GUIDE TO NETWORKING SNAP PAC PRODUCTS

Form 1796-220421—April 2022

OPTO 22
Your Edge in Automation.™

43044 Business Park Drive • Temecula • CA 92590-3614
Phone: 800-321-OPTO (6786) or 951-695-3000
Fax: 800-832-OPTO (6786) or 951-695-2712
www.opto22.com

Product Support Services
800-TEK-OPTO (835-6786) or 951-695-3080
Fax: 951-695-3017
Email: support@opto22.com
Web: support.opto22.com

Guide to Networking SNAP PAC Products
Form 1796-220421—April 2022

The information in this manual has been checked carefully and is believed to be accurate; however, Opto 22 assumes no responsibility for possible inaccuracies or omissions. Specifications are subject to change without notice.

Opto 22 warrants all of its products to be free from defects in material or workmanship for 30 months from the manufacturing date code. This warranty is limited to the original cost of the unit only and does not cover installation, labor, or any other contingent costs. Opto 22 I/O modules and solid-state relays with date codes of 1/96 or newer are guaranteed for life. This lifetime warranty excludes reed relay modules, *groov* and SNAP serial communication modules, SNAP PID modules, and modules that contain mechanical contacts or switches. Opto 22 does not warrant any product, components, or parts not manufactured by Opto 22; for these items, the warranty from the original manufacturer applies. Refer to Opto 22 form 1042 for complete warranty information.

Opto 22
Your Edge in Automation.

Table of Contents

1: Networking Basics

INTRODUCTION

We live in an increasingly connected world. Computers and mobile devices are everywhere, with new features and capabilities appearing in a wide variety of devices. To no one's surprise, automation engineers and technicians want to take advantage of these same abilities to monitor and control their systems, both within their company facility and remotely.

And now that many control systems are moving away from proprietary buses and into standard networks and protocols—like standard IEEE 802.3 wired Ethernet networks and IEEE 802.11 wireless networks—this kind of communication with computers and mobile devices is much easier.

What's in this Guide

Networking can be a complex subject. This guide tries to reduce the complexity by providing guidelines for how you might set up communications between your computer or mobile device and your SNAP PAC control system. (For a *groov* EPIC System, *groov* RIO, or *groov* Server for Windows, see form 2161 instead of this guide.)

The goal is for you to be able to monitor and control your system from anywhere you need to, either inside your facility or outside it. This guide addresses all of the following scenarios:

- Your PAC Display HMI on a PC in one part of the factory needs to access data from a SNAP PAC controller in another part.
- You're using the mobile apps Opto iPAC or Opto aPAC to commission your system.
- You need to share data between your SNAP PAC System and other systems using OptoOPCServer.
- You're using OptoDataLink to send data to a company database.
- Your SNAP PAC controller must communicate with I/O at a remote site.

It is possible to communicate in all these ways because Opto 22 control systems are built on standard protocols such as TCP and UDP over IP, which are the same protocols used by off-the-shelf computers, routers, and the internet. These standard protocols make it possible to build and connect networks. The distance between devices and the networks they're on is unimportant; they could be in the same building or thousands of miles apart.

Specifically, this guide shows you how to communicate with Opto 22's **SNAP PAC** controllers using wired Ethernet networks and wireless LANs. Field proven in a wide variety of applications worldwide, these PACs typically control reliable, guaranteed-for-life SNAP I/O. They may also control *groov* I/O, G4 I/O, and older legacy I/O systems.

SNAP PAC programmable automation controllers include:

- Standalone S-series PACs
- Rack-mounted R-series PACs

- SoftPAC software-based controller for PC-based control

For networking flexibility, hardware S-series and R-series SNAP PACs include two independent Ethernet interfaces.

This guide includes:

Chapter 1: Networking Basics—This chapter, which introduces basic networking concepts you need to understand.

Chapter 2: Communication within your Facility—Setting up communication internally, without using the internet.

Chapter 3: Communication over the Internet—Setting up remote communications using the internet.

Chapter 4: Glossary and Resources—Definitions of common networking terms as they apply to this guide, plus some resources online that may help you.

NOTE: *Although some information on using groov View with SNAP PACs is included in this guide, for complete information on networking groov EPIC systems or the groov Server, see form 2161, Guide to Networking groov Products.*

For Help

For help on Ethernet networking, setting up VPNs, and port forwarding, many good resources are available online. One we recommend is: Whatismyip.com, which includes FAQs on a number of subjects plus a forum for asking questions. Opto 22 customers also share help and answer questions on the OptoForums.

Related Documents

Be sure to check user's guides for help with your Opto 22 product. All guides are available on our website at any time. Follow the links below or go to www.opto22.com and search on the form number.

Guide name	Form #
SNAP PAC S-Series Controllers User's Guide	1592
SNAP PAC R-Series Controllers User's Guide	1595
SoftPAC Quick Start Guide	2045
Guide to Networking *groov*	2161

If your questions are specifically about setting up remote communications with SNAP PAC products, and you can't find the help you need in this guide or in the product user's guides, contact Opto 22 Product Support. Product Support is free.

Phone: 800-TEK-OPTO (800-835-6786 toll-free in the U.S. and Canada)
951-695-3080
Monday through Friday,
7 a.m. to 5 p.m. Pacific Time

NOTE: Email messages and phone calls to Opto 22 Product Support are grouped together and answered in the order received.

Email: support@opto22.com

Opto 22 website: www.opto22.com

CONNECTING TO COMPUTERS

How Does the Data Get There?

NOTE: See Chapter 4: Glossary and Resources for more information about the terms used in this guide.

We all know that computers and other electronic devices—printers, routers, laptops, smartphones, and more—are networked so they can exchange information. But how does that information get where it's supposed to go? How does a spreadsheet get to the printer, for example, or a YouTube video get to your smartphone?

It's similar to the way you call someone on your cell phone. You tap their name, the phone dials their phone number, and the phone system understands how to connect to the phone at that number. The format of the phone number tells the system how to connect.

In computer networking, the equivalent of a phone number is an IP address. Most of us don't have to pay attention to IP addresses, just like we don't memorize our friends' phone numbers. It's harder to remember a long number than a name (and computer IP addresses can change). So instead of typing the IP address, we click a printer name. And instead of entering an IP address, we just enter a domain name like opto22.com.

