GUIDE TO NETWORKING GROOV PRODUCTS

OPTO 22

The Edge of Automation.™

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

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

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*, *groov* EPIC, *groov* RIO, mobile made simple, The Edge of Automation, 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, PAC Project Basic, PAC Project Professional, 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. ARCNET is a registered trademark of Datapoint Corporation. Modbus is a registered trademark of Schneider Electric, licensed to the Modbus Organization, Inc. Wiegand is a registered trademark of Sensor Engineering Corporation. Allen-Bradley, CompactLogix, ControlLogix, MicroLogix, SLC, and RSLogix are either registered trademarks or trademarks of Rockwell Automation. CIP and EtherNet/IP are trademarks of ODVA. Raspberry Pi is a trademark of the Raspberry Pi Foundation. The registered trademark Ignition by Inductive Automation® is owned by Inductive Automation and is registered in the United States and may be pending or registered in other countries. CODESYS® is a registered trademark of 3S-Smart Software Solutions GmbH.

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
The Edge of Automation.

Table of Contents

1: Networking Basics

INTRODUCTION

We live in an increasingly connected world. Wearables and other intelligent devices (both stationary and mobile) 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. Why shouldn't your smartphone be able to show you a dashboard with data for remote pumps and pressures, or this shift's production compared to the past?

Engineers also want to take advantage of new advances like artificial intelligence (AI) to get data out of systems and equipment, process and analyze that data, and use it to improve products and processes. Do you need accurate usage data to bill customers, or environmental data tracked for compliance? Could machine failures be prevented and stoppages avoided by preventive maintenance? It's becoming easier to do all these things and many more.

Today, automation systems like Opto 22's *groov* EPIC® and *groov* RIO® are moving away from proprietary buses, instead offering standard networks and protocols—like IEEE 802.3 Ethernet, OPC UA, and MQTT—to connect more easily with both operation technology (OT) and information technology (IT) devices and software. Standard networks and protocols make it easier to communicate with computer systems, cloud services, and mobile devices to provide the information and control you need.

However, networking these devices and software and getting them to talk to each other isn't easy—and it opens up security issues that might not have been a concern in the past. Networking can be a complex subject.

This guide tries to reduce the complexity by providing guidelines for setting up communications among your *groov* products, other automation systems and equipment, and software or services either on premises or in the cloud.

groov products at the edge

Your equipment and the data it holds are at the edge of your network, whether they're at a remote location or in the same building. The edge is where the network meets the physical world of sensors and actuators: where the data is produced. *groov* EPIC, *groov* RIO, and the *groov* Box Edge Appliance are products designed for the edge—industrially hardened and ready to connect.

groov EPIC

Opto 22's *groov* EPIC is an edge programmable industrial controller. At its core, *groov* EPIC is an industrial control system with I/O modules—analog, discrete, and serial—but as a Linux®-based processor it also provides data handling, visualization, and connectivity tools for the edge.

Standard internet and IT-compatible tools are built into *groov* EPIC. Tools include:

- Node-RED for creating simple data flows from pre-built nodes
- RESTful APIs to PAC Control variables, *groov* I/O, and *groov* View Data Stores
- Either full Ignition or Ignition Edge® from Inductive Automation®
  - Ignition Edge provides OPC-UA drivers and the lightweight MQTT transport protocol (with Sparkplug, strings, or JSON payload).
  - Full Ignition includes OPC UA and MQTT, and also adds external access to the OPC-UA server, scripting, database support, and a wide array of optional Ignition modules.
- MQTT
- *groov* View HMI software
- VPN client
- LDAP support (*groov* EPIC firmware version 3.0 and higher)

groov RIO

groov RIO provides edge I/O: intelligent, distributed I/O at the edge, connecting directly to sensors and equipment and communicating their data where you need it. With its multifunction, multi-signal, software-configurable channels, *groov* RIO accommodates most field signals required by analog and discrete sensors and equipment.

To help you access and communicate data, *groov* RIO includes the following:

- Node-RED
- RESTful APIs to I/O
- MQTT
- VPN client
- LDAP support (*groov* RIO firmware version 3.0 and higher)

groov Box

The *groov* Box edge appliance has no I/O and is not a controller; it is an edge gateway device designed to communicate data among automation systems, software, databases, and devices and to serve *groov* View HMI pages to authorized users. Included with the *groov* Box are:

- Node-RED
- RESTful API to *groov* View
- Ignition Edge, offering OPC-UA drivers and MQTT communications
- *groov* View HMI software

To compare *groov* product features and specifications, see the *groov Product Comparison Chart* on the Opto 22 website (Products > Product Comparisons > Compare *groov* Products).

What's in this Guide

This guide shows you how to communicate with *groov* using wired Ethernet networks and wireless LANs. It does not cover serial networking or other kinds of networks.

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 communications internally, on one or more networks

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 system security, many good resources are available online. See "Resources" on page 33.

Related Documents

Be sure to check the user's guides for help with *groov* products. All guides are available under Help in the product itself (in *groov* Manage or *groov* Admin), and the most recent versions 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	Contents	Form #
groov EPIC User's Guide	Installing and using a groov EPIC system; using Node-RED, MQTT, and Ignition or Ignition Edge	2267
groov RIO User's Guide	Installing and using a groov RIO module; using Node-RED and MQTT	2324
groov Box User's Guide for GROOV-AR1	Installing the *groov* Edge Appliance; using Node-RED and Ignition Edge	2104
groov View User's Guide	Using *groov* View to build an operator interface that runs on computers and mobile devices	2027
groov Server for Windows User's Guide	Installing and using *groov* Server on a Windows computer	2078
Getting Started with MQTT in groov Products	Choosing MQTT methods and setting up MQTT communications in *groov* EPIC and *groov* RIO	2350

OptoForums

OptoForums focused on *groov* products and their tools are available 24 hours a day, 7 days a week, so you can get advice from experienced *groov* product users:

- *groov* EPIC Forum
- *groov* RIO Forum
- Node-RED Forum
- Ignition Edge Forum
- *groov* View Forum

Product Support

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

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

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

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, a YouTube video get to your smartphone, or a value from a sensor get to your computer?

Request and response

Computers communicating on a network typically use the request-response model. (Next we'll look at a *publish-subscribe* model, which is different.) In the request-response model, a client computer or software requests data or services, and a server computer or software responds to the request by providing 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 responds to the request and 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 responds by serving the video page to you, along with the other millions of video pages going to other millions of viewers worldwide.

Example: Node-RED nodes are clients and send requests

Within *groov* EPIC, *groov* RIO, and the *groov* Box, the nodes you use in your Node-RED flows are clients. They send requests to servers to request resources (like data from an online analysis service) or services (like pushing data to a database).

Example: *groov* View is a server and responds to requests

A *groov* product that runs *groov* View (like *groov* EPIC or the *groov* Box) acts as a web server for your *groov* View HMI. At the request of clients like authorized smartphones and tablets, *groov* View responds by serving the interface pages you've created to these clients on the network.

Special case: Ignition Edge is a server

In *groov* EPIC and the *groov* Box, Ignition Edge provides an internal OPC-UA server and drivers. *groov* View and Node-RED are the only clients for the Ignition Edge OPC-UA server; they send requests to it from within the EPIC or Box using a local address. No outside clients can access the internal Ignition Edge OPC-UA server.

However, if you run full Ignition in *groov* EPIC, external clients as well as internal ones can access the OPC-UA server.

Publish and subscribe

A different way for devices to communicate on a network is called publish-subscribe, or *pub-sub*. In a pub-sub architecture, a central server called a *broker* receives and distributes all data. Pub-sub clients can publish data to the broker or subscribe to get data from it—or both.

Clients that publish data send it only when the data changes. Clients that subscribe to data automatically receive it from the broker, but again, only when it changes.

The broker does not store data; it simply moves it from publishers to subscribers. When data comes in from a publisher, the broker promptly sends it off to any client subscribed to that data. You can think of data from a publisher as an incoming shipment on a truck. The broker sees the truck come in but doesn't unload it; it simply routes it intact to a subscriber (cloning the truck if there's more than one subscriber).

