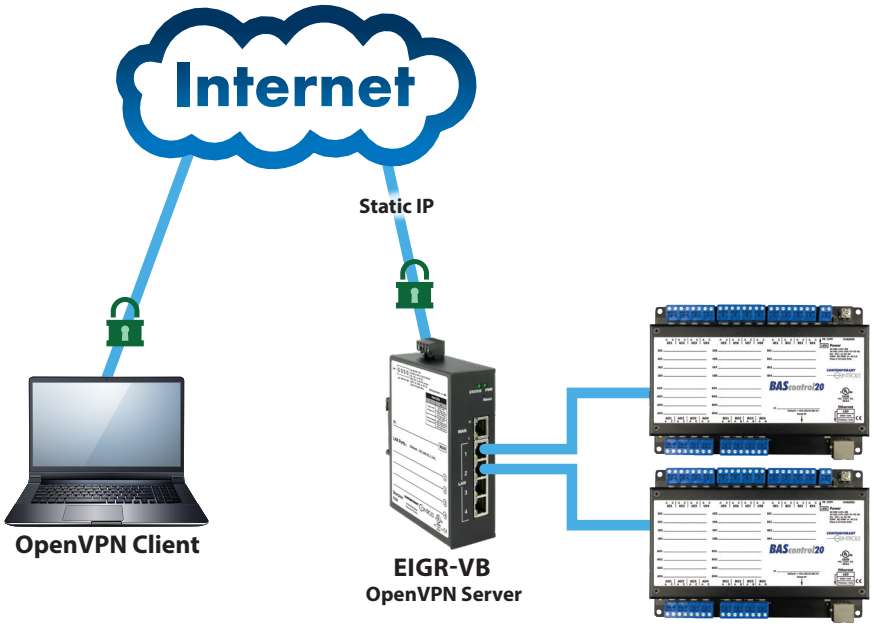
BridgeVPN – Facilitates Secure, Remote Communications for Single-Site Access

Utilizing the Internet for remote commissioning provides convenience while saving time and money. Contemporary Controls' EIGR-VB and EIGR-C Gigabit IP routers can be configured as a wired and wireless bridge VPN server for single-site, remote access solutions. With this configuration, users set up and maintain their own secure remote access without subscription fees and without the need for a cloud-based VPN server.



A simple VPN can exist between two end points, called a VPN tunnel, between a client and a server. One end point (client) is you at your office, and the other (server) is at the remote job site. Communication is encrypted – so only authorized devices can communicate over the VPN.

Operating in OpenVPN* server mode, the EIGR-VB and EIGR-C support bridge mode where up to 10 VPN clients (Windows/Linux PCs) are bridged to the router's LAN side and assigned an IP address from the LAN subnet. This provides the same application experience as if the client devices were part of the router's LAN and allows passage of multicast and broadcast messages through the VPN tunnel without the need for a BACnet/IP Broadcast Management Device (BBMD).

In addition to the BridgeVPN solution, Contemporary Controls offers a Self-HostedVPN solution which allows network savvy customers to set up and maintain their own wired or wireless remote access for multiple clients – up to 15 wired/cellular IP routers in OpenVPN client mode and 15 OpenVPN clients on PC/tablet/phone.

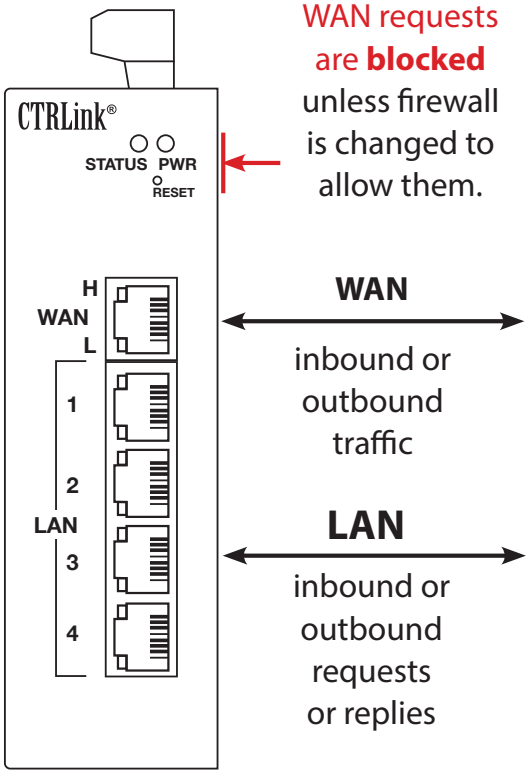
Another alternative is a VPN service, such as Contemporary Controls' RemoteVPN subscription service, which provides secure communication and the convenience of remote access without having to maintain the VPN server.

How it works

The EIGR-VB and EIGR-C high-speed routers link two 10/100/1000 Mbps Internet Protocol (IPv4) networks — passing appropriate traffic while blocking all other traffic. One network is the local-area-network (LAN); the other is the wide-area-network (WAN). The built-in stateful firewall passes communication initiated on the LAN-side while blocking WAN-side initiated communication. The lower part of the router connects the LAN side. The upper part connects the WAN side. The EIGR-C router adds support for cellular networks on the WAN side, allowing use at sites without Internet access. 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.

