

Controllers & Bridges

SERVICE MANUAL

Design, Configuration & Operation



CONTENTS

- BoxIQ™ Controller & Bridge Data Sheets : Pages 4-8
- Wiring Diagrams : Pages 9-10
- Network Configurations : Pages 11-14
- DHCP Programming in Software : Pages 15-18
- Setting Static IP Addresses : Pages 19-28
- Establishing WiFi Connectivity : Pages 29-34
- Open Port Requirements : Pages 35-37
- Bridge Layout Guidance : Pages 38-48

About the Contents

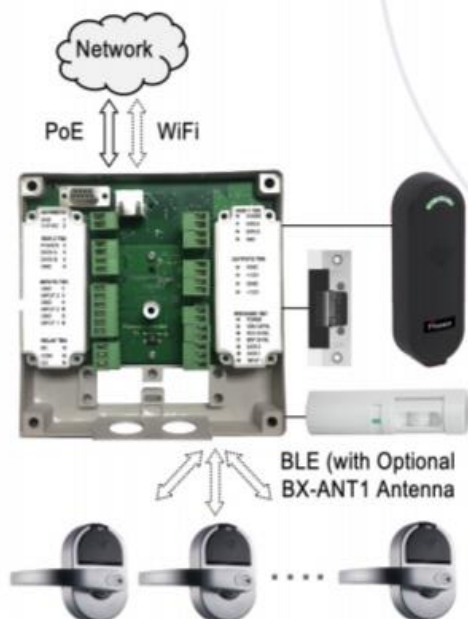
The intent of this document is to provide a life-cycle support guide for the planning, design, implementation and maintenance of the Proxess BoxIQ™ Controllers and Proxess Bridges.

- The first section is the Proxess BoxIQ™ controller data sheet, describing its key functionality and features/capabilities, as well as its electrical, mechanical, mounting and environmental specifications.
- The Proxess Bridge data sheet is next, describing its key functionality and features/capabilities, as well as its electrical, mechanical, mounting and environmental specifications.
- Ensuring the Network Connectivity of the controller and bridge is the purpose of the next document, which displays several connectivity diagrams to ensure their automated discovery by the software, as well as their DHCP (default) programming.
- Ports that are necessary to be open for the controller and bridge to communicate with the server are addressed in the next section.
- The Controller configuration section of the ProxessIQ software is next included.
- The alternative Static IP address programming guide is next provided, followed by the section on configuring the WiFi connectivity for the controllers and bridges.
- Finally, the BLE Bridge Layout Planner is included, providing guidance for the estimation of the placement of bridges in a system to best assure connectivity to all of the fielded locksets and mini controllers.

Proxess BoxIQ

PoE+, WiFi,
BLE Controller

For ProxessIQ™ Software Only



BoxIQ™ is the Proxess solution for the more conventional access control doors using a reader. BoxIQ™ wirelessly communicates with your Proxess electronic locksets “On-Demand”. BoxIQ™ also allows the user to control commands and further monitor access to high-security portals using the ProxessIQ™ software.

For communication reliability and optimal battery performance, Proxess locksets may be connected to BoxIQ™ via Bluetooth Low Energy (BLE). Proxess locksets are assigned in the ProxessIQ™ software to a specific BoxIQ™.

Proxess locksets may typically be located at distances of up to a 70-foot radius from the bridge (maximum of 100 feet) with potential reductions due to interference by walls, ceilings, floors and an abundance of other metal surfaces or equipment.

Our Network-on-Card credentials download transactions and upload rights for the offline Proxess locksets which reduces the installation of traditional, expensive, hardwired doors.











An unlimited number of BoxIQ™ controllers may be added to any site or ProxessIQ™ system.

Controllers are simply and quickly added to the system, plugging directly into the facility's existing PoE or PoE+ infrastructure and defined in the ProxessIQ™ software via static or DHCP addressing. On-demand wake-ups for Lockdowns and Door-Open commands, as well as events from Locksets to the ProxessIQ™ software.

For those difficult to reach areas (e.g. gates, out-buildings), the BoxIQ™ controller also includes a WiFi communications backhaul where it would draw low voltage power from near the panel.

Providing security flexibility with the separately ordered BX-ANT1 antenna, BoxIQ™ provides on-demand lockdown and open-door commands and also receives emergency Proxess lockset events.

FEATURES

	Brings your Proxess locksets "On-Demand" via Bluetooth (*Optional BX-ANT1 antenna required)
	Connect a PoE\PoE+ network cable or power with a transformer and use your existing WiFi
	Allows centralized Lockdown and Open Door commands to Proxess locksets (with BX-ANT1)
	Highest level security credentials using Mifare DESFire EV2™ and BLE
	Credentials collect transactions from Proxess locksets. Security handshakes for verification.
	CONNECTIVITY - Built-in PoE\PoE+ and WiFi communication backbone leverages existing and common infrastructure and reduces installation costs. Add, move and configure doors in minutes, even from remote locations.
	ON-DEMAND - On-demand Lockdowns and Open Door commands (with BX-ANT1) to always-awake Proxess Locksets...also events and notifications from Proxess locksets to the Proxess software.
	NETWORK-ON-CARD - Our credentials go beyond just passing a number to the reader. They know where they belong and perform a handshake with the readers for ultimate security.
	EXPANSION - Unlimited BoxIQ™ controllers, doors and sites in a ProxessIQ™ system. Unlimited users and credentials.
	ENCRYPTION - Upstream and downstream communications utilize AES 128-bit encryption.

Proxess Bridge™

Online BLE Bridge

For ProxessIQ™ Software Only



Proxess Bridge™

The Proxess Bridge™ communication

module brings your Proxess compatible electronic locksets online, upgrading the communication frequency and reducing manpower at the door to affect changes.

For communication reliability and optimal battery performance, up to eight (8) Proxess locksets may typically be connected to a Proxess Bridge™. Uniquely, locksets are assigned in the ProxessIQ™ software to a specific Proxess Bridge™.

Proxess Locksets may be located at distances up to a 90-foot radius although a typical recommendation is 50 feet from the gateway due to potential interference reductions by walls, ceilings, floors and other metal surfaces or equipment. Proxess locksets are always awake, allowing On-Demand Lockdown, open door and other commands. Our BLE communications technology and frequency hopping maximize lockset battery life, typically exceeding two (2) years.

An unlimited number of Proxess Bridges™ may be added to any site or ProxessIQ™ system. Gateways are simply and quickly added to the system, plugging directly into the facility's existing PoE or PoE+ infrastructure and defined in the ProxessIQ™ software via DHCP.


For those difficult to reach areas, the Proxess Bridge™ also includes a WiFi communications backhaul, where it would alternatively draw low voltage power from near the panel.

Providing security flexibility, Proxess Bridge™ provides on-demand lockdown and open-door commands and also receives emergency lockset events.



proxess.com

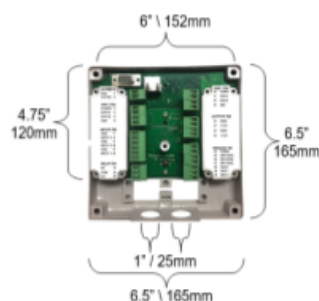
FEATURES

	Brings your Proxess locksets On-Demand via BLE (Bluetooth Low Energy)
	Just plug-in a PoE\PoE+ cable...or power with a transformer and use your existing WiFi
	Allows centralized Lockdown commands to locksets
	Gateway for Open Door commands to locksets
	CONNECTIVITY - Built-in PoE\PoE+ and WiFi communication backbone leverages existing and common infrastructure and reduces installation costs. Add, move and configure doors in minutes, even from remote locations.
	ON-DEMAND - On-demand wake-ups for Lockdowns and Door-Open commands, as well as events from Locksets to the ProxessIQ™ software.
	EFFICIENCY - Bluetooth Low Energy (BLE), with frequency hopping, ensures immediately available communication channels to locksets and maximum battery life. Each lockset is bound to specific Proxess Bridge™ gateways for stability and battery preservation.
	ENCRYPTION - Upstream and downstream communications utilize 128-Bit AES encryption.
	BATTERY LIFE - Our unique Always-Available BLE and our advanced battery life routines and technologies extend lockset battery life.

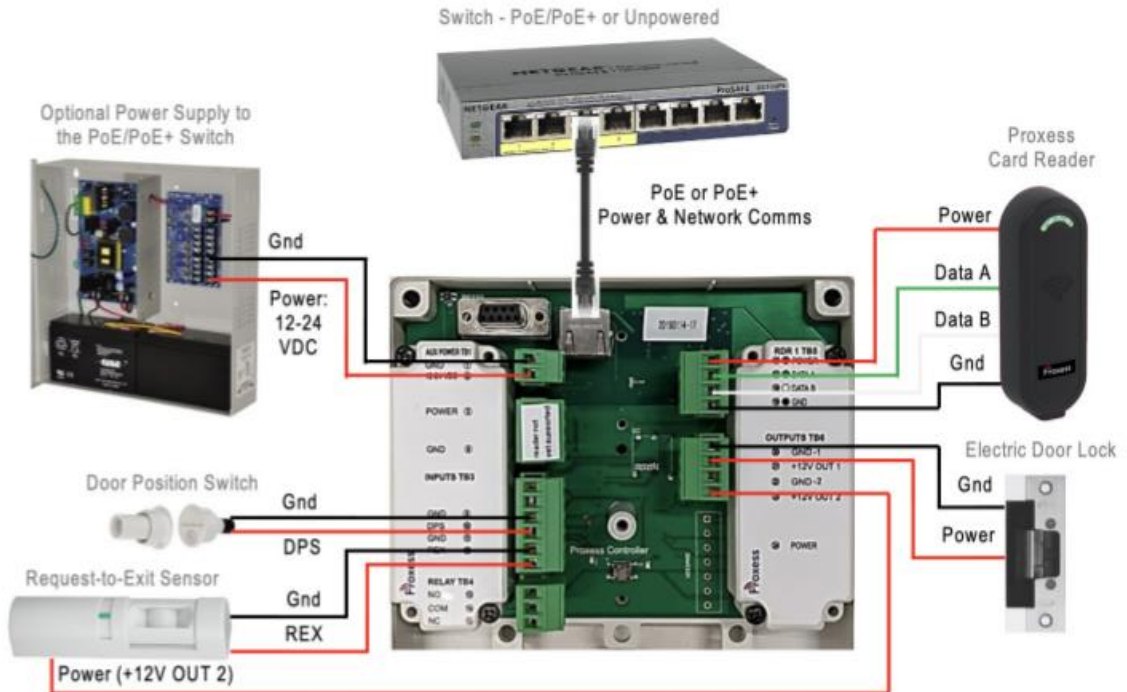
HOW TO ORDER:

Part Numbers:	BX-EN-POE Board with enclosure BX-ANT1 Antenna for On-Demand lockset comms BX-BR1 Proxess Bridge™
Compatibility:	Proxess RoxIQ™ bi-directional, read-write readers, via RS-485; Proxess electronic locksets, via Bluetooth Low Energy (BLE). For use within ProxessIQ™ software.
Simple Anti-Passback:	Simplified anti-passback alternative. One checkbox forces cardholders to use a chokepoint reader for their credential reauthorization, programmable from one day to many years.
Gateway Antenna:	Optional BX-ANT1 BLE antenna to provide "on-demand" communications to up to eight (8) Proxess locksets.
Electrical:	<p>PoE/PoE+ Voltage Input: 36-57 VDC at Line Voltage Input: .83A Current Consumption: 12-18 VDC, 200 mA</p> <p>Door Contact Switch Request to Exit (REX)</p> <p>Out 1 Voltage: 12 VDC Out 2 Voltage: 12 VDC Out 1 Current: 1A Out 2 Current: 1A</p> <p>Out 3 1 Amp (24 VDC) Dry Contact</p>
Communications:	<p>Communications: TCP/IP: Yes WiFi Backhaul (8.02.11): 100Mbps Bluetooth Low Energy (BLE): Yes RS-485: Yes Bandwidth: 230Kbps DHCP Support: Yes, Default Static IP Support: Yes</p>
System Specifications:	<p>Cardholders: 5000 Controllers per System: Unlimited Time Schedules: Unlimited Access Profiles: Unlimited Data Retention: 30 days, Flash Storage Reader Communication: RS-485, Bi-directional Door Hold Open Time: 0-255 seconds Operating System: Linux, SOM On-board</p>
Features:	<p>Reader Ports: 1 x RS-485 Input for Request-to-Exit: 1 Input for Door Contact: 1 Alarm Output: 1 Enclosure Tamper Input: Yes Enclosure Knock-Outs: Yes, 2 x 1 inch</p>
Environment:	<p>Operating Temperature: -20°C - +55°C, -20°F - +132°C Moisture Resistance: No-Provide Suitable Enclosure to Environment</p>
Hardware:	<p>Network Cable Type: CAT-5/6, 2C, 22AWG, OS Reader Cable Type: CAT5e/CAT6 REX Cable Type: 4C, 22AWG, OS Door Contact Cable Type: 2C, 22AWG, OS Lock Release Cable Type: 2C, 18AWG RS-485 Cable Output Type: 4C, 22AWG, OS</p>

MEASUREMENTS



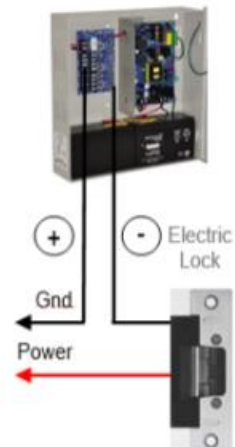
CONTROLLER, BRIDGE SYSTEM WIRING



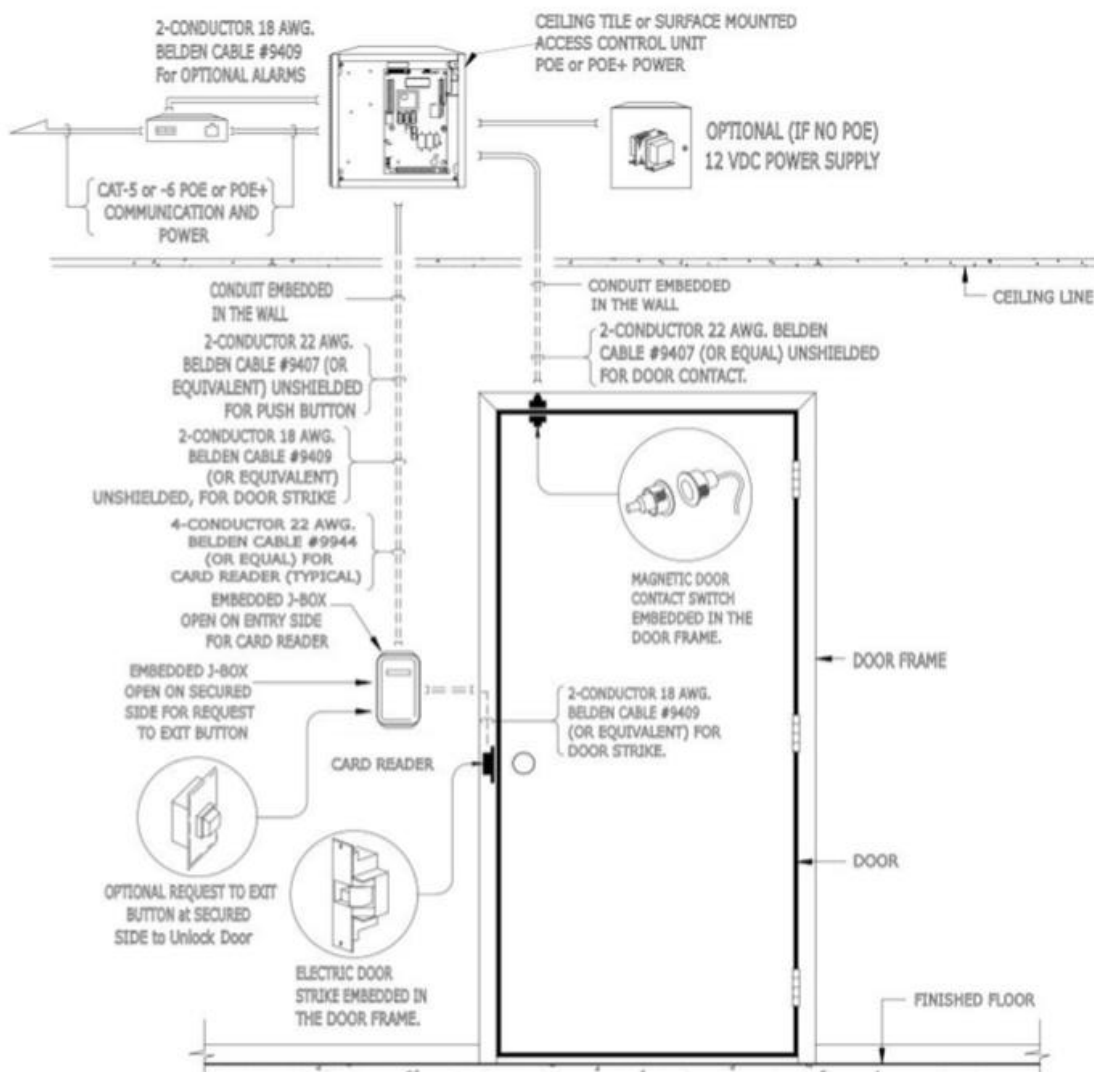
POWER NOTE: Verify the voltage and current requirements of your selected electric door lock prior to connecting to the Proxess BoxIQ. If you have any questions on the suitability of a direct power connection from the BoxIQ, please select and use a separate power supply and connect per the above drawing.

