

## How to Connect to an Ethernet Device for Communication



*Bulletin #8501122b-8501116*

<b>Introduction</b>	<b>3</b>
Making a Connection to An Ethernet Device	3
What is Ethernet?	3
The Internet Protocol (IP) and Ethernet Addressing	4
The Transmission Control Protocol (TCP)	5
The User-Datagram Protocol (UDP)	5
The MACHine Address	5
<b>Example 1: Directly Connecting One Host PC to One Ethernet Device</b>	<b>5</b>
Change the IP Address of the Wired Ethernet Adapter on a Windows 10 Computer for Direct Connection	6
Making a LAN Connection to an Ethernet Device	9
Public versus Private IP Addresses	9
IP Addresses and Sub-Netting	10
Named IP Addresses	11
Router Operation	11
Packet Routing	12
For Local Delivery within the Same Network LAN	12
For Remote Delivery between Different Network LAN's	12
<b>Example 2: Connecting an Ethernet Device to a Local Area Network</b>	<b>13</b>
Prepare the Device for Network Connection	13
Determine Your Router IP Address, Username/Password or Access Code	13
Log into Your Router at its LAN IP Address to Make a DHCP Reservation for Your Device	15
Optional – Setting a Static IP Address in the Device You Want to Connect to your Home Network	21
Contrast Example 2 for Making a home LAN Connection with Making a Corporate LAN Connection	21
<b>Example 3: Remotely Accessing an Ethernet Device Connected to Your LAN</b>	<b>22</b>
Connecting to an Ethernet Device	22
How Public Clients Talk to Private Clients?	22
Before You Start - Your Public IP Address Must be Static	22
Port Forwarding, Port Mapping, or Virtual Server	23
Port Number	24
Virtual Private Network (VPN) – A Recommended Option for Increased Security with Open Ports	25
Dynamic DNS Service (One Option for Added Convenience)	26
Firewall Protection	27
Example 3: Using Port Forwarding to Remotely Access a LAN Device on a Home Network	27
Get a Static Public IP Address	27
Connect Your Device to Your LAN Router	28
Pick a Port Number to Assign to your Device	28
Log into Your Router/Gateway at its LAN IP Address and Configure Port Forwarding	28
TIP: How to Find Your Public IP Address	23
Test to See If Your Port is OPEN	34
Contrast Example 3 with Achieving Remote Access on a Corporate Network	35
<b>Glossary</b>	<b>36</b>
<b>Conclusion</b>	<b>38</b>
<b>About Acromag</b>	<b>38</b>



---

## Introduction

Acromag manufactures [Ethernet-enabled devices](#) that monitor and isolate voltage, current, thermocouple, and RTD signals, plus control analog and digital outputs, and can transmit I/O information over Ethernet and on the internet. However, the complexities of Ethernet communication can make connecting to these devices difficult. This paper outlines each of three ways that you can make a connection to an Ethernet device.

### Making a Connection to An Ethernet Device

To connect and communicate to an Ethernet device like an Acromag Ethernet module, you have three potential connection scenarios:

1. Direct connect your Ethernet device to your computer – Easiest but the most restrictive, as it dominates the use of your Ethernet port and may temporarily take your computer off-line from the internet.
2. Network connect your Ethernet device to your LAN (Local Area Network) – A little more complicated and does not include remote access from another network.
3. Remotely connect to your Ethernet device over the internet – This requires the second scenario, but adds Port Forwarding, requires a static public IP address, and potentially adds the services of a VPN (Virtual Private Network).

The first connection method is simple and straight-forward, and often used to configure an Ethernet device for network communication. The second connection method is more common, but a little more complicated to do yourself. The third method of using the internet to remotely access your device can be very complex and usually involves the purchase of additional services. For each connection type, the background knowledge required to make the connection will be reviewed first, followed by an example. If you read the background information first, you should have enough information to make the example connection yourself. It is helpful to walk through these connection examples in the order presented and each scenario will build on the concepts of the prior example. If you make it all the way through the three connection scenarios, then at least your insomnia will be cured.

Before we delve into the first connection example of directly connect to an Ethernet device, we need to understand a few basic Ethernet concepts. The second connection example will add additional concepts as required to make a LAN connection. If you complete the third connection example you will have a good understanding of what really goes on when you connect to an Ethernet device and this should be helpful in managing the Ethernet connections of your home network.

### What is Ethernet?

Ethernet is a system of connecting more than two devices to form a Local Area Network (LAN) for sharing information and resources, technically referred to as the IEEE 802.3 protocol standard. Ethernet is considered a link layer protocol of a TCP/IP stack and controls how network data is formatted and how it is transmitted to other network devices. It includes protocols for passing information between devices while avoiding simultaneous transmission by devices and it is the most widely installed network topology used for Local Area Networks (LAN), Metropolitan Area Networks (MAN or confined to a single geographic area), and Wide Area Networks (WAN or spanning a large geographic area).

Briefly, Ethernet refers to a means for transporting messages across a network as datagrams. The actual payload (data) of a single datagram frame can be up to 1500 bytes. Long streams of Ethernet data are generally divided into shorter datagrams, each inserted into a frame for transport on the same LAN, or additionally in a packet for transport between networks.

A payload is first framed with fields that contain information about the data, such as its origin address and originating MAC (Media Access Control) address, its destination address and destination MAC address, its data type, VLAN tag information, plus QoS (Quality of Service) and error correction information helpful for detecting problems in transmission, allowing damaged frames to be discerned, discarded, and sometimes retransmitted. When destined for travel outside of a network, each framed datagram is additionally wrapped inside a packet which adds information used for establishing a connection and marking where the frame starts.