*OpenVPN® is a well-supported open-source VPN technology that incorporates SSL/TLS security with encryption.

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 unauthorized WAN-side access.



With Port Address Translation (PAT), LAN-side clients can access the Internet. Network Address Translation (NAT) allows a one-to-one translation between LAN-side and WAN-side devices. With Port Forwarding, LAN-side devices can be accessed from the Internet. The routers incorporate a four-port Ethernet switch for multiple LAN-side connections. An external Ethernet-based modem — cable or DSL— can be used to connect to the Internet. DSL modems connect via Point-to-Point Protocol over Ethernet (PPPoE).

The routers include real-time clock and OpenVPN client/server functionality. Although the EIGR routers have many of the same features found in high-end routers, they are simpler to install and commission. A resident DHCP server on the LAN-side will provide IP addresses to LAN-side clients, while a DHCP client on the WAN-side will accept IP address assignments from the attached network. Static addressing is accommodated as well. Configuration is via a web browser using authentication.

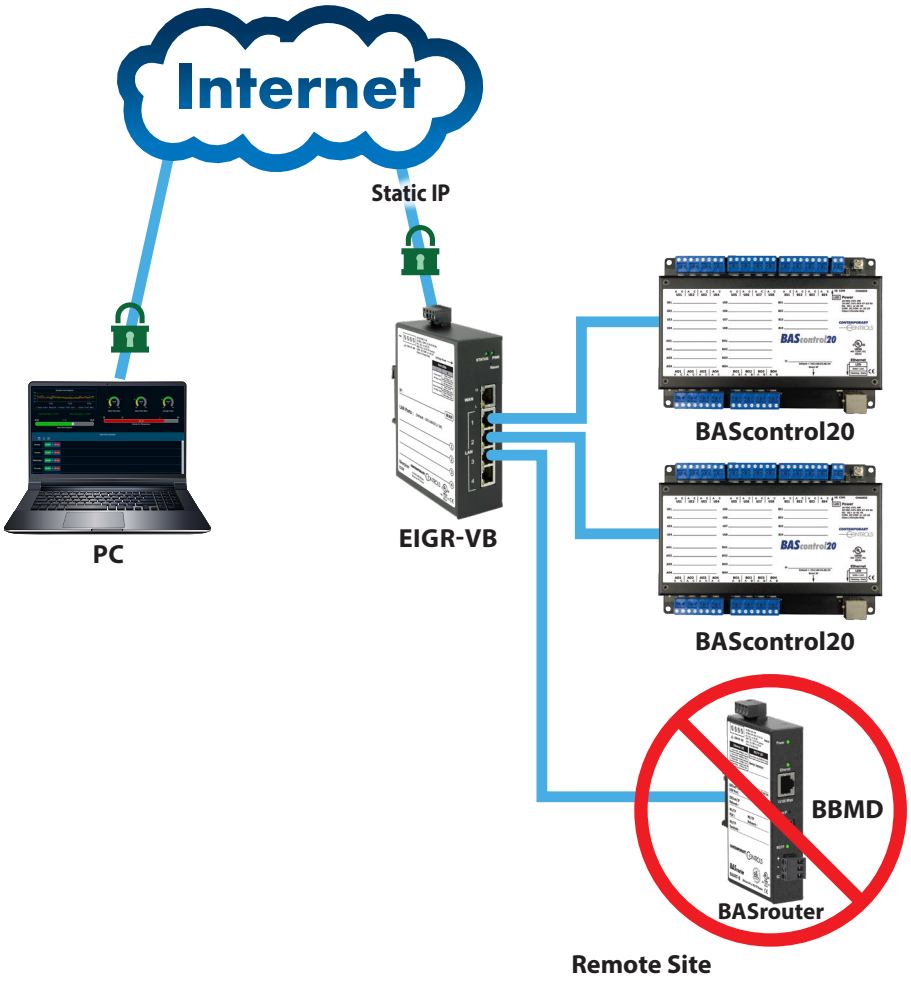
Features and Benefits

- Wired or wireless operation over the Internet
- Secure encrypted communication tunnel
- Free download of OpenVPN client software
- Stateful Firewall and Allowlist
- Support for Linux and Windows OpenVPN clients
- Passage of multicast and broadcast messages eliminates requirement for BBMD
- Internet communication to a client at a remote site or any convenient site with Internet connectivity
- Support for up to 10 PC clients (Windows/Linux)
- Independent client communication with one or more router
- Flexible man-machine and machine-machine applications
- Quick realization of a remote access project
- Individual access to multiple, remote sites

BridgeVPN is a single-site VPN solution that uses Contemporary Controls' EIGR-VB and EIGR-C IP routers operating as an OpenVPN server. The router, set to OpenVPN server mode and assigned a Static Public IP address, resides at the remote site and uses the Internet for communicating to OpenVPN clients. As a VPN server, the routers can support up to 10 VPN clients (Windows/Linux). The VPN clients are bridged to the LAN side and are assigned an IP address from the LAN subnet which provides the same application experience as if the client device were part of the router's LAN. Any Windows or Linux PC can run the open-source OpenVPN client software. Though OpenVPN client software is available from the Google Store for Android devices and App Store for iOS devices, it doesn't support TAP adapter required for bridge mode. For PCs, OpenVPN Version 2.x is required which corresponds to OpenVPN GUI on Windows. OpenVPN Connect (version 3.x) is not supported with BridgeVPN as it doesn't support the TAP adapter.