OPTION

Separate Power Supply for the Electric Lock



SAMPLE DOOR DEVICE LAYOUT AND CONNECTIVITY



Network Configurations

Sample DHCP Network Layouts for Controllers & Server

Network configuration diagrams to enable **DHCP** “automated” controller & bridge recognition and setup by the server

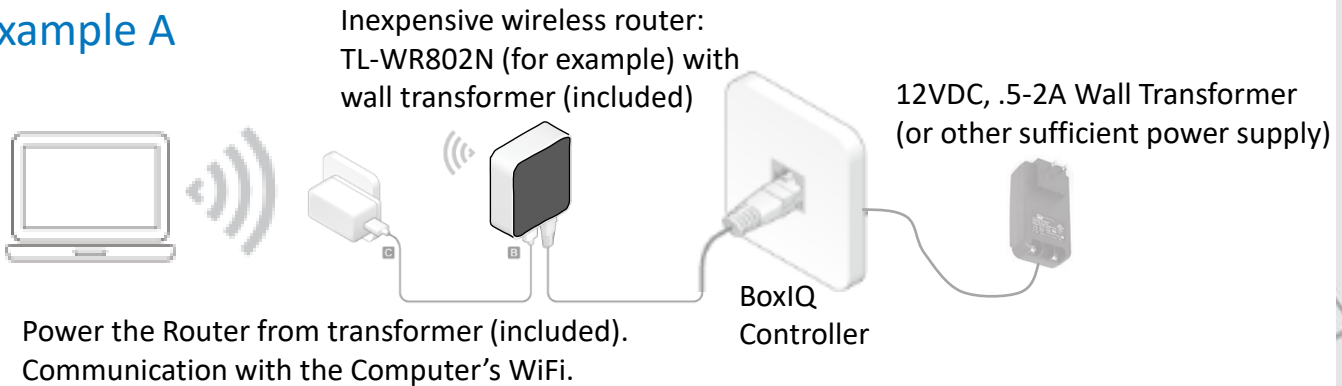
- To follow are the baseline representative network diagrams and requirements for the [Dynamic\Automatic IP addressing \(DHCP\)](#) of Proxess controllers and bridges.
- The goal of this document is to demonstrate the simplest way to configure the ProxessIQ™ software to communicate with a BoxIQ™ controllers and Proxess Bridge™.
- More complex network topologies can only be configured and supported by the local dealer or the customer’s IT department.
- The basic rule is that you must be able to “ping” the controller\bridge from the software, in order for the hardware and software to communicate.

DHCP Network Sample

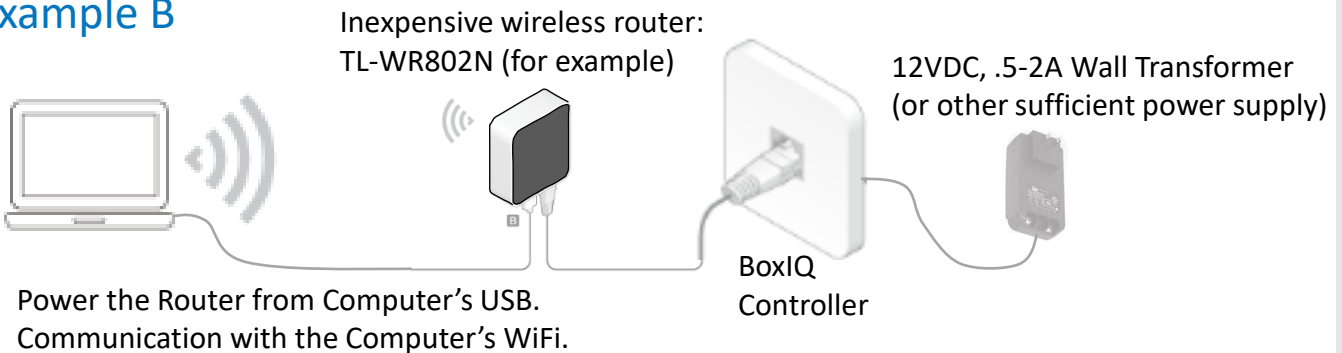
Examples A, B & C

These are examples of the Baseline\Minimum network layout, to enable the Dynamic\Automatic IP addressing of Proxess Controllers and Bridges. If your network looks like one of these & simplest software configuration. In other words, you need to be able to “ping” the controller’s/bridge’s IP address from the server computer for DHCP configuration to work and these layouts will enable this convenient function.

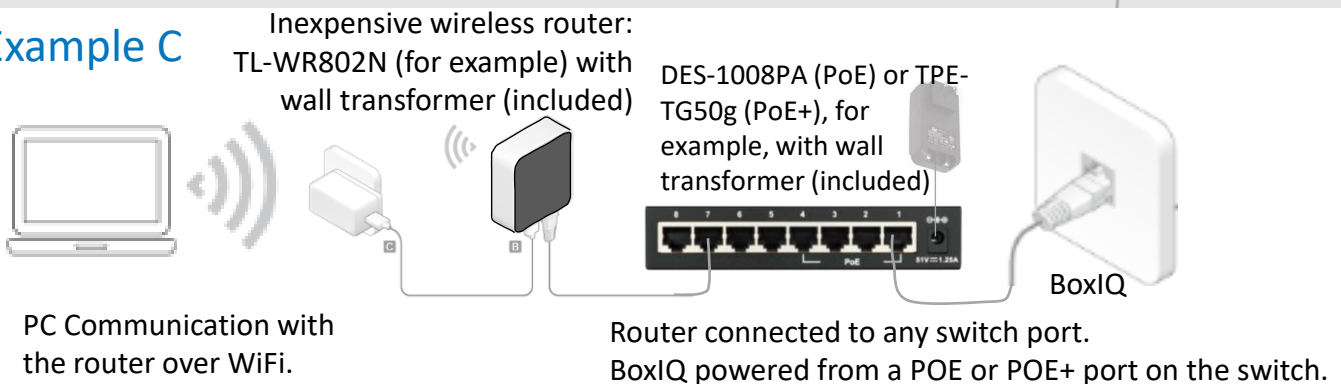
Example A



Example B



Example C



DHCP Network Sample

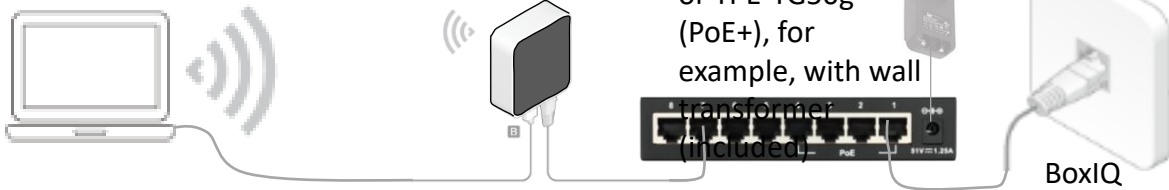
Examples D, E & F

These are examples of the Baseline\Minimum network layout, to enable the Dynamic\Automatic IP addressing of Proxess Controllers and Bridges. If your network looks like one of these & simplest software configuration. In other words, you need to be able to “ping” the controller’s/bridge’s IP address from the server computer for DHCP configuration to work and these layouts will enable this convenient function.

Example D

Inexpensive wireless router:
TL-WR802N (for example)

DES-1008PA (PoE)
or TPE-TG50g
(PoE+), for
example, with wall
transformer (included)

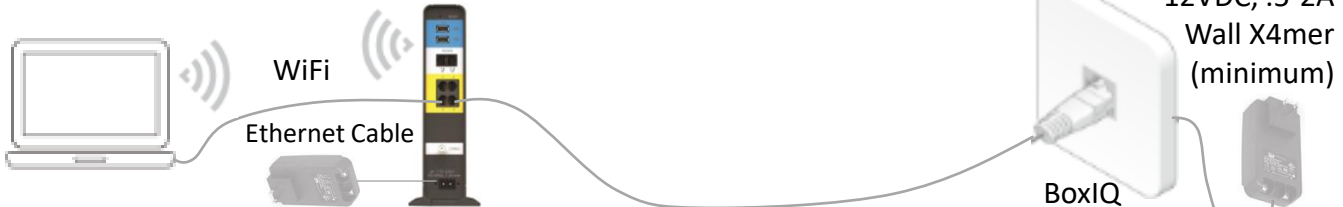


Power the Router from Computer’s USB.
PC Communication with the router over WiFi.

Router connected to any switch port.
BoxIQ powered from a POE or POE+ port on the switch.

Example E

Internet Service Provider (ISP) combination
Router-Modem with wall transformer (included)

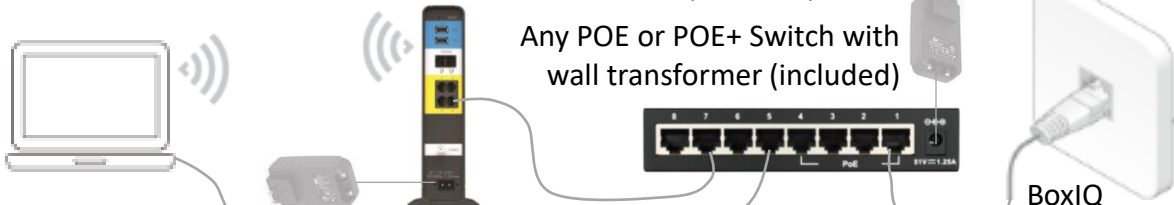


PC Communication to the router with either
ethernet cable or via the PC’s WiFi.

BoxIQ connected to ISP router and
powered from separate power supply.

Example F

Internet Service Provider (ISP) combination
Router-Modem with wall transformer (included)



PC Communication to the switch, or to the router
with either ethernet cable or via the PC’s WiFi.

ISP router connected to any switch port.
BoxIQ connected to and powered from a
POE\POE+ port on the switch.

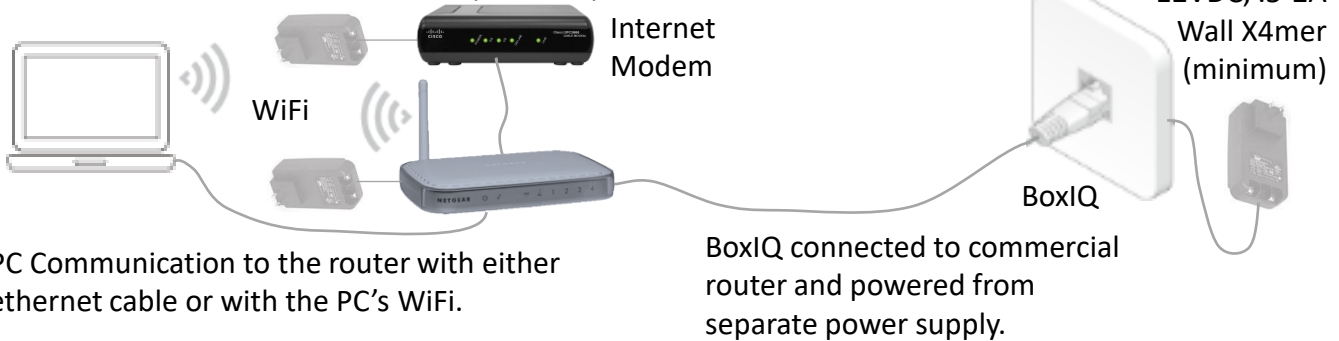
DHCP Network Sample

Examples G, H & I

These are examples of the Baseline\Minimum network layout, to enable the Dynamic\Automatic IP addressing of Proxess Controllers and Bridges. If your network looks like one of these & simplest software configuration. In other words, you need to be able to “ping” the controller’s/bridge’s IP address from the server computer for DHCP configuration to work and these layouts will enable this convenient function.

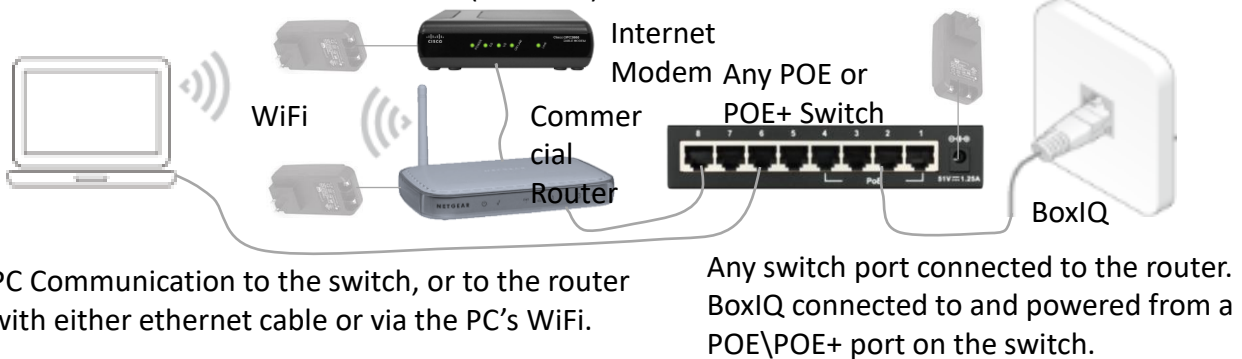
Example G

Commercial Internet Modem with wall transformer (included)



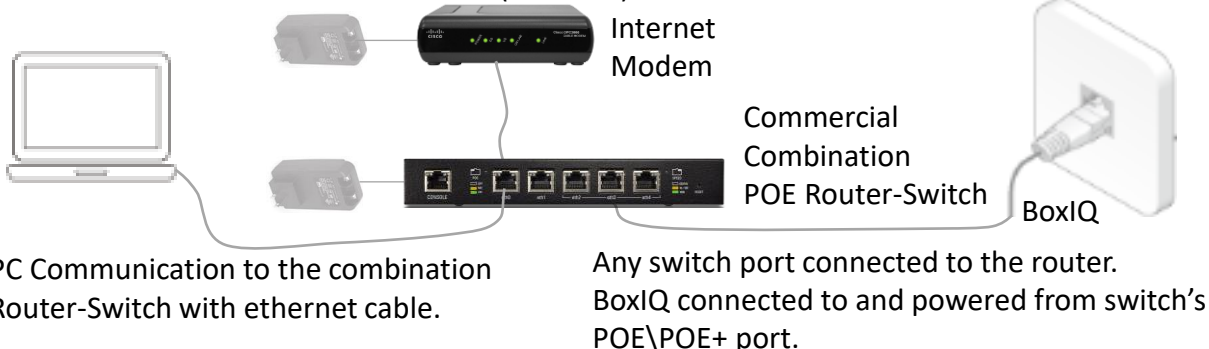
Example H

Commercial Internet Modem with wall transformer (included)



Example I

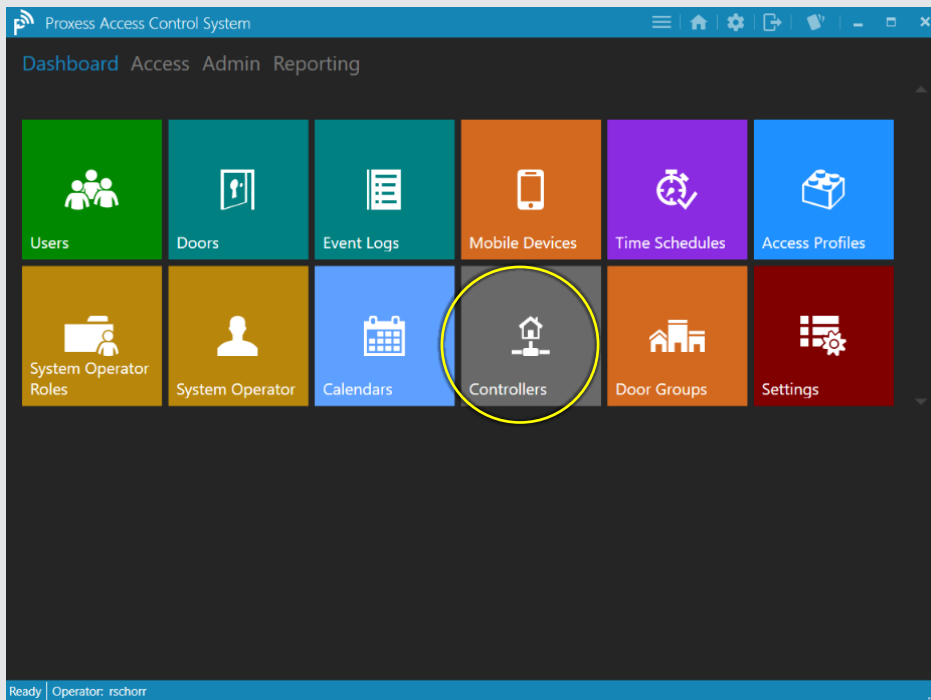
Commercial Internet Modem with wall transformer (included)



