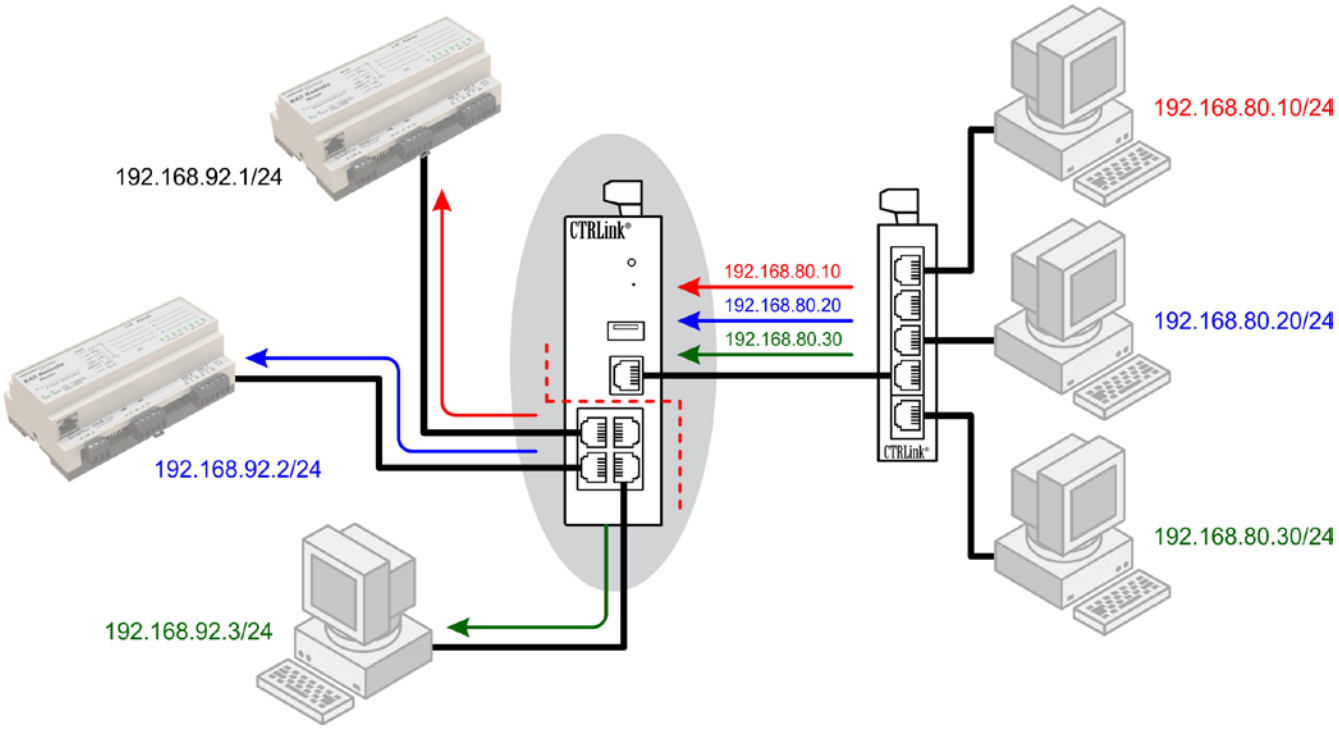


Application #5 — Disable the Firewall for Unrestricted Routing

There are times when you may want to disable the firewall. The firewall controls the passing of messages from the public (WAN) side of the router to the private (LAN) side — and normally this protects the private side from unauthorised public access.

Under the Advanced Tab, you may choose to disable the firewall. Typically the firewall is disabled when the LANs on both sides of the router are within one organization. That is, ***there is no public side*** — both sides are essentially private, so no firewall is needed.

