GUIDE TO NETWORKING *GROOV*

Form 2161-160115—January 2016

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 *groov*
Form 2161-160115—January 2016

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.

Opto 22
Automation Made Simple.

Table of Contents

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.

About *groov*

groov makes it simple to build an effective mobile operator interface—your own custom mobile app—so you can monitor and control virtually any automation or building systems and equipment from a mobile device.

The operator interface you build with *groov* can be used on smartphones and tablets, and also on laptops, computers, or even HDTVs with a web browser, regardless of their screen size or manufacturer.

groov comes either as 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 an optional wireless interface.

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 *groov* Box or Server and your automation systems and equipment.

The goal is for you to be able to monitor and control your equipment from anywhere you need to, either inside your facility or outside it.

This guide shows you how to communicate with *groov* using wired Ethernet networks and wireless LANs.

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 and Forum

Be sure to check the user's guides for help with *groov.* 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 Build and View User's Guide	2027
groov Box User's Guide for GROOV-AR1	2104
groov Server for Windows User's Guide	2078

The ***groov* Forum** is also available 24 hours a day, 7 days a week so you can get advice from experienced *groov* users.

Product Support

If you can't find the help you need in this guide or in the user's guides, contact Opto 22 Product Support. Product Support is free.

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

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
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?

Clients and servers

Computers communicating on a network typically use the *client-server* model. A *client* computer (or software) requests data or services, and a *server* computer (or software) responds to the request and provides the data or service.

For example, when you send a spreadsheet to the printer, your spreadsheet program is the client. Its request for printer service goes to your company's print server, which allocates resources for printers on the network. The print server handles all the client requests for printing, making sure your spreadsheet and your coworkers' print jobs are all completed in an orderly way.

When you want to watch that YouTube video on your smartphone, your web browser or YouTube app is the client, requesting the video over that giant of networks, the Internet. YouTube's web server receives the request and serves the video page to you, along with the other millions of video pages going to other millions of viewers worldwide.

groov is a server

The *groov* Box and *groov* Server for Windows both act as web servers. At the request of clients like authorized smartphones and tablets, *groov* serves the operator interface pages you've created to these clients on the network.

IP addresses

How does the client reach the server? 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 youtube.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.

Sometimes a computer network is very small—so small that both client and server are on the same PC. For example, when you load *groov* Server for Windows on your PC, you access *groov* View from the same computer by using the name `localhost` or the equivalent IP address: `127.0.0.1`

Networking within your facility

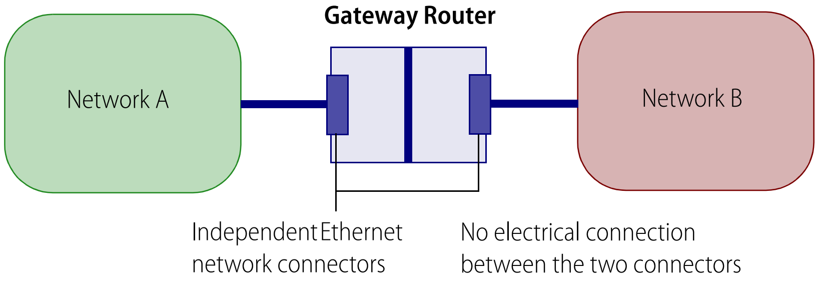
Within your facility you may have one or more subnetworks or local area networks (LANs).

Maybe you have all your devices on a single, flat network: your computers, printers, wireless access points, and control 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 13).

But many companies have more than one LAN. You may have your control system on a separate network from your company computers, for example, to keep the control system segmented for less traffic and 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. Communication between these two interfaces can occur only if software rules inside the router allow it. These software rules typically include routing tables and network address translation (NAT).


Gateway Router
Network A
Network B
Independent Ethernet network connectors
No electrical connection between the two connectors

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. Communication occurs only as allowed by software inside the router.

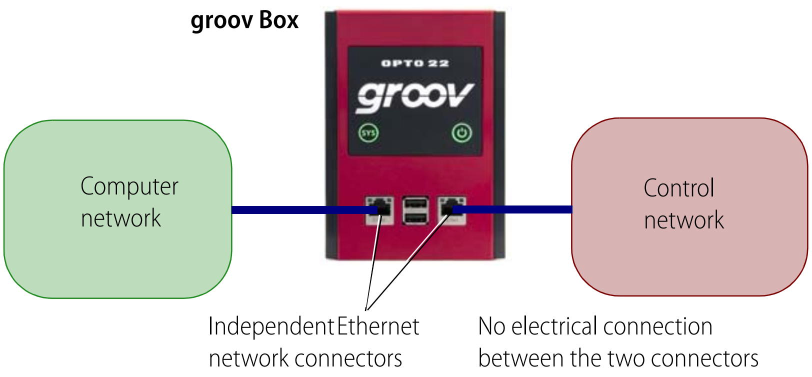
We'll talk more about networking over the Internet in Chapter 3.

The *groov* Box

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

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 ETH0 on the *groov* Box and your computer network is wired to ETH1, the two networks are segmented. Data packets cannot travel between them.

So if you've built an interface 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 interface or that's on a screen he's not authorized to see. Nor can he directly access any systems on the other network.


groov Box
OPTO 22
groov
Computer network
Control network
Independent Ethernet network connectors
No electrical connection between the two connectors

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

Remember: The independent network interfaces on *groov* Boxes must always be on separate networks (using different IP addresses and subnet masks). *groov* Boxes do not route IP traffic; they have no routing tables or network address translation. There is no communication between the two networks.

How do you want to use *groov*?