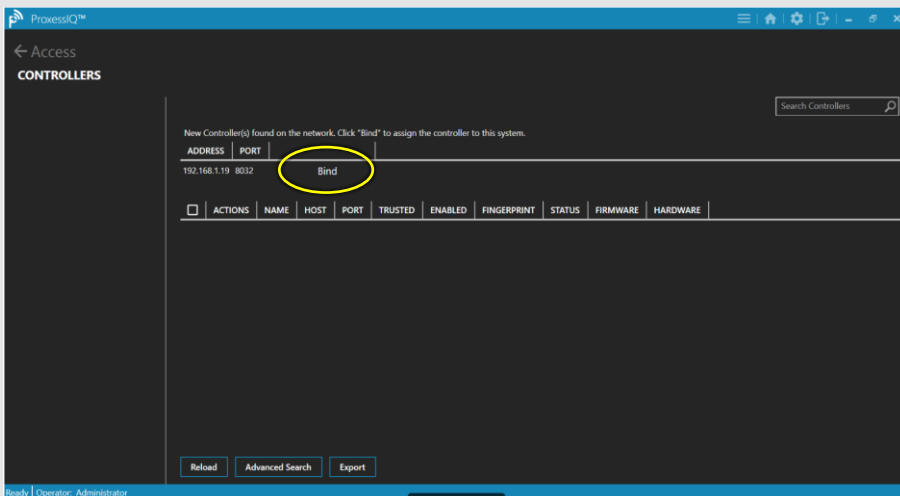
Software Configuration

Instructions for Programming Controllers & Bridges in the ProxessIQ Software

ProxessIQ Software Configuration



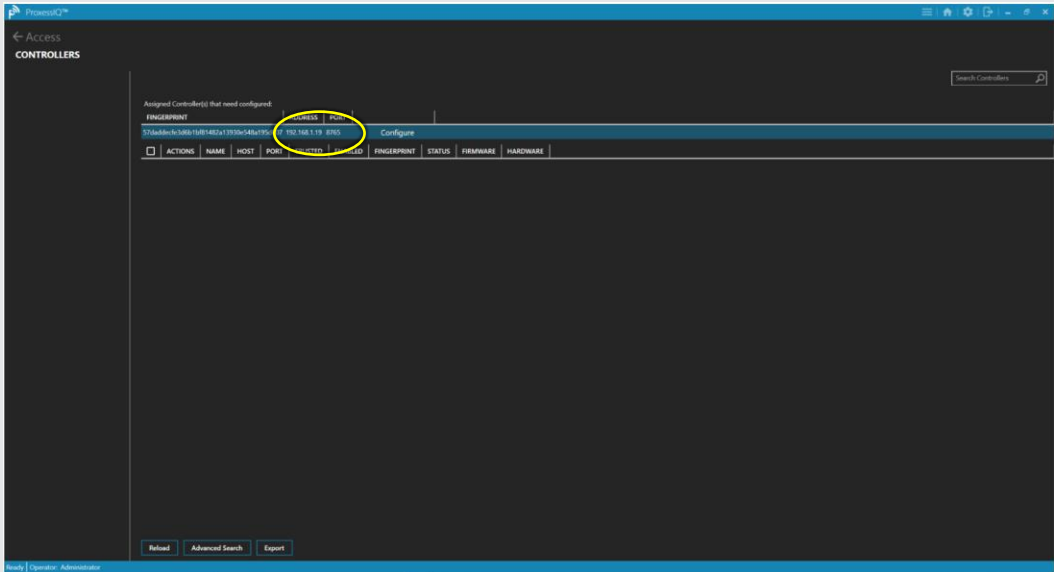
To add a controller to the system, click on the “Controller” module icon. After adding a Controller, you will then be able to select entry & exit readers that you have added into the “Doors” module to connect.



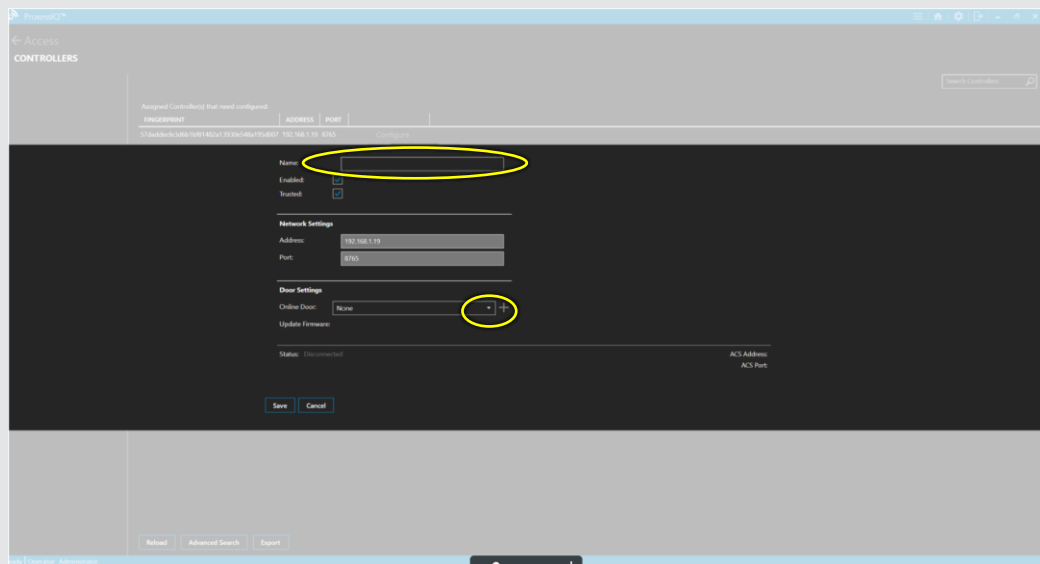
Any controller that is connected, within the guidelines of our BoxIQ Connectivity document located here on our website: www.proxess.com/documents/BoxIQConnect will automatically appear in this window. To avoid confusion, it is best to connect and configure one controller at a time.

Click “Bind” to connect the newly discovered controller with ProxessIQ

ProxessIQ Software Configuration



Now click “Configure” to have the software configure this controller for its proper function within this software instance.



Type a name for this controller.
Next, click on the drop-down arrow above.

ProxessIQ Software Configuration

The screenshot shows the 'Configure' page for a ProxessIQ controller. The 'Name' field is set to 'Proxess Office Controller'. The 'Enabled' and 'Trusted' checkboxes are checked. Under 'Network Settings', the 'Address' is '192.168.1.19' and the 'Port' is '8100'. Under 'Door Settings', the 'Online Door' is 'None' and the 'Update Firmware' dropdown is set to '1D Office Controller Demo'. The 'Status' is 'Disconnected'. The 'ACS Address' and 'ACS Port' fields are empty. At the bottom, the 'Save' button is circled in yellow.

Select any reader that you have already entered in the “Door” module to be connected to this controller. Then click “Save”.

The screenshot shows the 'Controller Saved' confirmation screen. The message states: 'Controller Saved. The controller changes have been saved.' At the bottom right, the 'OK' button is circled in yellow.

Click “OK” on the verification screen.

The Controller is now bound, configured enabled and will be shown as Connected and operational in the Controller screen.

Setting a Static IP

**Instructions for Setting a Static IP
address for the Controllers & Bridges**

Setting a Static IP Address

BoxIQ™

Customized Controller Settings Procedure

Setting a Static IP address and designating an ACS address

Setting the Controller for WiFi Connection

This purpose of this guide is to describe how to configure and connect Proxess BoxIQ™ controllers\bridges to the ProxessIQ™ PC-based software.

We will begin by describing the simple, default configuration process, which is valid for simple networks, with both the software and the controllers on the same network segment. Then we will fully describe the customization procedure for controllers that will reside outside of network the software resides on.

Out-of-the-Box Controller Configuration

The primary and simplest method for adding a BoxIQ Controller-Bridge to the ProxessIQ system is to connect both the BoxIQ™ controller and the computer with the ProxessIQ™ Server software into a common router. The router either needs to be a POE device, or the BoxIQ™ will need to be powered by a 12VDC or 24VDC source. When the “Controller” menu in the ProxessIQ™ software is entered, all connected controllers will appear in the window, asking the User if they wish to “Bind” (connect and encrypt) those controllers into the software (only to this specific instance of the software). The software steps are detailed in the ProxessIQ™ Software Guide, which can be found online at:

www.proxess.com/Proxess/media/Proxess/Images/Solutions/Proxess-Software-Manual.pdf?ext=.pdf .

Why do we need a router?

The router is required for the initialization\programming\configuration, as it automatically assigns the IP address for the controller, as opposed to just a switch, which requires an IP address be programmed into each connected device, in order for them to communicate.

Once the router is used to configure and initialize the controller into the software, it is not necessarily needed for the day-to-day operation and communication between the software and controller.

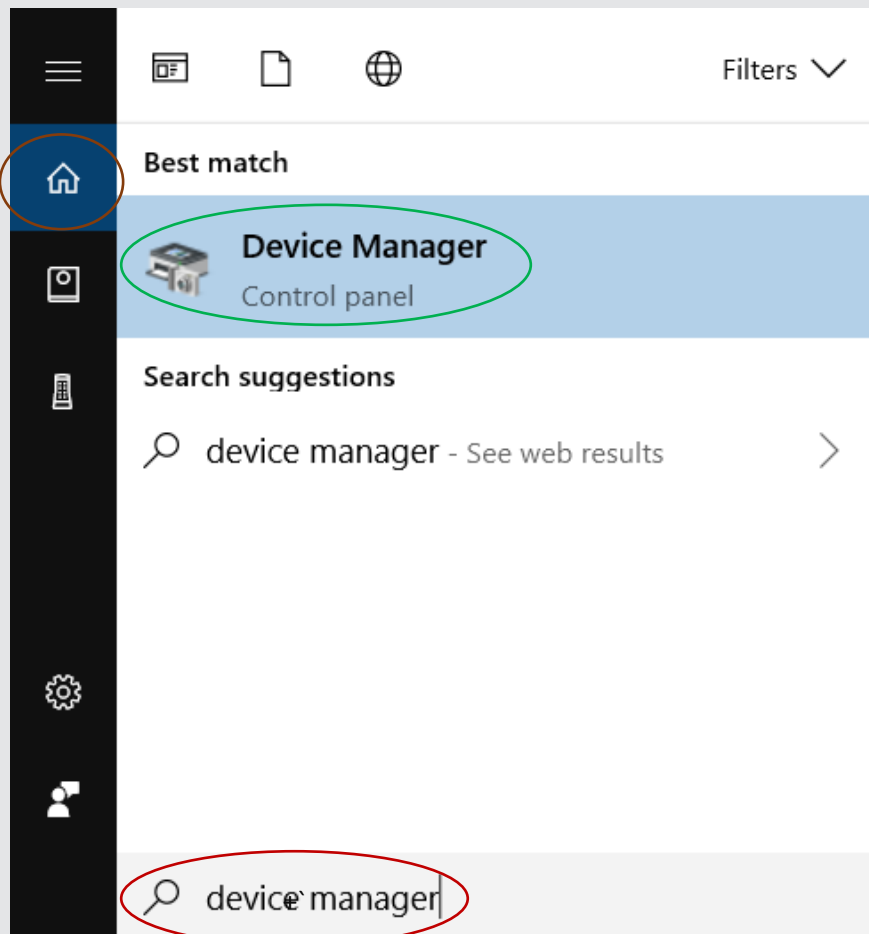
What if I have only a switch, but no router?

If only a switch is available for the initialization process and if the controllers will need to communicate with the software through an extended or open network (i.e. anything beyond a “flat” or single-level network, including the through the Internet), a static IP (as well as subnet and gateway addresses) will first need to be programmed into it, as well as the server IP address. To do this, the below process must be followed:

Setting a Static IP Address

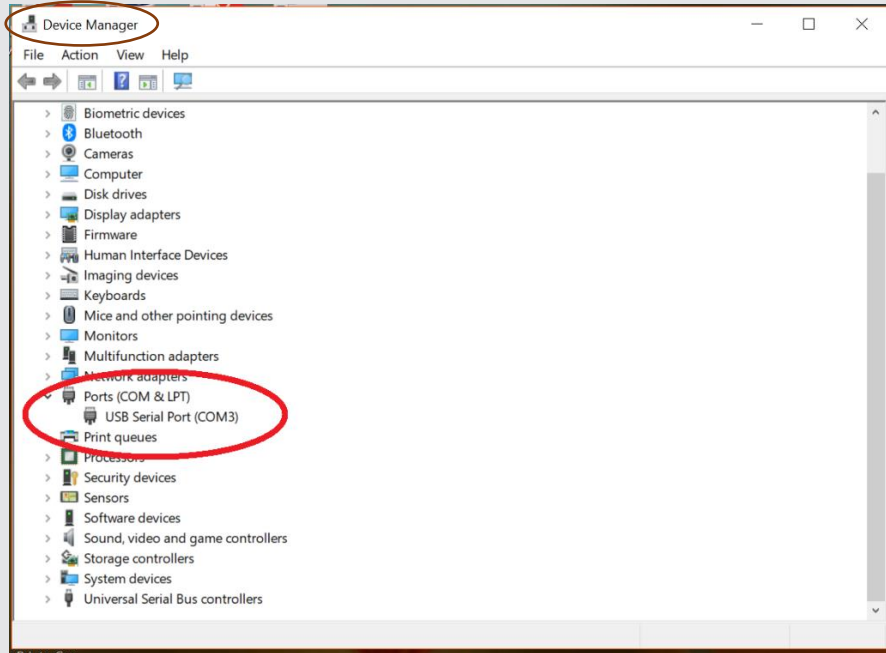
What equipment do I need and how do I do it?

1. You will need both a hardware and a software tool to accomplish this. The hardware tool needed is a USB-to-DB-9 (Serial) Male connector, or an RJ-45-to-DB-9 (Serial) Male connector: the USB or RJ-45 side will be plugged into your computer and the DB-9 (Serial) into the BoxIQ controller. These can be purchased from a typical electronics store, or online (e.g. https://www.bestbuy.com/site/insignia-1-3-usb-to-rs-232-db9-pda-serial-adapter-cable-black/5883029.p?skuId=5883029&ref=212&loc=1&extStoreId=1437&&ref=212&loc=1&ds_rl=1266837&gclid=Cj0KCOQiAnNXiBRCoARIsAJe_1cow1EEyKn8nASZn5qK0VQRfbSwuzX8-FDmv-FZ1BR8qSCVVTtH_gAYaAsyKEALw_wcB&gclsrc=aw.ds). For the free software tool, go to www.putty.org to download (we will show how to do this in the next section) and install Putty on the computer you will use to program the BoxIQ IP addresses.
 - a. Before making use of Putty, you will need to identify and set the Putty Serial Connection settings
 - i. Find the “Device Manager” tool on your computer. For example, click on your Windows button, then the Home button and then type in “device manager” in the search bar and click Enter. Click on the resultant “Device Manager” icon

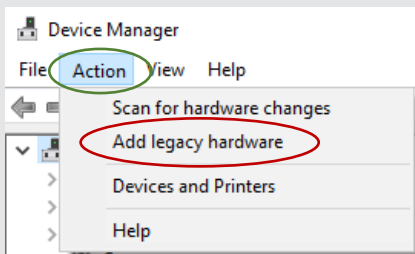


Setting a Static IP Address

- ii. The Device Manager application opens. Click on “Ports” to find the communication port number that you will plug either your USB(or Ethernet)-to-Serial adapter into. In this case, it is “COM3”

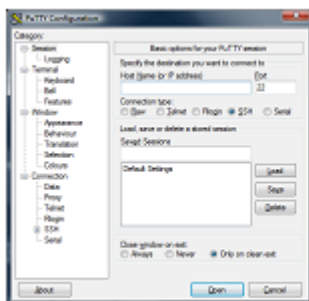


If the “Ports” selection does not appear, you will need to click on “Action” and “Add legacy hardware” to follow the Microsoft prompts to add communication ports. Then Ports will appear.



