

GUIDE TO NETWORKING OPTO 22 PRODUCTS

Form 1796-140626—June 2014

OPTO 22
Automation made simple.

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 Opto 22 Products
Form 1796-140626—June 2014

Copyright © 2013–2014 Opto 22.
All rights reserved.
Printed in the United States of America.

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, 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. These products include, but are not limited to, OptoTerminal-G70, OptoTerminal-G75, and Sony Ericsson GT-48; see the product data sheet for specific warranty information. Refer to Opto 22 form number 1042 for complete warranty information.

Wired+Wireless controllers and brains are licensed under one or more of the following patents: U.S. Patent No(s). 5282222, RE37802, 6963617; Canadian Patent No. 2064975; European Patent No. 1142245; French Patent No. 1142245; British Patent No. 1142245; Japanese Patent No. 2002535925A; German Patent No. 60011224.

Opto 22 FactoryFloor, *groov*, Optomux, and Pamux are registered trademarks of Opto 22. Generation 4, *groov* Server, ioControl, ioDisplay, ioManager, ioProject, ioUtilities, *mistic*, Nvio, Nvio.net Web Portal, OptoConnect, OptoControl, OptoDataLink, OptoDisplay, OptoEMU, OptoEMU Sensor, OptoEMU Server, OptoOPCServer, OptoScript, OptoServer, OptoTerminal, OptoUtilities, PAC Control, PAC Display, PAC Manager, PAC Project, SNAP Ethernet I/O, SNAP I/O, SNAP OEM I/O, SNAP PAC System, SNAP Simple I/O, SNAP Ultimate I/O, and Wired+Wireless are trademarks of Opto 22.

ActiveX, JScript, Microsoft, MS-DOS, VBScript, Visual Basic, Visual C++, Windows, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries. Linux is a registered trademark of Linus Torvalds. Unicenter is a registered trademark of Computer Associates International, Inc. ARCNET is a registered trademark of Datapoint Corporation. Modbus is a registered trademark of Schneider Electric. Wiegand is a registered trademark of Sensor Engineering Corporation. Nokia, Nokia M2M Platform, Nokia M2M Gateway Software, and Nokia 31 GSM Connectivity Terminal are trademarks or registered trademarks of Nokia Corporation. Sony is a trademark of Sony Corporation. Ericsson is a trademark of Telefonaktiebolaget LM Ericsson. CompactLogix, MicroLogix, SLC, and RSLogix are trademarks of Rockwell Automation. Allen-Bradley and ControlLogix are a registered trademarks of Rockwell Automation. CIP and EtherNet/IP are trademarks of ODVA.

groov includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org>)

All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

Opto 22
Automation Made Simple.

Table of Contents

Chapter 1: Networking Basics	1
Introduction	1
What's in this Guide	1
For Help	2
Related Documents	2
Connecting to Computers	3
How Does the Data Get There?	3
Networking within Your Facility	3
How a Gateway Router Works	4
SNAP PACs and the <i>groov</i> Box	4
What's Your Network Setup?	6
Chapter 2: Communication within your Facility	7
Introduction	7
Single, Flat Network.....	7
Notes for Mobile Communication with <i>groov</i>	8
Separate Network Subnets	8
Separate Network Subnets with <i>groov</i>	9
Separate Network Subnets with a SNAP PAC	10
Chapter 3: Communication over the Internet	11
Why Communicate over the Internet?	11
Cautions: Security, Speed, and Reliability	12
Internet Gateway Routers	12
Gateway Router Identification	13
Fixed (Static) vs. Dynamic IP Addresses	13
Consider Your Options	14
VPN vs. PF	14
Working with Your IT Department	15
Common Communications and Required Ports	15
Opto 22 Port Usage	15
Setting Up a Virtual Private Network (VPN)	16
Setting Up a VPN Server	16

Setting Up VPN Clients	16
VPN: Computer to <i>groov</i> or PAC	17
VPN: Android Mobile to <i>groov</i>	18
VPN: iOS Mobile to <i>groov</i>	18
VPN: Opto iPAC/aPAC to SNAP PAC	19
VPN Special Cases	19
Using Port Forwarding (PF)	20
Determining the IP Address	20
Establishing Port Forward Rule(s)	21
Creating the Port Forward Rule	21
Setting up Port Forwarding on PCs and Mobile Devices	21
PF: PC or Mobile to <i>groov</i> using a Web Browser	21
PF: Mobile to <i>groov</i> using the <i>groov</i> View Mobile App	21
Testing Communication	22
Computer to SNAP PAC	22
Communication to <i>groov</i>	22
Testing <i>groov</i> from inside your facility	22
Testing <i>groov</i> from outside your facility	22
Troubleshooting	23

Chapter 4: Glossary and Resources25

Networking Terms.....	25
DHCP	25
DNS/DDNS	25
domain	25
gateway	26
IP address	26
LAN	26
network	26
network switch	26
node	26
port	26
port forwarding	27
router	27
subnet mask	27
VPN (virtual private network)	28
WAN	28
Resources.....	28
Opto 22 Resources	28

1: Networking Basics

Introduction

We live in an increasingly connected world. Computers and mobile devices are proliferating, 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 new 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.

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:

- You've built operator interfaces with Opto 22's *groov* and want to access your *groov* screens on your mobile device while away from your facility.
- 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 devices from another manufacturer 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 and *groov* using wired Ethernet networks and wireless LANs.

- **SNAP PAC** programmable automation controllers include the standalone S-series, rack-mounted R-series, and SoftPAC software-based controller for PC-based control. Field proven in a wide variety of applications worldwide, these PACs control reliable, guaranteed-for-life SNAP I/O. For networking flexibility, hardware SNAP PACs include two independent Ethernet interfaces plus an optional wireless interface.
- **groov** makes it simple to build effective operator interfaces (human-machine interfaces, or HMI) on any computer using only a web browser. The HMI you build with *groov* can be used on virtually any device with a web browser, regardless of its size or manufacturer. *groov* comes either in the *groov* Box appliance or as *groov* Server for Windows, which runs on a Microsoft Windows computer. The *groov* Box has two independent Ethernet interfaces and one wireless interface.