Now let's take a look at your network setup and how you may want to use *groov* in it. The next few pages show several possible network architectures:

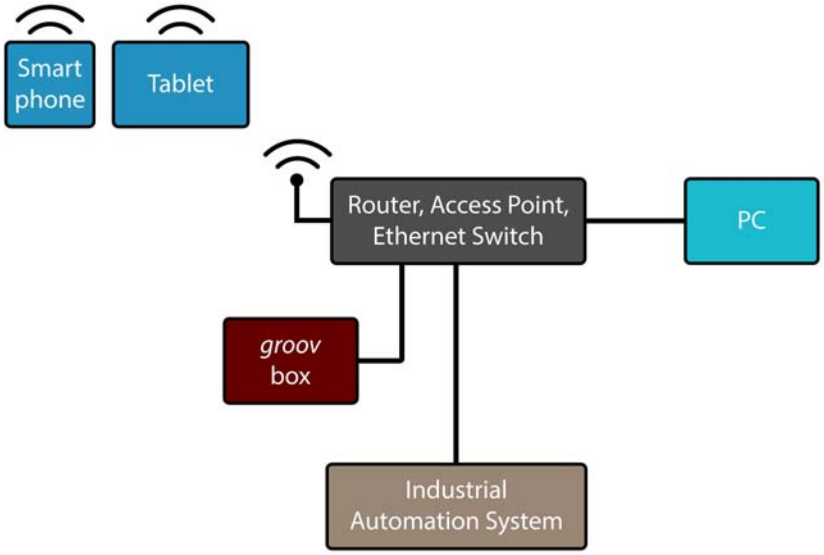
- Using *groov* in your facility with an existing wireless network—page 6
- Using *groov* in your facility without a wireless network (SoftAP)—page 7
- Using *groov* in your facility with segmented systems—page 8
- OEMs and machine builders: Use *groov* as a machine HMI or for access to machine—page 9
- Using *groov* over the Internet, with recommended VPN—page 10
- Using *groov* over the Internet, with VPN and segmented systems—page 10

Use *groov* in facility with existing wireless network

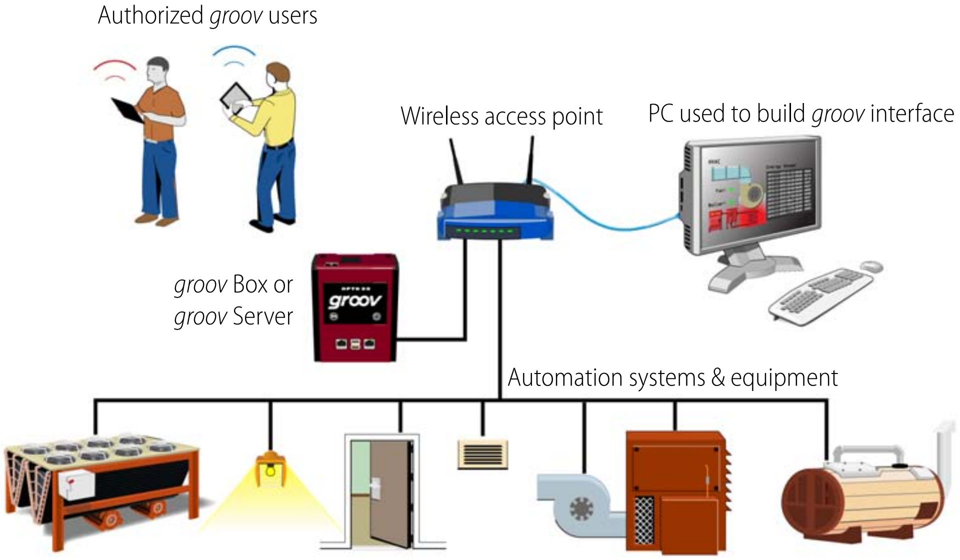
If you want to use your *groov* interface within your facility only (not remotely) and have a wireless network already in place for your control system or equipment, you can just plug *groov* in. Authorized users can monitor and control equipment in your interface as long as they are on the wireless network.

The following diagram shows the basic architectural components:

- You plug the *groov* Box (or *groov* Server) into the same network as the industrial automation system you want to monitor or control.
- You build your *groov* mobile interface on a PC, on the same wired network as *groov*.
- Authorized users can use your interface from their mobile devices with a WiFi connection.


Smart phone
Tablet
Router, Access Point, Ethernet Switch
PC
groov box
Industrial Automation System

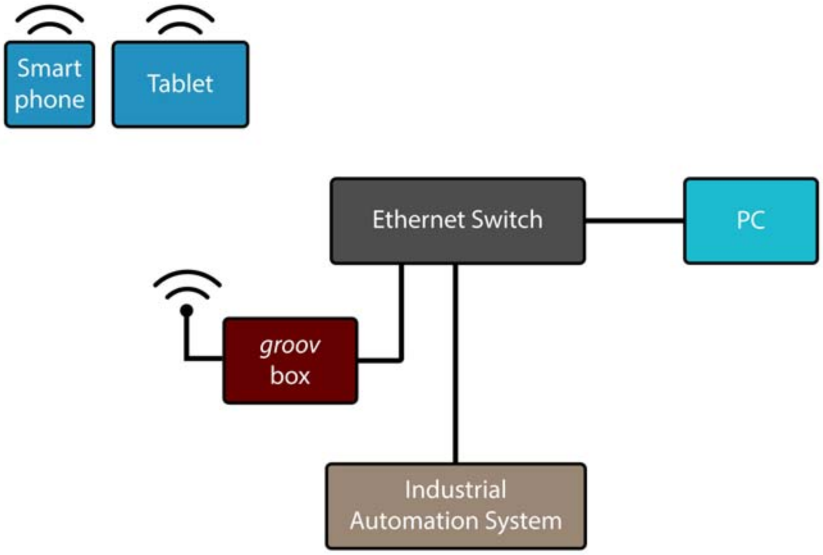
Here's the same network, but with people and systems in place of boxes:


Authorized groov users
Wireless access point
PC used to build groov interface
groov Box or groov Server
groov
Automation systems & equipment

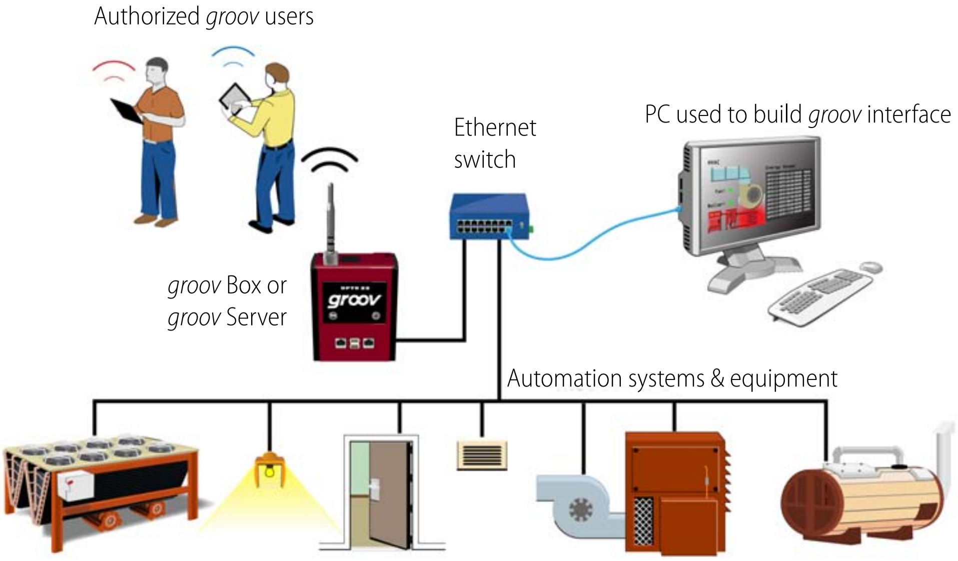
Use *groov* in facility without a wireless network

If you use your *groov* interface within your facility only but do not have a wireless network already in place, you can use the groov Box as a SoftAP (software enabled wireless access point).