We are finished with Device Manager, so, after noting the communication port, it can be closed.

- iii. The Device Manager application opens. Click on “Ports” to find the communication port number that you will plug either your USB(or Ethernet)-to-Serial adapter into. In this case, it is “COM3”



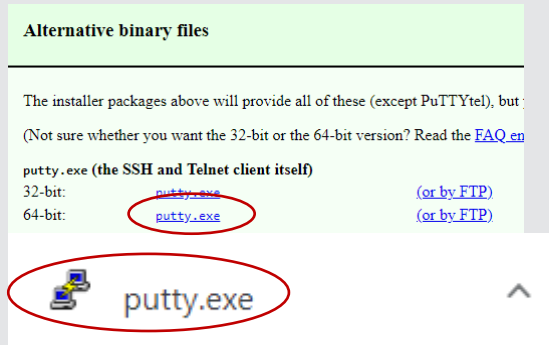
Download PuTTY

PuTTY is an SSH and telnet client source code and is developed and

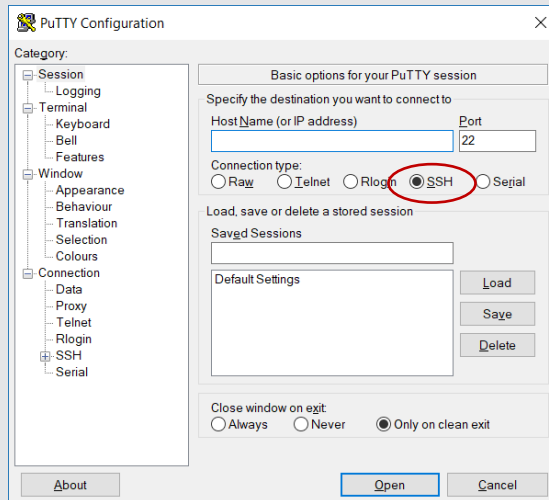
You can download PuTTY [here](#).

Setting a Static IP Address

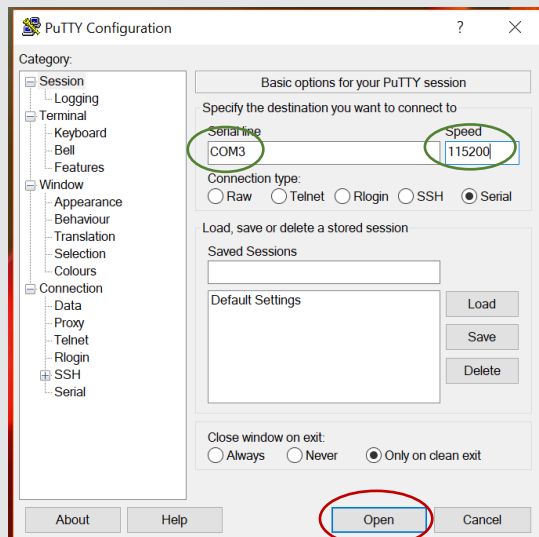
- iv. For example, for a 64-bit Windows computer, click on the following link and then the following icon that appears after the program had been downloaded:



- v. The Putty program will open. Click “Serial”.

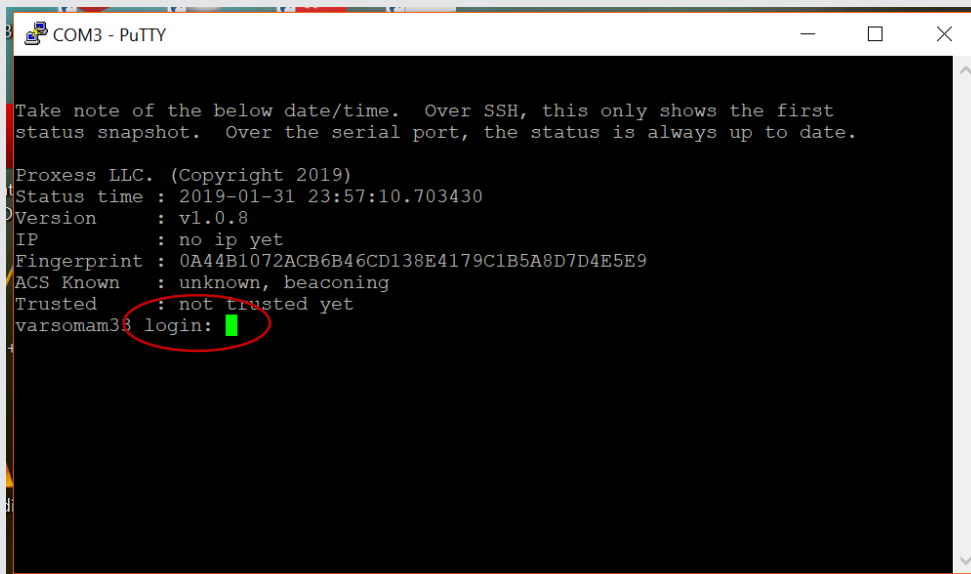
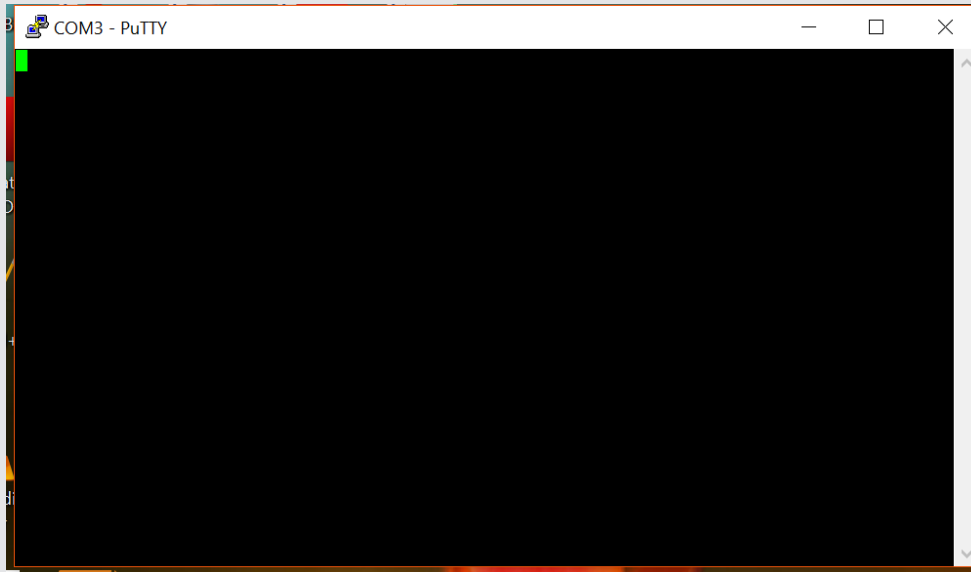


- vi. Enter the port name you found in the previous steps. In this case, it's COM3 and set the “Speed” (Baud Rate) to “115200”. Then click “Open”



Setting a Static IP Address

2. A black screen will appear during the opening process and the Putty programming tool will then open. The top of the window confirms your computer's comm port and the body of the screen shows the version of the BoxIQ, any IP address it may have, its unique identifying Fingerprint, any ACS (access control system) it may be connected with and if it has been linked and trusted with an ACS.

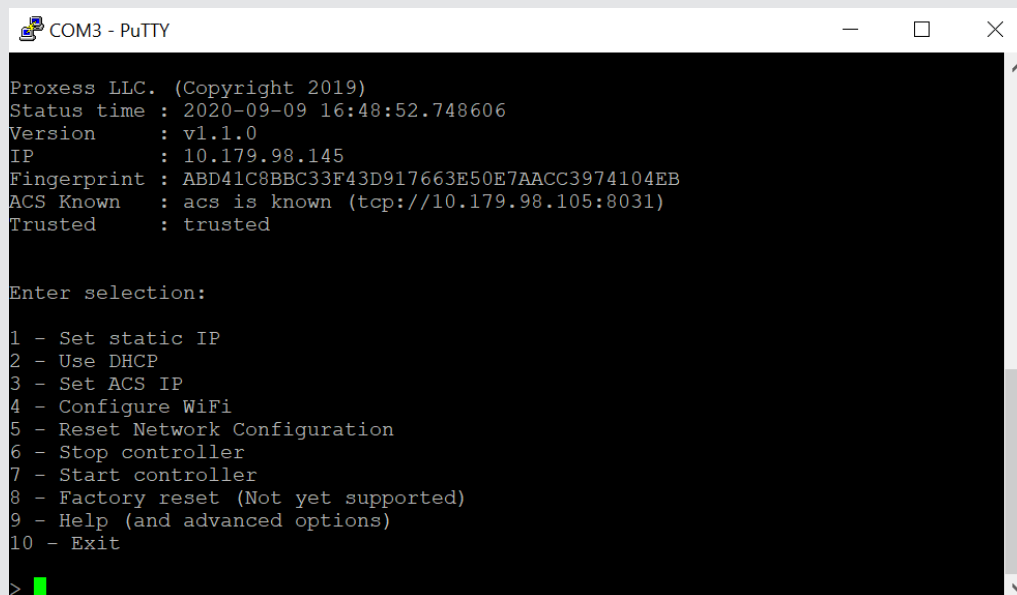


3. The Login screen will open. Use the following Login credentials:
 - a. ID: "root"
 - b. Password: "ProxessControllers" (case sensitive, please don't forget the 's' at the end of 'Controllers')

Note: If the login credentials do not work, it is likely that the controller has already been encrypted with an ACS software. If this is the case, a hardware reset on the controller will need to be performed, which will reset the default login credentials and will require the controller to be configured with the software, on a "flat" network, as earlier described.

Setting a Static IP Address

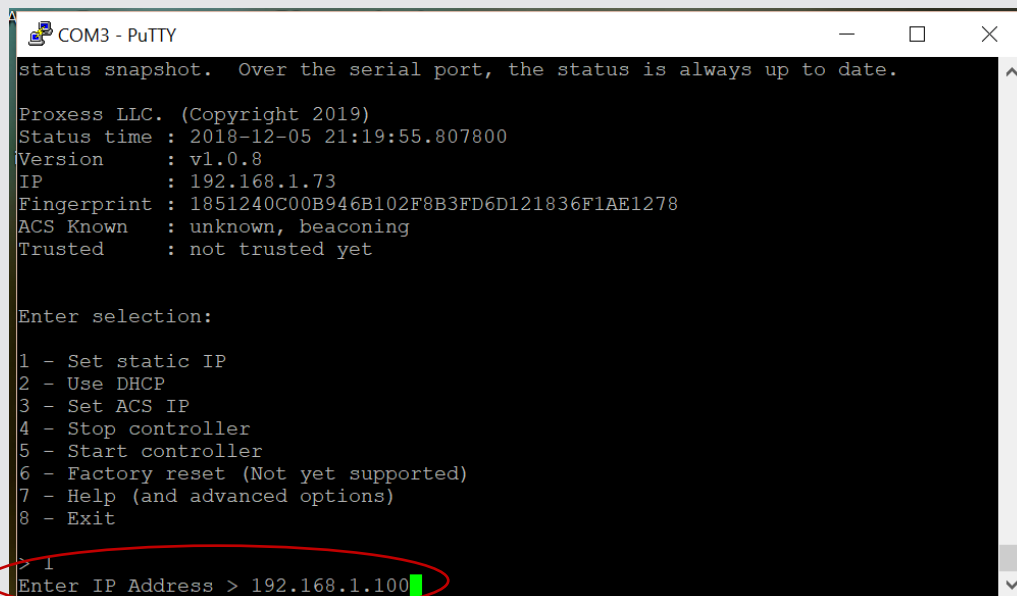
4. A correct login will open the controller setting screen. During the typical “flat” network automatic-configuration process, an IP address will be automatically assigned to the controller. In this case, we are preparing for the remote connection between the software and a controller and will manually set the IP address. At the prompt type “1” and hit your Enter button.



```
COM3 - PuTTY
Proxess LLC. (Copyright 2019)
Status time : 2020-09-09 16:48:52.748606
Version      : v1.1.0
IP           : 10.179.98.145
Fingerprint  : ABD41C8BBC33F43D917663E50E7AACC3974104EB
ACS Known    : acs is known (tcp://10.179.98.105:8031)
Trusted      : trusted

Enter selection:
1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Configure WiFi
5 - Reset Network Configuration
6 - Stop controller
7 - Start controller
8 - Factory reset (Not yet supported)
9 - Help (and advanced options)
10 - Exit
>
```

5. Enter the IP address that you want the controller to have and then hit your Enter button.



```
COM3 - PuTTY
status snapshot. Over the serial port, the status is always up to date.

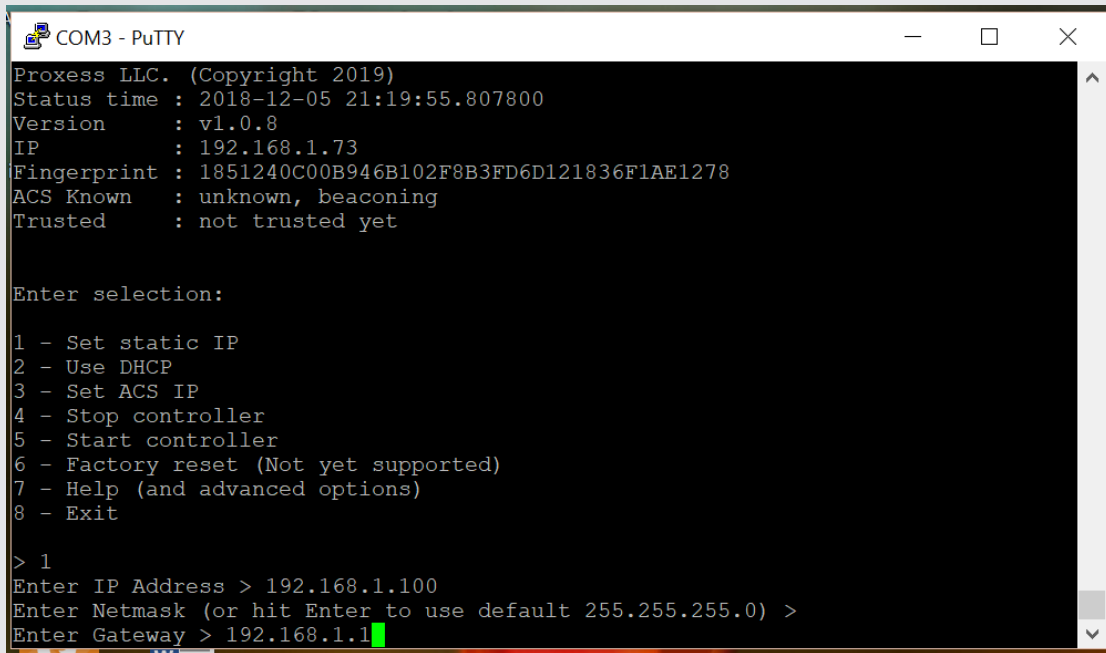
Proxess LLC. (Copyright 2019)
Status time : 2018-12-05 21:19:55.807800
Version      : v1.0.8
IP           : 192.168.1.73
Fingerprint  : 1851240C00B946B102F8B3FD6D121836F1AE1278
ACS Known    : unknown, beaconing
Trusted      : not trusted yet

Enter selection:
1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Stop controller
5 - Start controller
6 - Factory reset (Not yet supported)
7 - Help (and advanced options)
8 - Exit
> 1
Enter IP Address > 192.168.1.100
```

Setting a Static IP Address

6. The next screen asks if you want to enter the default Subnet Mask (Netmask) of 255.255.255.1 or enter a custom address. Unless IT instructs otherwise, press Enter for the default. Now type in the gateway address.