MQTT—a pub-sub protocol

MQTT (formerly MQ Telemetry Transport) is a standard, open-source transport protocol that uses the pub-sub architecture. MQTT is extremely lightweight: it takes up almost no space in a device, so that even small devices with very little computing power can use it.

In our analogy, MQTT defines the truck and the routes. But it doesn't define how the load (the data) is packed or unpacked. Two payloads often used with MQTT are Sparkplug and plain-text strings.

MQTT with Sparkplug payloads

The Sparkplug B open-source MQTT client specification provides a messaging format appropriate for industrial use. Sparkplug encodes the data payload: it defines how the data is packed on the truck before it's sent by the publisher, and how it is unpacked in the subscriber.

Data sent over MQTT with a Sparkplug payload is encoded for efficiency and can be compressed. MQTT trucks that have been packed with the Sparkplug definition must also be unpacked with Sparkplug, so both publishers and subscribers must use it in order to understand the data.

MQTT with Sparkplug payloads also provides an efficient way to track the state of clients and make sure that clients on a tenuous connection can still deliver or receive data. If the client goes offline (breaks its connection with the broker), the broker sends a "death certificate" to clients subscribed to that data. When the client comes back online (re-establishes the connection), the broker issues a "birth certificate" with the current status of all data tags. A certain amount of missed data can also be sent, depending on client configuration.

MQTT with string payloads

An alternative payload is strings. MQTT with strings payload is useful for simple applications that typically require data from your *groov* product only.

Comparison: request-response and pub-sub

In a request-response architecture, each client must open a direct connection to each server, because the client requests data directly from the server. Also, because the client doesn't know when data may change, it must request it at regular intervals. So clients are repetitively sending requests to servers—often once per millisecond—and servers are repetitively responding:

Q: What's the sensor value? A: 10
Q: What's the sensor value? A: 10
Q: What's the sensor value? A: 10
Q: What's the sensor value? A: 10
Q: What's the sensor value? A: 10
Q: What's the sensor value? A: 9
Q: What's the sensor value? A: 9

If you have multiple servers and multiple clients, the volume of traffic can quickly become a problem. Below you see an example of the request-response model. Each client is individually connected to each server it needs to request data from, and each connection may even be opened, queried, answered, and shut, over and over:

Request-response architecture
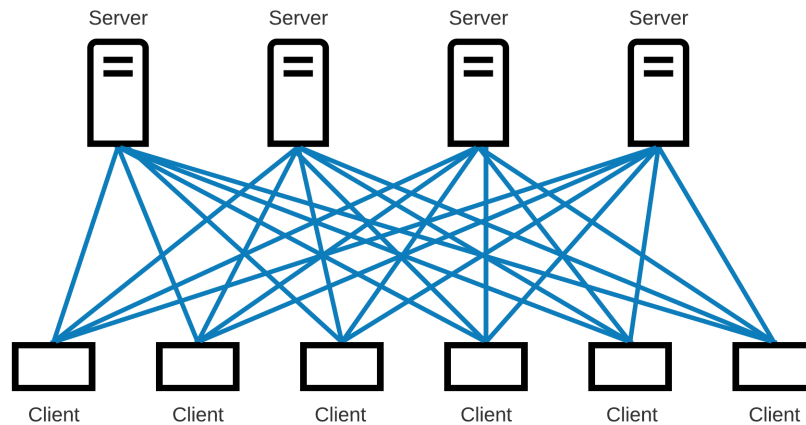
In contrast, a pub-sub architecture simplifies communications. Direct connections and repetitive requests for data are not needed. The web of links is replaced by a single link from each device to the broker. The connection between client and broker is kept open and is incredibly lightweight. Only two things travel over this connection: changed data, and a tiny heartbeat to let the broker know that the client is still there.

Publish-subscribe architecture
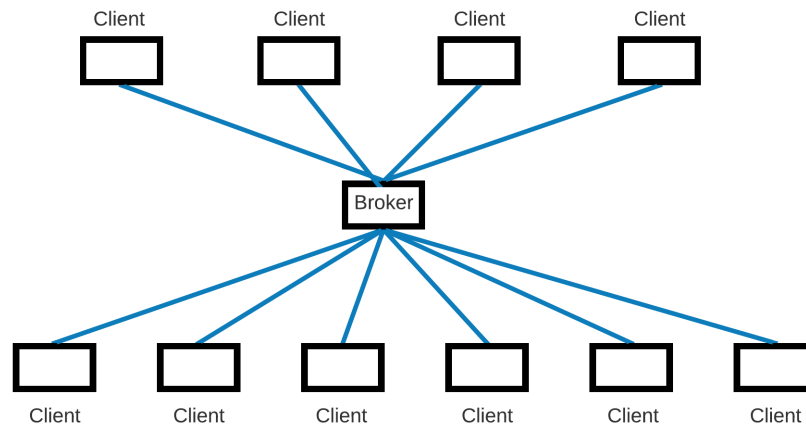
MQTT in IIoT applications

For industrial internet of things (IIoT) applications, MQTT pub-sub transport can offer several key advantages over request-response:

- All data is published using a device-originated connection (also called an *outbound* connection). Firewalls typically block inbound traffic (for example, an external client requesting data from an internal server), but allow outbound connections over TCP ports. Because all connections are device originated (for example, from the *groov* device to the broker), no ports need to be open, and neither a VPN nor port forwarding is required.

- Once the connection has been made, data can travel in both directions.

- Since the broker is the central clearinghouse for data, individual servers don't have to strain to serve multiple clients, and clients don't have to connect to multiple servers.

- Network traffic is reduced overall, because data is published and sent only when it changes, rather than at regular intervals.

- Because payloads can be compressed and data moves efficiently, even remote devices with irregular connections or low bandwidth can publish or subscribe to data.

- Devices that go offline can reconnect with the broker, sending or receiving current data and (optionally) a specified amount of buffered data to help fill in the gap.

MQTT in *groov* products

Depending on your *groov* device, MQTT transport is available directly through the *groov* product itself, through Node-RED, or via Ignition. For long-term use of MQTT via Ignition or Ignition Edge, you'll need a *groov* Edge license (GROOV-LIC-EDGE), but you can try it on a repeatable two-hour trial for free.

The following table summarizes your choices for using MQTT with *groov* products. For more information on payloads and steps to set up MQTT, see form 2350, *Getting Started with MQTT in groov Products*.

MQTT Method	*groov* EPIC	*groov* RIO	*groov* Box
MQTT with strings payload	Yes	Yes	Yes
• MQTT tools available	*groov* Manage Node-RED	*groov* Manage Node-RED	Node-RED
• Publish data from:	*Using groov Manage:* • *groov* EPIC local I/O • PAC Control strategy running on *groov* EPIC (including variables and data from I/O units) *Using Node-RED:* Any Node-RED payload	*Using groov Manage:* *groov* RIO local I/O *Using Node-RED:* Any Node-RED payload	Any Node-RED payload
• License required	None	None	None
MQTT with Sparkplug B payload sent via *groov* Manage	Yes	Yes	No
• MQTT tools available	*groov* Manage	*groov* Manage	
• Publish data from:	• *groov* EPIC local I/O • PAC Control strategy running on *groov* EPIC (including variables and data from I/O units)	*groov* RIO local I/O	
• License required	None	None	
MQTT with Sparkplug B payload sent via Ignition/Ignition Edge	Yes	No	Yes
• MQTT tools available	Ignition Edge or full Ignition*		Ignition Edge only
• Publish data from:	• *groov* EPIC processors • SNAP PAC controllers • PAC Control strategy running on *groov* EPIC • *groov* RIO modules • SNAP PAC I/O units • Allen-Bradley® PLCs • Siemens® PLCs • Modbus®/TCP devices		• *groov* EPIC processors • SNAP PAC controllers • *groov* RIO modules • SNAP PAC I/O units • Allen-Bradley PLCs • Siemens PLCs • Modbus/TCP devices
• License required	GROOV-LIC-EDGE or full Ignition license**		GROOV-LIC-EDGE

* Other data sources are available by using additional Ignition modules.
** Contact Opto 22 or Inductive Automation.

IP addresses

How does a client reach a server or a broker? It's similar to the way you call someone on your cell phone. You tap their name or number, the phone dials it, 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 or enter a domain name like youtube.com or opto22.com.