This guide includes:

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

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.

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.

Related Documents

Be sure to check the user's guide 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 #
groov User's Guide	2027
groov Box User's Guide	2077
groov Server User's Guide	2078
SNAP PAC S-Series Controllers User's Guide	1592
SNAP PAC R-Series Controllers User's Guide	1595
SoftPAC Quick Start Guide	2045

If your questions are specifically about setting up remote communications with Opto 22 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) 951-695-3080 (Hours are Monday through Friday, 7 a.m. to 5 p.m. Pacific Time)	<i>NOTE: Email messages and phone calls to Opto 22 Product Support are grouped together and answered in the order received.</i>
Fax:	951-695-3017	
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` or `groov.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

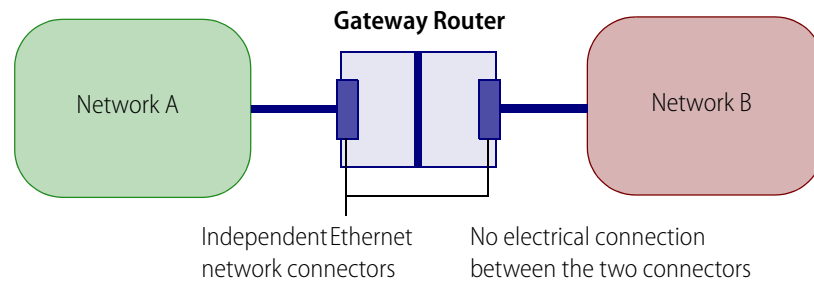
Within your facility you may have one or more subnetworks or local area networks (LANs).

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 internal electrical connection between the two. Because there is no electrical 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. Because there is no electrical 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](#).

SNAP PACs and the *groov* Box

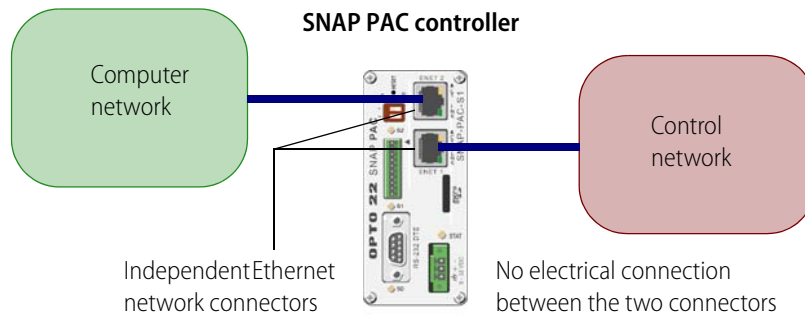
Like a gateway router, SNAP PAC controllers and the *groov* Box each have two independent Ethernet network interfaces (and in some cases also an independent wireless interface). Each of these independent interfaces must be wired to a separate network. That means their network addresses (a combination of IP addresses and subnet masks) must be different.

SNAP PACs and *groov* Boxes are not routers, because they do not provide routing or address translation, but their separate interfaces work like a router's interfaces:

- If your control network is wired to ENET1 on a SNAP PAC and your computer network is wired to ENET 2, there is no electrical connection inside the PAC to connect the two networks. Because there is no electrical connection, communication between the two networks can occur only if the software inside the PAC—your PAC Control strategy—allows it.

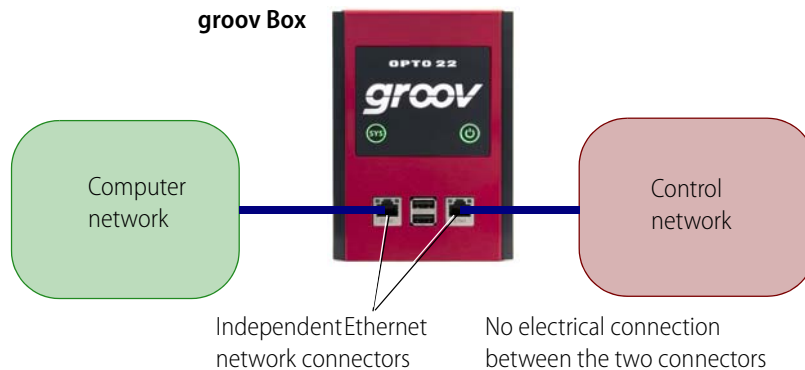
NOTE: The two wired interfaces on SNAP-PAC-EB1 and -EB2 brains are different from those on SNAP PAC controllers. On the brains the two interfaces are connected, so these brains act as a two-port

switch and therefore can be daisy-chained. In contrast, on a SNAP PAC controller, data packets cannot travel directly between interfaces. That's why the PAC provides security.



PAC Control strategy in the SNAP PAC determines what data moves between the two networks.

- If your control network is wired to ETH0 on the *groov* Box and your computer network is wired to ETH1, there is no electrical connection between the two. Data packets cannot travel directly between them; the only communication that can happen is that allowed by the *groov* software inside the Box. If you've built an HMI with a switch to turn on a pump, an authorized user can switch on the pump. But he cannot control a valve that isn't in the HMI or that's on a screen he's not authorized to see. Nor can he directly access any systems on the other network.



Your groov project determines what data a groov View user can see and change.

Remember: The independent network interfaces on SNAP PACs and *groov* Boxes must always be on separate networks (using different IP addresses and subnet masks). SNAP PACs and *groov* Boxes do not route IP traffic; they have no routing tables or network address translation. The only communication they allow between the two networks is what you've built into your PAC Control strategy or *groov* project.