Note: It is mandatory that a valid IP address be entered here. If there is no known IP address, choose any IP address that will not interfere with other devices on your network. In other words, do not duplicate IP addresses on this network. Click Enter. **Note: The same process below can also be used to set the ACS (Access Control System) computer to a static (fixed) IP address, so the controller knows where to find it.**



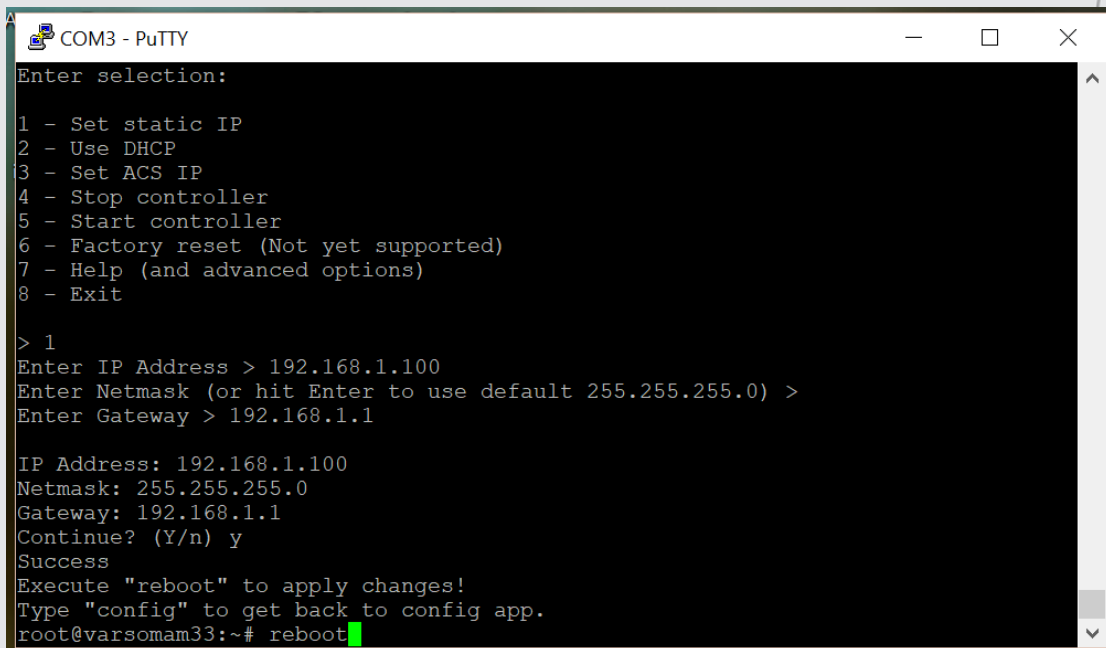
```
COM3 - PuTTY
Proxess LLC. (Copyright 2019)
Status time : 2018-12-05 21:19:55.807800
Version      : v1.0.8
IP           : 192.168.1.73
Fingerprint  : 1851240C00B946B102F8B3FD6D121836F1AE1278
ACS Known    : unknown, beaconing
Trusted      : not trusted yet

Enter selection:

1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Stop controller
5 - Start controller
6 - Factory reset (Not yet supported)
7 - Help (and advanced options)
8 - Exit

> 1
Enter IP Address > 192.168.1.100
Enter Netmask (or hit Enter to use default 255.255.255.0) >
Enter Gateway > 192.168.1.1
```

7. When asked if you are sure you want to change the IP address type “Y” and then enter. There will be a message that the controller will need to be rebooted to complete this action, type “reboot” and click Enter. This will complete having the custom static IP address set for the controller.



```
COM3 - PuTTY
Enter selection:

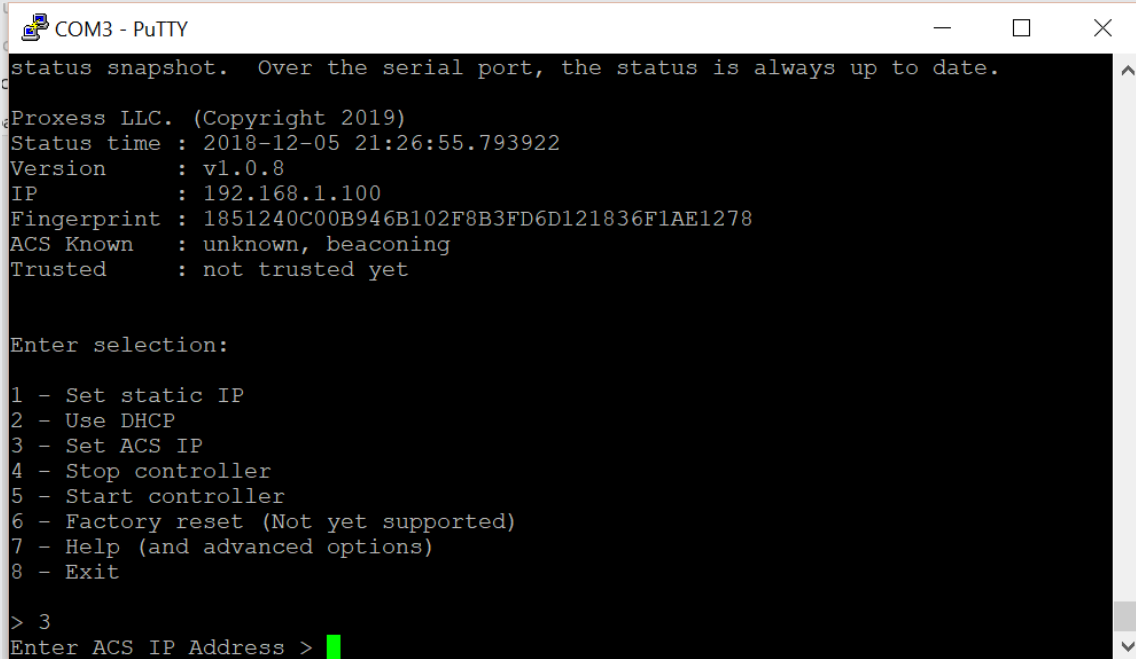
1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Stop controller
5 - Start controller
6 - Factory reset (Not yet supported)
7 - Help (and advanced options)
8 - Exit

> 1
Enter IP Address > 192.168.1.100
Enter Netmask (or hit Enter to use default 255.255.255.0) >
Enter Gateway > 192.168.1.1

IP Address: 192.168.1.100
Netmask: 255.255.255.0
Gateway: 192.168.1.1
Continue? (Y/n) y
Success
Execute "reboot" to apply changes!
Type "config" to get back to config app.
root@varsomam33:~# reboot
```

Setting a Static IP Address

8. You will be taken back on the main screen, where the IP address that you entered is listed. If it is not, please reset the device and repeat the process until it is complete and you see the IP address. Press enter again and then Log back into the controller using the same “root” ID login, and password “ProxessControllers”. We will now need to set the ACS server computer to a static IP address, so that the controller knows how to find it, as they will likely reside on different network segments, or even across the Internet.

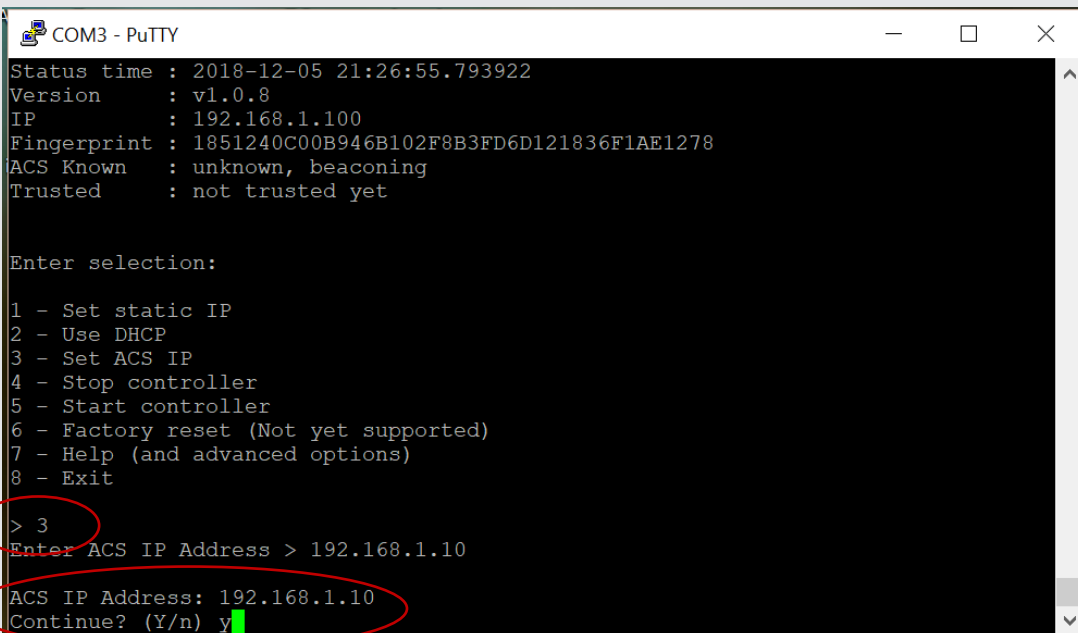


```
COM3 - PuTTY
status snapshot. Over the serial port, the status is always up to date.
Proxess LLC. (Copyright 2019)
Status time : 2018-12-05 21:26:55.793922
Version      : v1.0.8
IP           : 192.168.1.100
Fingerprint  : 1851240C00B946B102F8B3FD6D121836F1AE1278
ACS Known    : unknown, beaconing
Trusted      : not trusted yet

Enter selection:
1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Stop controller
5 - Start controller
6 - Factory reset (Not yet supported)
7 - Help (and advanced options)
8 - Exit

> 3
Enter ACS IP Address > █
```

9. Type “3” and then press Enter. Now type the IP address of your ACS server computer and then press Enter. When asked to Continue, or if you are sure, type “y” and the press Enter.



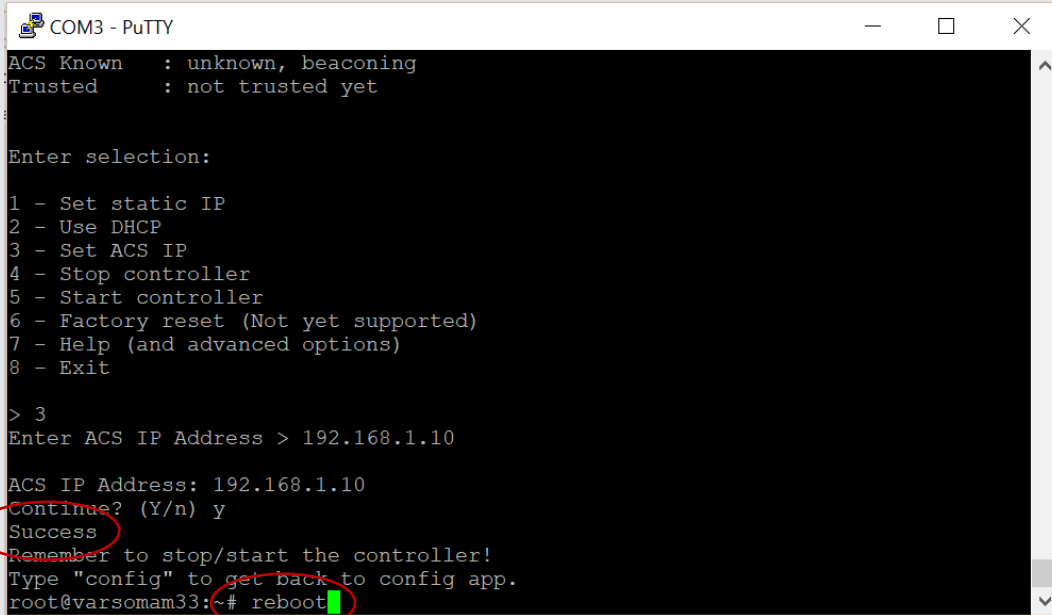
```
COM3 - PuTTY
Status time : 2018-12-05 21:26:55.793922
Version      : v1.0.8
IP           : 192.168.1.100
Fingerprint  : 1851240C00B946B102F8B3FD6D121836F1AE1278
ACS Known    : unknown, beaconing
Trusted      : not trusted yet

Enter selection:
1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Stop controller
5 - Start controller
6 - Factory reset (Not yet supported)
7 - Help (and advanced options)
8 - Exit

> 3
Enter ACS IP Address > 192.168.1.10
ACS IP Address: 192.168.1.10
Continue? (Y/n) y █
```

Setting a Static IP Address

10. Make sure that get a “Success” message, and then type “reboot” and then press enter.



```
COM3 - PuTTY
ACS Known : unknown, beaconing
Trusted : not trusted yet

Enter selection:

1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Stop controller
5 - Start controller
6 - Factory reset (Not yet supported)
7 - Help (and advanced options)
8 - Exit

> 3
Enter ACS IP Address > 192.168.1.10

ACS IP Address: 192.168.1.10
Continue? (Y/n) y
Success
Remember to stop/start the controller!
Type "config" to get back to config app.
root@varsomam33:~# reboot
```

11. Press enter again and at this point you should see that the IP address is entered. The ACS IP address will be shown as known, but its “Trusted” status will be listed as “not trusted yet”.
12. If you are done programming the IP addresses with Putty, then this application may be closed and the serial connector removed from the controller. Now, go back to the ProxessIQ™ software and return to the “Controllers” menu to bind with and encrypt the controller with the software. This process may be performed using any client software, as well as the server software, as long as the server software is online.
13. If you wish to continue with Putty to Configure the WiFi connection settings for the controller, see the next section.

END

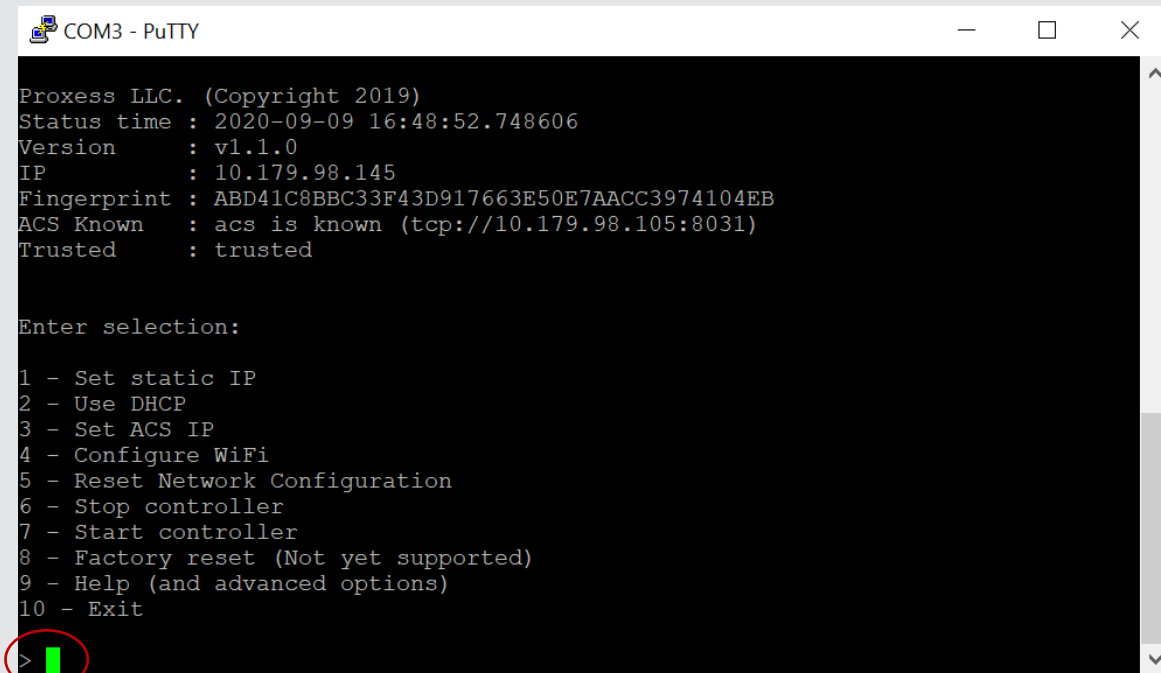
WiFi Connection

Instructions for Connecting Controllers & Bridges to the Server via WiFi

Connecting Controllers & Bridges over WiFi

The controller may also be connected to the ProxessIQ™ software through an existing permanent or temporary WiFi network. The controller WiFi communication can be used as the exclusive communication method, or as a backup to the ethernet or POE connection. WiFi is also an effective means to set up a Proxess system in a new construction or retrofit environment, where the IT system may not yet be available.