LAN IP Address	WAN IP Address
192.168.92.1/24	192.168.80.10/24
192.168.92.2/24	192.168.80.20/24
192.168.92.3/24	192.168.80.30/24



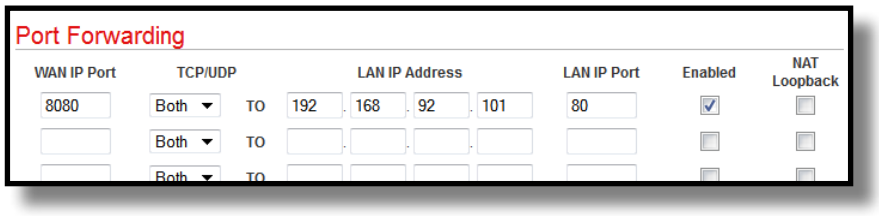
Application #6 — Port Forwarding to Access a Private Web Server

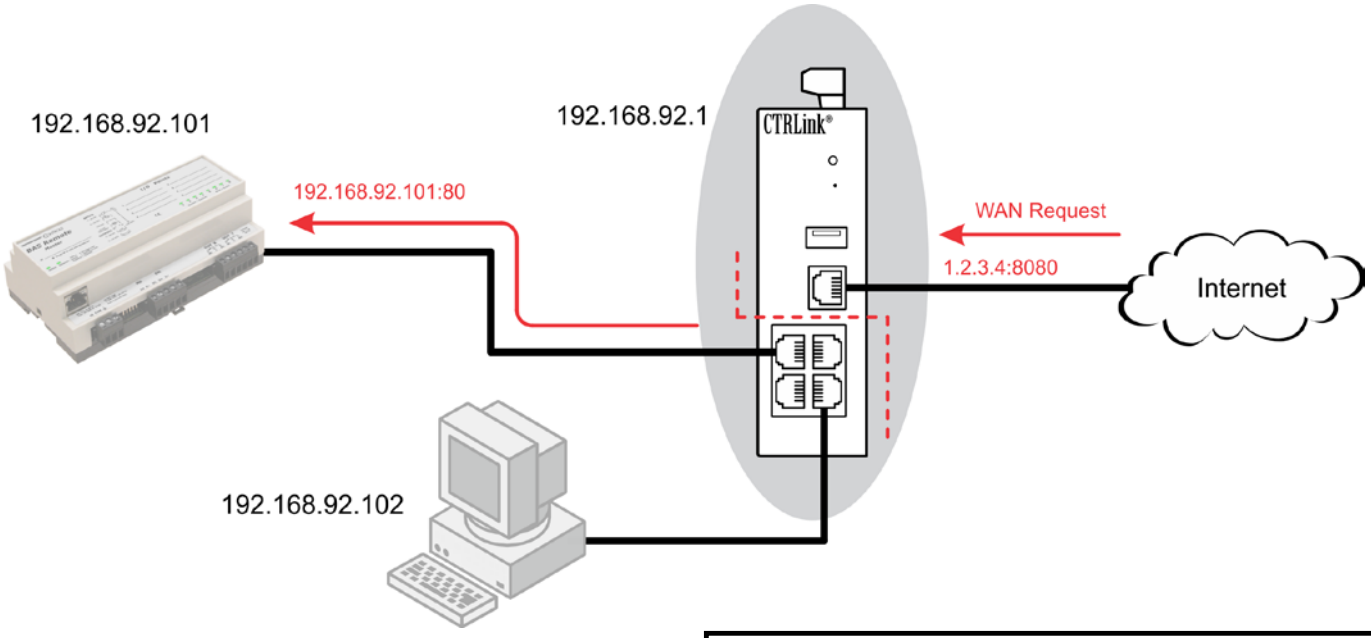
The firewall will normally block all WAN-side requests. Port forwarding allows computers on the WAN side to access devices on the LAN side by opening up ***selected*** WAN IP ports. The only WAN-side requests that will be forwarded through the IP router are those that specify both the router's WAN address and a destination IP port number that exists in the router's IP port forwarding table. When this match is made, the message is forwarded to the indicated IP address on the LAN side.

This is very useful when only one public IP address is available, but there is a need to access multiple LAN-side devices. In this example, we want to access a private web server at 192.168.92.101 which is normally invisible from the Internet. Using port forwarding, we allow a WAN-side request made to the router's public (WAN) address. For additional security, the port numbers have been translated.

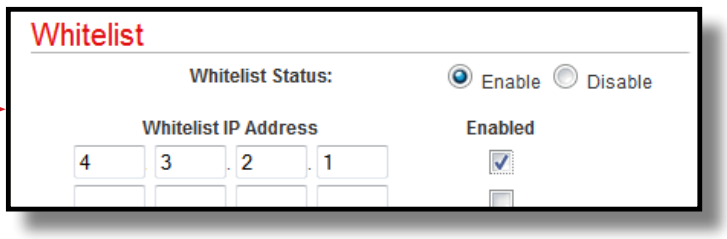
You can also select Port Range Forwarding to allow an ***entire range*** of addresses through the firewall. Note that ***any WAN-side device*** can use port forwarding — but you can greatly enhance security by creating a ***whitelist*** of allowed WAN-side devices. This is illustrated at the bottom of the page.