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 Eth0 and Eth1 interfaces on a *groov* Box, 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. Or one of the network subnets might use the wireless LAN interface on a PAC or *groov* Box. 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 *groov* Box at one location and your SNAP PAC at another, or you are using *groov* on a smartphone inside your facility but are out of range of your wireless LAN, so the phone switches to cellular service. For this kind of remote communication, see [Chapter 3: Communication over the Internet](#).

2: Communication within your Facility

Introduction

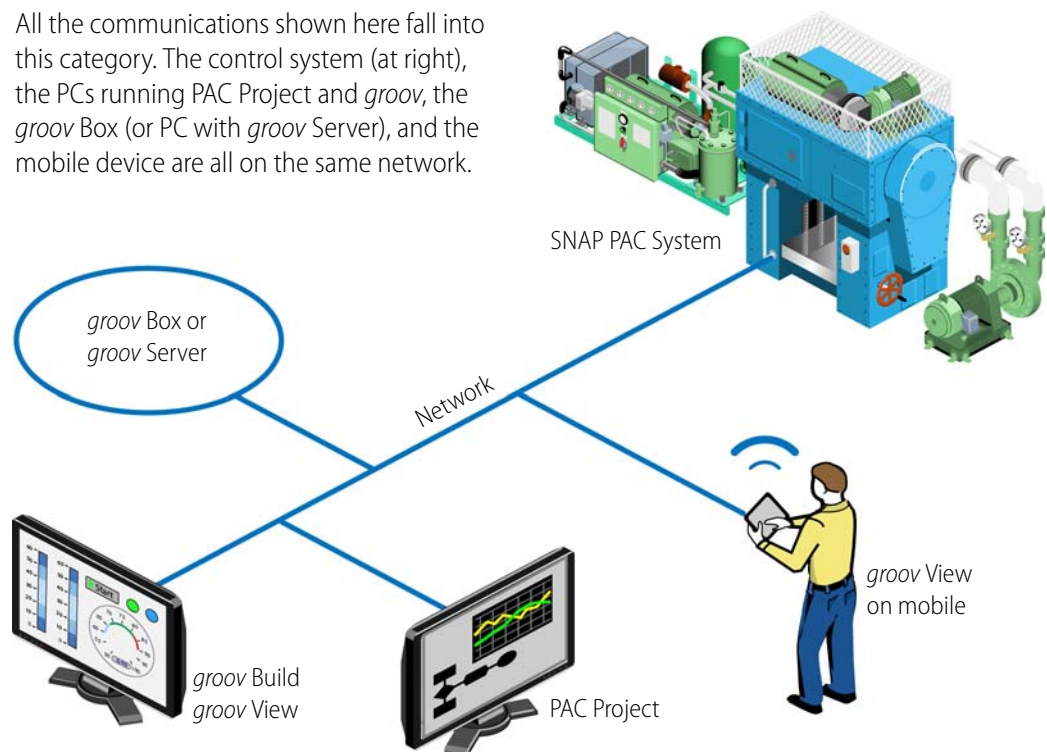
Inside your facility, you may want to have computers and/or mobile devices communicate with your control system. Maybe you want to monitor production numbers, check equipment, operate machinery, or control processes. How you do so depends on your network setup:

- 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*, the *groov* Box (or PC with *groov* Server), 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
PC <--> groov	Only one Ethernet interface on each is used
Mobile <--> groov	Same wireless LAN. Note that the groov Box is not a wireless access point, just a wireless client. The groov Box and the mobile device must join the same wireless network.
groov <--> SNAP PAC	Only one Ethernet interface on each is used
PC <--> SNAP PAC	Only one Ethernet interface on each is used
Mobile with Opto iPAC or aPAC app <--> SNAP PAC	Same wireless LAN. Note that the SNAP PAC is not a wireless access point, just a wireless client. The PAC and the mobile must join the same wireless network.

Notes for Mobile Communication with groov

If you're using a smartphone or tablet on your local network to connect with groov, you may need to be more specific with the URL to direct the mobile device's browser:

- On an iOS device, the browser always tries port 80 first, so the secure connection to your groov Box or groov Server times out. To prevent this, add a colon and the port number to your groov hostname. For example, if `https://hostname` times out, try adding the port number (default is 443): `https://hostname:443` (substituting your groov Box's actual hostname)
- For Android, add a period and your local domain name. For example, if `https://hostname` results in an error, try: `https://hostname.domainname.com` (substituting the actual hostname of your groov and your company's domain name)

Separate Network Subnets

You may choose to take advantage of the multiple network interfaces on your SNAP PAC controller or groov to separate your control network traffic from your computer network for security reasons. In fact we recommend that architecture for groov. If you've done so, then you have separate network subnets.

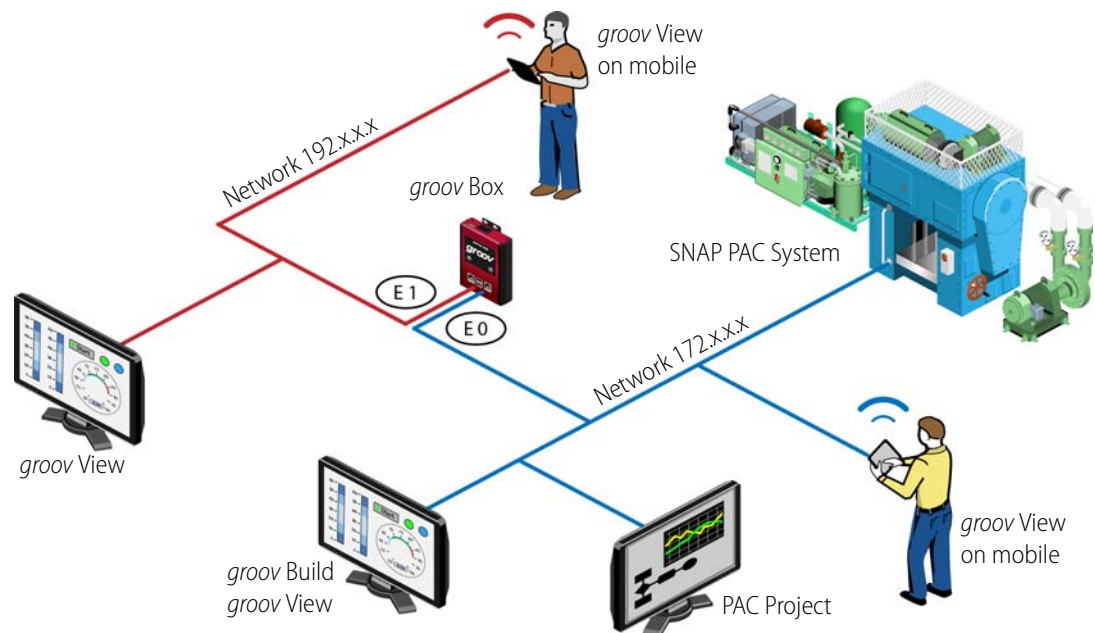
As explained on [page 4](#), the two wired Ethernet interfaces (and the WLAN interface, if present) on a SNAP PAC controller or a groov Box are independent from each other. The same thing applies to two network interface cards (NICs) on a PC. Data packets can't travel directly between the interfaces. The only communication that can occur between the two interfaces (and therefore between the two networks) is communication specifically allowed by the PAC Control strategy in the PAC, or the groov software in the groov Box.