1. You may begin from the end of the previous section, with the Putty Main Menu open.
2. Or, you may begin from scratch and follow the instructions on pages 1-5 above and bring up the Putty Main Menu.
3. At the prompt type “4” and hit your Enter button.



```
COM3 - PuTTY

Proxess LLC. (Copyright 2019)
Status time : 2020-09-09 16:48:52.748606
Version      : v1.1.0
IP           : 10.179.98.145
Fingerprint  : ABD41C8BBC33F43D917663E50E7AACC3974104EB
ACS Known    : acs is known (tcp://10.179.98.105:8031)
Trusted      : trusted

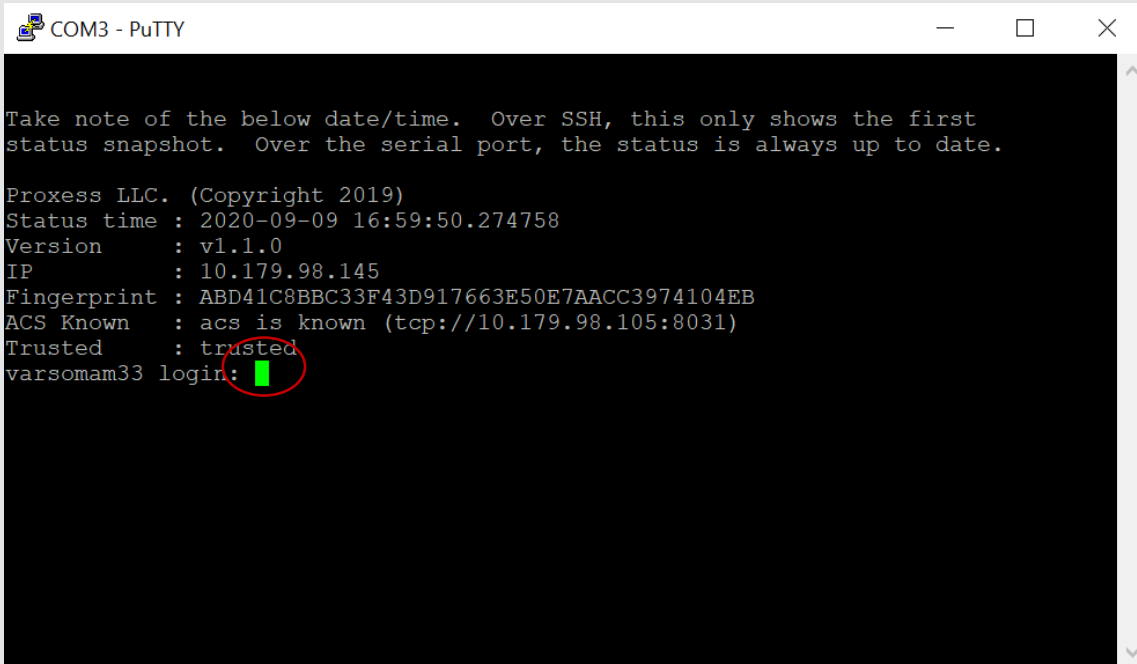
Enter selection:

1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Configure WiFi
5 - Reset Network Configuration
6 - Stop controller
7 - Start controller
8 - Factory reset (Not yet supported)
9 - Help (and advanced options)
10 - Exit

>
```

Connecting Controllers & Bridges over WiFi

4. The following screen opens. At the prompt, type “root” for the login and hit your Enter button..

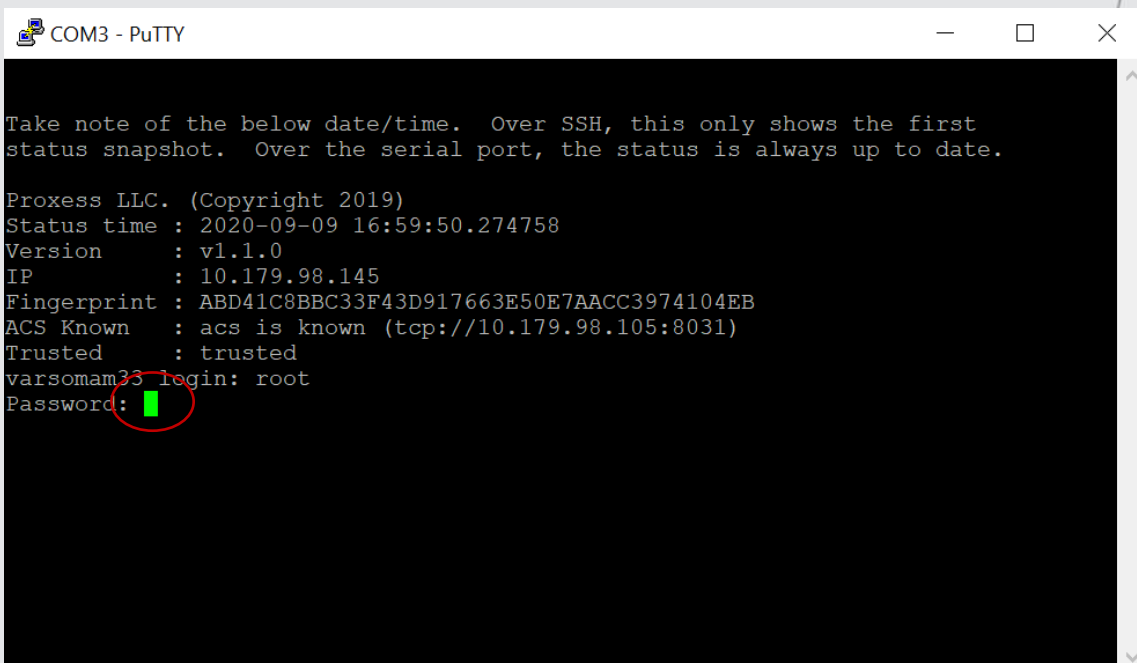


```
COM3 - PuTTY

Take note of the below date/time. Over SSH, this only shows the first
status snapshot. Over the serial port, the status is always up to date.

Proxess LLC. (Copyright 2019)
Status time : 2020-09-09 16:59:50.274758
Version      : v1.1.0
IP           : 10.179.98.145
Fingerprint  : ABD41C8BBC33F43D917663E50E7AACC3974104EB
ACS Known    : acs is known (tcp://10.179.98.105:8031)
Trusted      : trusted
varsomam33 login: █
```

5. At the Password prompt, type “XYZ” and hit your Enter button.



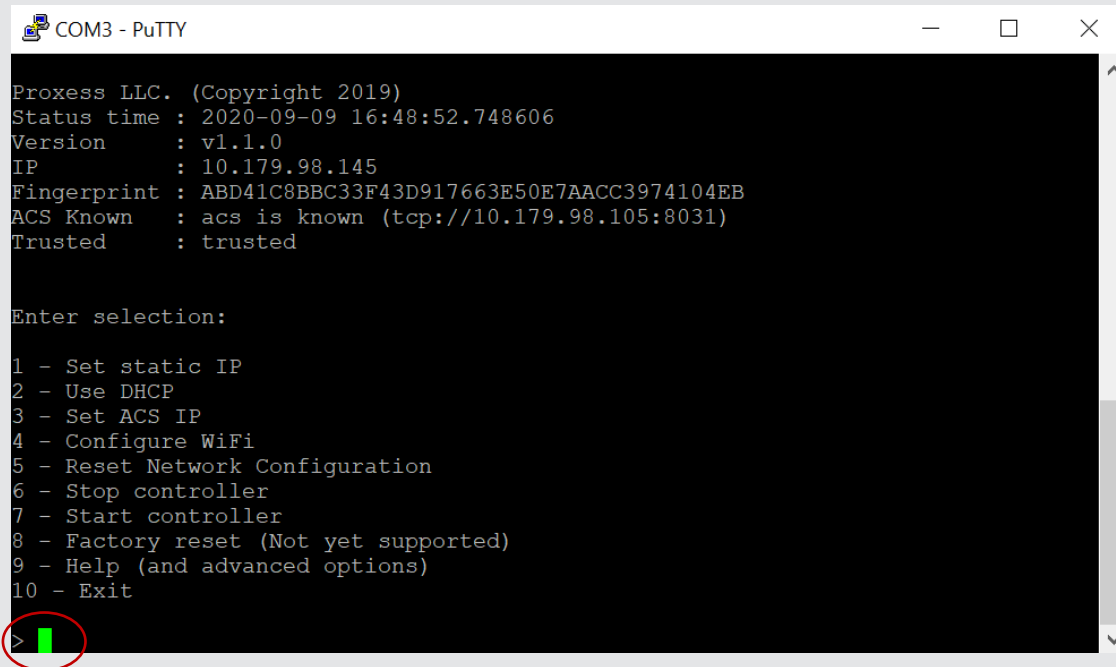
```
COM3 - PuTTY

Take note of the below date/time. Over SSH, this only shows the first
status snapshot. Over the serial port, the status is always up to date.

Proxess LLC. (Copyright 2019)
Status time : 2020-09-09 16:59:50.274758
Version      : v1.1.0
IP           : 10.179.98.145
Fingerprint  : ABD41C8BBC33F43D917663E50E7AACC3974104EB
ACS Known    : acs is known (tcp://10.179.98.105:8031)
Trusted      : trusted
varsomam33 login: root
Password: █
```

Connecting Controllers & Bridges over WiFi

6. The following screen opens. At the prompt, type “4” to Configure WiFi and hit your Enter button.



```
COM3 - PuTTY

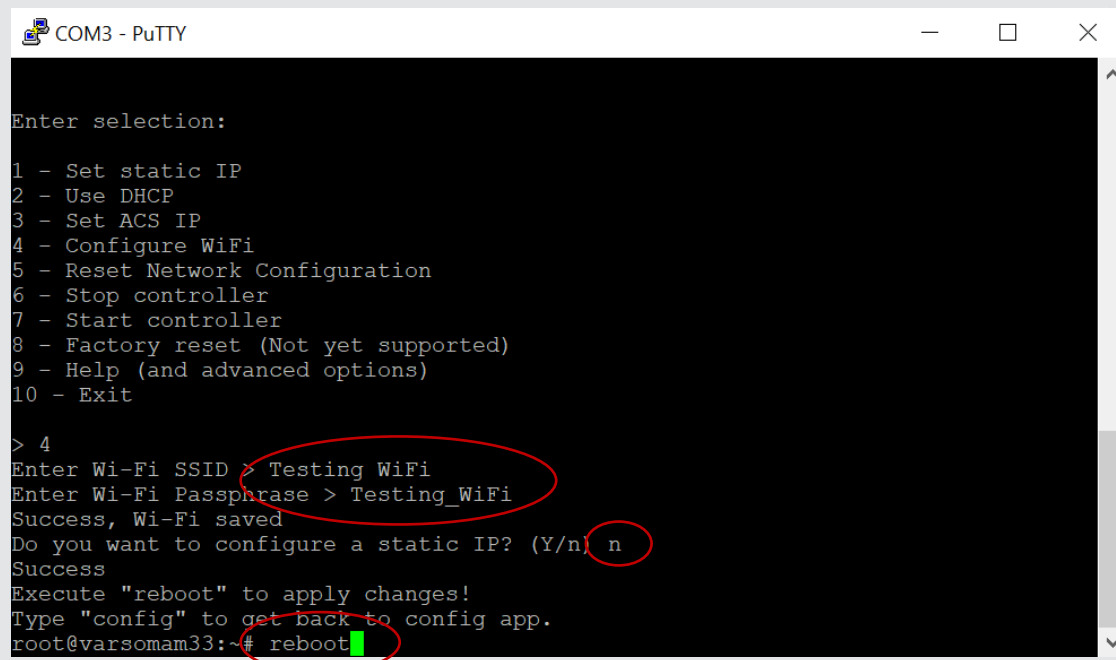
Proxess LLC. (Copyright 2019)
Status time : 2020-09-09 16:48:52.748606
Version      : v1.1.0
IP           : 10.179.98.145
Fingerprint  : ABD41C8BBC33F43D917663E50E7AACC3974104EB
ACS Known    : acs is known (tcp://10.179.98.105:8031)
Trusted      : trusted

Enter selection:

1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Configure WiFi
5 - Reset Network Configuration
6 - Stop controller
7 - Start controller
8 - Factory reset (Not yet supported)
9 - Help (and advanced options)
10 - Exit

>
```

7. Enter the SSID of your WiFi – “Testing WiFi” in this case. Enter its Passphrase (password) – “Testing_WiFi” in this case. For this training segment, enter “n” for configuring a static IP. At the prompt, type “reboot”.



```
COM3 - PuTTY

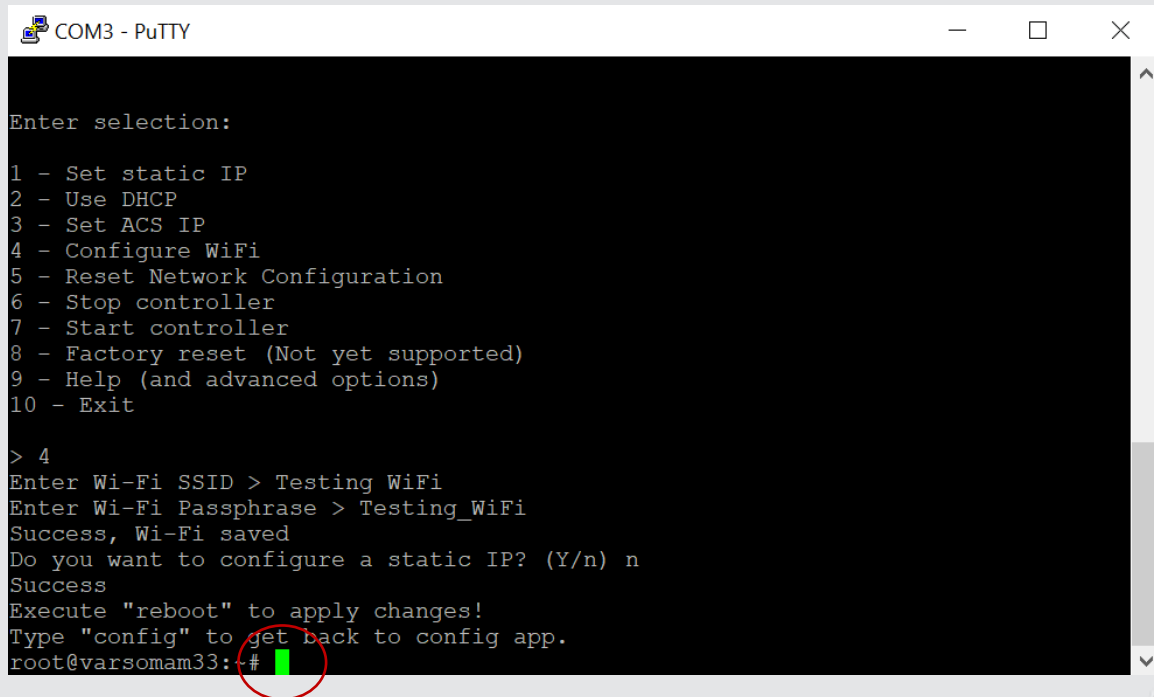
Enter selection:

1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Configure WiFi
5 - Reset Network Configuration
6 - Stop controller
7 - Start controller
8 - Factory reset (Not yet supported)
9 - Help (and advanced options)
10 - Exit

> 4
Enter Wi-Fi SSID > Testing WiFi
Enter Wi-Fi Passphrase > Testing_WiFi
Success, Wi-Fi saved
Do you want to configure a static IP? (Y/n) n
Success
Execute "reboot" to apply changes!
Type "config" to get back to config app.
root@varsomam33:~# reboot
```

Connecting Controllers & Bridges over WiFi

8. At the prompt, type "config" and hit your Enter button.



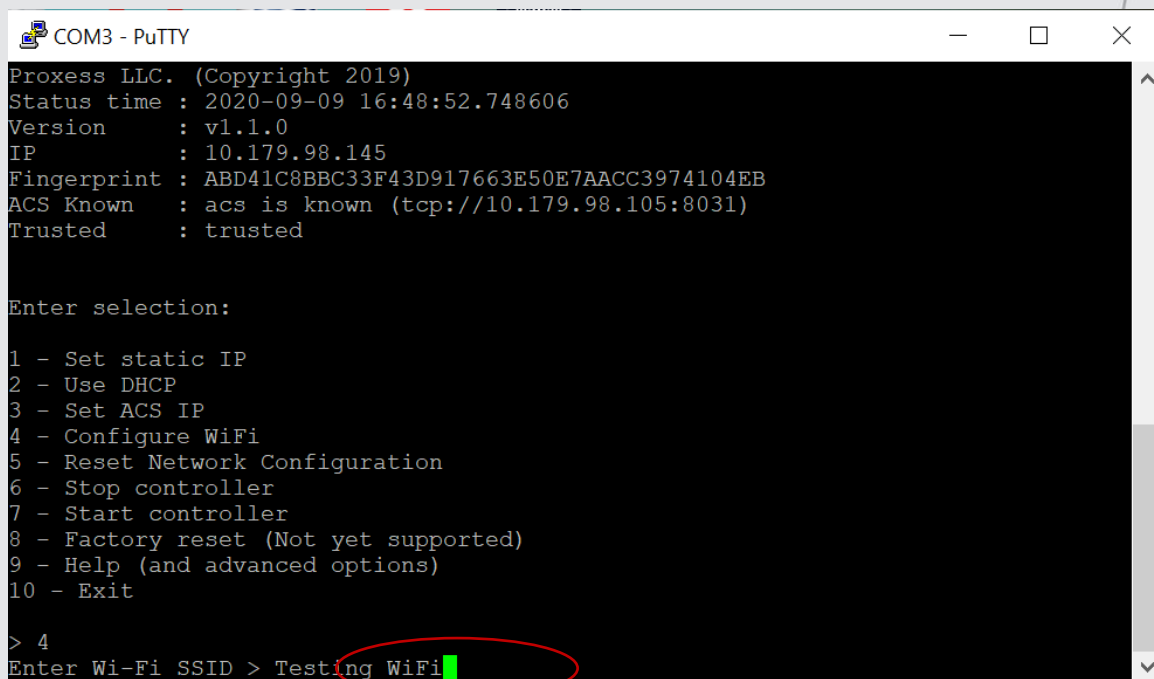
```
COM3 - PuTTY

Enter selection:

1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Configure WiFi
5 - Reset Network Configuration
6 - Stop controller
7 - Start controller
8 - Factory reset (Not yet supported)
9 - Help (and advanced options)
10 - Exit

> 4
Enter Wi-Fi SSID > Testing WiFi
Enter Wi-Fi Passphrase > Testing_WiFi
Success, Wi-Fi saved
Do you want to configure a static IP? (Y/n) n
Success
Execute "reboot" to apply changes!
Type "config" to get back to config app.
root@varsomam33:~#
```