Internal IP Address	LAN IP Port	WAN IP Port	External IP Address
192.168.92.101/24	80	8080	1.2.3.4





Enhance Security with a Whitelist
Specify which WAN-side devices can use port forwarding.



Application #7 — Router Access from a WAN-side Device

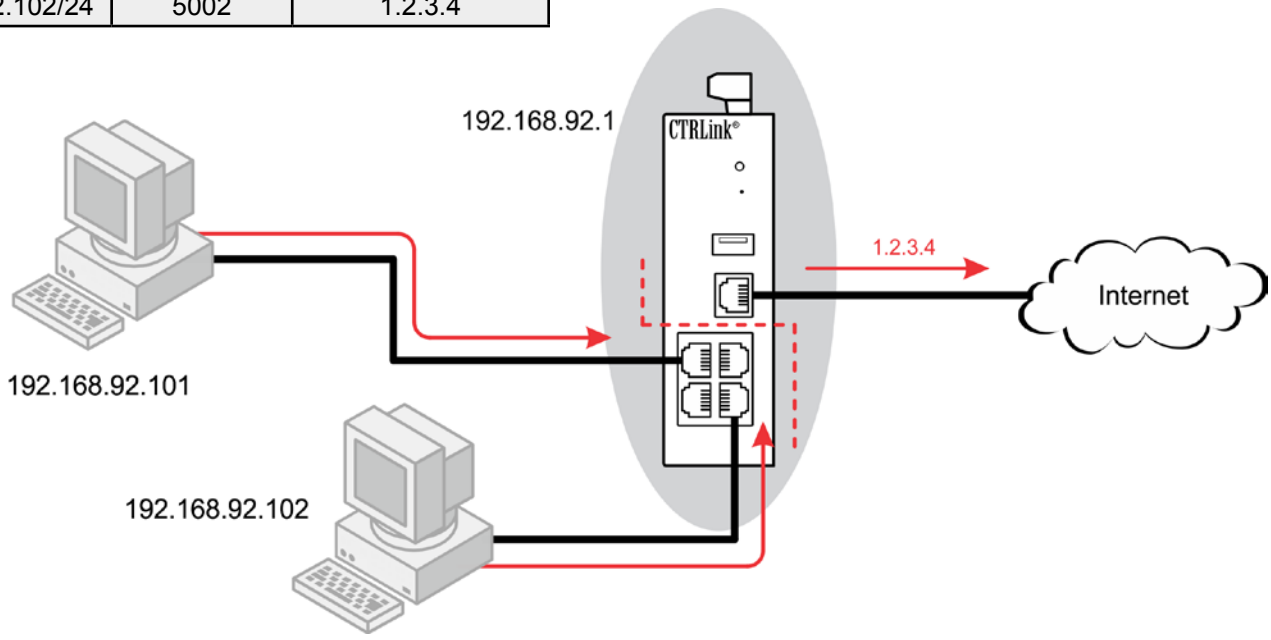
In some situations you may want a WAN-side device to access and possibly configure the router. This is enabled via the Remote Router Access control (shown below) found under the Administration tab.
Caution: Enabling this control grants access to any device on the public or WAN-side. To restrict access to just certain WAN devices, you must construct a whitelist such as the example below which specifies an outside (public or WAN-side) device that has the IP address of 4.3.2.1.

Application #8 — Port Address Translation (PAT)

PAT (also known as a *firewall*) allows a many-to-one mapping of private IP addresses to one public address. Not only does this provide enhanced security for the devices on the LAN side, it also allows multiple LAN-side devices to communicate to devices on the WAN side using only one WAN IP address. When the WAN network is connected to the Internet, this allows the LAN devices to communicate on the Internet via one public IP address.

Most ISPs will limit the number of public IP addresses provided to their customers. PAT is done by the use of port assignments — thus, granting private IP addresses access to the Internet. In this example, the ISP provided the router the public address of 1.2.3.4. Both LAN-side PCs have automatically been assigned local IP ports and granted access to the Internet — and no configuration was needed.