IMPORTANT: Because their network interfaces are not connected, you must ALWAYS assign the network interfaces on one PAC or groov Box **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 the control network or the computer network, except initially when you must use the lower-numbered interface (ETH 0 on the groov Box, or ENET 1 on a PAC).

Let's look at two examples of separate network subnets. In both, the key advantage to separating networks is security. Only authorized people can gain access to the control network, and then only in the ways you allow within the PAC Project or *groov* software.

Separate Network Subnets with *groov*

What the two network subnets offer is a secure way to access specific data in specific ways. The following image shows an example of network subnets separated by a *groov* Box. The 172.x.x.x network is for control. The 192.x.x.x network is for company computers not directly involved in the control network.

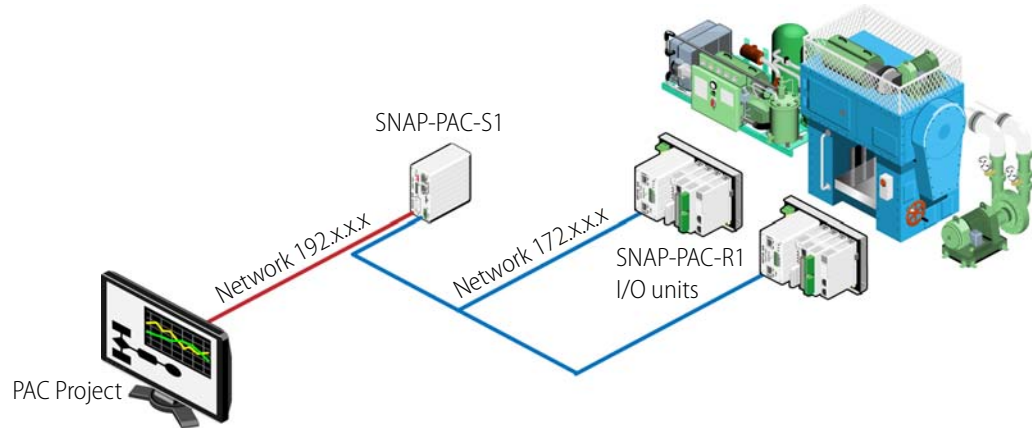


In this example, your *groov* Box is connected to your company computer network using Eth0 and to your control network using Eth1. (You could do the same thing with *groov* Server for Windows running on a PC that has two network interface cards.)

The PCs and mobile devices on the computer network have no direct connection with the SNAP PAC System on the control network. But authorized employees on these devices can use a *groov* interface you've built to monitor and control any part of the system *groov* gives them access to. For example, you might give a supervisor the ability to check production figures but not turn a conveyor on or off.

Separate Network Subnets with a SNAP PAC

Here's another example of two LANs or subnets, this time using a SNAP PAC controller as the gateway between the two.



In this example one of the PAC's network interfaces is connected to the control network and the other to the computer network. If you're using PAC Project on the computer network, you can communicate with that PAC. But you cannot communicate directly with a different PAC that is wired only to the control network.

So in this illustration you could get data about the SNAP-PAC-R1 I/O units only if it's available in the SNAP-PAC-S1—for example, you could run a PAC Display HMI from the PC on the computer network. Or you could download a PAC Control strategy to the S1. But you could not download a PAC Control strategy from the PC to the SNAP-PAC-R1s (nor upgrade firmware on the R1s), because they are on a different network and you have no direct connection with them.