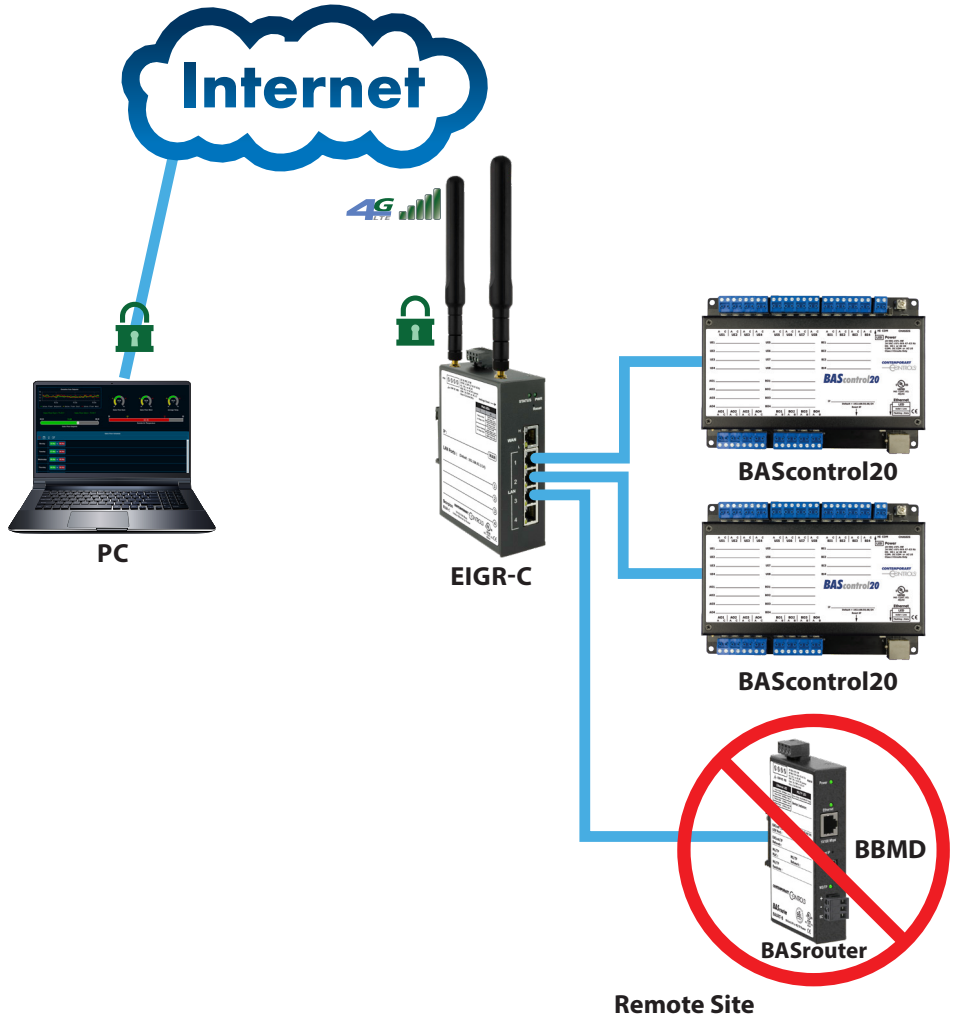
Application 1 – Building Automation System using Wired Remote Access

Here we have a Windows or Linux PC sitting in your office running OpenVPN client software behind a firewall. It connects to your BridgeVPN EIGR-VB OpenVPN server over the Internet. At the remote site is an EIGR-VB OpenVPN server with its WAN port connected to the Internet directly or via an existing Internet router. The PC can communicate over BridgeVPN to any IP device used in building automation systems, such as BACnet controllers or routers connected to the IP router's LAN ports. Ethernet switches can be used to add more devices. The VPN client is bridged to the LAN side and is assigned an IP address from the LAN subnet which provides the same application experience as if the client device were part of the EIGR-VB's LAN. This allows passage of multicast and broadcast messages through the VPN tunnel. The PC can easily run BACnet client applications to discover and communicate with BACnet devices at the remote site. Since the PC VPN interface is on the same subnet as the EIGR-VB LAN, there is no need for a BBMD.