To set up SoftAP, you'll need an approved wireless adapter. See the groov Box User's Guide for a list of approved adapters and instructions for setting up SoftAP.



Again, the same network showing people and systems:

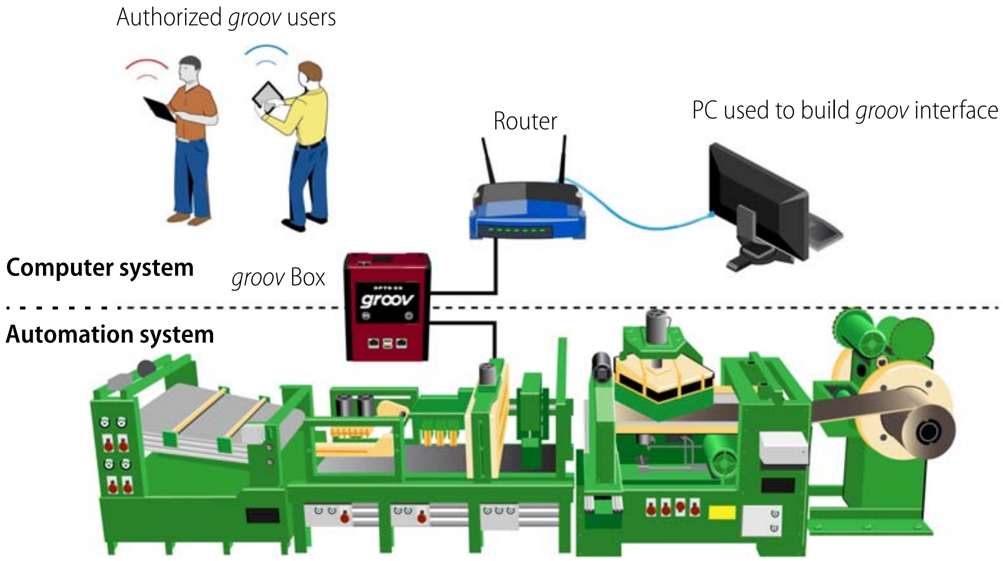

Authorized *groov* users
Ethernet switch
PC used to build *groov* interface
groov Box or *groov* Server
Automation systems & equipment

Use *groov* in facility with segmented systems

For security reasons, we strongly recommend that you segment your automation system from your computer system. Your computer system typically has Internet access; your automation system is safer if it does not have Internet access.

As we mentioned, an easy way to segment systems is to use the two independent wired network interfaces on the *groov* Box. Authorized users can see the interface pages *groov* serves, but users do not have access to the system itself.

The image below shows the *groov* Box with the computer system connected to one network interface and the automation system connected to the other. With *groov* Server for Windows, you can accomplish the same segmentation with two NICs (network interface cards) in the PC.



OEMs and machine builders: Use *groov* as machine HMI or for access to machine

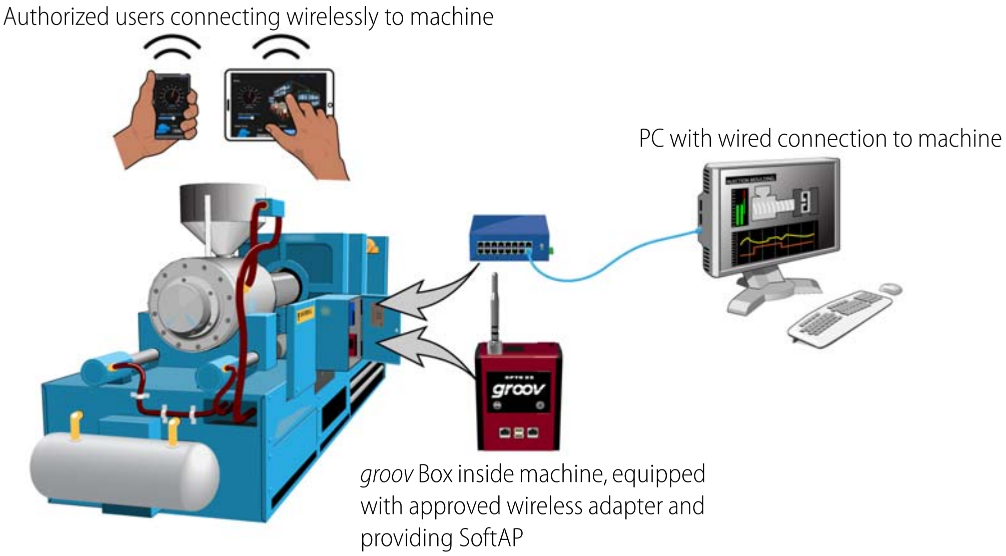
Machine builders and OEMs use *groov* in two ways:

- For an inexpensive, off-the-shelf HMI for machine operators
- To quickly access machines themselves for troubleshooting and updates

The fanless, small-footprint *groov* Box (or *groov* Server for Windows, if your machine already includes a PC) takes up little space.