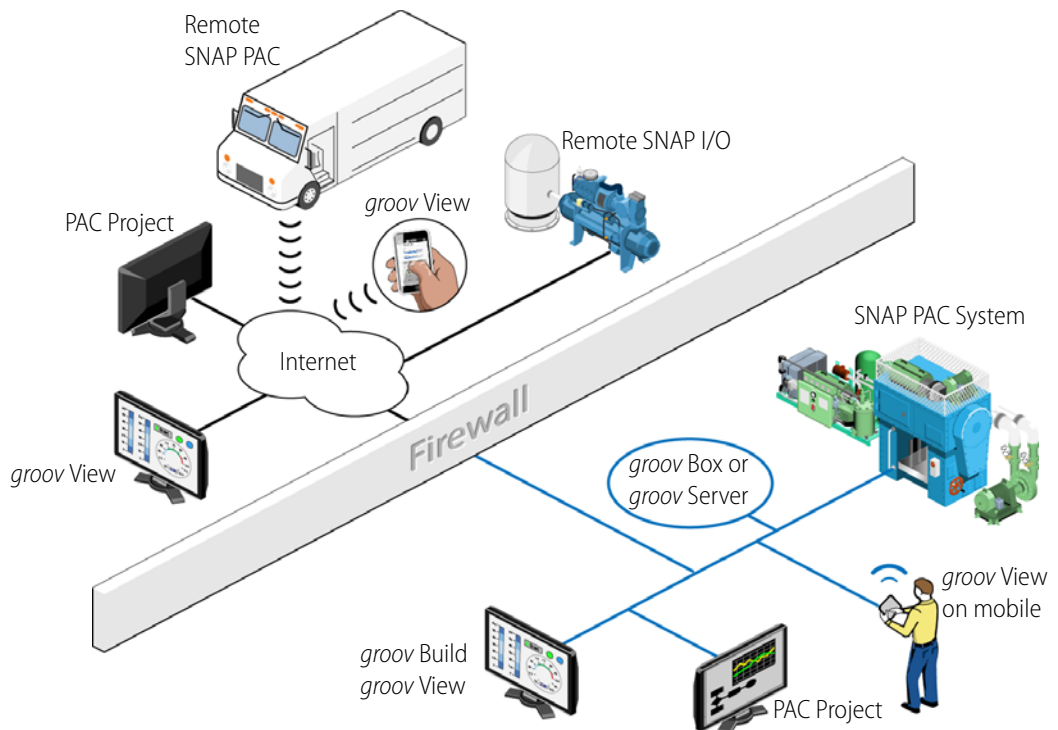
3: Communication over the Internet

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. The following image shows some examples.



Any two networks can be used as long as both are connected to the Internet:

- A PC in one location can get data from a SNAP PAC at another location.
- You can use *groov* on a computer or mobile device far away from your control system.
- A mobile device with cellular service (which goes through the Internet) can use the cellular network if it can't reach the wireless LAN.

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.

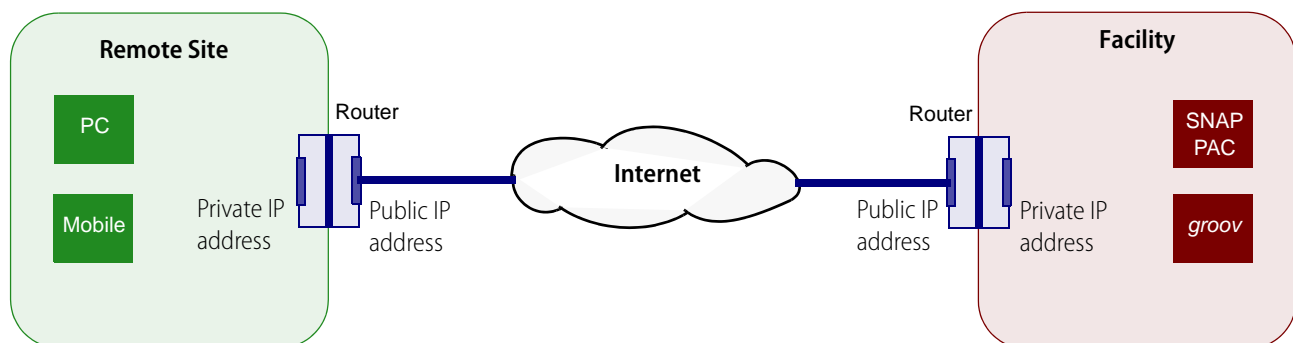
Internet Gateway Routers

Remember our gateway routers from Chapter 1 ([“How a Gateway Router Works” on page 4](#))?

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 network interface cards (NICs), one connected to the public Internet and one connected to your facility's private network. There's no electrical 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.x.x.x
- 172.x.x.x
- 192.x.x.x

All other IP addresses are on public networks.

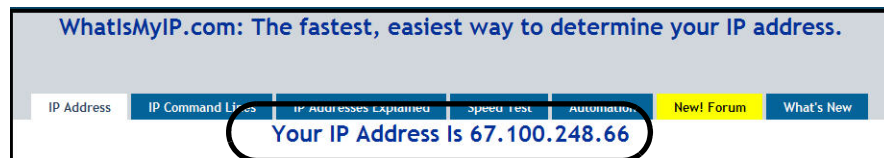
This distinction between the public and private IP addresses on the router becomes important as you set up communication.

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 or port forwarding.
- 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 *groov* Box) or a service (like *groov* Server) that's on a private network, you need a way around this block.

You have two possible methods for communication from the Internet: a virtual private network (VPN) or port forwarding (PF).

- **If you're using a PC or mobile device to communicate with *groov*,** you can use either a VPN or port forwarding. A VPN is preferred because it is much more secure.
- **CAUTION: 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 *groov* and a SNAP PAC, between computers and SNAP PACs, and between SNAP PACs and remote I/O.

VPN vs. PF

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.

Port forwarding may be easier to set up than a VPN but 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 trusted packets of information (yours) from an untrusted network (the Internet) to pass through.

In addition to security, if you have more than one *groov*, a VPN may be the better choice for practical reasons: you can set up all *groovs* at once instead of one at a time with PF.

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 unfortunately won't work for either method.

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 16 or ["Using Port Forwarding \(PF\)"](#) on page 20.

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 *groov* or 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 Required Ports,”](#) 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 16](#). Note that two special cases require a VPN set up in a particular way; see [“VPN Special Cases” on page 19](#).)

Common Communications and Required Ports

Communication between	Communication methods	
	VPN	PF
PC <--> <i>groov</i>	Yes	Yes. Use port 443/8443 (TCP)
Mobile <--> <i>groov</i>	Yes	Yes. Use port 443/8443 (TCP)
<i>groov</i> <--> SNAP PAC	Yes*	No
PC <--> SNAP PAC	Yes	No
Mobile** <--> SNAP PAC	Yes	No
SNAP PAC <--> Remote I/O	Yes*	No

* See [“VPN Special Cases” on page 19](#).

**Mobile with Opto iPAC or Opto aPAC app

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

Opto 22 Port Usage

If your IT Department plans to use port forwarding, here is the port information they need.