But in the background, computer networks, just like the phone system, know how to make the connection. A domain name server (DNS) translates the device name or domain name into an IP address. Routing tables and software rules tell routers how to send your packets of data to the right destination.

Networking within Your Facility

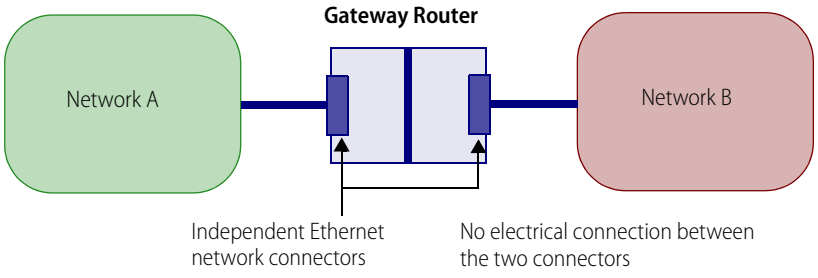
Within your facility you may have one or more subnetworks or local area networks (LANs).

Maybe you have all your devices on a single, flat network: your computers, printers, wireless access points, and SNAP PAC System are all on one LAN, so all these devices can freely communicate. This network architecture makes communication simple (see "Single, Flat Network" on page 7).

Many companies have more than one LAN, though. You may have your SNAP PAC System on a separate network from your computers and printers, for example, to keep the control system segmented for less traffic or increased security. If you want a person or device on one LAN to communicate with a person or device on another, you need a *gateway router*.

How a Gateway Router Works

A gateway router is wired to both subnetworks through independent Ethernet network interfaces, but inside the router there is no direct connection between the two. Because there is no direct connection, communication between the two networks can occur only if software rules inside the router allow it. These software rules typically include routing tables and network address translation (NAT).



Software rules (routing tables, network address translation) determine whether and how communication moves between Network A and Network B.

In addition to managing communication between LANs within your facility, a gateway router is also used to manage communication between a LAN and a WAN (wide area network). A WAN may be private or public; the internet is a public WAN.

The gateway router acts in exactly the same way whether it's managing communication between two LANs or between a LAN and a WAN. The LAN is plugged into one Ethernet network interface on the router and the WAN is plugged into another. With no direct connection between the two interfaces, communication occurs only as allowed by software inside the router.

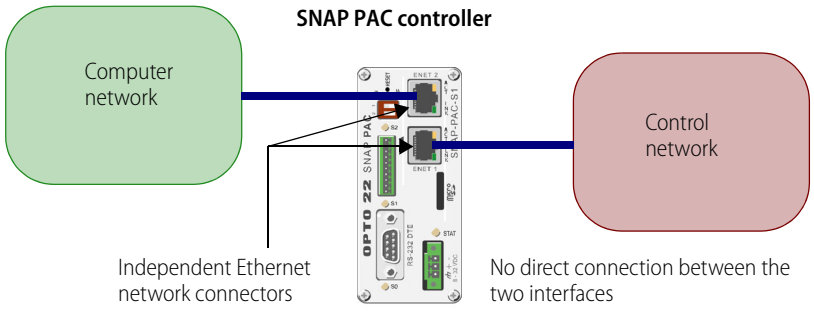
We'll talk more about networking over the internet in Chapter 3: Communication over the Internet.

SNAP PAC Controllers

Like a gateway router, SNAP PAC controllers have two independent Ethernet network interfaces. Each of these independent interfaces must be wired to a separate network. That means their network addresses (a combination of IP addresses and subnet masks) must be different. (For detailed information on IP addresses and subnet masks, see the Simplified IP Addressing Technical Note, form 1362.)

SNAP PAC controllers are not routers, because they do not provide routing or address translation, but their separate interfaces work like a router's interfaces. If you have redundant networks, with one network wired to ENET 1 on the controller and the other wired to ENET 2, data packets cannot travel between them, because there is no direct connection inside the controller between the two networks.

NOTE: The two wired interfaces on SNAP-PAC-EB1 and -EB2 brains are different from those on SNAP PAC controllers. On the brains the two interfaces are connected, so these brains act as a three-port switch, with one port going to the brain and the other ports allowing connections to two other devices. These brains can therefore can be daisy-chained. In contrast, on a SNAP PAC controller, data packets cannot travel directly between interfaces. That's why the controller provides security.



SNAP PAC controllers have no direct connection between their two independent Ethernet network interfaces.

Remember: *You must ALWAYS assign the two network interfaces on a SNAP PAC controller* ***different IP addresses and different subnets****. For more information, see the product user's guide. Note that it doesn't matter which interface you use for each network, except initially when you must use the lower-numbered interface (ENET 1).*

WHAT'S YOUR NETWORK SETUP?

Now let's take a look at your network setup and how to handle communication on it.

- All devices are on a **single, flat network.** This one's easy; see Chapter 2: Communication within your Facility.
- Devices are on **separate network subnets** or LANs within the same location. For example, you are using the ENET1 and ENET2 interfaces on a SNAP PAC controller, or multiple NICs (network interface cards) on a PC, to separate your control network from your company computer network. To communicate between two networks like this, see Chapter 2: Communication within your Facility.
- Networks are geographically separated from each other, so **communication must go over the internet.** For example, you have a SNAP PAC controller at one location and remote I/O at another, or a PC running PAC Display needs data from a PAC at another location, or you are using an Opto iPAC or Opto aPAC app on a smartphone outside your facility. For these kinds of remote communication, see Chapter 3: Communication over the Internet.