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

Sometimes a computer network is very small—so small that both client and server in a request-response architecture are on the same computing device. 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`
* When your *groov* View operator interface and your Node-RED project on your *groov* Box get data from the internal Ignition Edge OPC-UA server, they access the server by using the localhost address and port.

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 11).

But many companies have more than one LAN. You may have your *groov* EPIC 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, but inside the router there is no direct connection between the two. Because there is no direct connection, communication between the two networks can occur only if the software rules inside the router allow it. These software rules typically include routing tables and network address translation (NAT).
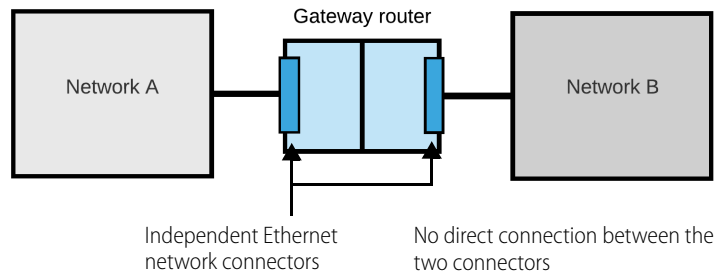
Software rules (routing tables, network address translation) determine whether and how communication moves between Network A and Network B.

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

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

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

Network interfaces in *groov* products

All *groov* products are designed to automatically connect to a standard Ethernet network with a DHCP server, which provides the device's IP address. All you have to do is plug the Ethernet cable into the lowest-numbered Ethernet interface on the device, and it automatically connects to the network. However, *groov* products also offer more complex networking options.

Like gateway routers, *groov* EPIC processors and the *groov* Box each have two independent Ethernet network interfaces. *groov* RIO modules, in contrast, have two switched network interfaces that are not independent.

This difference in *groov* products is significant for networking.

groov EPIC and *groov* Box: two independent interfaces

Although *groov* EPICs and *groov* Boxes are not routers (because they do not provide routing or address translation), their separate interfaces work like a router's interfaces. When you use both of these independent interfaces, each must be wired to a separate network—that is, their network addresses (a combination of IP addresses and subnet masks) must be different. So if your trusted network (perhaps your control network) is wired to ETH0 on *groov* EPIC and your untrusted network (such as a computer network with internet access) is wired to ETH1, the two networks are segmented. Data packets cannot travel between them.

For example, if your EPIC serves a *groov* View 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.

The software in your *groov* EPIC or *groov* Box determines the data an authorized user can see and change.
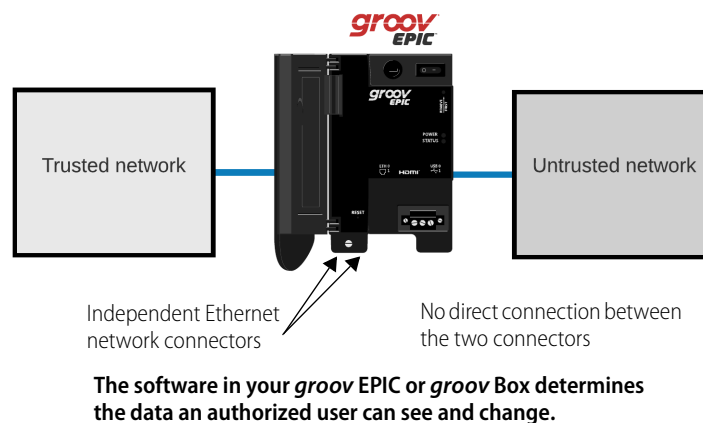
Remember: You must **ALWAYS** assign the two network interfaces on a groov EPIC or groov Box different IP addresses and different subnets. For more information, see the product's user's guide. Note that it doesn't matter which interface you use for each network except for initial setup, when you must use the lower-numbered interface.

groov RIO: two switched interfaces

The two wired network interfaces on a *groov* RIO module are not independent; they are connected. A *groov* RIO module acts as a two-port switch, with one port going to the module and the other port allowing a connection to one other device. These modules can therefore be daisy-chained. Daisy-chaining has advantages and disadvantages and must be done correctly in order to work. See Chapter 6 in the *groov RIO User's Guide* for details.

NOTE: You cannot daisy-chain groov RIO modules that are using Power over Ethernet (PoE).

groov EPIC, *groov* RIO, and *groov* Box: optional wireless network

groov EPIC, *groov* RIO, and the *groov* Box can also communicate wirelessly, through one approved USB WiFi adapter connected to a USB port on the device. This wireless network is independent from either wired network, so no communication or routing can occur between them.

groov EPIC and *groov* RIO: VPN client

groov EPIC and *groov* RIO also include an OpenVPN client for establishing a virtual private network (VPN) connection. The VPN can be connected through Ethernet or WiFi.

Summary: *groov* Product Networking Options

Option	*groov* EPIC	*groov* RIO	*groov* Box
Two independent Ethernet interfaces	x		x
Two switched Ethernet interfaces		x	
Wireless network via USB WiFi adapter	x	x	x
OpenVPN client	x	x	
Total possible IP addresses	4	3	3
Total possible independent network connections	3	2	3

In *groov* EPIC and *groov* RIO, you can configure all networks through *groov* Manage. In the *groov* Box, use *groov* Admin to configure networks. See the device's user's guide for more information.

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 network.** This one's easy; see "Single flat network" on page 11.
- Devices are on **separate network subnets** or LANs within the same location. For example, you are using the two Ethernet interfaces on a *groov* EPIC processor to separate a trusted network from an untrusted network. To communicate between two networks like this, see "Two or More Networks" on page 13.
- Networks are geographically separated from each other, so **communication must go over the internet.** For example, you have a *groov* EPIC at your main location and *groov* RIOs at remote sites. For these kinds of remote communication, see Chapter 3: Communication over the Internet on page 15.

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 control processes, operate machinery, send equipment data to a database or spreadsheet, or monitor production numbers. 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 trusted control network and an untrusted computer network that has internet access. See "Two or More Networks" on page 13.

SINGLE FLAT NETWORK

Use *groov* products in your facility with an existing Ethernet network

A single network simplifies setup. If you are using *groov* products within your facility only (not remotely) and you already have a wired Ethernet network in place for your automation system, you can just plug your *groov* product in. As long as your network uses DHCP and DNS, the *groov* product will be automatically assigned an IP address and be visible on the network, just like a computer. (If your network does not use DHCP/DNS, you can assign a fixed IP address to your *groov* product.)

Authorized users (human or software) can use data, or monitor and control equipment, as long as they are on the same wired Ethernet network. The diagram on the next page shows the basic architectural components:

- You plug your *groov* product(s) into the single Ethernet network, which includes the industrial automation system.
- *groov* EPIC and *groov* RIO can connect directly to sensors and equipment to monitor, control, and acquire data from them.
- *groov* EPIC runs a control program you build on a network PC using PAC Control, CODESYS, or secure shell access.
- *groov* RIO can act as remote I/O in the control system or communicate data independently.
- *groov* Box has no I/O but can collect and communicate data using Ignition Edge or Node-RED.
- Node-RED in *groov* EPIC, *groov* RIO, and the *groov* Box can connect to computers on the network running software such as SCADA systems, building automation systems, and databases that use and store data.
- Ignition or Ignition Edge in *groov* EPIC, or Ignition Edge in the *groov* Box, can use OPC UA to connect to PLCs as well as Modbus devices and software. Full Ignition on *groov* EPIC opens many other possibilities.
- You can build a *groov* View HMI on any computer on the same network and serve the HMI pages from your *groov* EPIC or *groov* Box (or *groov* Server for Windows running on the PC).
- Authorized users can access data and use your HMI from computers on the same wired network.