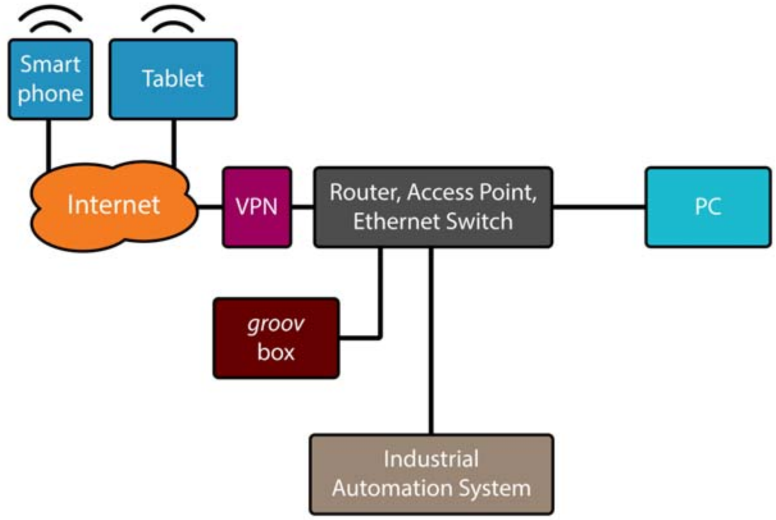
If you use a *groov* Box with an approved WiFi adapter and SoftAP, you can provide a localized wireless network around the Box. See the *groov Box User's Guide* for more information. This diagram shows the *groov* Box inside the machine, accessed using SoftAP.

Or you can build a mobile device into the machine to use as an HMI. On an iPhone or iPad, use Guided Access mode to lock down the device so all it does is show your *groov* interface.


Authorized users connecting wirelessly to machine
PC with wired connection to machine
groov
groov Box inside machine, equipped with approved wireless adapter and providing SoftAP

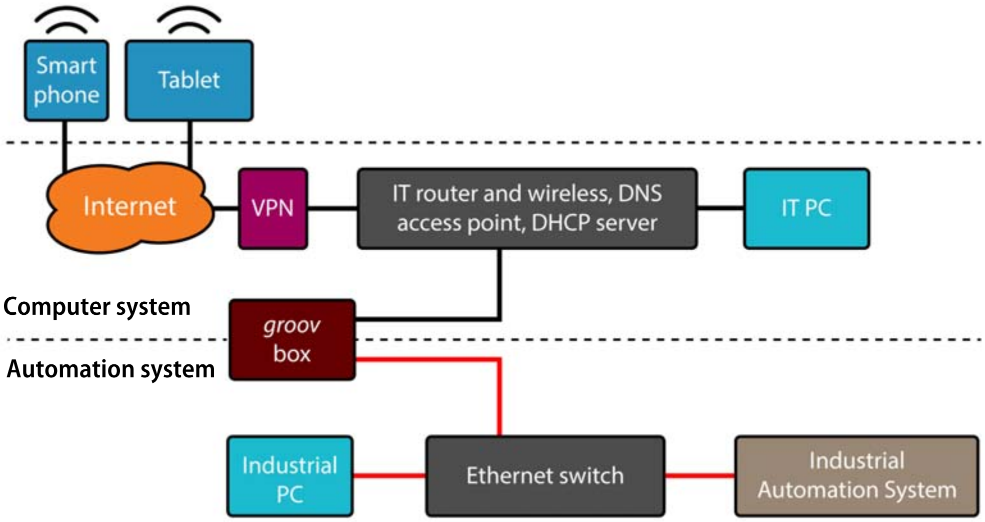
Use *groov* over the Internet, with VPN

When you use a smartphone or tablet to monitor or control systems from outside your facility, you're using the Internet. Or if you're on premises but out of range of a WiFi access point and your phone switches to cellular service, you're using the Internet. For security, we strongly recommend using a VPN (virtual private network) for this type of access.


Smart phone
Tablet
Internet
VPN
Router, Access Point, Ethernet Switch
PC
groov box
Industrial Automation System

Use *groov* over the Internet, with VPN and segmented systems

Here again, for security reasons we advise that you segment your computer system (which is on the Internet) from your automation system (which should not be on the Internet). Keeping your control system separate is one important key to keeping unauthorized people out of your systems. The *groov* Box can simplify segmentation with its two independent Ethernet network interfaces.



What’s next?

Now that you’ve seen some sample network architectures and thought about how you want to use your *groov* interface, let’s see how to do it.

- To use *groov* **in your facility** on a network that is not segmented, see “Single, flat network” on page 13.
- To use *groov* with **segmented systems**, see “Separate network subnets” on page 14.
- To use *groov* **outside your facility or over the Internet** (for example, if you are using *groov* on a smartphone in your facility but are out of range of your wireless LAN), see Chapter 3: Communication over the Internet.

2: Communication within your Facility

Introduction

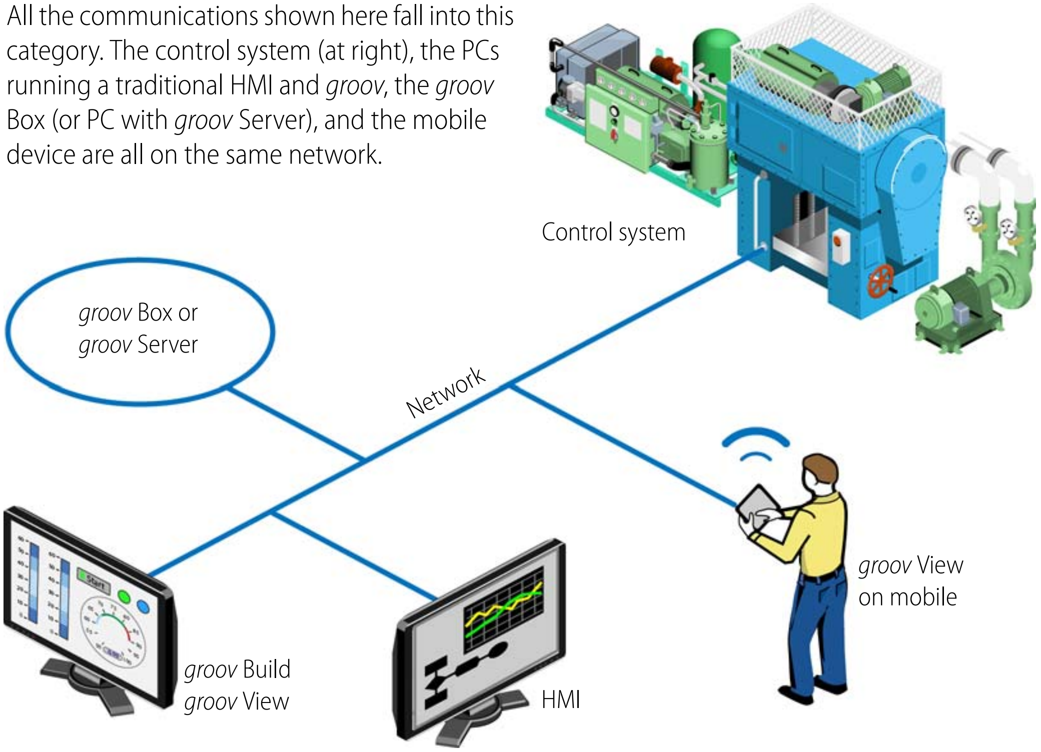
Inside your facility, you may want to have computers and/or mobile devices communicate with your control system. Maybe you want to monitor production numbers, check equipment, operate machinery, or control processes. How you do so depends on your network setup:

- Everything is on one network. See "Single, flat network," below.
- Two or more networks exist—for example, a company computer network and a control system network. See "Separate network subnets" on page 14.