2: Communication within your Facility

INTRODUCTION

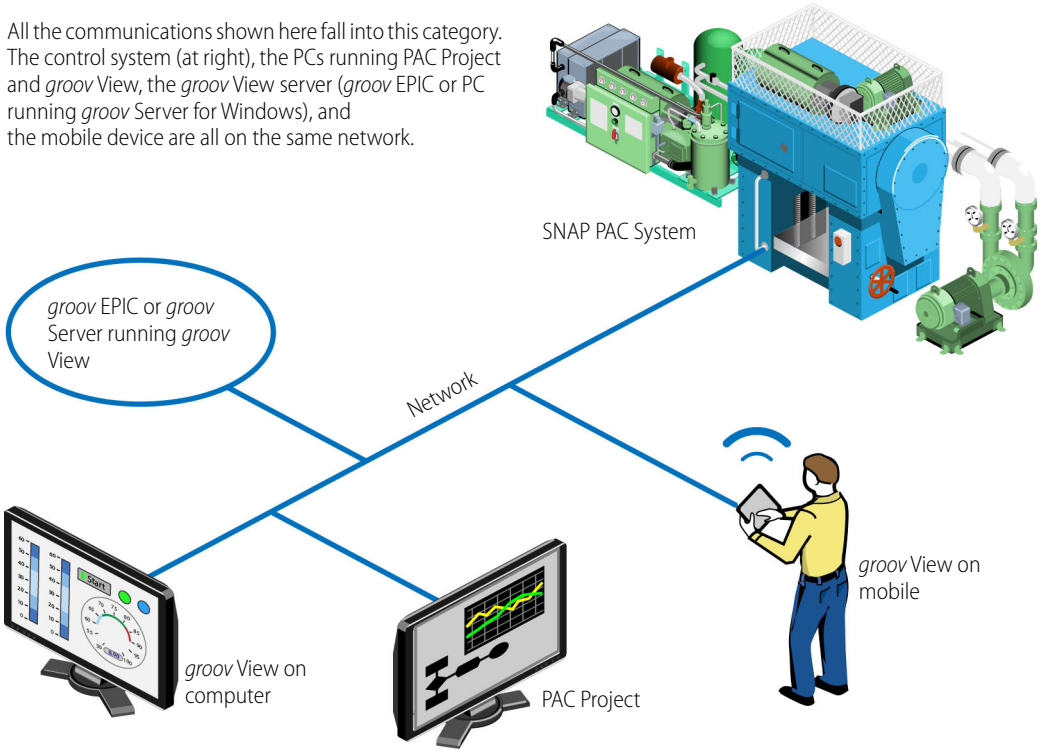
Inside your facility, you may want to have computers and/or mobile devices communicate with your control system. Maybe you want to monitor production numbers, check equipment, operate machinery, or control processes. How you do so depends on your network setup:

- Everything is on a single, flat network. See "Single, Flat Network," below.
- Two or more separate networks exist—for example, a company computer network and a control system network. See "Separate Network Subnets" on page 8.

SINGLE, FLAT NETWORK

If the devices you're communicating between are on the same network (wired Ethernet or wireless LAN), then communication requires no special setup.

All the communications shown here fall into this category. The control system (at right), the PCs running PAC Project and *groov* View, the *groov* View server (*groov* EPIC or PC running *groov* Server for Windows), and the mobile device are all on the same network.



Here's a summary of communications that require no special setup:

Communications between			Network notes
groov View in *groov* EPIC or *groov* Server	<-->	SNAP PAC	Only one Ethernet interface on each is used
PC	<-->	SNAP PAC	Only one Ethernet interface on each is used

SEPARATE NETWORK SUBNETS

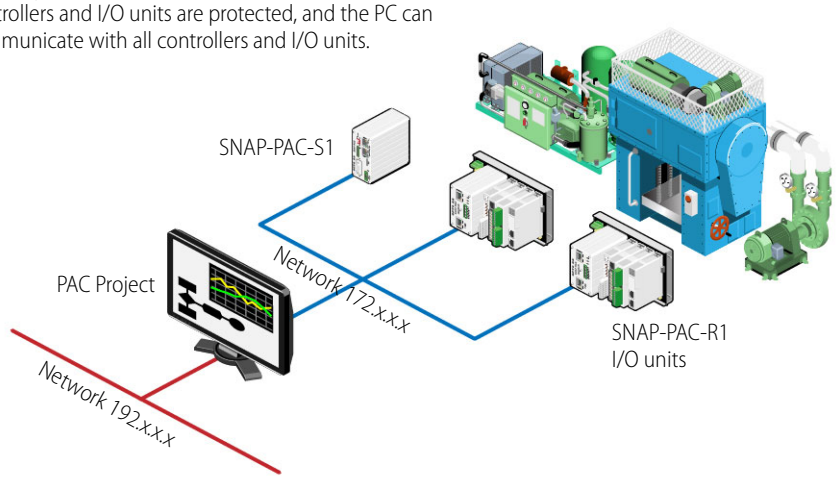
You may choose to use multiple network interface cards (NICs) on your PC to separate your control network from your computer network for security reasons, creating separate network subnets. As explained on page 3, the two wired Ethernet interfaces on a SNAP PAC controller are independent from each other. The same thing applies to two NICs on a PC. Data packets cannot travel directly between the interfaces.

Recommended Architecture

For security, we recommend that you have separate Ethernet adapters in the computers you use for PAC Project, HMI, SCADA, and so on, using one NIC for the company network and the other for the control network. Then connect the PAC to the control network using only one of its Ethernet interfaces.

This architecture provides beneficial separation between company and control networks in the easiest way possible. It also allows efficient communication between the PC and I/O units for updating firmware, diagnosing the system, and HMI purposes.

Recommended. The PC, with two NICs, segments the company network from the control network. All SNAP PAC controllers and I/O units are protected, and the PC can communicate with all controllers and I/O units.