Here's how a single flat network like this might look:
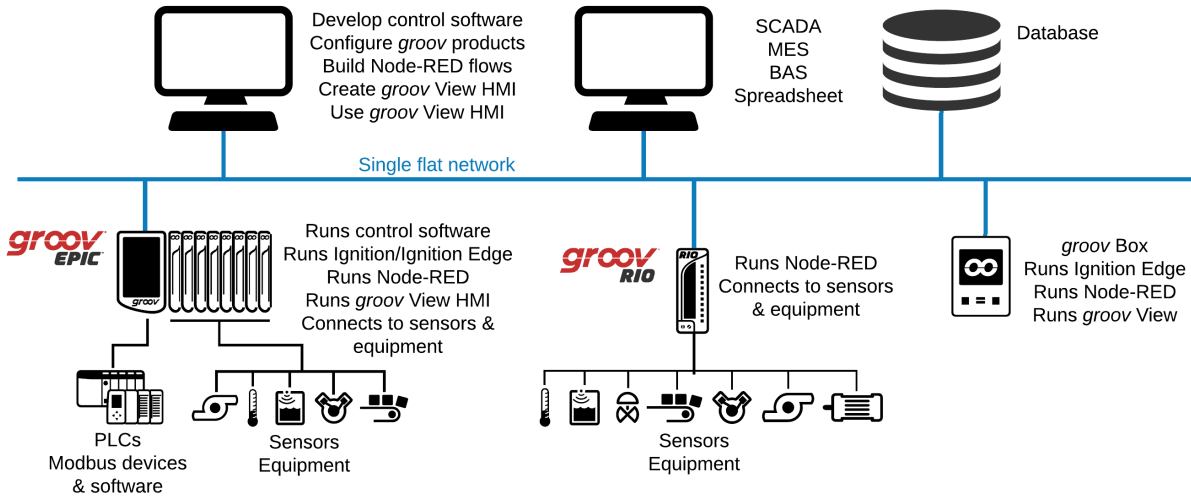
Adding mobile devices. For users on mobile devices, you can add wireless access points. With a WiFi connection, authorized users on tablets and phones can also configure *groov* EPIC and *groov* RIO and use your HMI. Authorized users on laptops with WiFi can do the same things as a user on a wired computer.
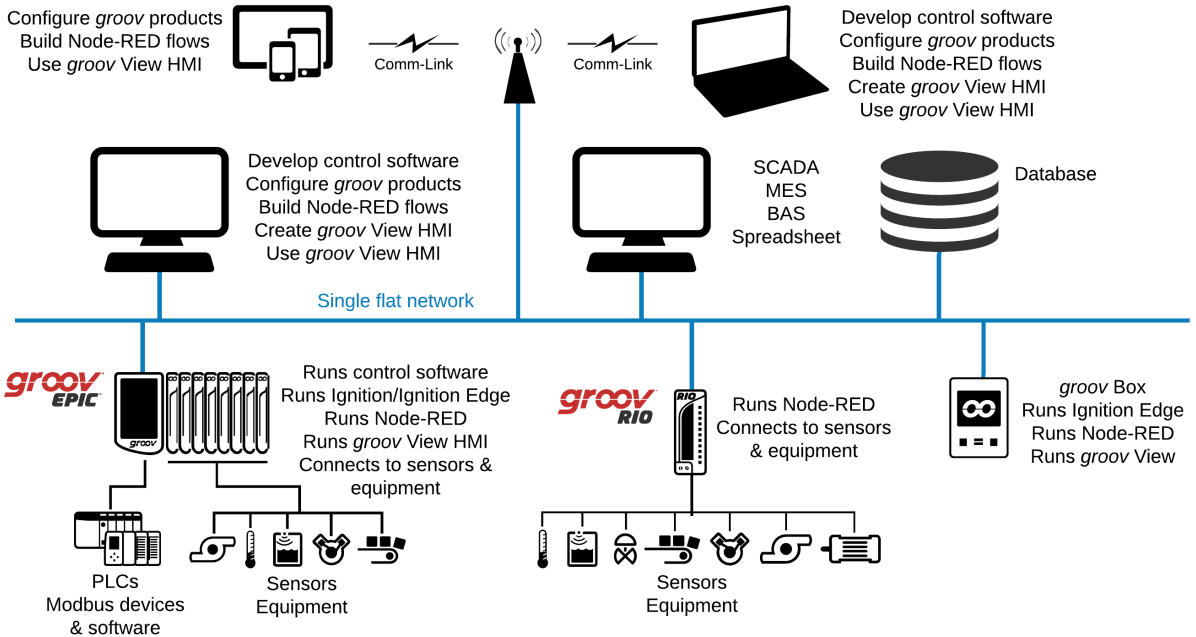
Notes for mobile communication with a *groov* View operator interface

If you're using a smartphone or tablet on your local network to connect with a *groov* View operator interface, 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)

TWO OR MORE NETWORKS

Use independent interfaces to improve security

For security reasons, we strongly recommend segmenting networks to keep control systems safe. You can choose to take advantage of the multiple network interfaces on your *groov* EPIC or *groov* Box to separate your trusted network traffic from your untrusted network. Your automation system should not have internet access, while your company computer system typically needs internet access.

As we saw on page 9, the two wired Ethernet interfaces on a *groov* EPIC or *groov* Box are independent. Data packets cannot travel directly between the interfaces. So, for example, users can use pages in *groov* Manage or *groov* View that they are authorized to view, but they cannot access the rest of the control system.

On *groov* RIO, the two Ethernet interfaces are not independent. However, an approved WiFi adapter connected to a USB port on any *groov* product is independent from its wired interfaces.

*Remember: You must **ALWAYS** assign the independent interfaces on a groov product different IP addresses and different subnets. For more information, see the product's user's guide.*

The image below shows an example of networks segmented by a *groov* EPIC processor. The 192.x.x.x network is for company computers not directly involved in the control network. The 172.x.x.x network is for control.
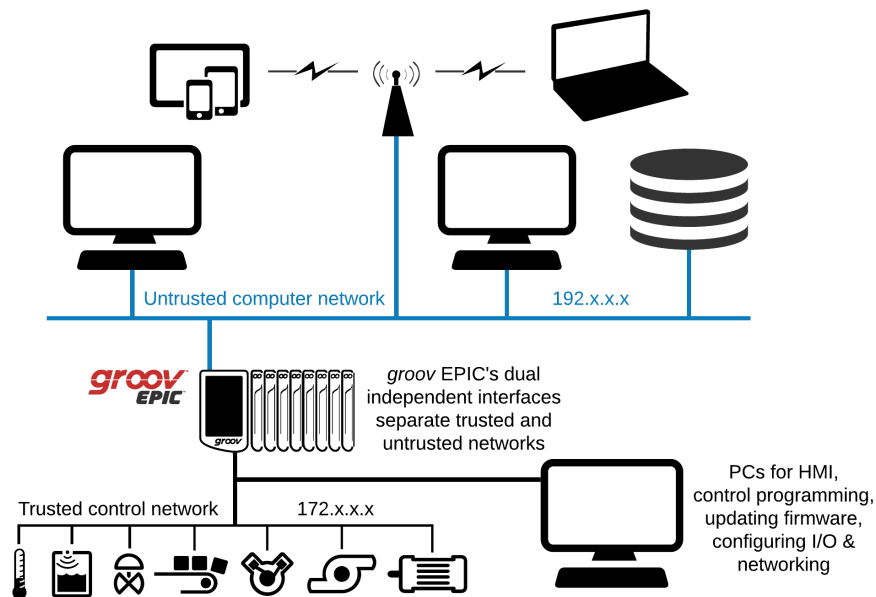
NOTE: It doesn't matter which wired interface you use for each network, except that when you first plug a groov EPIC or groov Box into the network, you must use its lower-numbered interface for initialization.

Solve facility network issues with MQTT

Sometimes a facility has multiple networks, for example, separate networks for controlling each process plus a separate network for office computers. Using control data in the office network can be problematic, involving IT expense, time, and security concerns.

One effective way to solve these problems is to use MQTT in your *groov* product to communicate data among networks. Instead of setting up firewalls and VPNs for each network, place a *groov* RIO, *groov* EPIC, or *groov* Box on each control network and enable MQTT. You'll also need to set up a local MQTT broker on premises.