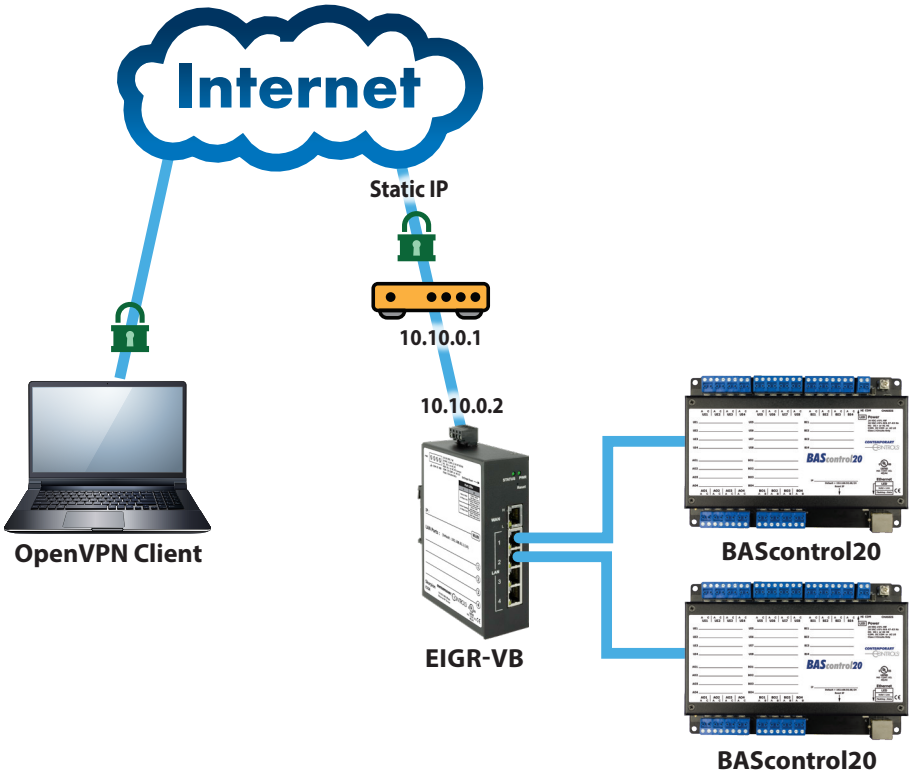
Application 2 – Building Automation System using Wireless Remote Access

Here we have a Windows or Linux PC sitting in your office running OpenVPN client software behind a firewall. It connects to your BridgeVPN EIGR-C OpenVPN server over the Internet. At the remote site is an EIGR-C OpenVPN server with its WAN port connected to the Internet directly or via an existing Internet router. The PC can communicate over BridgeVPN to any IP device used in building automation systems, such as BACnet controllers or routers connected to the IP router's LAN ports. Ethernet switches can be used to add more devices. The VPN client is bridged to the LAN side and is assigned an IP address from the LAN subnet which provides the same application experience as if the client device were part of the EIGR-C's LAN. This allows passage of multicast and broadcast messages through the VPN tunnel. The PC can easily run BACnet client applications to discover and communicate with BACnet devices at the remote site. Since the PC VPN interface is on the same subnet as the EIGR-C LAN, there is no need for a BBMD.



Application 3 – Connecting the OpenVPN Server Router Behind an Enterprise Router/Firewall

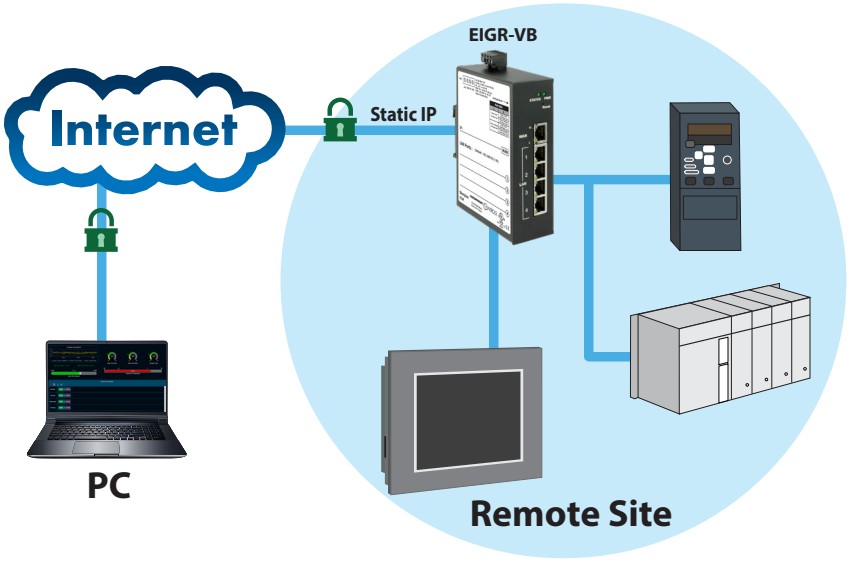
This application shows the ability to connect the EIGR-VB OpenVPN server behind an existing enterprise router/firewall that has a static IP address. The router doesn't have to be connected directly to the Internet with a static IP for the BridgeVPN solution. The enterprise router needs to have a Port Forwarding entry for the OpenVPN port to the VPN router's IP address.



In the example above, if UDP port 5845 is being used as the OpenVPN port, the enterprise router/firewall at 10.10.0.1 will have a Port Forward entry for UDP port 5845 going to the VPN router at 10.10.0.2 at UDP port 5845. The EIGR-VB will use the Static IP of the enterprise router for OpenVPN configuration setup webpage.