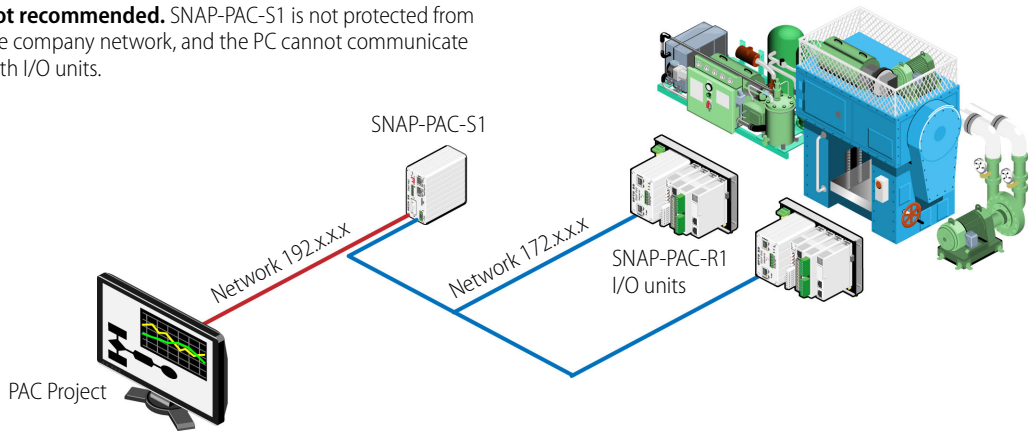


Not Recommended

In contrast, if you create separate network subnets using the two PAC controller ports (one controller port for the company network and the other for I/O), the I/O is separated from the company network but the PAC is not.

In the example below, one of the PAC's network interfaces connects to the control network and the other to the computer network. The PC can communicate with the PAC S1, but it cannot communicate with the PAC R1s or other I/O units that are wired only to the control network. The PC can get data about the I/O units only if it's available in the SNAP-PAC-S1. It cannot download a PAC Control strategy to an R1, upgrade firmware on the I/O units, or get PAC Display HMI data directly from them.

Not recommended. SNAP-PAC-S1 is not protected from the company network, and the PC cannot communicate with I/O units.



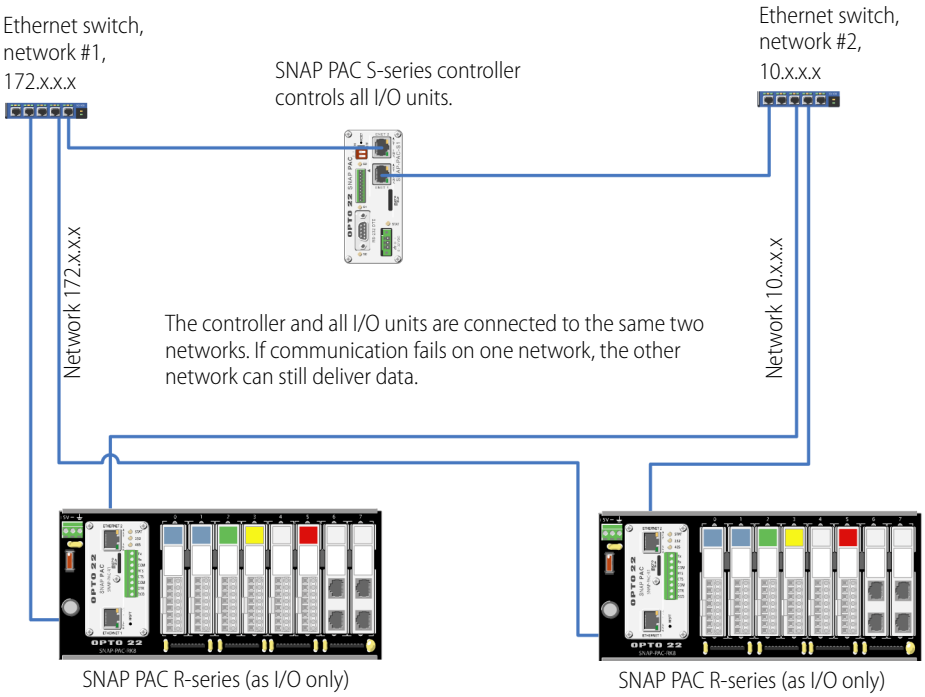
REDUNDANT NETWORKS

If you are concerned about the stability of your network links, you may want to consider redundant networking using the two independent network interfaces on SNAP PAC controllers. If communication fails on one network, the other network can still deliver data.

You'll need an S-series PAC as your main controller, R-series controllers for your distributed I/O units, and PAC Project Professional for software support. Create redundant Ethernet links using both interfaces on each device.

The diagram on the following page shows an example. The SNAP PAC S-series controller is the main controller of the system, with SNAP PAC R-series controllers acting as distributed I/O processors. Each SNAP PAC controller is connected to two separate Ethernet network links.

Example of a redundant network, using the two independent network interfaces on SNAP PAC controllers



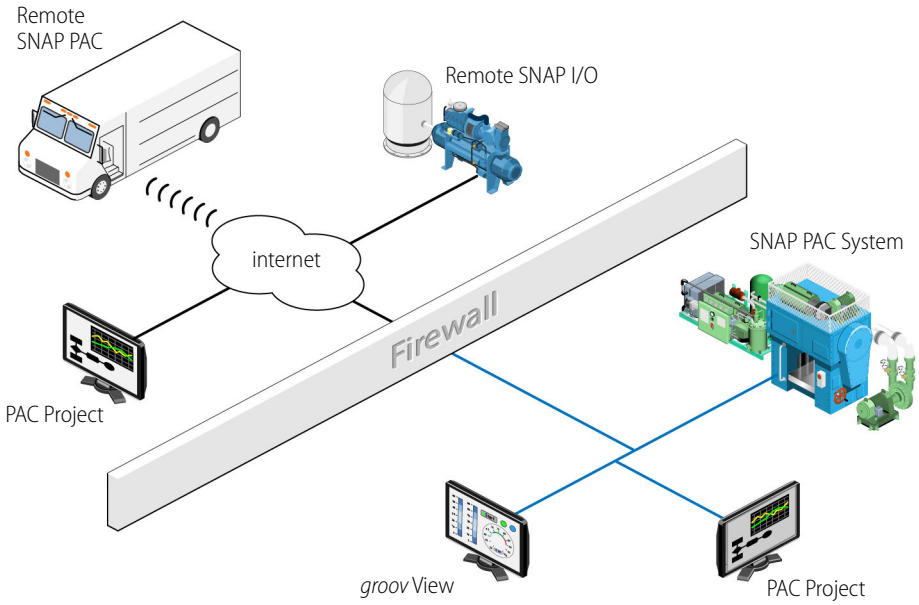
3: Communication over the Internet

WHY COMMUNICATE OVER THE INTERNET?