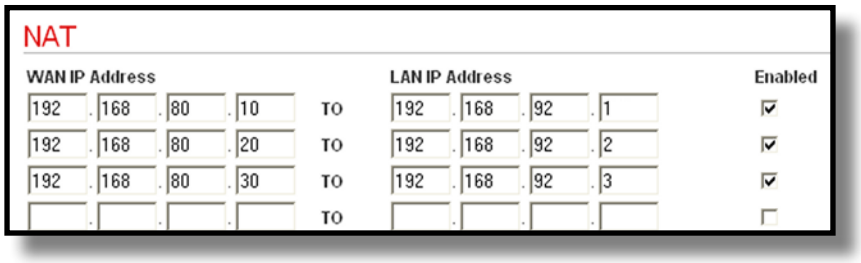
Internal IP Address	LAN IP Port	External IP Address
192.168.92.101/24	5001	1.2.3.4
192.168.92.102/24	5002	1.2.3.4

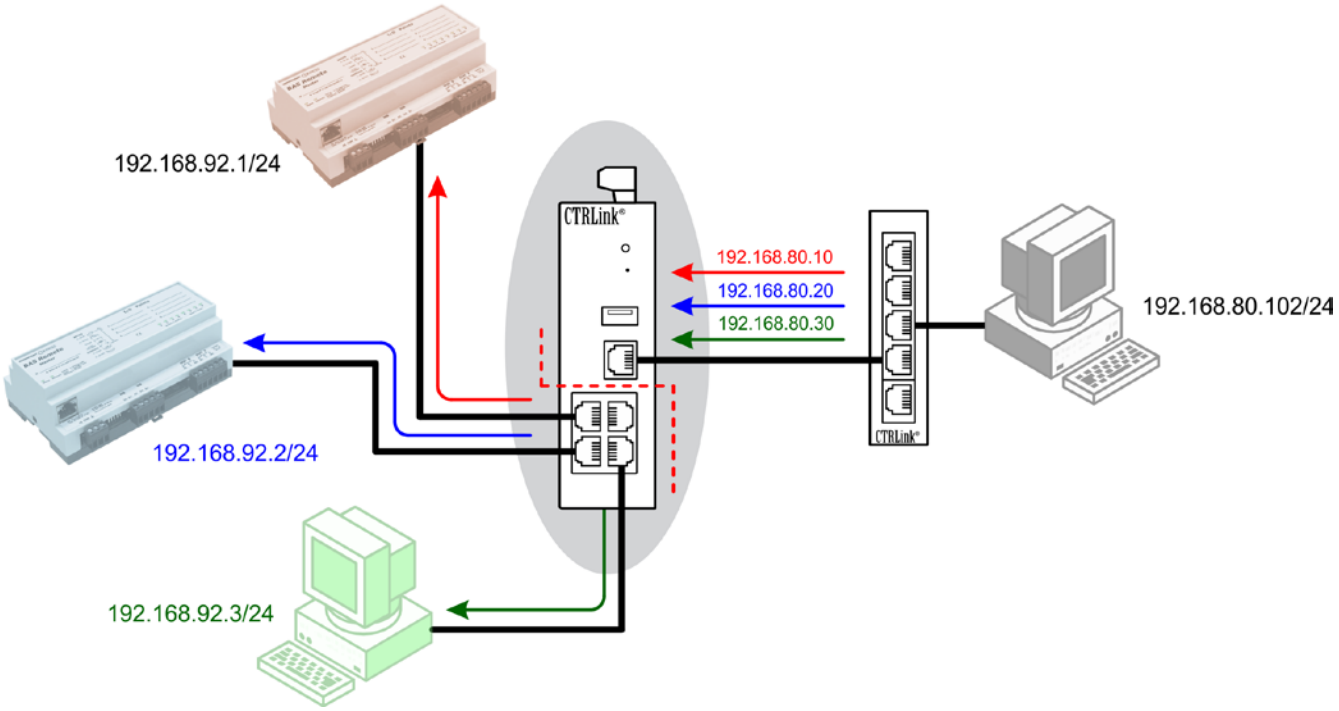


Application #9 — Network Address Translation (NAT)

NAT allows for a one-to-one mapping of internal IP addresses to external IP addresses. This could be helpful when accessing duplicate systems that are configured the same. The actual LAN-side addresses are hidden. Notice that the LAN and WAN subnets are different.