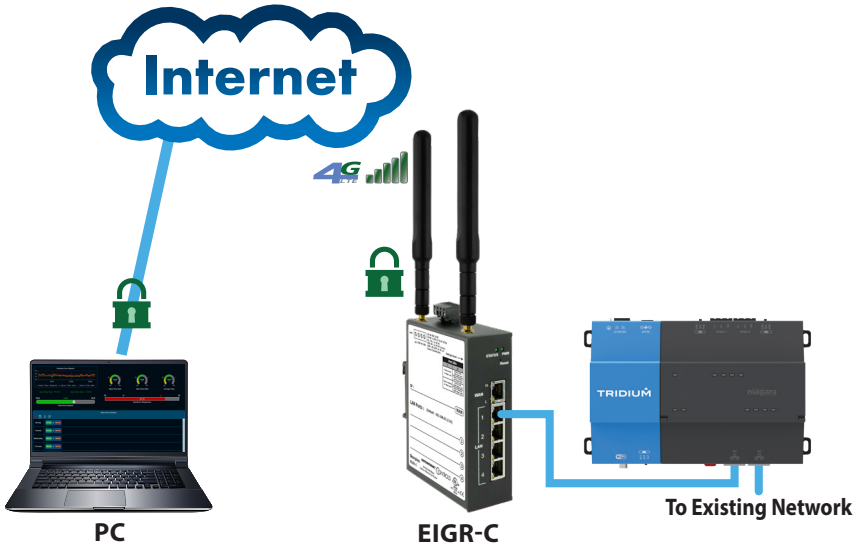
Application 4 – Industrial Automation System using Wired or Wireless Remote Access

Here we have a Windows or Linux PC sitting in your office running OpenVPN client software behind a firewall. It connects to your BridgeVPN EIGR-VB or EIGR-C OpenVPN server over the Internet. At the remote site is an EIGR-VB or EIGR-C OpenVPN server with its WAN port connected to the Internet. The PC can communicate over BridgeVPN to any IP device used in industrial automation systems, such as HMI, PLC, and drives connected to the IP router's LAN ports. Ethernet switches can be used to add more devices. The VPN client is bridged to the LAN side and is assigned an IP address from the LAN subnet which provides the same application experience as if the client device were part of the router's LAN. This allows passage of multicast and broadcast messages through the VPN tunnel. This allows programming and gathering of PLC data remotely.



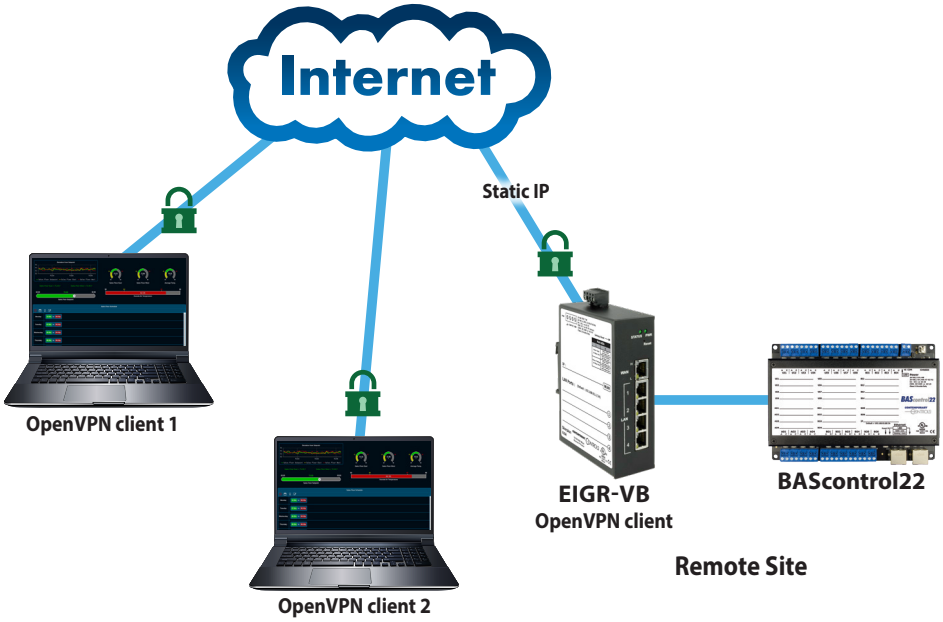
Application 5 – Remote Access to an Existing Automation System such as a JACE

Here we can isolate our remote communications to one device, such as a JACE®, which is frequently used in building automation systems. In this example you can have all the automation devices connected to the primary port of the JACE while the secondary port of the JACE is connected to the LAN port of the VPN router (EIGR-VB or EIGR-C). Remote access, even though it is encrypted and secure, can thus be isolated to one device for an added layer of security. BridgeVPN supports the ability to communicate to the JACE using its secondary port if the JACE primary port is communicating to an existing network on a different subnet leaving the gateway address setting configured for the primary port subnet.