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. You can plug in the *groov* Box and go.

All the communications shown here fall into this category. The control system (at right), the PCs running a traditional HMI 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*	The *groov* Box and the mobile device can join the same existing wireless network. OR the *groov* Box* can create a private WiFi network that the mobile device can join.

* SoftAP requires a GROOV-AR1 with groov Admin v 1.570.39 or higher. See page 16 for more information.

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 may time 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 *groov* Box 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.

You can also set up *groov* Server for Windows in the same way using separate network interface cards (NICs) in the PC: one for your company computer network and one for the control network.

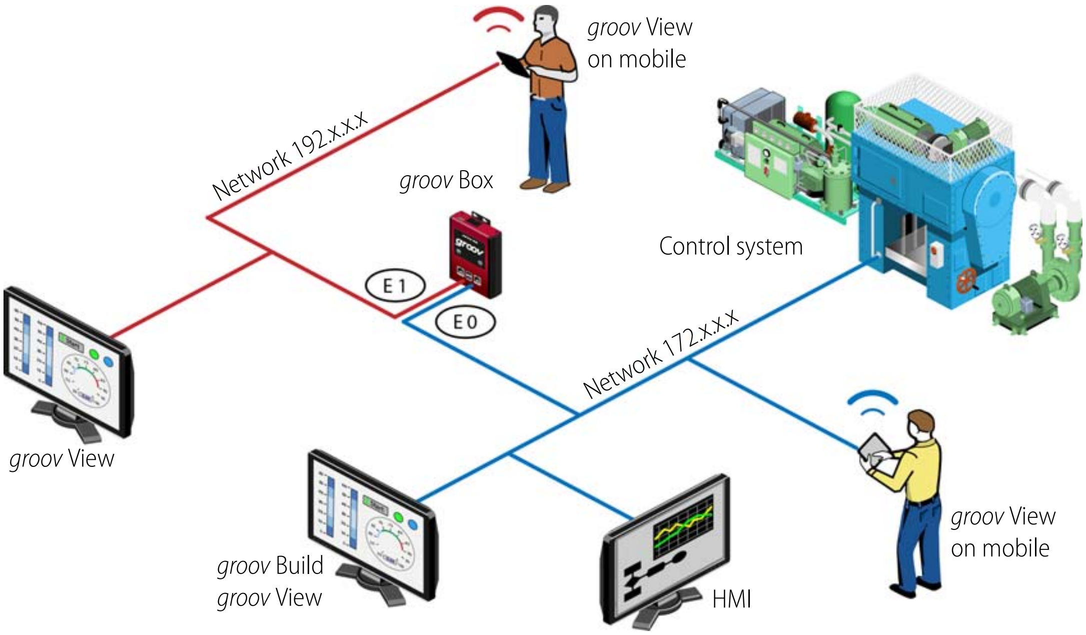
As explained on page 4, the two wired Ethernet interfaces (and the WLAN interface, if present) on a *groov* Box are independent from each other. The same thing applies to two network interface cards (NICs) on a PC. Data packets can't travel directly between the interfaces. The only communication that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

IMPORTANT: *Because their network interfaces are not connected, you must ALWAYS assign the network interfaces on a groov Box* ***different IP addresses and different subnets****. For more information, see the groov Box 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).*

Let's look at two examples of separate network subnets. In both of them, the key advantage to separating networks is security. Only authorized people can see and use the tags configured in the *groov* project, and then only in the ways you allow within the *groov* software.

Separate network subnets with *groov*

Two network subnets offer a secure way to access specific data in specific ways. The following image shows 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 Eth1 and to your control network using Eth0. (You could do the same thing with *groov* Server for Windows running on a PC that has two network interface cards.)

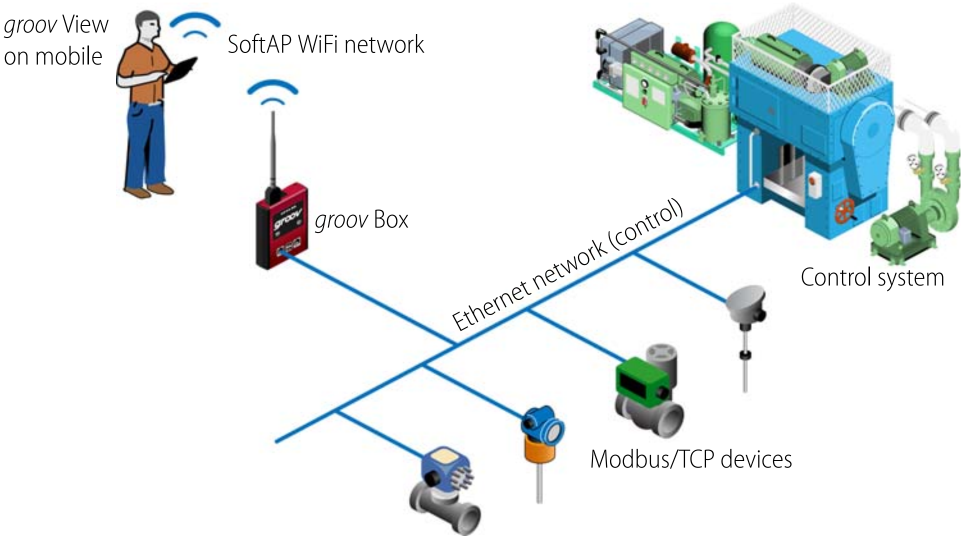
The PCs and mobile devices on the computer network have no direct connection to the equipment on the control network, so employees on these devices cannot access it directly. But the *groov* interface you've built can serve authorized employees the data they need to monitor and take their requests for changes to systems and equipment they are authorized to control. For example, you might give a supervisor the ability to check production figures but not turn a conveyor on or off.

groov Box creating its own WiFi network (SoftAP)

If a wireless network does not exist in your facility but you need to connect wirelessly to *groov,* you can configure a *groov* Box to create its own private WiFi network with WPA2-PSK security.