The image below shows a *groov* RIO module attached to each control network. The *groov* RIO can connect directly to sensors and equipment on the control network and communicate their data via MQTT out of the box, with no additional expense required. The office database subscribes to data from all the *groov* RIOs, making that data available for tracking, analysis, and historization. Because MQTT communication is device-originated (in this example, from each *groov* RIO to the broker), each control network remains secure.
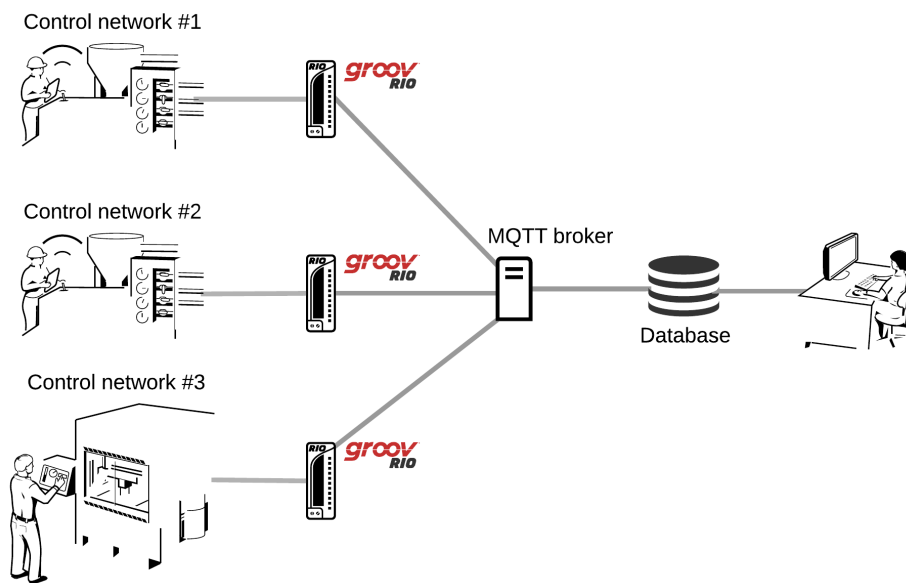
Add a wireless network for mobile users (*groov* Box only)

If a wireless network does not exist in your facility, but mobile device users need to connect wirelessly to *groov* products (for example, to use a *groov* View HMI), you can configure a *groov* Box to create its own private WiFi network with WPA2-PSK security. This feature is called **SoftAP** (software enabled wireless access point).

To set up SoftAP, you'll need a GROOV-AR1 with groov Admin v1.570.39 or higher, and an approved wireless adapter. See the *groov Box User's Guide* (form 2104, Chapter 3 and Appendix D) for a list of compatible adapters, plus details on configuring SoftAP and installing the adapter.

For example, you could separate two network subnets with a *groov* Box., using a wired Ethernet network for control and the SoftAP wireless network for nearby mobile devices using *groov* View. Authorized employees on mobile devices who join the SoftAP network can see only the data and controls you've built into the *groov* View 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* View 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

BEYOND YOUR FACILITY: 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 there are very good reasons to communicate with your control system from a different network, miles away. Here are just a few:

- Status data from remote equipment must be tracked and stored for regulatory requirements.
- Production managers need to know widget production for the last hour, even while they're traveling.
- A technician sees an alarm for another building and needs to quickly switch from pump #1 to pump #2.
- An OEM wants to access their machines at customer sites, for operational data and machine updates.

This is the industrial internet of things (IIoT) at work: when two or more networks are connected to the internet, devices on them can communicate. The following image shows some examples:
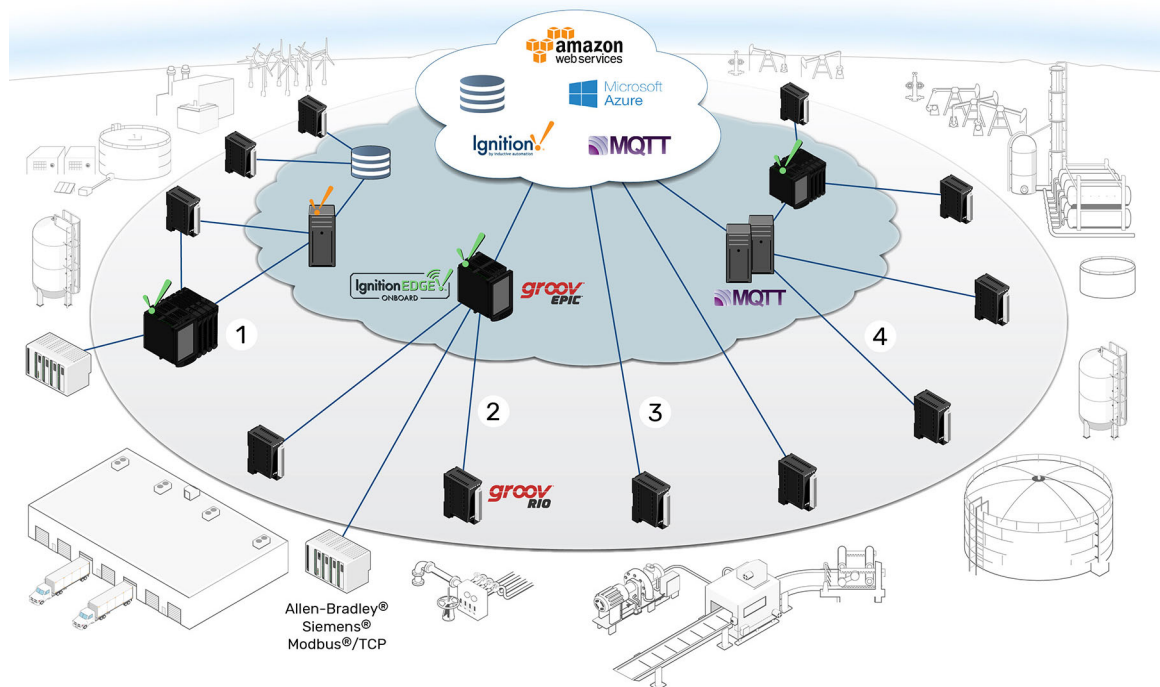
In area 1, a shared infrastructure with edge data processing links several remote locations to central software.

In area 2, legacy PLCs are integrated with current I/O systems and all data sent to the cloud using a groov EPIC processor as an IoT gateway.

Area 3 shows a direct-to-cloud I/O network (no PLC or PC required to share data)

In area 4, MQTT communication creates a many-to-many infrastructure that's lightweight and efficient.

Any two networks can be used for the IIoT as long as both are connected to the internet:
- A computer in one location can get data from a control system at another location.
- Online software can supply data and receive, analyze, and store data.
- A mobile device far away from your control system can access it for monitoring or control, and use cellular service (which goes through the internet) if it can't reach the wireless LAN.
- Node-RED logic flows can incorporate data from local, remote, and online sources, including environmental and geographical services and regulatory information.
- Ignition or Ignition Edge OPC UA drivers can tap into data from legacy and remote automation equipment.

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 8)? 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.

A gateway router has two separate network interface cards (NICs), one connected to the public internet (an untrusted network) and one connected to your private network (a trusted network). 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 following diagram.
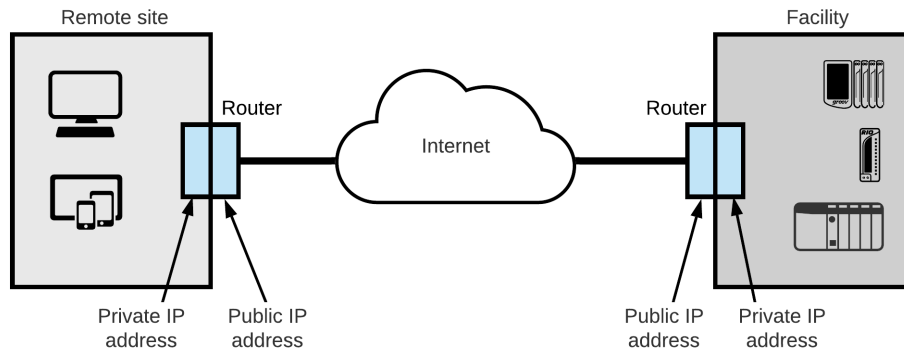
When you're looking at IP addresses, the following IP addresses are always on private networks:

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

All other IP addresses may be on public networks.