When your control system and your company computers or mobile devices are connected by a local network, communication between them is easy. But you may have good reasons to communicate with your control system from a different network, miles away. Here are just a few:

- A production manager wants to know the number of widgets produced in the last hour, even while he's traveling.
- An engineer needs to adjust a setpoint at another site.
- A technician has been notified of a malfunction in another building and needs to quickly switch from pump #1 to pump #2.

If two networks are each connected to the internet, devices on them can communicate using the internet. Any two networks can be used as long as both are connected to the internet; as shown below, for example, a PC in one location can get data from a SNAP PAC at another location.



For cases like these, you can establish communication over the internet by following a few extra steps. The rest of this chapter shows you how.

CAUTIONS: SECURITY, SPEED, AND RELIABILITY

Especially in the case of sensitive data or equipment control, security is a key consideration when you're using the internet for communications. This chapter emphasizes ways to communicate in order to maximize security.

Communication speed can vary a great deal depending on your internet connection speed, the quality of the internet service provider (ISP), and even the time of day. You'll need to take this possible delay into account if you are controlling equipment or transferring data between devices.

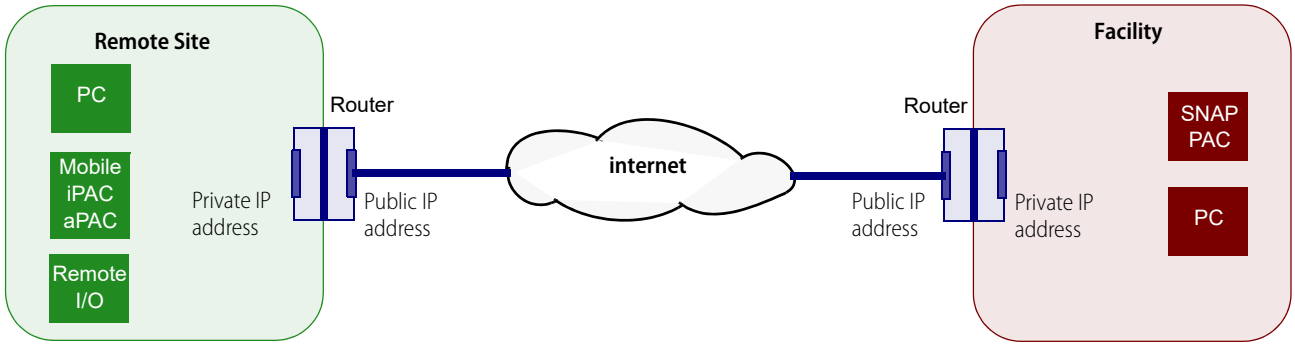
Also, because many companies and steps along the way are outside your control, you should consider the connection tenuous and plan other ways to accomplish what you need to do, in case the link goes down for a short while or for a long time.

INTERNET GATEWAY ROUTERS

Remember our gateway routers from Chapter 1 ("How a Gateway Router Works" on page 3)? Gateway routers are essential parts of remote networking over the internet for the same reason they're essential for connecting networks within your facility: they provide security.

That's because the gateway router has two separate interfaces, one connected to the public internet (an *untrusted* network) and one connected to your facility's private network (a *trusted* network, where you know everyone who can access it). There's no direct connection between the two interfaces, so the only data that can cross to the other side is what's allowed by software rules within the router. The router's private IP address—and the IP addresses of all devices on the private network—are hidden from its public IP address.

You can see how this works in the diagram below.



When you're looking at IP addresses, the following IP addresses are always on private networks:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

Other IP addresses may be on public networks.

This distinction between the public and private IP addresses on the router becomes important as you set up communication.

Gateway Router Identification

At some point in configuring communication over the internet, you may need to know a gateway router's public IP address (also called its WAN IP address). Your internet Service Provider (ISP) provides this address, and the address may be fixed (static) or dynamically assigned.

1. Go to a computer that has internet access on the network whose public IP you need to know. Open a web browser and go to one of these:

   ```
   http://whatismyip.com/
   http://www.ipchicken.com/
   http://icanhazip.com
   ```

2. Find the IP address assigned to your company by your ISP, near the top of the page. Copy the address down exactly.

   Note that this address does not start with 10, 192, or 172. It's a public address.

Fixed (Static) vs. Dynamic IP Addresses

As we said, the public IP address you discover may be fixed (static) and never change, or it may be dynamic and change from time to time. If you don't know, ask your ISP. (Generally you will know if it is static, because you have to pay more for a static address.)

- If the router has a static public IP address, you can use that address when setting up a VPN server.
- If the router has a dynamic public IP address, use a DDNS (dynamic domain name service) to assign the router a public domain name. (Remember that a DNS resolves static IP addresses into domain names; a DDNS updates DNS if your dynamic IP addresses change.)

  If your router includes a DDNS feature, set it up there. If not, set up a DDNS service on the web, for example at dyn.com/dns or noip.com. First you'll create an account on the service, and then you'll pick your domain name. Some of these services are free. Free services usually check for a change in IP address every 10 minutes. That means you might have to wait up to 10 minutes to gain remote access. You can also pay for the service and reduce the length of time between checks.

CONSIDER YOUR OPTIONS

Gateway routers prevent direct communication from the internet to a private network. If you want to directly communicate with a device (like a SNAP PAC) or a service (like *groov* Server) that's on a private network, you need a way around this block.

Typically there are two possible methods for communication from the internet: a virtual private network (VPN) or port forwarding (PF). **For any communication involving a SNAP PAC controller, use a VPN only!** Port forwarding is not secure with a SNAP PAC because there is no user authentication built into the controller. This caution applies to communication between a *groov* product and SNAP PAC, between computers and SNAP PACs, and between SNAP PACs and remote I/O.

About VPNs

A virtual private network employs dedicated connections, authentication, and encryption to connect you to your private network from the internet while maintaining all the same functionality and security you would have inside the network. Authentication is built into the VPN server. When you use a VPN, it's like having your own private tunnel through the internet. It feels just like being on site.

In contrast, port forwarding is not secure. PF allows remote computers or mobile devices to connect to a specific computer or service within a private local area network through a specific port. Essentially it pokes a "pinhole" in your company firewall to allow packets of information to pass through.