This feature is called **SoftAP**. It requires a GROOV-AR1 with *groov* Admin v1.570.39 or higher and a compatible USB WiFi adapter. See the *groov Box User's Guide* (form 2104, Chapter 4 and Appendix D) for a list of compatible adapters, plus details on configuring SoftAP and installing the adapter.

The following image shows two network subnets separated by a *groov* Box. The wired Ethernet network is for control. The SoftAP wireless network is for nearby mobile devices using *groov* View; these can include any WiFi-capable device, such as phones, tablets, and laptops.



Again, the mobile devices on the SoftAP WiFi network have no direct connection with the automation equipment on the control network. Authorized employees on mobile devices who join the SoftAP network can see only the data and controls you've built into the *groov* interface.

A similar network architecture can exist on a much smaller scale; for example, a machine builder or OEM can use a *groov* Box with SoftAP to provide local access to machine data and controls through the *groov* mobile app, with no impact on existing IT networks in customer facilities.

To maximize security, **SoftAP cannot be used as a wireless hotspot** and does not allow tethering. That means other devices cannot use it to connect to the Internet. SoftAP works only as an access point for local mobile devices to connect to the *groov* Box.

3: Communication over the Internet

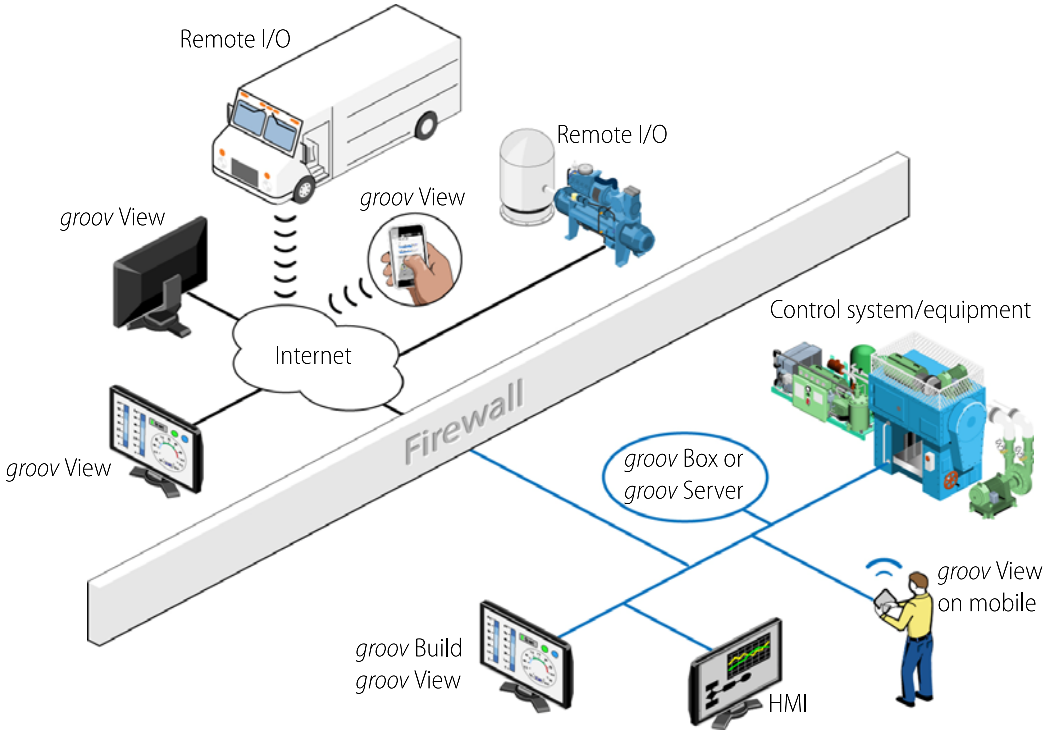
OPTO 22

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. Here are some examples:



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

- A computer in one location can get data from a control system 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.

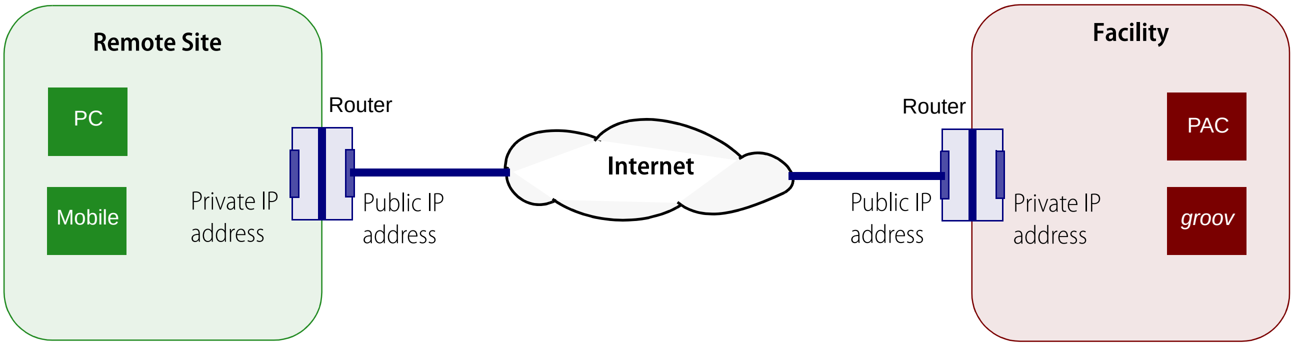
Also, because many companies and steps along the way are outside your control, you should consider the connection tenuous and plan other ways to accomplish what you need to do, in case the link goes down for a short while or for a long time.

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. 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.

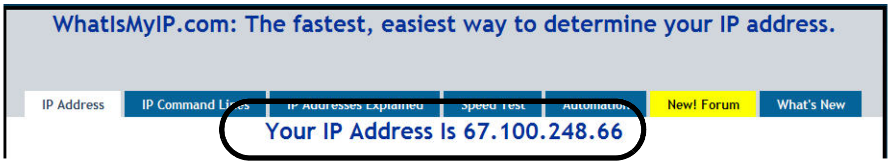
This distinction between the public and private IP addresses on the router becomes important as you set up communication.