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

Gateway router identification

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

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

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

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

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

Fixed (static) vs. dynamic IP addresses

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

- If the router has a static public IP address, you can use that address when setting up a VPN server 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 *groov* EPIC) or a service that's on a private network, you need a way around this block. You have three choices: a VPN, MQTT, or port forwarding.

VPN

A virtual private network (VPN) 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.

A VPN supplies a request-response connection, which is required for some actions you may want to do. These actions cannot be done over MQTT's pub-sub communication structure. For example::

- Accessing *groov* Manage, *groov* Admin, *groov* View, Node-RED, or Ignition Edge from outside the network the *groov* product is on
- Monitoring or controlling systems through a *groov* View interface from outside your facility
- Using a *groov* View operator interface on premises but out of range of a WiFi access point (because your phone switches to cellular service, just as if it were outside)

If you're controlling industrial equipment through your *groov* View interface or getting into *groov* Manage, you want your connection to be secure. For security, we advise that you segment your (untrusted) computer system from your (trusted) automation system using the independent network interfaces on your *groov* EPIC or *groov* Box, or two NICs on a computer.

groov EPIC and *groov* RIO have an OpenVPN client built in, which makes it easy to connect with any VPN server that's compatible with OpenVPN. See setup instructions in the *groov EPIC User's Guide* or the *groov RIO User's Guide*.

- **If you already have a VPN server** available, check to see if it is compatible with OpenVPN.
- **If you don't have a VPN server** compatible with OpenVPN and you have an IT department, work with them to set up communication over a VPN (see "Working with your IT department" on page 21). If you don't have an IT department, you'll have to set it up yourself. See "Setting up a virtual private network (VPN)" on page 22.

NOTE: If you're using a 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 a VPN (or for port forwarding). In this case, MQTT is the best solution, because it uses device-originated, outgoing connections only.

MQTT

As we saw in Chapter 1 ("Publish and subscribe" on page 4), MQTT provides excellent security and is often ideal for data communications where a request-response connection is not required. Connections between an MQTT client and broker are always outgoing from the client. Because almost all firewalls allow outgoing communications over TCP ports, there is no need to modify your firewalls. Once connected, data can travel in both directions. Data communications are efficient, easier to set up, and more secure.

groov EPIC, *groov* RIO, and the *groov* Box all provide ways to use MQTT communications (see "MQTT in groov products" on page 7). You will also need an MQTT broker, which can be set up either on premises or in the cloud.

The following image shows an example of MQTT used to connect remote sites with company headquarters.

Plant
- Production rate
- Batch numbers
- Material use
- Waste products

Firewall

Tank farm
- Tank levels
- Gate access
- Power

MQTT broker

Warehouse
- Fuel levels
- Shipping data
- Inventory

Company headquarters

Plant:
- ☐ Production rate
- ☐ Batch numbers
- ☐ Material use
- ☐ Waste products

Tank farm:
- ☐ Tank levels
- ☐ Gate access
- ☐ Power

Warehouse:
- ☐ Fuel levels
- ☐ Shipping data
- ☐ Inventory
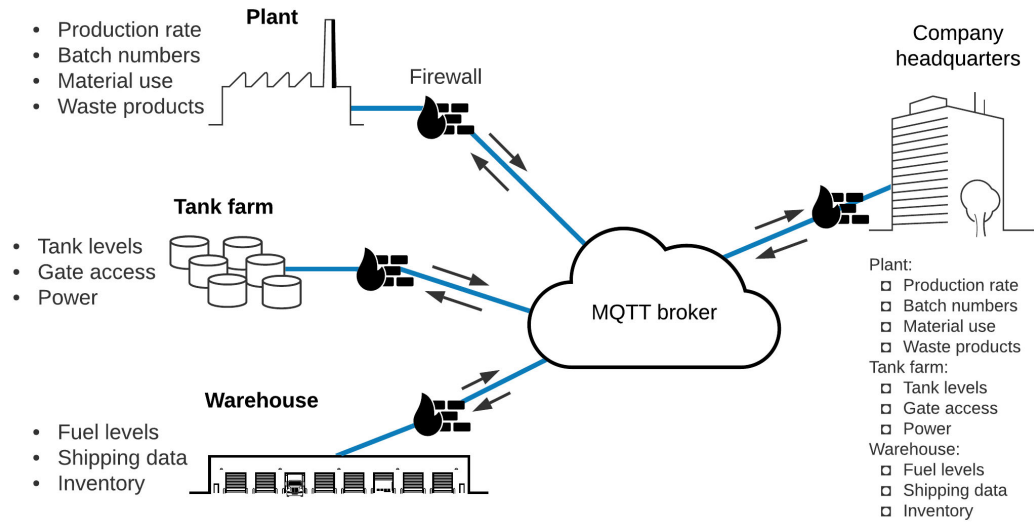
VPN vs. MQTT

You can do many of the same things using a VPN or using MQTT. Both provide secure communication with remote systems, but they offer different options. The following table summarizes uses and considerations.

	VPN	**MQTT**
Description	Private tunnel through the internet, joining two private networks	Lightweight, device-originated, outgoing data communication
Uses	Administer a *groov* product (for example: configure, update firmware, update control programs) Use a *groov* View HMI outside your facility	Share device data and process variables with one or many subscribers. Once shared, data can be read, written, analyzed, and interpreted from remote locations.
Communication type	Request-response (individual connections between devices through the VPN)	Publish-subscribe (device sends data to central broker; subscribers receive data when it changes)
Requires	VPN client at the data source and a VPN server reachable via a gateway from the data source	MQTT broker on premises or in the cloud
Notes for usage	*groov* EPIC and *groov* RIO include OpenVPN client.	*groov* EPIC: Send data directly or via Ignition or Ignition Edge in EPIC. *groov* RIO: Send data directly. *groov* Box: Send data via Ignition Edge.
Security	Encryption, authentication, & security features are provided by the VPN server and clients.	Encryption and authentication. *groov* EPIC and *groov* RIO provide device firewall and security certificates; *groov* Box provides security certificates. Additional security features provided by MQTT broker.

Port Forwarding

Another alternative sometimes used for connections over the internet is port forwarding (PF). However, PF is much less secure than a VPN or MQTT, and we do not recommend it. 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.

PF may be an acceptable option if:

- You have no IT department.
- You have no VPN server and cannot set one up yourself.
- You have no MQTT broker and cannot set one up.
- You have just one *groov* product.

For more information, see "Using port forwarding (PF)" on page 25.

CAUTION: *Do not use port forwarding for any communication with an Opto 22 SNAP PAC controller. For information on networking SNAP PAC controllers, see form #1796, Guide to Networking SNAP PAC Products.*

A note on cell modems

Because *groov* products do not support USB cellular modems, we recommend the use of Ethernet cell modems. These modems don't require device drivers, are generally more robust, and can be sourced through your cell modem provider in your region or country. They also allow more options for external antennas for better signal strength and can often be selected for 3G, 4G, or 5G coverage.

Note that not all cell modems support a WAN-addressable IP address, so you may not be able to access a server like *groov* View or *groov* Manage. In this case we recommend using MQTT and VPN to facilitate communication.

OEMS AND MACHINE BUILDERS

Original equipment manufacturers (OEMs) and machine builders may find *groov* products especially useful for:

- Tracking data about the machine's use and condition, through a database, spreadsheet, online service, or other software
- Troubleshooting and updating machines, either at customer sites or remotely
- Providing an inexpensive, off-the-shelf HMI for machine operators

groov products are industrially hardened and take up little space inside your machine.

Tracking machine data

Machines installed at customer sites can provide valuable data, including for billing, improving machine performance, and predicting maintenance. A *groov* EPIC can provide complete control for the machine through one interface and connect to a network with internet access through the other. You can use Node-RED to communicate machine data to software either locally or in the cloud for tracking, logging, and analysis.