NOTE: If you're using cellular data radio (for example, a mobile hotspot) at a remote location, check your plan for details. Some plans don't allow incoming connections to your gateway router and won't work for either VPN or PF.

If you have an IT Department, work with them to set up communication over a VPN (see "Working with Your IT Department," below).

If you don't have an IT group, you'll have to set it up yourself. See "Setting Up a Virtual Private Network (VPN)" on page 14.

WORKING WITH YOUR IT DEPARTMENT

If you have an IT Department, work with them to set up communications over a VPN, create VPN accounts for you and any other authorized users, and make sure those accounts have access to the network your SNAP PAC is on.

The information in this guide should give you enough basic knowledge to be able to talk with your IT Department about what you need. If you (or they) need more help, contact Product Support (see "For Help" on page 2).

Tell your IT Department which devices you need to have communicate with each other (see "Common Communications and Methods," below) and give them a copy of this section. Then follow their instructions to set up communication on your computers and mobile devices. (For help, see "Setting Up VPN Clients" on page 15. Note that two special cases require a VPN set up in a particular way; see "VPN Special Case: SNAP PAC to Remote I/O" on page 16.)

Common Communications and Methods

Communication between			Communication methods	
			VPN	PF
PC	<-->	SNAP PAC	Yes	No
Mobile*	<-->	SNAP PAC	Yes	No
SNAP PAC	<-->	Remote I/O	Yes**	No

*Mobile with Opto iPAC or Opto aPAC app
** See "VPN Special Case: SNAP PAC to Remote I/O" on page 16.

Remember, do not use port forwarding for communication with SNAP PAC over a public network, because SNAP PAC does not provide user authentication.

SETTING UP A VIRTUAL PRIVATE NETWORK (VPN)

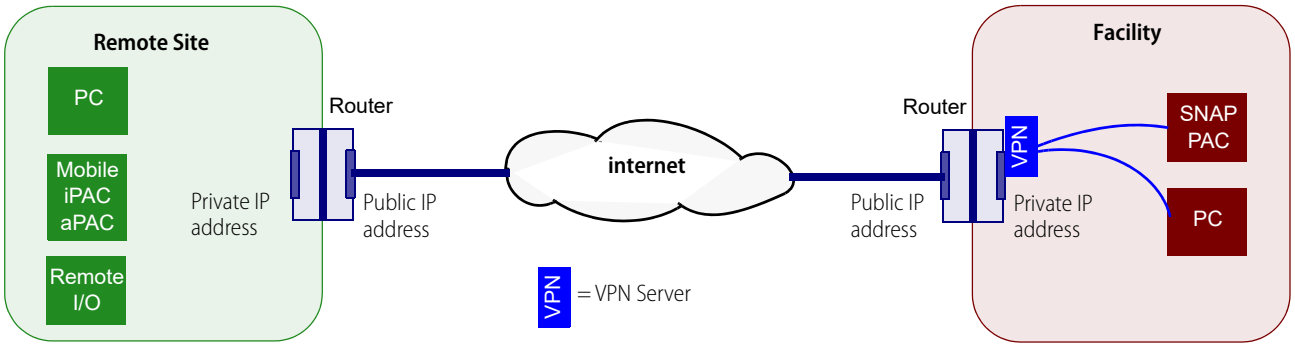
In most cases communication over a VPN requires two things: setting up a VPN server on your network and setting up VPN clients.

Setting Up a VPN Server

If you don't have an IT Department, you can google for ways to set up your own VPN server. You can use a computer or network VPN appliance, for example a Microsoft Windows Server machine configured for VPN Server. Several protocols are available for VPN, including PPTP, IPSec, and OpenVPN. Choose the VPN protocol based on what your VPN clients (your PCs and mobile devices) need to use. If you have a choice, OpenVPN is somewhat more secure than PPTP; but PPTP is often built into modern PCs and mobile devices.

NOTE: If you are using or plan to use groov EPIC in your architecture, OpenVPN is the best choice, because an OpenVPN client is included in the processor.

Place the VPN server inside your private network, behind the router, at your facility:



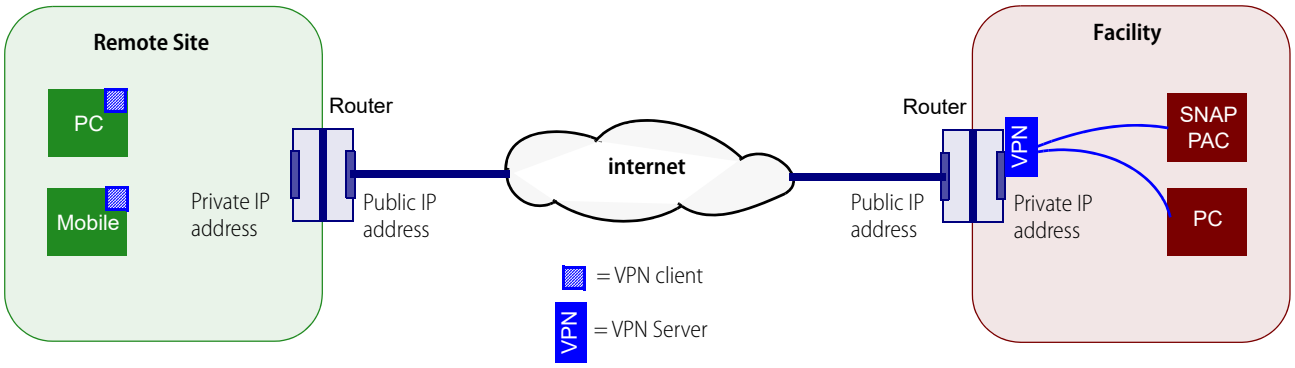
In the router, set up a port forward rule so the router will know to send data through the proper port to reach the VPN server. Port numbers depend on the VPN protocol you're using:

VPN protocol	Ports used
OpenVPN	1194
PPTP	47 and 1723
IPSec	50, 51, and 500

On the VPN server, set up users and accounts so authorized individuals have usernames and passwords to use the VPN.