9. Now that the controller has rebooted, enter the WiFi SSID – “Testing WiFi” in this case and hit your Enter button.



```
COM3 - PuTTY

Proxess LLC. (Copyright 2019)
Status time : 2020-09-09 16:48:52.748606
Version      : v1.1.0
IP           : 10.179.98.145
Fingerprint  : ABD41C8BBC33F43D917663E50E7AACC3974104EB
ACS Known    : acs is known (tcp://10.179.98.105:8031)
Trusted      : trusted

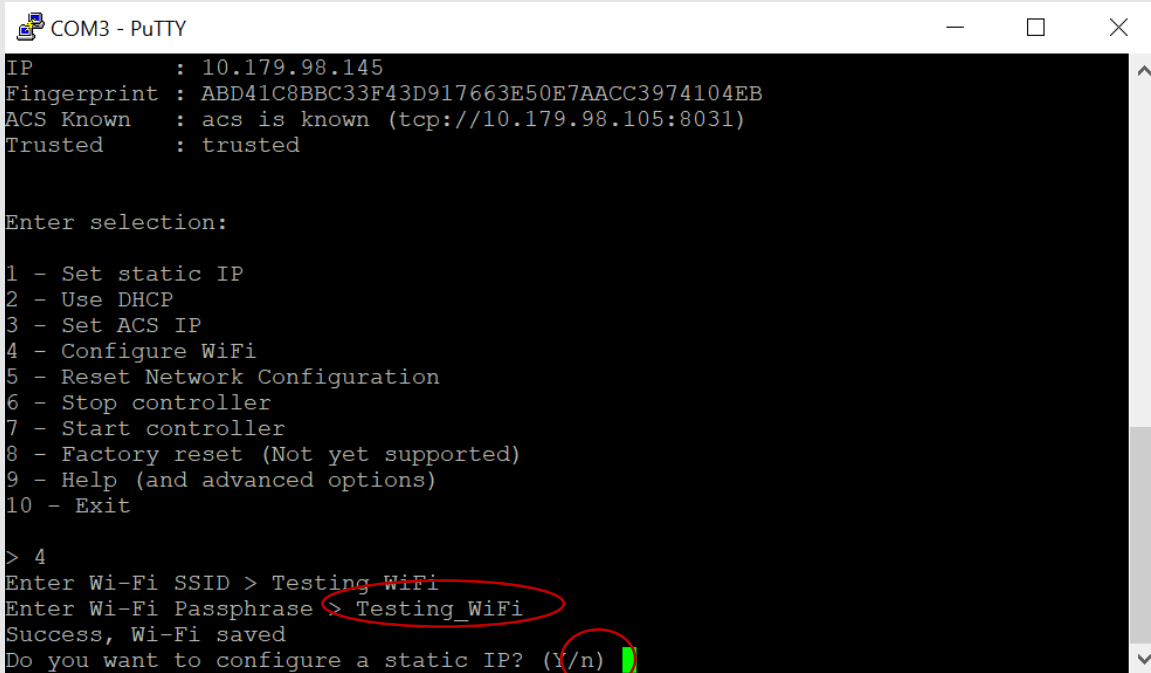
Enter selection:

1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Configure WiFi
5 - Reset Network Configuration
6 - Stop controller
7 - Start controller
8 - Factory reset (Not yet supported)
9 - Help (and advanced options)
10 - Exit

> 4
Enter Wi-Fi SSID > Testing WiFi
```

Connecting Controllers & Bridges over WiFi

10. Enter the Passphrase (password) – “Testing_WiFi” in this case, and hit your Enter button. Click “n” when asked to configure a static IP and hit your Enter button.



```
COM3 - PuTTY
IP      : 10.179.98.145
Fingerprint : ABD41C8BBC33F43D917663E50E7AACC3974104EB
ACS Known  : acs is known (tcp://10.179.98.105:8031)
Trusted    : trusted

Enter selection:

1 - Set static IP
2 - Use DHCP
3 - Set ACS IP
4 - Configure WiFi
5 - Reset Network Configuration
6 - Stop controller
7 - Start controller
8 - Factory reset (Not yet supported)
9 - Help (and advanced options)
10 - Exit

> 4
Enter Wi-Fi SSID > Testing_WiFi
Enter Wi-Fi Passphrase > Testing_WiFi
Success, Wi-Fi saved
Do you want to configure a static IP? (Y/n) █
```

You are now complete with the WiFi programming and can verify that your controller appears in the Controller menu.

END

Open Port Requirements

Ports to Open for Controllers & Bridges

Open port requirements for
Controller & Bridge-to-Server
Communications

Open Port Requirements

BoxIQ-to-Server

The Proxess BoxIQ door controller (and bridge) Beacons on **UDP Port 8032**

The controller communicates with the access control system server on **TCP port 8031**

By Default, the client communicates with the server on **TCP Ports 8009, 8011, and 8008**

This is a summary of the firewall rules that the installer attempts to create:

```
<fire:FirewallException Id="ProxessControllerCommunication"
    Name="Proxess Controller Communication"
    Protocol="tcp"
    Port="8031"
    Scope="any"
    IgnoreFailure="yes"
    Profile="all" />
<fire:FirewallException Id="ProxessControllerBeacon"
    Name="Proxess Controller Beacon"
    Protocol="udp"
    Port="8032"
    Scope="localSubnet"
    IgnoreFailure="yes"
    Profile="all" />
<fire:FirewallException Id="ProxessServerSecureCommunication"
    Name="Proxess Server Secure Communication"
    Protocol="tcp"
    Port="8009"
    Scope="any"
    IgnoreFailure="yes"
    Profile="all" />
<fire:FirewallException Id="ProxessServerOpenCommunication"
    Name="Proxess Server Open Communication"
    Protocol="tcp"
    Port="8011"
    Scope="any"
    IgnoreFailure="yes"
    Profile="all" />
<fire:FirewallException Id="ProxessIdentityServer"
    Name="Proxess Identity Server"
    Protocol="tcp"
    Port="8008"
    Scope="any"
    IgnoreFailure="yes"
    Profile="all" />
```

Open Port Requirements

BoxIQ-to-Server

Other Things to take into Consideration

Resolving Local Host Names

When using the computer name for a server's host name, any client trying to access the server will need to be able to resolve that host name. In a local network environment this happens automatically through either local DNS (typically in a domain environment) or through NetBIOS name resolution. If you are attempting to connect to the server's host name outside of your local network environment, these name resolution methods will not be available. The simplest approach for creating this mapping is to create an entry for the host name in the local host file of the client computer that is attempting to reach the server.

The Windows Host file is located at `c:\Windows\System32\Drivers\etc\hosts`. To make edits to this file, you will need to open the file with a simple text editor (like Notepad) with administrator privileges (Right-Click and select Run as administrator). The host file does not have an extension (.txt) so you will need to select "All Files (*.*)" in the file Open dialog. Once the host file is open, you will need to create a new line that contains the routable IP address followed by the computers host name. Assuming this is outside the internal network, this will need to be the public IP with proper routing/NAT rules setup. For example, if your public IP is "123.456.0.100" and your server's host name is "myservername", the host file entry should look like this:

```
123.456.0.1 myserversname
```

A robust alternative to this is to use a registered domain name with a public DNS record for your server's host name.

NAT/Port Forwarding

To connect to a server inside a local network from outside of the local network, you will need to set up the appropriate NAT or Port Forwarding rules on your gateway /firewall. These rules need to provide a path from the public IP (provided by your ISP) to the internal network IP for all ports required for communication to the AxessIQ server. The default ports that are used for this communication are 8008, 8009, and 8011. Setting up NAT/Port Forwarding rules will be specific to your gateway manufacture. Please refer to the manufactures documentation for setting this up.

Example documentation for setting up port forwarding on a Comcast gateway can be found here:

<https://www.xfinity.com/support/articles/port-forwarding-xfinity-wireless-gateway>

BLE Bridge Design Guide

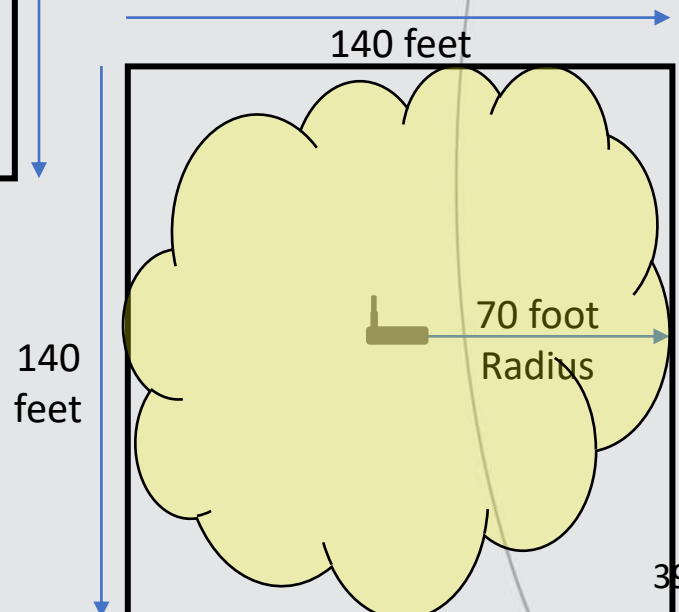
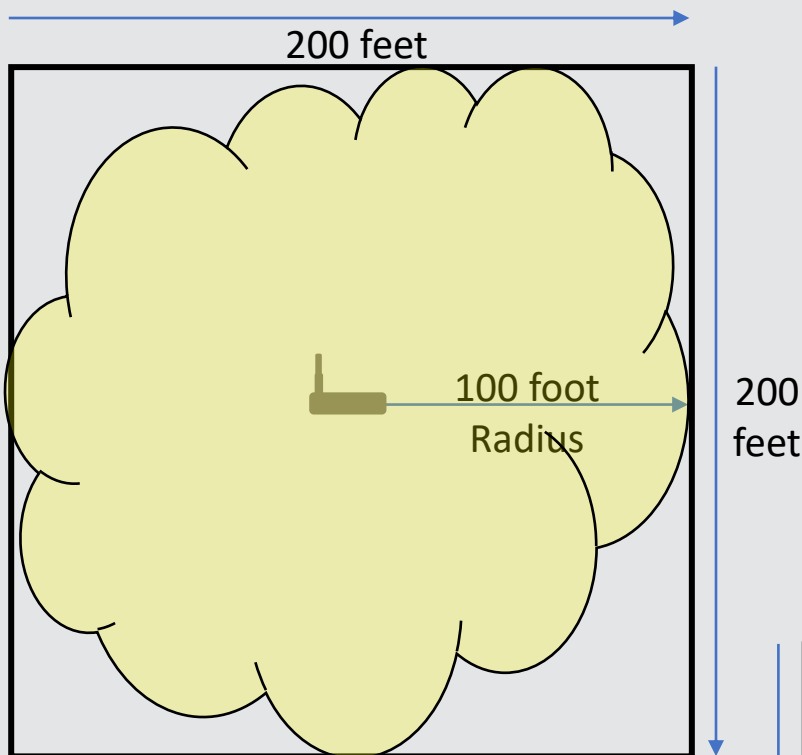
For connection to Locksets & Mini-Controllers

Bringing *Online* to the *Offline*

General Bridge Coverage

Ideal Bridge

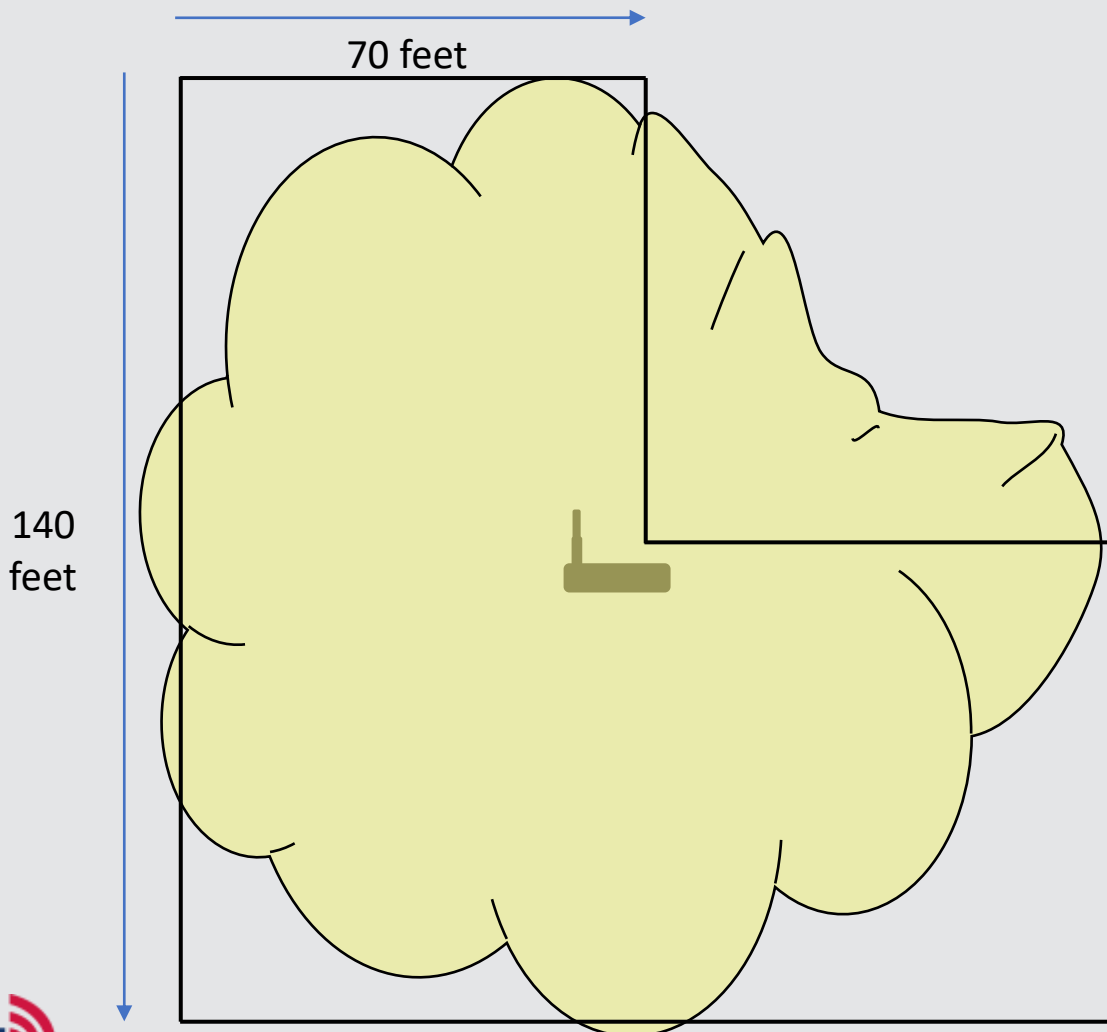
- A bridge can, by its specification, cover a maximum 100-foot radius\200-foot diameter area, which would mean that only one bridge is required to cover the below-left space.
- Throughout this guide we will instead use the more practical free-space coverage of an 80-foot radius 160-foot diameter.
- However, even when they are properly placed in the public side of the ceiling tiles, the signal from *any* wireless bridge is not a perfect circle and can not be guaranteed to cover the full extent of the specified distance.