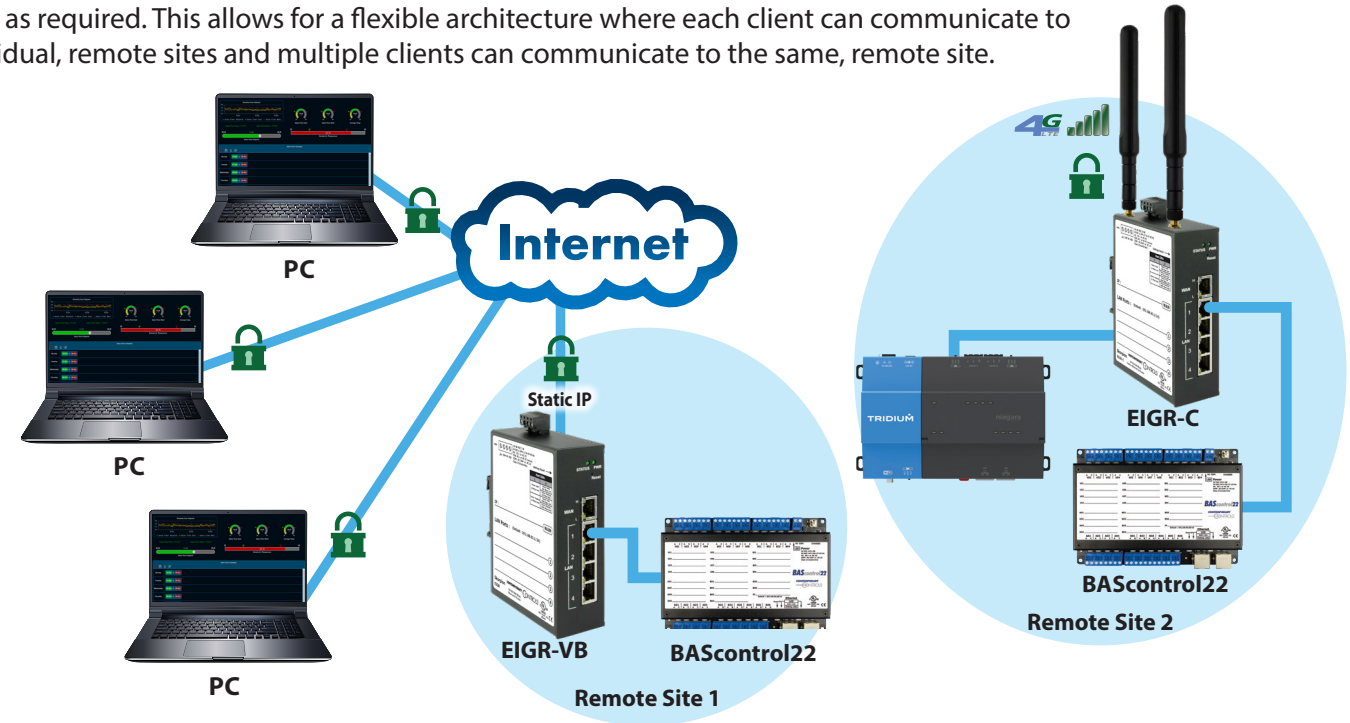
Application 6 – Access from Multiple Clients to a Remote Site

In this application, in addition to having a workstation with an OpenVPN client at your office, you also have an OpenVPN application on a second Windows or Linux PC for simultaneous access to the remote site. Both PCs communicate directly to the VPN router via the Internet and secure VPN communication occurs. One EIGR-VB or EIGR-C can support up to 10 clients on Windows and Linux PCs. These clients can be located anywhere that has Internet connectivity. This allows collaboration between multiple people to resolve any issues at the remote site.



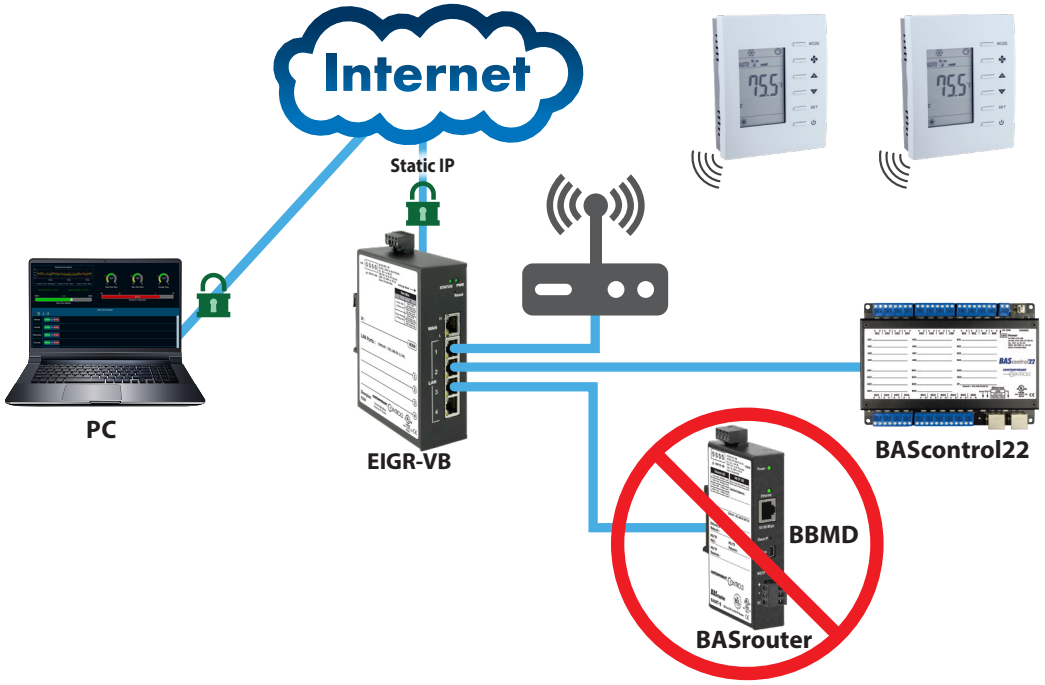
Application 7 – Varied Clients and Accessing Multiple Remote Sites