By default, *groov* uses all of the following ports for communication. *Exception:* For *groov* Server, port 10000 does not apply.

Port	Used for	Authenticated?
443 (or 8443)	<i>groov</i> View and <i>groov</i> Build	Yes
10000	<i>groov</i> Admin (applies to <i>groov</i> Box appliance only)	Yes

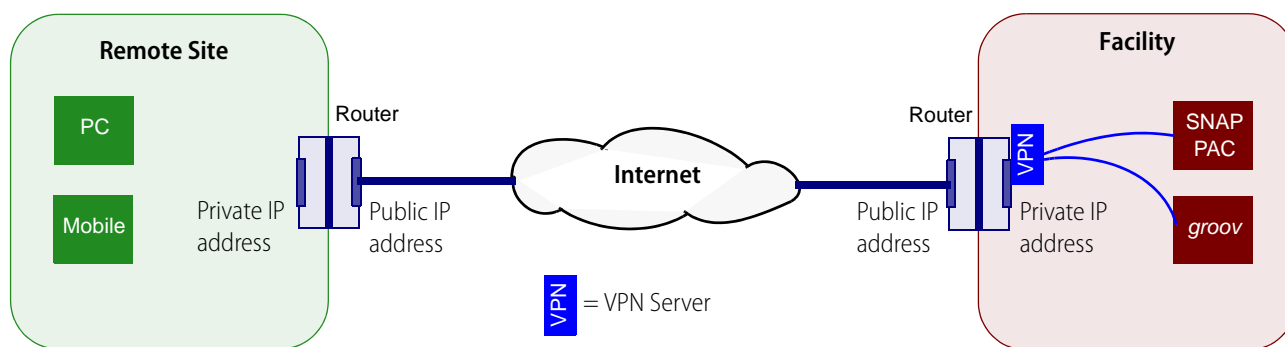
Setting Up a Virtual Private Network (VPN)

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, PPTP is somewhat less secure than OpenVPN; but it is often built into modern PCs and mobile devices.

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



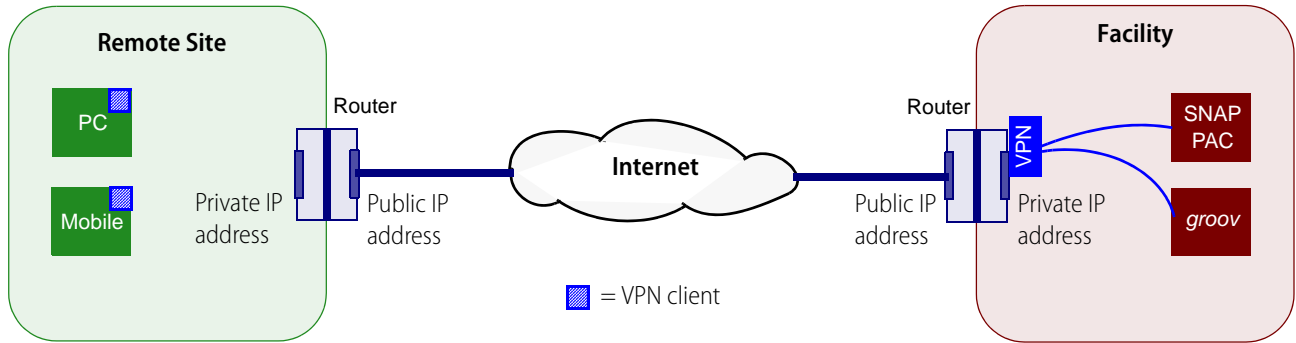
In the router, set up a port forward rule so the router will know to send data through the proper port to reach the VPN server. Port numbers depend on the VPN protocol you're using:

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

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:



NOTE: In our diagram we're assuming that the SNAP PAC and groov are at the same location. What if they're not, and you need to have groov communicate with a remote PAC? For this scenario, see "VPN Special Cases" on page 19.

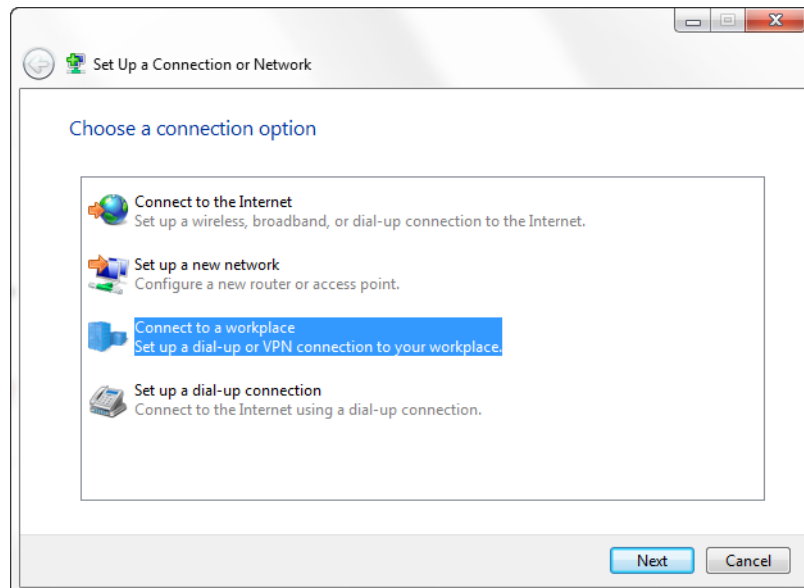
Most current PCs and mobile devices have VPN client software built in. The VPN client must use the same VPN protocol (PPTP, IPSec, OpenVPN) as the VPN server. Some clients give you a choice: for example, the VPN client in iOS devices supports connections to a server using PPTP or IPSec.

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

- [VPN: Computer to groov or PAC—page 17](#)
- [VPN: Android Mobile to groov—page 18](#)
- [VPN: iOS Mobile to groov—page 18](#)
- [VPN: Opto iPAC/aPAC to SNAP PAC—page 19](#)

VPN: Computer to groov or 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 7:
 - a. Choose Start > Control Panel > Network and Sharing.
 - b. Click Set Up a New Connection or Network.