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
```



WhatIsMyIP.com: The fastest, easiest way to determine your IP address.

Your IP Address Is 67.100.248.66

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 *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 over the Internet: a virtual private network (VPN) or port forwarding (PF). A VPN is preferred because it is much more secure.

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 a lot like being on site.

Port forwarding may be easier to set up than a VPN but is less 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 that packets of information can 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 21 or "Using port forwarding (PF)" on page 25.

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* 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 (computer with *groov*, or mobile devices with *groov*) 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 22.

Common Communications and Required Ports

Communication between	Communication methods	
	VPN	PF
PC <--> *groov*	Yes	Yes. Use port 443/8443 (TCP)
Mobile <--> *groov*	Yes	Yes. Use port 443/8443 (TCP)

NOTE: Port forwarding for communication between groov and an Opto 22 SNAP PAC controller over a public network is NOT recommended, because the controller does not provide user authentication and encryption. For more information on networking SNAP PAC controllers, see form #1796, the Guide to Networking Opto 22 Products.

Opto 22 Port Usage

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

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

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

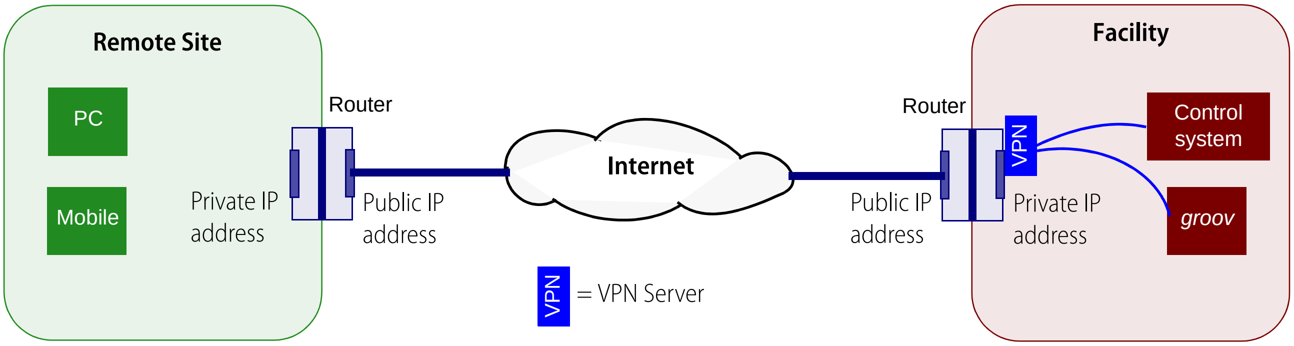
Setting up a virtual private network (VPN)

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

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



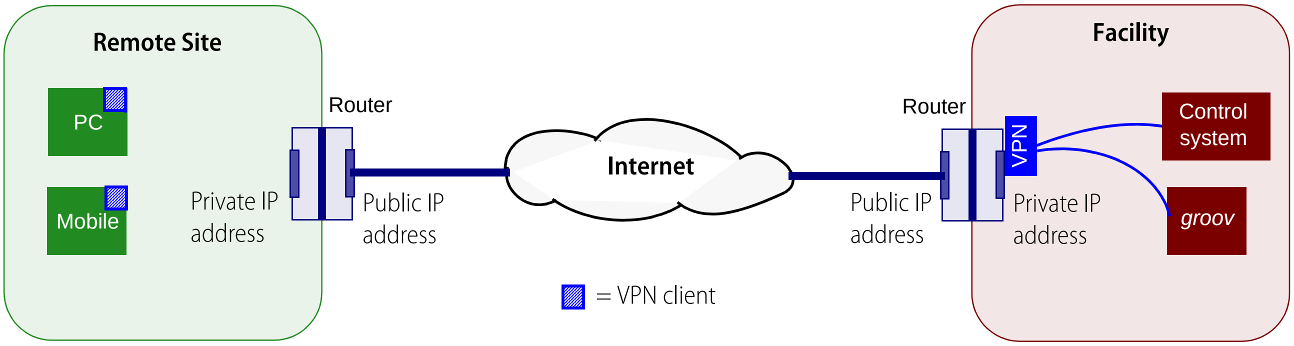
In the router, set up a port forward rule so the router will know to send data through the proper port to reach the VPN server. Port numbers depend on the VPN protocol you're using:

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 control system and groov are at the same location. If they're not, and you need to have groov communicate with a remote PAC? For this scenario, see "VPN special case" on page 24.

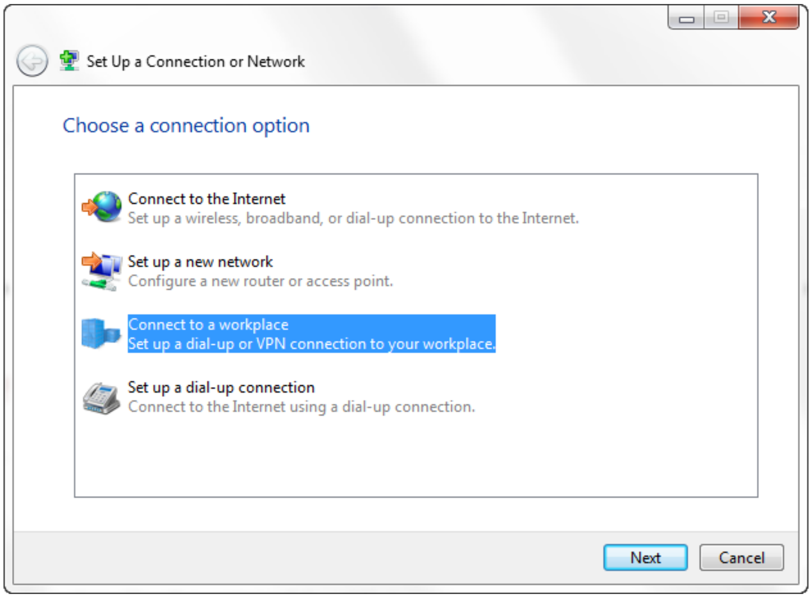
Most current PCs and mobile devices have VPN client software built in. The VPN client must use the same VPN protocol (PPTP, IPSec, OpenVPN) as the VPN server. Some clients give you a choice: for example, the VPN client in iOS devices supports connections to a server using PPTP or IPSec.

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

- VPN: Computer to groov—page 23
- VPN: Android mobile to groov—page 24
- VPN: iOS Mobile to groov—page 24

VPN: Computer to *groov*

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.



Set Up a Connection or Network

Choose a connection option

Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a new network
Configure a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

   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 19.)
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 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`

5. Test your connection: see “Testing communication” on page 27.

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 “Testing groov from inside your facility” on page 27.

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:

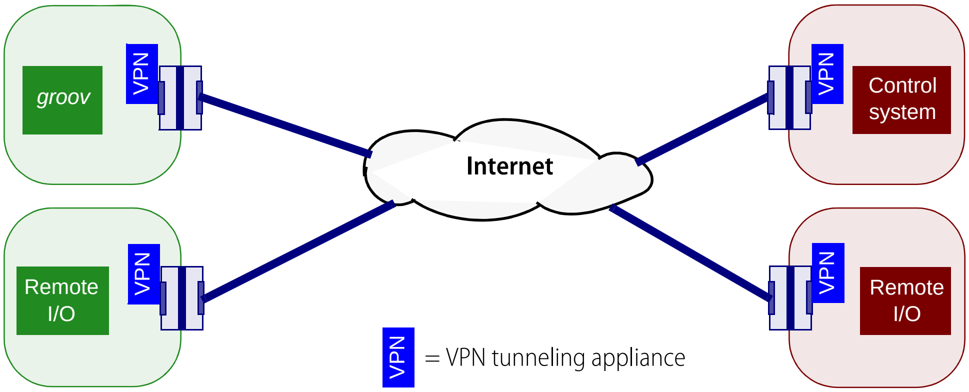
1. When connecting to the VPN, enter your username and password.
2. Once connected, open a web browser and type https:// plus the IP address of the *groov* Box or the PC running *groov* Server for Windows. Example: `https://172.20.52.5`

   If you have problems connecting, see “Testing groov from inside your facility” on page 27.

VPN special case

If your groov Box is in a different location from your control system, you’ll probably need to set up the VPN in a different way: by using a **VPN tunneling appliance** rather than separate VPN server and VPN client. The *groov* Box, as well as many control systems and equipment, cannot be VPN clients nor accept a VPN client. And it is unsafe to use port forwarding unless the controller or device has built-in 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, *groov* and your control system communicate just as if they were on the same local area network.



Using port forwarding (PF)

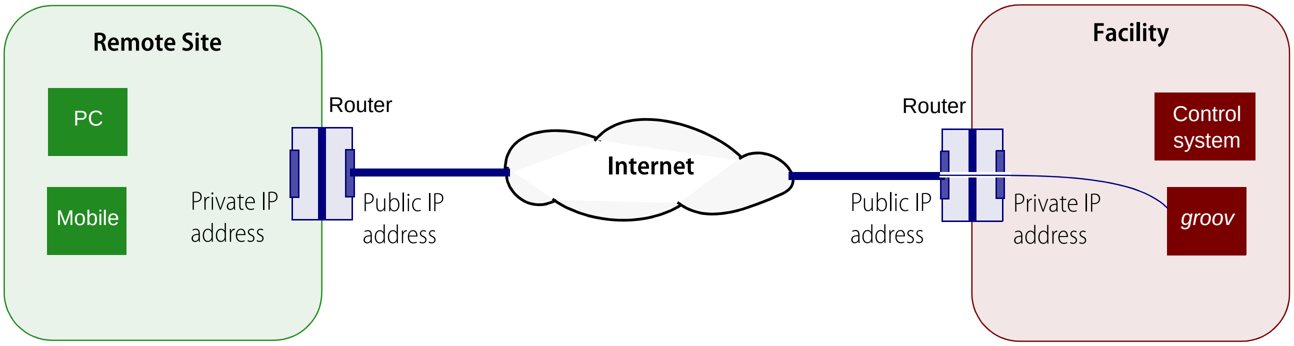