In the previous examples we only showed one VPN router being used at a time to communicate remotely with a workstation. With BridgeVPN, you can interconnect up to 10 clients on Windows and Linux PCs. The OpenVPN client (Windows/Linux PC) can have VPN configuration files for multiple remote sites allowing it to connect to a site (one at a time) as required. This allows for a flexible architecture where each client can communicate to individual, remote sites and multiple clients can communicate to the same, remote site.



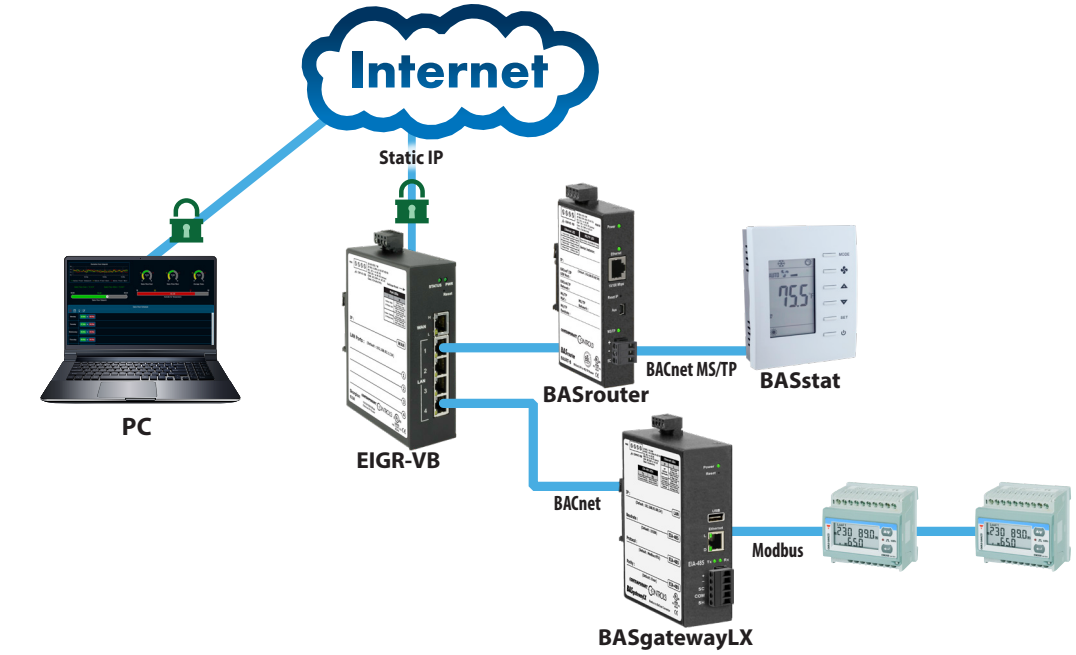
Application 8 – Accessing Wi-Fi devices at Remote Site