- c. 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 13.](#))
3. Establish a VPN connection to your VPN server from your PC. For example, in Windows 7, choose Start > Control Panel > Network and Sharing. Click Connect to a Network and choose the VPN network you just set up.

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*, in your web browser, type `https://` plus the hostname or IP address of the *groov* Box or the PC running *groov* Server for Windows. Example: `https://mygroov`
6. Test your connection: see [“Testing Communication” on page 22.](#)

VPN: Android Mobile to *groov*

On an Android device, follow the steps here to set up a VPN client:

<http://www.howtogeek.com/135036/how-to-connect-to-a-vpn-on-android/>

Use the steps under *Integrated VPN Support*. It is not necessary to install any third party apps or root your phone like other sections of the article mention.

For a VPN server running PPTP (point-to-point tunneling protocol), choose the following:

- VPN server running PPTP
- VPN Server address
- DNS search domains

Leave everything else at the default selection.

When connecting to the VPN, enter your username and password.

Once connected, open a web browser and type `https://` plus the hostname or IP address of the *groov* Box or the PC running *groov* Server for Windows. Example: `https://172.20.52.5`

If you have problems connecting, see [“Communication to *groov*” on page 22.](#)

For an OpenVPN server, visit the Google Play Store and download the OpenVPN app:

<https://play.google.com/store/apps/details?id=net.openvpn.openvpn&hl=en>

Configuration is slightly different, because OpenVPN uses IPSEC and requires a certificate (generated by the administrator of the OpenVPN server) to be installed on your phone. Work with your IT Department or OpenVPN administrator to install the certificate.

VPN: iOS Mobile to *groov*

For a VPN server running PPTP, follow this guide: <http://support.apple.com/kb/ht1424>

For an OpenVPN server, download the OpenVPN app from the iTunes store.

For both:

1. When connecting to the VPN, enter your username and password.
2. Once connected, open a web browser and type `https://` plus the IP address of the *groov* Box or the PC running *groov* Server for Windows. Example: `https://172.20.52.5`

If you have problems connecting, see [“Communication to groov”](#) on page 22.

VPN: 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.

You are connected. If you have problems, see [“Communication to groov”](#) on page 22.

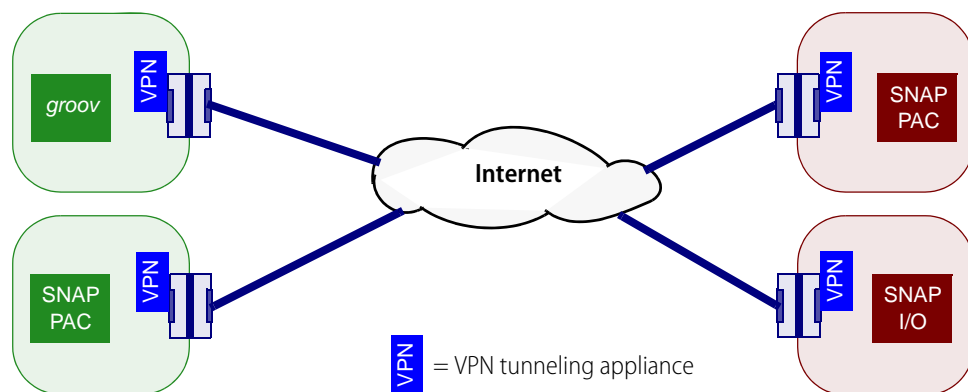
VPN Special Cases

Two special cases require a VPN set up in a specific way:

- *groov* Box to a remote SNAP PAC
- SNAP PAC to remote I/O. 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 is 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 communications fail for any reason over any length of time.

In both these cases you’ll need to use a **VPN tunneling appliance** rather than separate VPN server and VPN client. That’s because SNAP PAC controllers, SNAP PAC brains, and the *groov* Box cannot be VPN clients nor accept a VPN client. And it is unsafe to use port forwarding because PACs do not have user authentication.

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.



Using Port Forwarding (PF)

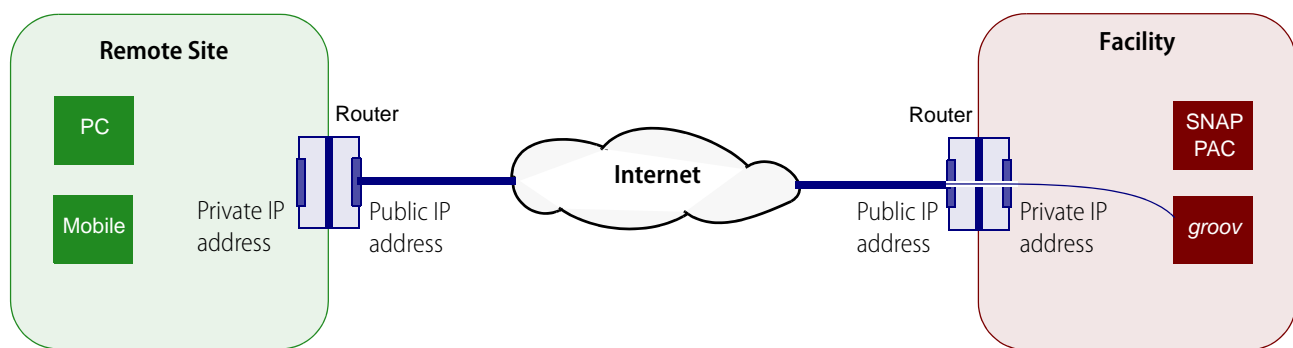
Port forwarding is a less secure way than a VPN to communicate between a PC or mobile device and *groov*, but it may be an acceptable option if:

- You have no IT Department.
- You have no VPN server and do not want to set one up yourself.
- You have just one *groov*.