Internal IP Address	External IP Address
192.168.92.1/24	192.168.80.10/24
192.168.92.2/24	192.168.80.20/24
192.168.92.3/24	192.168.80.30/24

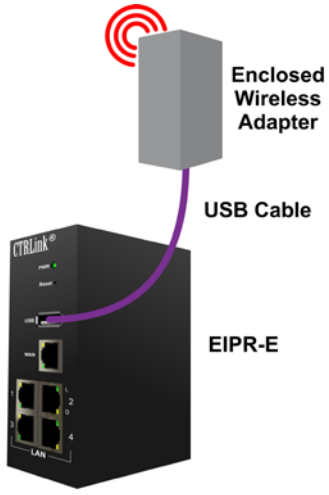




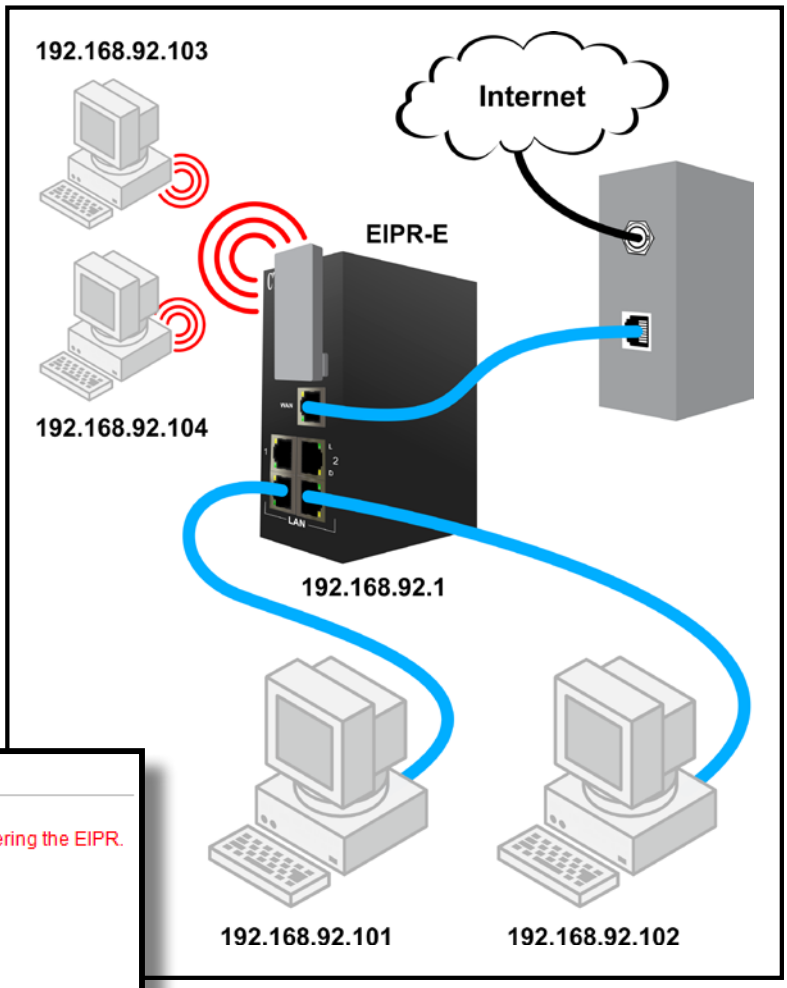
Application #10 — Wi-Fi Access Point via the USB Port

The resident USB port on the EIPR-E allows expansion to wireless networks once an appropriate wireless adapter is inserted into the port. One possibility is implementing a Wi-Fi access point — thereby increasing the number of LAN-side clients.