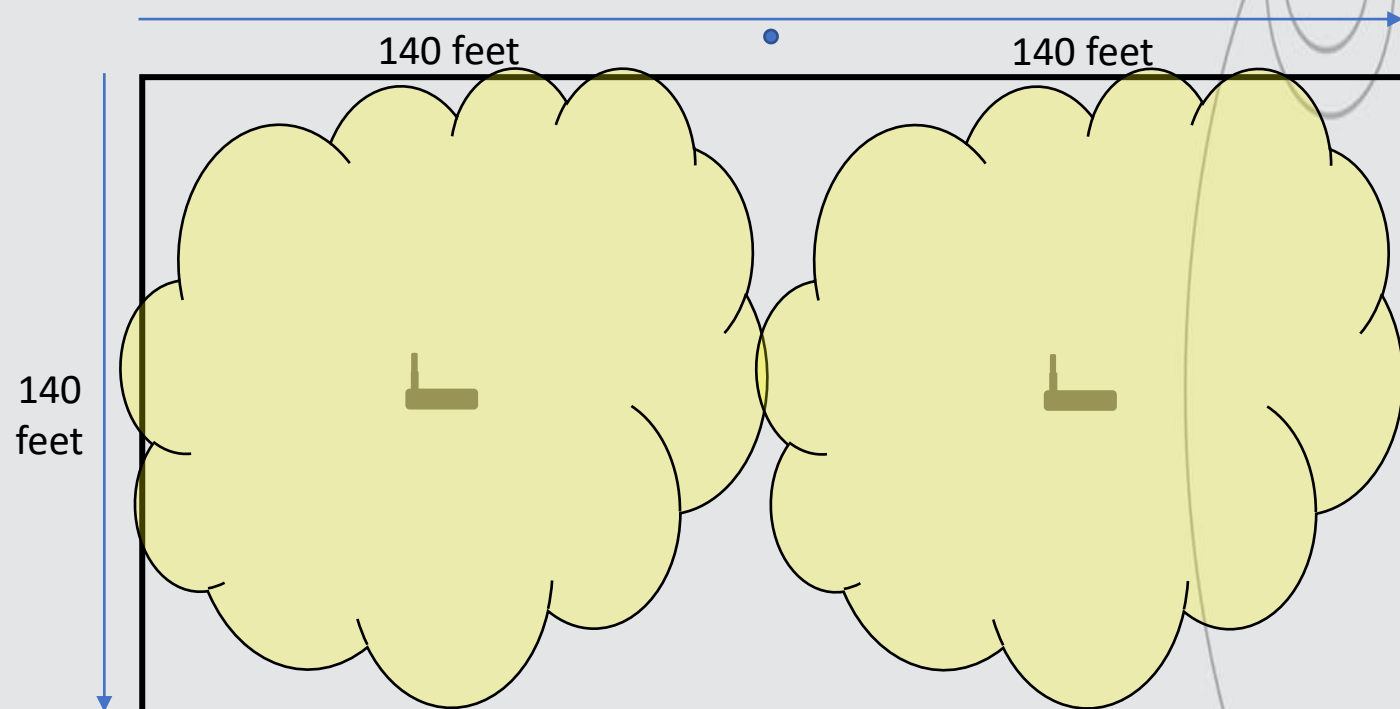
General Bridge Coverage

Realistic Bridge

- A bridge can, by its specification, cover a maximum 70-foot radius\distance, which would mean that only one bridge is required to cover this area.
- However, even when they are properly placed in the public side of the ceiling tiles, the signal from any wireless bridge is not a perfect circle and can not be guaranteed to cover the full extent of the specified distance. In addition, walls and other obstacles will reduce the communication distances.
- Therefore, the deployment shown below would not produce assured constant connectivity to locksets or mini-controllers on the perimeter of the building.



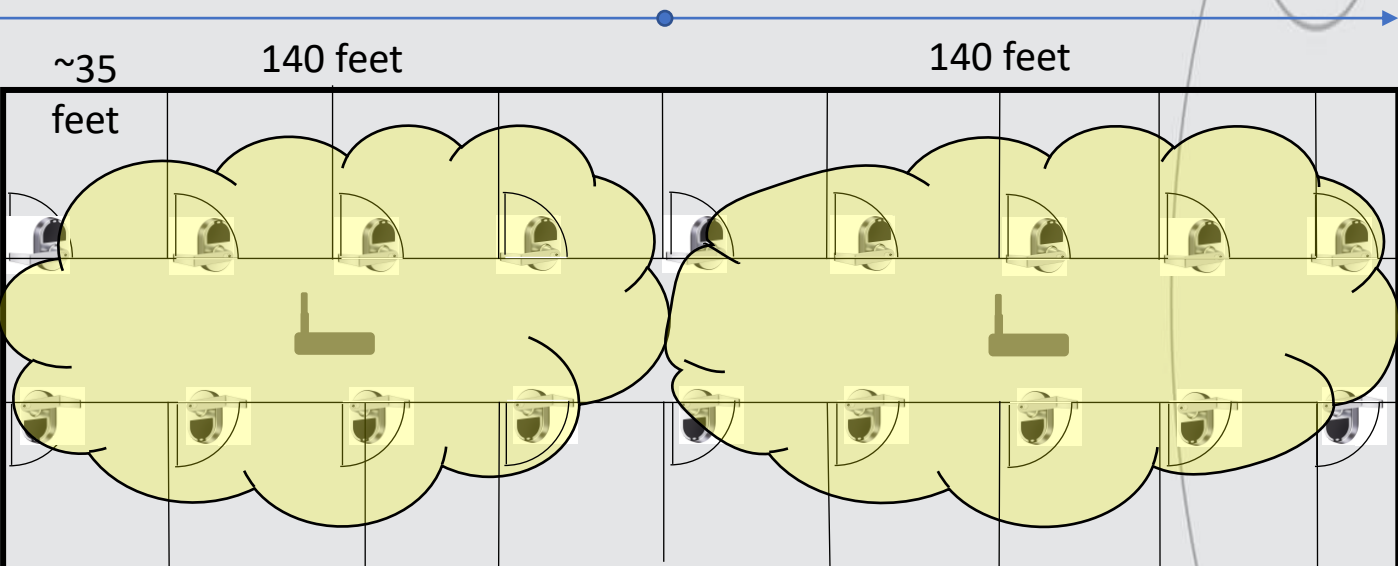
- Two bridges can, by their specification, cover a maximum 160-foot diameter\distance each, which would mean that only two bridges are required to cover this 320 by 160-foot area.
- However, even when they are properly placed in the public side of the ceiling tiles, the signal from any wireless bridge is not a perfect circle and can not be guaranteed to cover the full extent of the specified distance.
- Therefore, the deployment shown below would not produce assured constant connectivity to locksets or mini-controllers on the perimeter of the building.



General Bridge Coverage

Hallway Wrong

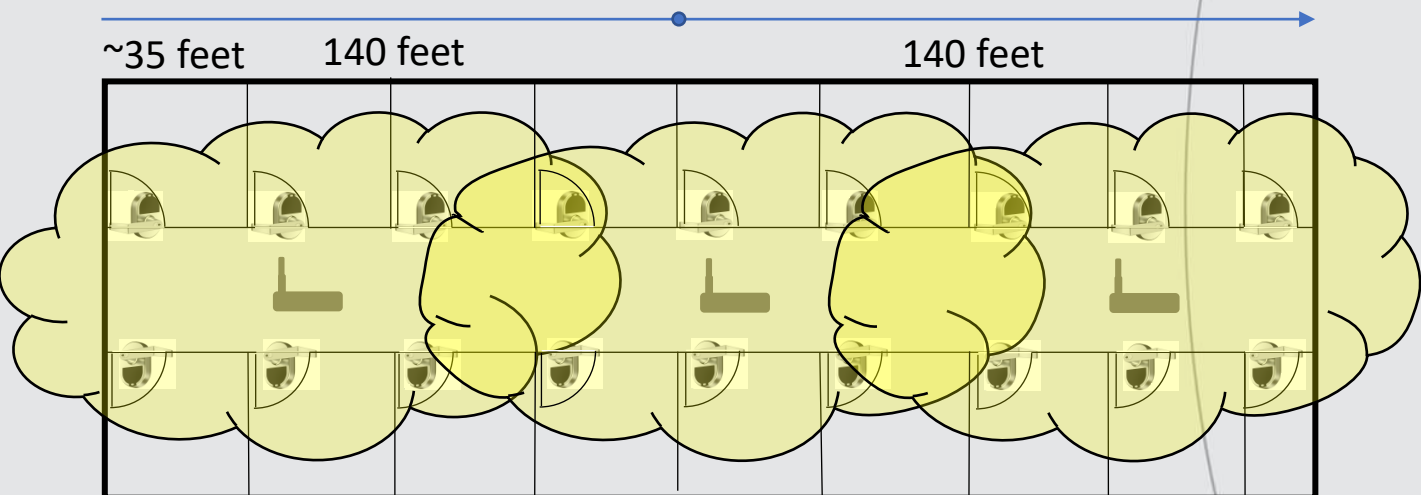
- Two bridges can, by their specification, cover a maximum 140-foot diameter\distance each, which would mean that only two bridges are required to cover this 280-foot long hallway.
- However, even when they are properly placed in the public side of the ceiling tiles, the signal from any wireless bridge is not a perfect circle and can not be guaranteed to cover the full extent of the specified distance, especially when the normal obstructions and interference from building materials are taken into consideration.
- Therefore, the deployment shown below may not assure constant connectivity to the locksets in this hallway.



General Bridge Coverage

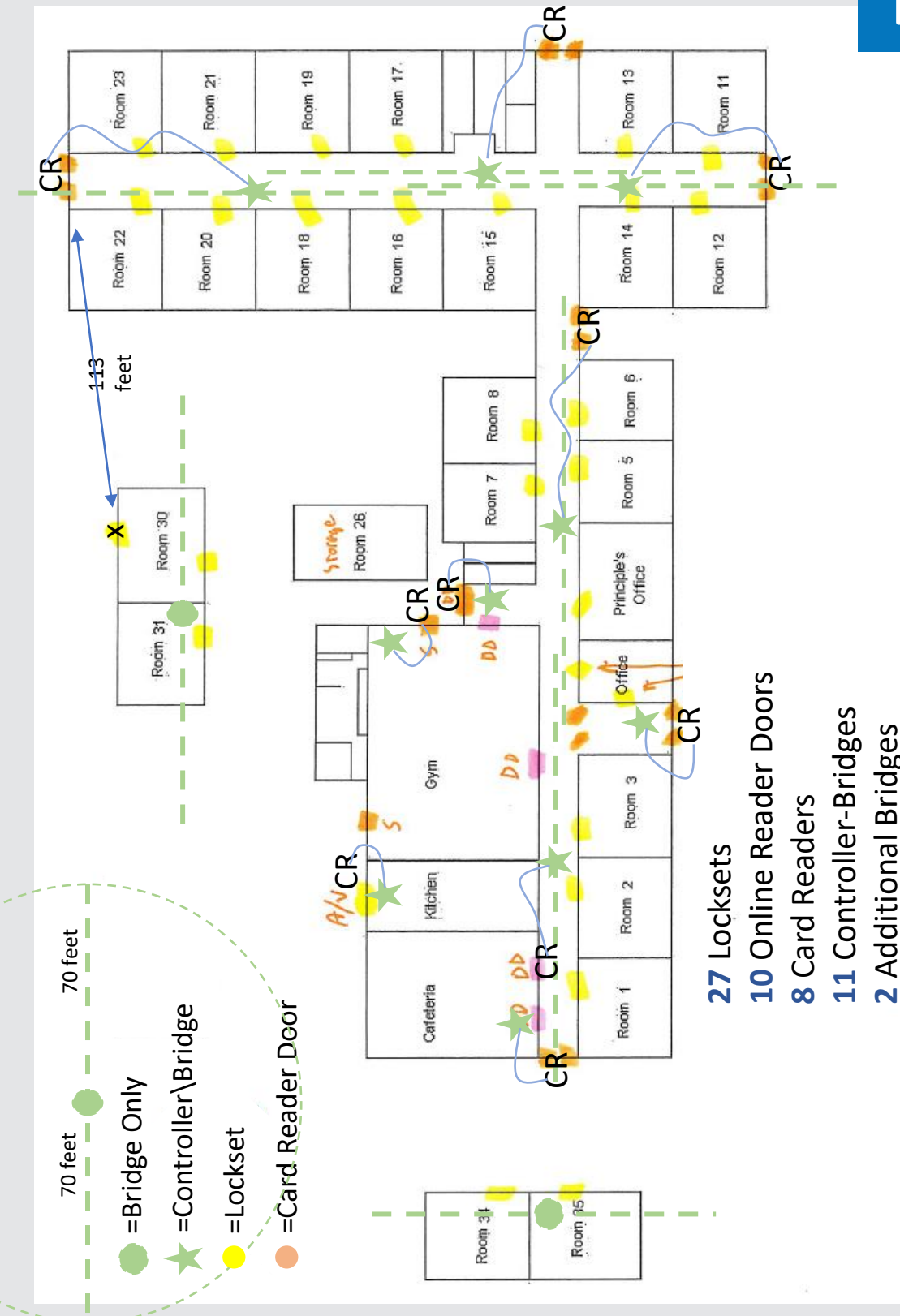
Hallway
Correct

- This building layout will produce reliable connectivity from the locksets to the bridges and therefore to the software.
- By adding an additional bridge, we have compensated for the imperfections of a wireless signal pattern and the normal obstructions and possible interference from building materials.



School Bridge Coverage

Practical Example



- An even better estimate requires knowing the material type of each wall. If internal wall material is brick, cement, or cinderblock, the number of access points needed will increase.
- The below diagrams depict the signal drop\loss when going through certain walls or barriers.
- As your locksets approach the practical limit of the bridge's reach, the biggest issue isn't going to be the access point signal reaching locksets, but the lower power lockset signal getting back to the bridge. So, measuring distances in visible straight lines between bridges and locksets will yield the best chance of success and tests should be performed to assure your design will work.



Drywall

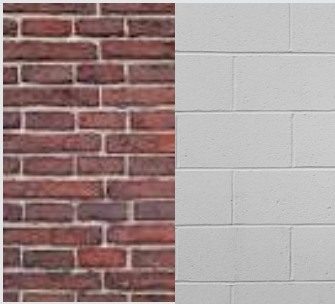


Brick

Fixed Obstructions

Building Interference

- Building materials, fixtures and fittings will have an effect on the signal strength. While the signal is capable of passing through certain objects, doing so will reduce the range which needs to be considered during the installation. Metallic objects will also cause the signal to reflect, which can cause a signal to fluctuate in strength. Also, an active building, with flowing water and electricity may also have an impact on performance, should designs or tests be performed prior to the building construction or turnover.



Brick & Cinder
Block Walls



Plumbing
Infrastructure



Metal
Construction



Stairwells



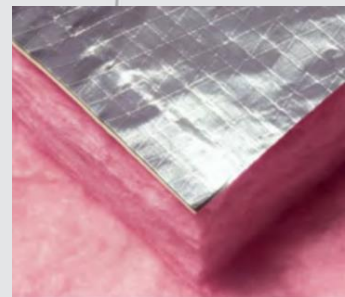
Elevator &
Equipment
Rooms



Communications
Raceways



Water &
Sprinkler
Infrastructure



Wall Insulation














Building Construction Considerations

Interference Budgets

- Compared to an office building, larger spaces, such as auditoriums or cafeterias are built differently and will likely require different bridge layouts. High ceilings and thicker wall material can necessitate other placement options. In these cases, it is possible that the use of directional antennas might be required due to the fact that most omnidirectional antenna cells cannot cover enough vertical distance. It is important to understand that a bridge mounted to a high ceiling or flush to a wall, will not work the same as one mounted on a normal height ceiling.

2.4 GHz Signal Loss (dB) through various materials:

Proxess Bridge Power Budget = 100 dB

	Air (30 feet = 60dB, 60 feet = 68dB, 100 feet = 90dB)
	Thin Window (2 dB)
	Plasterboard Wall (3 dB)
	Window Office (3 dB)
	Cinder Block Wall (4 dB)
	Dry Wall (4 dB)
	Light (Wood) Door (4 dB)
	Thick Window (4 dB)
	Glass Wall with Metal Frame (6 dB)
	Brick Wall (8 dB)
	Metal Door (11 dB)
	Concrete Wall (12 dB)
	Heavy Door (15 dB)
	Reinforced Concrete Floor (30 dB)

Overlapping

Issues with Others

- When planning the bridge\gateways\access points layout for a network, it is important to bear in mind that the coverage cells of the bridges will most likely overlap with others. While there generally should be some overlap, how much will depend on the intended use of the network. Typically, roaming and location-based services will require more overlap than networks that do not require these services. However, too much overlap can lead to increased interference, if the overlapping bridges are transmitting on the same channel as well as bumping\crowding out and orphaning nearby locksets. This problem is often exacerbated in multi-level buildings.
- ****Proxess assigns locksets to bridges, locking them down and preventing wandering and orphaning.***