Port forwarding is a less secure way than a VPN to communicate between a PC or mobile device and *groov*, but it may be an acceptable option if:

- 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 18 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 data packets to get through to the private network. PF is less secure than a VPN because a VPN creates a layer of authentication and encryption which may or may not be present with PF. PF can work with *groov* because *groov* provides encryption and 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* provides encryption and 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 26).
- Set up port forwarding on the client PCs or mobile devices (page 27).

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 19). 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 19).

Establishing port forward rule(s)

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

NOTE: Sometimes changing the port number is recommended, but because changed port numbers are easy to discover, this "security by obscurity" suggestion provides no real extra security. If you make a port forward rule that port 4321 goes to port 443 of the groov Box's IP address, 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 21. For more general information on ports, see "port" on page 31.

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 "Testing groov from inside your facility" on page 27.

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.

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 to 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 19.

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.

client

In the client-server model of computer networking, a *client* requests data or services that are then supplied by a server on the same network. A client is typically a software program. For example, a client such as Microsoft Word might request a print server on the network to print a Word document.

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 `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 accessible via fully qualified hostnames that contain the same domain name. The *domain name* 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 and transport protocol. For example, a *groov* Box can communicate with Modbus/TCP devices, a SNAP PAC controller, and an OPC UA server, all at once using the same IP address and protocol.

Each of these "services" uses a unique protocol and *port* number combination (for example, TCP 443 or UDP 443) for communication. The combination of IP address/protocol/port number keeps communication running smoothly. It's like an apartment building where all the apartments have the same street address (IP address and protocol), 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 IP address and forwards it based on established rules 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).

server

In the client-server model of computer networking, a *server* shares resources and data among clients on the network. The server provides data or services when requested by a client.

For example, print servers manage and allocate printer resources for a network; file servers store and allow access to folders and files needed by multiple users on a network; web servers present web pages to clients like PCs, tablets, and smartphones.

softAP

A software-enabled access point, or *softAP,* is software that turns a computer device into a WiFi access point. The typical use is to allow other devices to access the Internet through the device that has softAP. A softAP can also be used to create a separate WiFi network not connected to the Internet, as in the *groov* Box.

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, limiting access to specific IP addresses unless communication passes through a router. All devices with the same network prefix (calculated by a bitwise AND between the subnet mask and the IP address) are on the same LAN or subnet.

When you configure a device 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 `192.168.1.254`*.

	Network	Node
Subnet mask	255.255.255.0	
Beginning IP address	192.168.1.0	
Ending IP address	192.168.1.254	

* The last address (x.x.x.255) is reserved for subnet-directed broadcasts.

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.

Article from Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team: Resources for Cybersecurity

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

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/