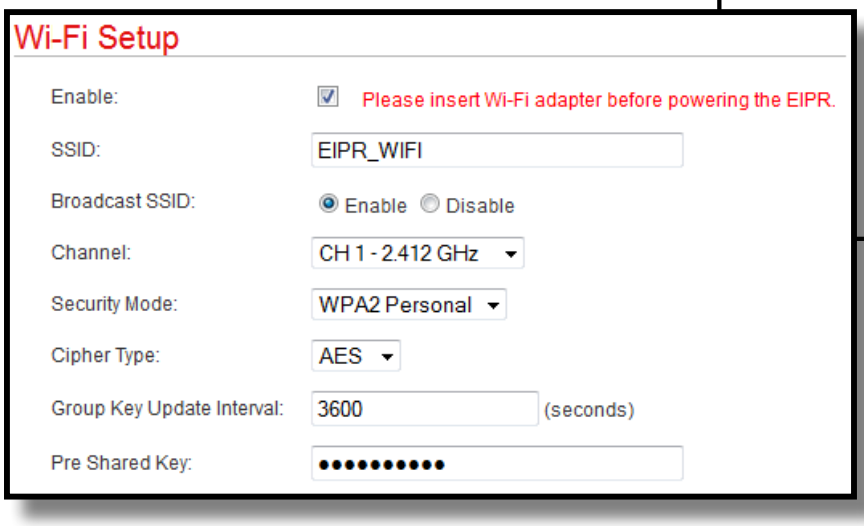
After connecting a USB Wi-Fi adapter (IEEE 802.11b, 802.11g, etc.), the EIPR can become a Wi-Fi access point. This will allow Wi-Fi devices to wirelessly communicate with the EIPR and with each other. Each wirelessly connected Wi-Fi device can receive a DHCP assigned address from the EIPR. When wirelessly connected, each Wi-Fi device can also communicate directly with any EIPR LAN-connected devices and can also route through the EIPR WAN port for access to other subnets or to the Internet. The EIPR supports Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA, WPA2) security in its communications. The other EIPR features, such as port forwarding, can also be applied to the wirelessly connected Wi-Fi devices. A list of supported Wi-Fi adapters can be found on the Contemporary Controls website under the EIPR product page.



Remote Wireless Adapter



Wired and Wireless Access to the Internet



Specifications

Power Requirements	10–36 VDC ±10% 6 W	or	24 VAC ±10% 9 VA 47–63 Hz
Operating Temperature	0°C to 60°C		
Storage Temperature	–40°C to 85°C		
Relative Humidity	10–95%, non-condensing		
Protection	IP30		
Mounting	TS-35 DIN-rail		
Ethernet Communications	IEEE 802.3 10/100 Mbps data rate 10BASE-T, 100BASE-TX physical layer 100 m (max) CAT5 cable length		
USB Port	USB 2.0, Type A 5 m (max) cable length delivered power (max) 500mA		
LEDs	Power	Green = power OK	
	L	Green = 100 Mbps communication established Yellow = 10 Mbps communication established Flash = activity	
	D	Green = Full-duplex operation Off = Half-duplex operation	
Regulatory Compliance	CE Mark; CFR 47, Part 15 Class A; RoHS; UL 508; C22.2 No. 142-M1987		

Ordering Information

Model	*RoHS*	*Description*
EIPR-E	✓	Skorpion IP Router with Four-port Switch and USB port for wireless connectivity
ACC-WIFISTK-1	✓	USB 802.11 b/g/n Wireless USB adapter
ACC-USBADPT-1	✓	USB Right Angle Swivel Adapter
ACC-MTGKIT-1	✓	Wall Mount USB Adapter Enclosure with 15’ (4.5m) cable
ACC-USBCBL-15	✓	15’ USB Extension Cable

United States
Contemporary Control Systems, Inc.
2431 Curtiss Street
Downers Grove, IL 60515
USA

Tel: +1 630 963 7070
Fax:+1 630 963 0109

info@ccontrols.com
www.ccontrols.com

China
Contemporary Controls (Suzhou) Co. Ltd
11 Huoju Road
Science & Technology
Industrial Park
New District, Suzhou
PR China 215009

Tel: +86 512 68095866
Fax: +86 512 68093760

info@ccontrols.com.cn
www.ccontrols.asia

United Kingdom
Contemporary Controls Ltd
14 Bow Court
Fletchworth Gate
Coventry CV5 6SP
United Kingdom

Tel: +44 (0)24 7641 3786
Fax:+44 (0)24 7641 3923

info@ccontrols.co.uk
www.ccontrols.eu

Germany
Contemporary Controls GmbH
Fuggerstraße 1 B
04158 Leipzig
Germany

Tel: +49 341 520359 0
Fax: +49 341 520359 16

info@ccontrols.de
www.ccontrols.eu