Setting Up VPN Clients

Once your VPN server is set up and user accounts established for those who need them, you'll need to set up a VPN client on each PC or mobile device that will use the VPN. In the diagram below, a PC and a mobile device are shown at the same remote site, but they can be anywhere:



Most current PCs and mobile devices have VPN client software built in. The VPN client must use the same VPN protocol (PPTP, IPSec, OpenVPN) as the VPN server. Some clients give you a choice: for example, the VPN client in iOS devices supports connections to a server using PPTP or IPSec.

To set up VPN clients, follow the steps below for the devices you're communicating with:

- VPN: Computer to SNAP PAC—page 15
- VPN: Mobile Opto iPAC/aPAC to SNAP PAC—page 16

VPN: Computer to SNAP PAC

1. Make sure you have a VPN account on the VPN Server.
2. Set up a VPN client on your PC. For example, in Windows 10:
   a. Press the Windows key and open Control Panel.

   b. Click Network and Sharing Center.
   c. Click Set Up a New Connection or Network.
   d. Choose Connect to a Workplace and follow instructions in the wizard to set up the connection. For internet address, use the domain name or public IP address of the gateway router where the VPN server is located. (For more on this, see "Gateway Router Identification" on page 12.)

3. Establish a VPN connection to your VPN server from your PC. For example, in Windows 10, press the Windows key, open Remote Desktop. Choose the VPN network you just set up and log in.

   When you connect, the remote VPN network assigns your PC an additional IP address to match the local network.
4. To communicate with a SNAP PAC, use PAC Project software just as if you were on the same local network.
5. To use *groov* View, in your web browser, type https:// plus the hostname or IP address of the *groov* EPIC or the PC running *groov* Server for Windows. Example: `https://mygroov`
6. Test your connection: see "Testing Communication" on page 17.

VPN: Mobile Opto iPAC/aPAC to SNAP PAC

If you're using the Opto 22 mobile apps Opto iPAC (for iOS) or Opto aPAC (for Android), follow these steps to set up a VPN client:

1. On your **iOS** mobile device, go to Settings > General > VPN and enter the required information. When configuring a PPTP network, set "Send all traffic" to ON.
2. On your **Android** device, go to Settings and find VPN, then enter the information required.
3. Open the app and enter your username and password.

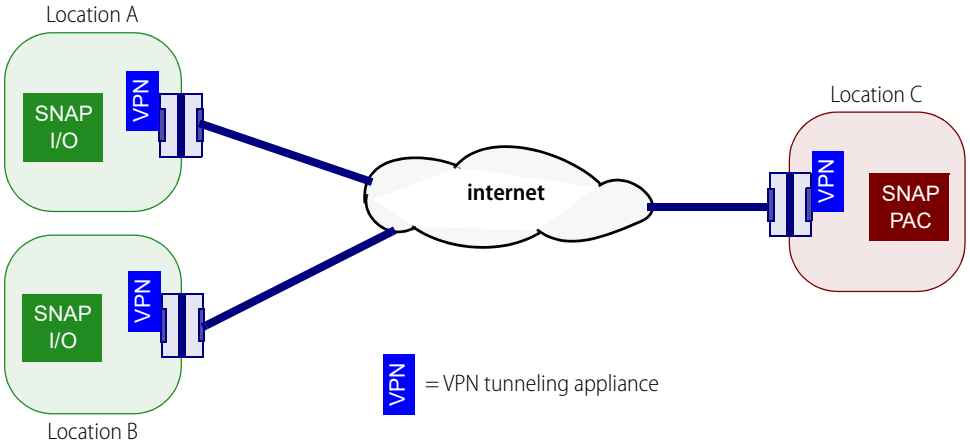
VPN Special Case: SNAP PAC to Remote I/O

Connecting a SNAP PAC to remote I/O is a special case that requires a VPN set up in a specific way. Before setting up communication between a SNAP PAC and remote I/O, be aware of its limitations:

- Controller to I/O communications is via UDP, which uses unacknowledged Ethernet packets.
- You need a chart that monitors the online status of each rack of I/O and ensures that communications and commands are not lost over the network. (An I/O Enabler sample chart is available on our website in Samples and Freeware.)
- Since communication is unacknowledged, make sure that the process will be left in a safe state if communication is lost for any reason over any length of time.

In this case you'll need to use a **VPN tunneling appliance** rather than a separate VPN server and VPN client. That's because SNAP PAC controllers and SNAP PAC brains cannot be VPN clients and cannot accept a VPN client.

A VPN tunneling appliance solves the problem by incorporating both server and client in one box, which may or may not also include a gateway router. You place a VPN tunneling appliance at each end of the communication to create a tunnel that can go both ways. The VPN tunneling appliances create a site-to-site VPN, not just a device-to-device VPN. Once you set up the two appliances, your Opto 22 devices communicate just as if they were on the same local area network.



TESTING COMMUNICATION

You're now ready to test communication between your two networks.

IMPORTANT: *On your SNAP PAC controller, make sure that you configure only ONE of its interfaces with a valid gateway and DNS IP address, and connect that interface to the gateway router that's connected to the internet. Set the other interface's gateway and DNS addresses to 0.0.0.0. If more than one interface has a gateway configured, the PAC will use the gateway associated with the lowest numbered Ethernet interface that currently has a connection.*

Computer to SNAP PAC I/O Unit or Controller

You can test communication to both SNAP PAC I/O units and controllers using PAC Manager.

1. On your PC, open PAC Manager.
2. Choose Tools > Inspect.
3. In the Device Name field, enter the hostname or IP address of the I/O unit or controller you want and click Status Read.

   Data appears on the screen.

Computer to SNAP PAC Controller

An easy way to test is with PAC Terminal.

1. On your PC, open PAC Terminal.
2. Double-click the name of the SNAP PAC on the control network.

   The Inspecting window opens, showing your controller just as if you were on site.

   Notice that the Comm Loop Time can be considerably longer than it would be if both devices were on the same network. As with any internet connection, communication may be slower at some times than at others.

4: Glossary and Resources

NETWORKING TERMS

This short glossary includes some of the networking terms and concepts we use in this guide. For a lot more information, search the internet for these terms and any others you're not sure about.

DHCP

DHCP (dynamic host configuration protocol) helps devices on a network communicate with each other. A DHCP server uses the protocol to assign each device an IP address and other configuration information as soon as it appears on the network.