To avoid having to ask customers to set up a VPN or change their firewall for this purpose, use MQTT to publish machine data to a broker. With either Node-RED or MQTT, all communications from your *groov* product are outbound, so no changes are required to the customer's firewall.
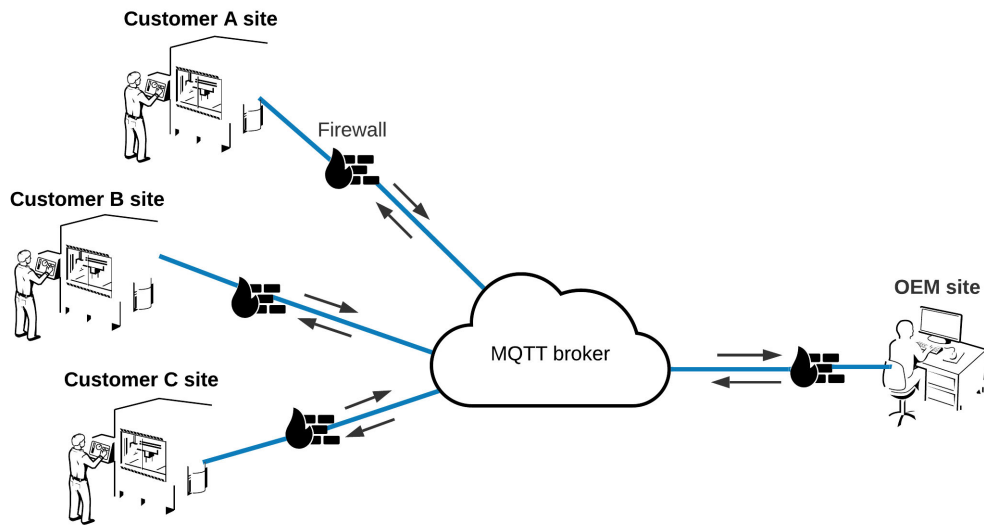
Troubleshooting and updating machines

Using a VPN for direct access to your machine at a customer's site gives you additional advantages: you don't have to be on site to update your control program, install new firmware, change configurations, or troubleshoot problems. Remember that both *groov* EPIC and *groov* RIO include an OpenVPN client. If your customer has a VPN server compatible with OpenVPN, it's easy to configure the client in *groov* Manage.

Providing a machine HMI

You can provide customers visualization into your machine and processes in several ways:

*   Run a *groov* View operator interface on the *groov* EPIC processor's built-in high-resolution color touchscreen or, for a larger view, on a monitor connected to the EPIC's HDMI port.
*   Use a simple Node-RED dashboard in *groov* RIO.
*   With a *groov* Box (or *groov* Server on a PC) in your machine, run a *groov* View HMI on a PC connected to the same network.
*   Build an off-the-shelf mobile device into the machine to use as an operator interface. On an iPhone or iPad, use Guided Access mode to lock down the device so all it does is show your *groov* View interface.
*   Provide a localized wireless network around a machine containing a *groov* Box, so operators can use it from phones, tablets, or laptops, and you or a technician can troubleshoot or update the machine on site. Use a *groov* Box with an approved WiFi adapter and SoftAP (see "Add a wireless network for mobile users (groov Box only)" on page 14).

WORKING WITH YOUR IT DEPARTMENT

If you have an IT department, work with them to set up connections over the internet. For pub-sub, IT can help you set up an MQTT broker. For request-response, they can set up the VPN, create VPN accounts for authorized users, and make sure those accounts have access to the network your *groov* product is on. Let your IT department know that user accounts for both *groov* EPIC and *groov* RIO with firmware version R3.0 or higher can be managed via LDAP (lightweight directory access protocol). LDAP can simplify user authentication and permissions, especially if you have multiple *groov* devices. For specifics on setting up connections to the LDAP service, see the *groov* device's user's guide.

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 Opto 22 Product Support (see "For Help" on page 3). Product support is free.

Tell your IT department which devices you need to have communicate with each other and give them a copy of this chapter. Then follow their instructions to set up communication on your computers and mobile devices. (For help, see "Setting up VPN clients" on page 23.)

Opto 22 port usage

We do not recommend port forwarding, but if your IT department plans to use PF, here is the port information they need:

groov product	Port	Use to access...
groov EPIC	443	groov Manage or groov View, depending on how groov EPIC is set up
groov RIO	443	groov Manage*
groov Box	443 or 8443	groov View
	10000	groov Admin
	8043	Ignition Edge
	3000	Node-RED Admin
	1880	Node-RED Editor
groov Server	443 (or port used on your PC)	groov View

* To access Node-RED editor on groov RIO, log into groov Manage, select Node-RED, and select Open Node-RED Editor.

## SETTING UP A VIRTUAL PRIVATE NETWORK (VPN)

A virtual private networks requires both VPN clients and a VPN server. If your application requires a VPN and you don't have one, or if you want to use the OpenVPN client in groov EPIC and groov RIO but your VPN is not compatible with OpenVPN, you will need to set up a VPN server on your network. If you have an IT department, work with them.

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 install VPN software on a network device or a computer. Several protocols are available for VPN, including OpenVPN, IPsec, and others. (Note that the older PPTP is generally not considered as secure as OpenVPN or IPsec and is no longer recommended by Apple)

Choose the VPN protocol based on what your VPN clients require. For groov EPIC and groov RIO, choose OpenVPN to make it easy. Also consider other clients that may want to use the VPN, such as PCs, a groov Box, or mobile devices.

Place the VPN server inside your private network, behind the router, at your facility (see the diagram on the following page).
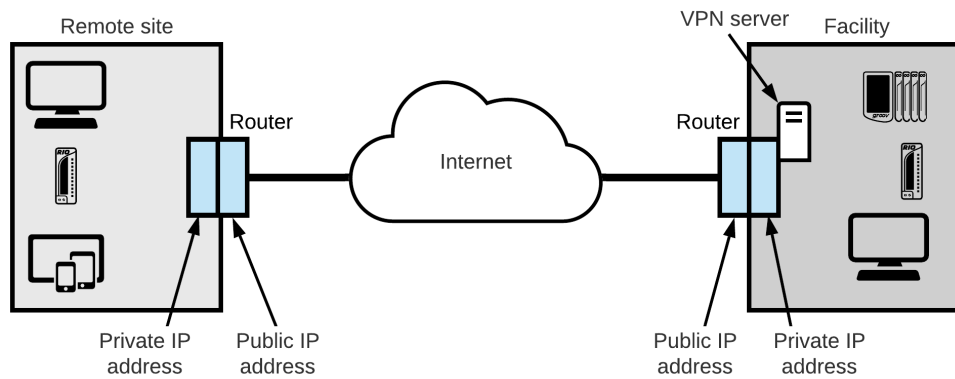
In the router, set up a port forward rule so the router will know to send data through the proper port to reach the VPN server. Port numbers depend on the VPN protocol you're using:

VPN protocol	Ports used
OpenVPN	1194
IPsec	50, 51, and 500

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

Setting up VPN clients

Once your VPN server is set up and user accounts established for those who need them, you'll need to set up a VPN client on each computer or other device that will use the VPN. In the diagram below, a PC , a *groov* RIO module, and some mobile devices are clients. They are shown at the same remote site, but they could be anywhere.
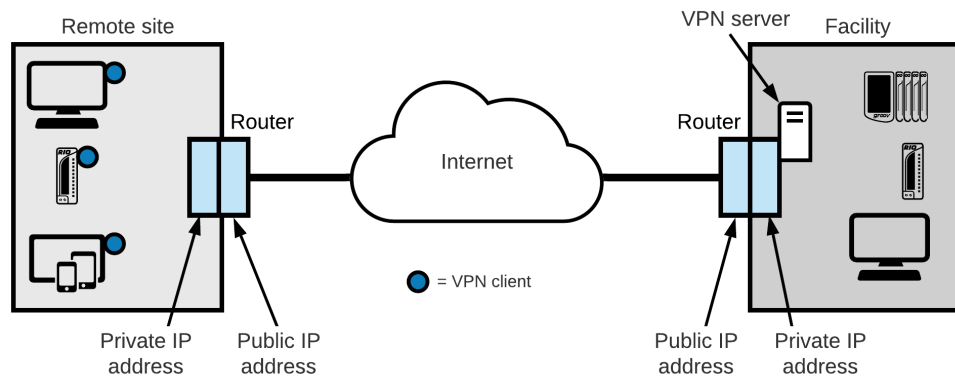
Most current PCs and mobile devices have VPN client software built in. The VPN client must use the same VPN protocol as the VPN server. Some clients give you a choice.