CAUTION: *Port forwarding is NOT recommended for any communication with a SNAP PAC controller.*

In “Internet Gateway Routers” on page 12 we saw how communication happens over the Internet. Your private network is hidden from the public Internet behind a gateway router (a firewall) that shows only its public IP address to the world.

A port forward rule creates a small hole in that firewall to allow specific data packets to get through to the private network. PF is less secure than a VPN because it creates this hole. This is why PF is not recommended for SNAP PACs. But PF works for *groov* because *groov* requires user authentication with usernames and passwords; unauthorized users cannot get in.



Port forwarding creates a hole in your firewall to allow certain packets through. PF works for *groov* because *groov* requires authentication from all users.

For more information on port forwarding, see: <http://portforward.com/>

To use port forwarding, you need to:

- Determine the IP address (see “Determining the IP Address,” below).
- Establish a port forward rule on the gateway router (see page 21).
- Set up port forwarding on the client PCs or mobile devices (page 21).

Determining the IP Address

On the private network where *groov* is, find out the gateway router’s public IP address (see steps in “Gateway Router Identification” on page 13). In the diagram above, that’s the Facility’s router, which gives access to *groov*. You’ll use this address to reach your devices, or you’ll map a domain name to it.

Determine whether you will use the router’s IP address or its domain name for your connection (see “Fixed (Static) vs. Dynamic IP Addresses” on page 13).

Establishing Port Forward Rule(s)

By default, *groov* communicates over port 443 or 8443.

NOTE: For greater security, you can use an obscure port number. For example, you can make a port forward rule that port 4321 goes to port 443 of the groov Box's IP address. This is called "security by obscurity." If you do this, you'll need to always add the port number when you access your groov Box.

If you have more than one *groov* Box behind the router/firewall, you must configure a port forward rule in the router for each one. Each rule has to have a different port number going to a different IP address. Otherwise the router can't differentiate between them.

Avoid using the reserved port numbers listed in "Opto 22 Port Usage" on page 15. For more general information on ports, see "port" on page 26.

Creating the Port Forward Rule

You'll need to know the following:

- How to access the web page or configuration software for your router/firewall, including its username and password
 - IP address of the *groov* Box (If your router requires an IP address for port forwarding, assign a fixed IP address to your *groov* Box.)
1. Open the web page or configuration software program for the router/firewall.
 2. Locate the link to create the port forward rule.
 3. Create a rule that says any Internet traffic coming in on a specific port number should be sent to the IP address and port number of the *groov* Box.
 - Use the default port number 443 (or 8443), unless you have changed it, have more than one *groov*, or want to obscure the port number by setting it to something else.
 - If given an option to apply the rule to TCP or UDP or both, make the rule apply to both.

Setting up Port Forwarding on PCs and Mobile Devices

PF: PC or Mobile to *groov* using a Web Browser

If you've already set up the port forward rule on your router or firewall, you're ready to test communication: see "Communication to *groov*" on page 22.

PF: Mobile to *groov* using the *groov* View Mobile App

1. On an **iOS** mobile device, go to Settings > *groov*.
On an **Android** mobile device, launch the *groov* App and tap Connect to *groov*.
2. In the URL field, enter `https://` and the hostname or IP address of the router that has the port forward rule. Example: `https://myrouter`
3. In the Port field, enter the port number you used when setting up the rule (usually 443).
You're ready to use the app. See the *groov User's Guide* for instructions.

Testing Communication

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

Computer to SNAP PAC

An easy way to test is with PAC Terminal.

1. On your PC, open PAC Terminal (Start > Programs > Opto 22 > PAC Project > Tools > 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.

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 won't know which one to use for communications.*

Communication to groov

Testing groov from inside your facility

Since you've set up your VPN or port forward rule while on your local network, you're likely to want to test it from there as well. But testing an outside connection from inside may not work. Internet Service Providers (ISPs) often won't allow communication go outside only to come right back in.

To test the connections you've set up from inside, don't use your computer. Instead, use your smartphone or another mobile device with cellular service.

1. Turn off wifi to force the phone to connect with the nearest cell tower and thus be outside your local network.
2. **VPN:** Open a web browser and type `https://` plus the *groov* Box's hostname (or its fixed IP, if you assigned one).

VPN example: `https://mygroov`
or `https://10.162.89.1`

PF: Open a web browser and type `https://` plus the IP address or domain name of the router for the *groov* network, plus a colon and the port number.

PF example: `https://203.208.65.21:443`
or `https://mydomain:443`

Testing groov from outside your facility

To connect with *groov* from outside your LAN, use either a computer or mobile device.

- **VPN:** Open a web browser. For the URL, type `https://` plus the *groov* Box's hostname (or its fixed IP, if you assigned one).

VPN example: `https://mygroov`
or `https://10.162.89.1`

- **PF:** Open a web browser. For the URL, type `https://` plus the IP address or domain name of the router for the *groov* network, plus a colon and the port number.

PF example: `https://203.208.65.21:443`
or `https://mydomain:443`

Troubleshooting

If you have any problems connecting, see the [groov Troubleshooting Q&A](#) or the [groov User's Guide](#).

If you've been able to communicate with your *groov* in the past and suddenly receive timeouts and can't connect, your IP address has likely changed. That's why you need to use a domain name and a DDNS. See "[Fixed \(Static\) vs. Dynamic IP Addresses](#)" on page 13.

IMPORTANT: *On your groov Box, 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 groov Box won't know which one to use for communications.*

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. If you assign a fixed IP address to a *groov* Box, you also enter the subnet mask.

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:

- An introduction to VPNs and how they work
<http://www.rawbytes.com/virtual-private-networks-in-depth-technical-details/>
- Microsoft technical information for Windows Server 2008
[http://technet.microsoft.com/en-us/library/cc772120\(v=ws.10\).aspx](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 using PPTP: <http://support.apple.com/kb/ht1424>

Information about port forwarding: <http://portforward.com/>

Opto 22 Resources

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

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