Because these assigned IP addresses are valid only for a certain length of time, the address of a specific device on the network is likely to change over time and is referred to as dynamic. (In contrast, a fixed or static IP address is permanently assigned to a device and will not change.)

DNS/DDNS

DNS (domain name system) is a service that resolves domain names (like `www.google.com`) or computer names (like `//mypc`) into IP addresses. Typically the DNS service is provided by a computer or router.

Communication between computers and other devices on a network is based on IP addresses; each address is a series of numbers. A DNS is useful because humans cannot remember numbers as easily as they can remember words.

A *DDNS (dynamic domain name service)* updates domain names in the DNS that have dynamic (changing) IP addresses. Most IP addresses change over time; a DDNS periodically checks and sends the change to DNS servers.

domain

A *domain* is a group of computers networked together and using a common address for remote communications. The *domain name* is the address, and it usually reflects the company's or organization's name so it is easy for people to remember when they want to access it over the internet.

A company like Opto 22, for example, has a domain that's used for all internet communications. Opto 22's domain name is opto22.com.

gateway

Gateway is a general term that refers to a means of providing access to a place or to data. A router may be called a gateway, especially when it provides access to the internet.

IP address

An *IP address* is a numeric address assigned to a computer or other device on a network that uses the internet Protocol (IP) for communication. An IP address identifies a device and provides a location for communication. Current IP addresses (IPV4) are in the format of four decimal numbers (values 0–255), separated by dots. For example: `192.168.10.4` or `10.172.0.244`

LAN

A *LAN* is a local area network, usually a private network set up by an individual, a business, or an organization to connect computers and other electronic devices within a limited physical area. Compare to WAN.

network

A *network* is a group of computers or other electronic devices linked together so they can exchange information. The link requires some form of physical connection, usually through wires or airwaves, and a common *protocol*, which is a language through which information is exchanged.

This guide covers Ethernet networks and wireless networks. It does not include information about serial or other kinds of networking with Opto 22 products.

network switch

A *network switch* directs data traffic between the devices connected to it. The switch transmits data from one device to another using the device addresses. In contrast to a *hub*, which transmits any communication to all devices on the network, a switch transmits only to the specific device the data is addressed to.

node

An individual computer or other device on a network is called a *node*.

port

One device can communicate in a number of different ways using the same IP address. For example, a SNAP PAC controller can communicate with I/O units, a PC running PAC Display, a Modbus/TCP device, and an Allen-Bradley ControlLogix PLC, all at once using the same IP address.

Each of these "services" uses a unique *port* number for communication. The combination of IP address and port number keeps communication running smoothly. It's like an apartment building where all the apartments have the same street address (the IP address), but each apartment has a number (the port number).

Generally, ports 0 to 1023 are well-known ports and should not be used for anything other than their assigned service. For example, port 80 is used for HTTP (web communication), port 25 is used for email, and port 21 is used for FTP (file transfer protocol).

Ports 1024 to 49151 are registered ports. Many of these have been assigned to specific companies to use for their specific services. For example, ports 22000–22005 are registered to Opto 22. But many port numbers between 1024 and 49151 are available for use by anyone.

Official port assignments are maintained by IANA, the Internet Assigned Numbers Authority.

port forwarding

Port forwarding allows remote computers (for example, computers on the internet) to connect to a specific computer or service within a private local-area network (LAN).

Port forwarding opens certain ports on your home or small business network, usually blocked from access by your router, to the internet.

router

A *router* is a networking device that lets packets of information from one network end up on another. The router is connected to two or more networks. When a data packet arrives at the router, the router checks its address using network address translation (NAT) and forwards it based on established rules, which are often kept in a routing table.

Routers may allow communication between private networks, for example two LANs in the same business, or between a private network and the internet (a LAN and a WAN).

subnet mask

The *subnet mask* defines the IP address range of a local area network, or LAN. A subnet mask is a way of logically segmenting a network, and all devices with the same subnet mask are on the same LAN or subnet. The subnet mask reduces the amount of traffic on the network by making sure a device can only talk to network addresses inside its network mask.

When you configure a device such as a SNAP PAC controller on the network, you assign a subnet mask together with the IP address.

The subnet mask and the IP address work together, a little like a country code on the phone. You add the country code to the phone number, and the system uses that information to connect you. The most common subnet mask is `255.255.255.0`. In this mask the first three parts identify the network, and the last part identifies the node or host. For this subnet mask, all devices on the network would have addresses between `192.168.1.0` and `192.168.1.255`.

	Network	Node
Subnet mask	`255.255.255.`	`0`
Beginning IP address	`192.168.1.`	`0`
Ending IP address	`192.168.1.`	`255`

VPN (virtual private network)

A *VPN (virtual private network)* is a method of connecting computers or other devices remotely, over the internet, as if they were on a private local area network (LAN). A VPN provides a kind of shielded tunnel through the internet, maintaining private security and encryption.

From the user's point of view, the VPN makes it feel as though he were right there on the same private network. VPNs are often used for employees who are traveling or working at remote sites.

WAN

A *WAN* is a wide area network, which may be private or public. The internet is the prime example of a public WAN. Compare to LAN.

RESOURCES

These are just a few of the many resources online that deal with remote networking.

Networking FAQs plus a forum for asking questions: Whatismyip.com

Some DDNS services:

- http://dyn.com/dns/
- http://www.noip.com/

Additional information about VPNs:

- Microsoft technical information for Windows Server 2008
  http://technet.microsoft.com/en-us/library/cc772120(v=ws.10).aspx

Setting up a VPN:

- On Android: http://www.howtogeek.com/135036/how-to-connect-to-a-vpn-on-android/
- Download the OpenVPN app for Android:
  https://play.google.com/store/apps/details?id=net.openvpn.openvpn&hl=en
- On iOS:
  https://support.apple.com/guide/deployment-reference-macos/intro-to-vpn-ior9f7b5ff26/1/web/1

Opto 22 Resources

For user's guides, see "Related Documents" on page 2.

For Opto 22 Product Support, see "For Help" on page 2.

Ask and answer questions with other Opto 22 customers in the OptoForums