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

- For *groov* EPIC, see Chapter 7 in the *groov EPIC User's Guide*.
- For *groov* RIO, see Chapter 6 in the *groov RIO User's Guide*.
- VPN client: Computer—page 24
- VPN client: Android mobile—page 24
- VPN client: iOS mobile—page 24

VPN client: Computer

1. Make sure you have a VPN account on the VPN Server.

2. Set up a VPN client on your computer.

    –   For Windows 10, see:
        https://support.microsoft.com/en-us/help/20510/windows-10-connect-to-vpn

    –   For macOS Sierra, see: https://support.apple.com/kb/PH25513?locale=en_US&viewlocale=en_US

3. Establish a VPN connection to your VPN server from your PC.

    When you connect, the remote VPN network assigns your PC an additional IP address to match the local network.

4. In your web browser, type https:// plus the hostname or IP address of the *groov* product you want to access. Example: `https://mygroov`

5. Test your connection: see "Testing communication" on page 26.

VPN client: Android mobile

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 an OpenVPN server, visit the Google Play Store and download the OpenVPN Connect app:
https://play.google.com/store/apps/details?id=net.openvpn.openvpn&hl=en

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 client: iOS mobile

1. Go to the iTunes store and download an SSL VPN client app (such as OpenVPN Connect).

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

3. Once connected, open a web browser and type https:// plus the IP address of the *groov* product. Example: `https://172.20.52.5`

    If you have problems connecting, see "Testing from inside your facility" on page 26.

VPN for a *groov* Box at a different location

If you have a *groov* Box 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, like many control systems and equipment, cannot be a VPN client nor accept a VPN client. And it is unsafe to use port forwarding unless the controller or device has built-in user authentication and encryption.

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, the *groov* Box and your control system communicate just as if they were on the same local area network.
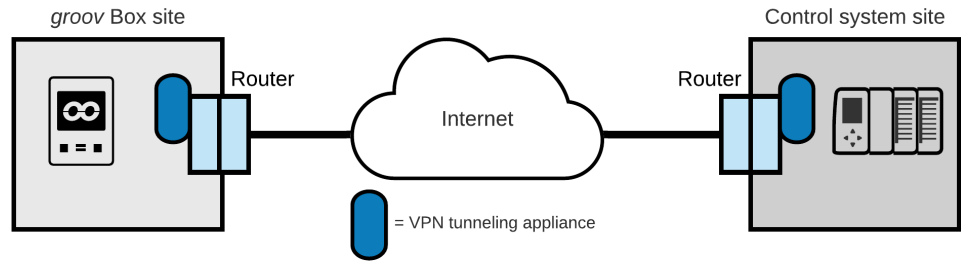
USING PORT FORWARDING (PF)

We do not recommend port forwarding, as it is less secure than either a VPN or MQTT. A port forward rule creates a small hole in that firewall to allow data packets to get through to the private network.

CAUTION: *Do not use port forwarding for any communication with a SNAP PAC controller.*

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 25).
- Set up port forwarding on the client PCs or mobile devices (page 26).

Determining the IP address

On the private network where the *groov* product is, find out the gateway router's public IP address (see steps in "Gateway router identification" on page 17). 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 17).

Establishing port forward rule(s)

See the port number table in "Working with your IT department" on page 21.

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 your groov product's IP address, you'll need to always add the port number when you access it.

If you have more than one *groov* product 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. For more information on ports, see "port" on page 31.

PF: *groov* EPIC and *groov* RIO

groov EPIC and *groov* RIO both contain device firewalls, and you can change their firewall rules in *groov* Manage. Note that adding or changing firewall rules (which effectively opens ports in the firewall) does not start any listening services that may be behind those ports. If you encounter problems accessing those services, check that the services are on and listening.

groov Box has a device firewall, but it is not user configurable. To create a port forward rule for a *groov* Box, 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.)

Follow these steps:

1. Open the webpage 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 more than one *groov* Box (each Box needs a separate port number).
   - 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

If you've already set up the port forward rule on your router or firewall, you're ready to test communication: see "Testing from inside your facility" on page 26.

1. On an **iOS** mobile device, go to Settings > groov.
   On an **Android** mobile device, launch the *groov* View 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 *groov* View app.

TESTING COMMUNICATION

You're now ready to test communication between your two networks.
- To test MQTT data communications, see form 2350, *Getting Started with MQTT in groov Products*.
- For a VPN or port forwarding, follow steps below.

Testing 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 and then 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:** Using your mobile device network menu, connect with your VPN server. Open a web browser and type https:// plus the *groov* product'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 network the *groov* product is on, plus a colon and the port number.

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

Testing from outside your facility

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

VPN: Using your mobile device network menu, connect with your VPN server. Open a web browser. For the URL, type https:// plus the *groov* product'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 network the *groov* product is on, 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* product's user's guide.

If you've been able to communicate with your *groov* product 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 17.

IMPORTANT: *On a groov EPIC or 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.*

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 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 an IP address and other configuration information to each device 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. The more familiar IPv4 addresses 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`

IPv6 addresses (which are becoming increasingly more common) are formatted in eight groups of four hexadecimal digits, separated by colons. For example:
`2001:0db8:0000:0042:0000:8a2e:0370:7334`

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.

LDAP

LDAP (lightweight directory access protocol) is often used by IT departments as a centralized method for authenticating users and managing access information for users, groups, and applications.

MQTT

MQTT (at one time called MQ Telemetry Transport) is a lightweight communication protocol based on the pub-sub architecture. It is often used for internet of things (IoT) applications because it is suitable for data communication with remote devices that don't have much computing power or are on networks with irregular connections or low bandwidth.

MQTT is the transport protocol; messages may be sent over MQTT with payloads in specific formats, for example strings or Sparkplug B.

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* EPIC processor can communicate with Modbus/TCP devices, a SNAP PAC controller, and an OPC UA server, all at once using the same IP address.

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 separate 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 firewall, to the internet.

pub-sub

A *pub-sub* (or *publish-subscribe*) architecture differs from a request-response architecture in ways that make it useful for internet of things (IoT) applications.

In pub-sub, all data is held by a broker, which may be located on your network or in the cloud. Devices and software publish data to the broker, or subscribe to data the broker holds, or both. Data is published only when it changes (report by exception) and sent to subscribers only when it changes.

request-response

Request-response (also called command-response or query-response) is a basic communcation method among computers and devices on a network. One computer or device sends a request for data or services, and another responds by sending the requested data or performing the service. The computer or device that sends the request is the client, and the one that responds is the server.

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 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. SoftAP can also be used to create a separate WiFi network not connected to the internet, as in the *groov* Box.

Sparkplug B

An open messaging system developed by Cirrus Link Solutions that defines topic namespace, session state management, and data payload encoding for devices and software using the MQTT transport protocol. Sparkplug adds specific features designed to standardize MQTT messages for industrial applications.

For more information, see the Sparkplug B specification.

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* product, 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.

trusted network

A *trusted network* is a network where you know every person and every software application that has access to it, and you trust them. An example of a trusted network is your own private network, where only you have access. Another example might be your corporate IT network, where your IT department manages users on the network through tools they have. Compare with untrusted network.

untrusted network

An *untrusted network* is a network where you don't know all the people and software applications that might have access to it. The internet is a good example of an untrusted network. Compare with trusted network.

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 remotely.

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.

Information from Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team: Recommended Practices for Industry

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

Some DDNS services:
* http://dyn.com/dns/
* http://www.noip.com/

MQTT:
* MQTT 101: How to Get Started
* mqtt.org
* Sparkplug messaging
* Sparkplug specification
* List of MQTT brokers for testing or prototyping

Additional information about VPNs:
* Microsoft technical information for Windows Server 2016 and Windows 10
  https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/vpn-top

Setting up a VPN:
* On Android: http://www.howtogeek.com/135036/how-to-connect-to-a-vpn-on-android/
* Download the OpenVPN Connect app for Android:
  https://play.google.com/store/apps/details?id=net.openvpn.openvpn&hl=en
* On iOS:
  https://support.apple.com/guide/deployment-reference-macos/intro-to-vpn-ior9f7b5ff26/1/web/1
* For an iOS mobile device, download the OpenVPN Connect app for iOS from the App Store.

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