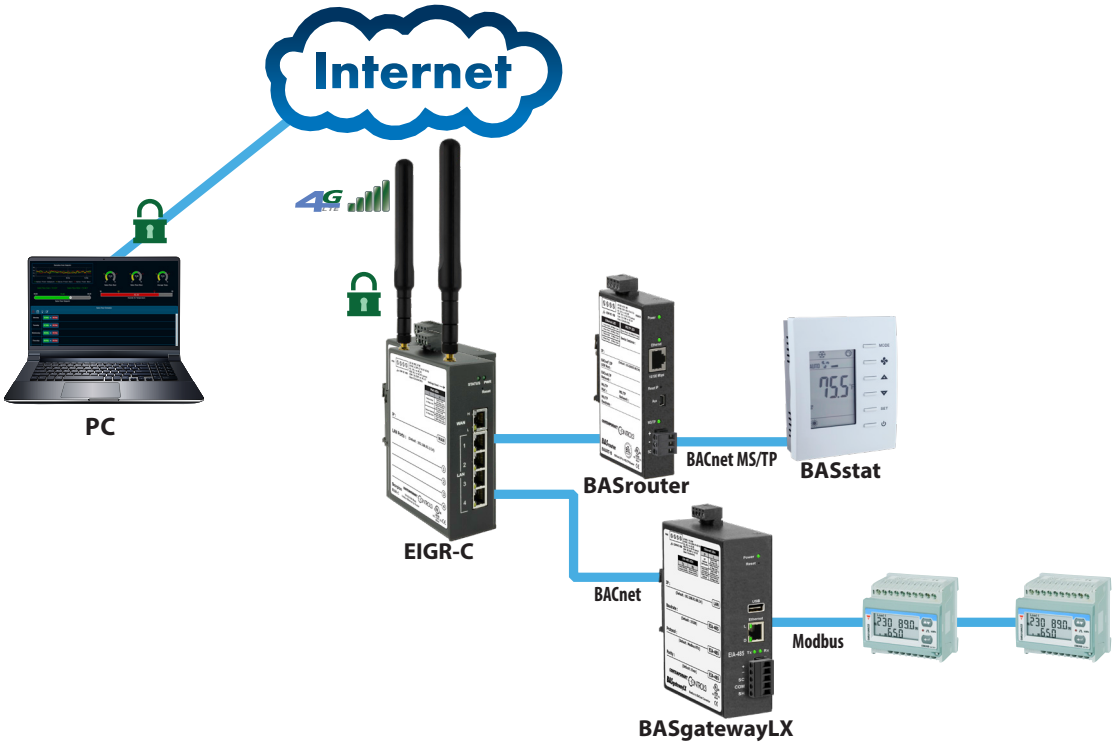
Wi-Fi enabled devices, such as our BASstat thermostats, can communicate within a Wi-Fi infrastructure. The VPN client, such as the Windows or Linux PC in this example, is bridged to the LAN side and is assigned an IP address from the LAN subnet which provides the same application experience as if the PC were part of the VPN router's LAN. Thus, in this example, the PC and the Wi-Fi thermostats are on the same subnet. This allows passage of multicast and broadcast messages through the VPN tunnel without the need for a BBMD, such as a BASrouter.



Application 9 – Interconnect to Other Topologies

There are numerous data communication protocols that utilize Ethernet, but we focus our efforts on BACnet. In this application we utilize a BASrouter to interconnect BACnet Ethernet to a BACnet MS/TP network and a BASgatewayLX to interconnect BACnet to a Modbus serial network. The EIGR-VB or EIGR-C located on the Ethernet side of these networks allows secure Internet access to these devices using BridgeVPN.





What is the Difference Between BridgeVPN and What I have Today?

If you have Internet access through a firewall and you want to achieve remote access to a facility without using BridgeVPN, you will need to enable port forwarding in your firewall for the ports used in your communications.

Opening Ports

Typically, port 80 is used for web browsers, and port 47808 is used for BACnet communications. In this case, you would need to set up your firewall to do port forwarding for these ports. When you open a port, you must indicate which device is to receive this communication. Each port typically only allows you to remotely access one device so multiple ports will be required. Plus, you have now exposed these devices to malicious Internet activities. With BridgeVPN there is no need to change firewall configurations, and you do not need to expose your devices to the Internet. Your devices remain safe and can easily communicate with the Internet using our secure BridgeVPN solution.

Security Exposure

Many wireless providers are offering wireless routers to their customers. These devices may offer Wi-Fi or wired connections. However, in most cases when using these devices your own devices will still be behind a firewall, and you won't be able to reach them remotely over the Internet. In rare cases, the wireless provider will offer a fixed public IP address (usually for an extra fee). In this case your devices are now directly exposed to the Internet. With one network as the LAN and the other as the WAN, BridgeVPN passes appropriate traffic while blocking all other traffic. The built-in stateful firewall passes communication initiated on the LAN-side while blocking WAN-side initiated communication except the one occurring over the secure VPN connection. The EIGR-C router adds support for cellular networks on the WAN side, allowing use at sites without Internet access.

Computer Emulation

Some people tell us they have a PC on-site at the remote location and they just use an application like TeamViewer or GoToMyPC to access the site. There are a couple of issues with this arrangement. One is that you are relying on this device to be running when you need it to perform your remote access. You need to keep it up to date with security patches, anti-virus programs, etc. This PC must also contain all the tools you use when troubleshooting your network. This could be very expensive with licensing requirements for these programs. With BridgeVPN you only have an EIGR-VB or EIGR-C onsite (mounted securely in a control panel) and you can have all your tools installed on your access devices back at the office.

To learn how to configure the EIGR-VB or EIGR-C as a VPN server, see the Application Note, Configuring an EIGR-VB and EIGR-C Gigabit IP Router as an OpenVPN Server.

United States
Contemporary Control Systems, Inc.
Tel: +1 630 963 7070
Fax:+1 630 963 0109
info@ccontrols.com

China
Contemporary Controls (Suzhou) Co. Ltd
Tel: +86 512 68095866
Fax: +86 512 68093760
info@ccontrols.com.cn

United Kingdom
Contemporary Controls Ltd
Tel: +44 (0)24 7641 3786
Fax:+44 (0)24 7641 3923
ccl.info@ccontrols.com

Germany
Contemporary Controls GmbH
Tel: +49 341 520359 0
Fax: +49 341 520359 16
ccg.info@ccontrols.com

www.ccontrols.com