As a network standard, Ethernet was designed to use a shared medium for communication with other devices. When a device connected to an Ethernet network wants to send data to another device, it senses the presence of the carrier or main wire connecting the devices. If the carrier is free and no other devices are sending data, it transmits the datagram onto the network. All other devices connected to the carrier check that data message to see whether they are the intended destination, until the actual intended recipient discovers and consumes the packet. If instead, the sending device determines there is already a message on the carrier, it holds the datagram back for a moment and retries sending it when it senses the carrier is free. This approach to sharing its connection medium is referred to as CSMA/CD (Carrier Sense Multiple Access with Collision Detection).



## The Internet Protocol (IP) and Ethernet Addressing

For any network, its “protocols” refer to the various rules its network devices use when they communicate over the network. You can view your own network and the internet as a collection of protocols for accomplishing network services/tasks. One key protocol is the Internet Protocol (IP). IP governs the rules for addressing network messages and exchanging message packets. It operates by placing messages/data into frames that include both destination and return addresses, and sending them along an IP network where they can be routed among many possible destinations, and in packets for traversing across many networks, but will ultimately be delivered to the right address. Linked sub-networks of a WAN do not know the specific location to which a packet is being sent, but only to what network the destination node resides at. They discern this using information stored in their routing tables to determine if a destination address matches a node in their own address domain or subnet, whereupon it can ultimately be routed to the appropriate host.

The Internet Protocol address (IP address) refers to the numerical label assigned to each network node—each host computer, printer, router, or other Ethernet device that has been inter-connected to form a network and that uses the Internet Protocol to communicate. An IPv4 address is 4 bytes long (32-bits), and IPv6 address 16 bytes long (128-bits). IPv4 addressing still dominates the internet, but IPv6 has been implemented in parallel to continue to uniquely address Ethernet devices once IPv4 address space has been exhausted. Many modern devices support both IPv4 and IPv6 addressing and should remain operable when that day comes. The most widely supported IPv4 addresses are made up of four octets (four groups of 8 bits), where each octet has an integer value between 0 and 255 (00-FF Hexadecimal), allowing IPv4 to support up to 4.3 billion unique numeric addresses (232= 4,294,967,296 addresses). You will see IPv4 addresses commonly expressed as a series of four integers from 0 to 255 with a period placed between them and this format is referred to as dotted-decimal (like 128.1.1.2). A numeric IPv4 address like this is behind every web address name that you commonly use when you surf the internet. Every Ethernet device has an IP address assigned to it either manually, or automatically as part of connecting to a network, and the IP address serves as both a host or network interface ID, and a host/node location address (more on this later). Each node of a sub-network can only communicate directly with another node in its own address space (its own subnet).

While IP is the only addressing protocol used by Ethernet, Ethernet networks use two types of data transmission: TCP and UDP. Briefly, TCP refers to Transmission Control Protocol, and UDP refers to User Datagram Protocol. Contrasting the two, TCP is connection-oriented and first seeks to establish the connection, then transmits the data bi-directionally. UDP is simpler and connectionless—it just sends the data without first establishing a connection. The combination TCP/IP denotes the Transmission Control Protocol/Internet Protocol, while UDP/IP denotes User-Datagram Protocol/Internet Protocol. But for Ethernet, each of these protocols represent larger suites of communication protocols or stacks of protocols that define the details of how data is sent and received through inter-connected Ethernet devices such as: adapters, hubs, switches, gateways, and routers.

The **Dynamic Host Configuration Protocol (DHCP)** is a method used to *automatically assign temporary* IP addresses to devices as needed. A device set to obtain its IP address automatically via DHCP looks up the LAN DHCP server and requests an IP address when connected. The DHCP server maintains a “pool” or range of IP addresses that are dynamically assigned and recycled as needed. If the DHCP server has an address available, it assigns it to the device on a *temporary* basis. If the server checks its supply and none are available, it returns a busy signal to the client to try again later. The DHCP server itself can be a separate piece of hardware on large corporate networks, but its function is normally built into the small routers used by home networks. Most home routers want to control address assignment to LAN devices via their DHCP, and require that the LAN devices are setup to obtain their IP address via DHCP when connected. To avert delay, some LAN devices can optionally be set to use DHCP but revert to a default IP address if no DHCP server is present. Some home routers and most business class routers will also allow a LAN device to use a static IP address set inside itself. A static IP address does not change and can ensure a connection every time, if the static IP address is unique and within the LAN's address domain.

A *Static IP Address* is as the name implies—static and doesn't change on the network and is fixed into the device itself. Conversely, a *Dynamic IP Address* is an address *temporarily* assigned to a network node by another host/service provider on that network each time the node connects and may be subject to change “dynamically” as required. Ethernet devices may have the option of being assigned an IP address or have a default IP address already assigned (static assignment), or may be set up to determine their IP address automatically when they connect to a network (dynamic assignment via DHCP).



### The Transmission Control Protocol (TCP)

With Ethernet, the Transmission Control Protocol complements the Internet Protocol as one of the two main protocols used on the internet. While network IP deals with addressing the nodes, TCP is the method used to manage the data transfer between nodes and provides the following service:

- TCP establishes a connection before transferring data between local hosts/clients/servers using a three-way handshake with each node exchanging SYNch and ACKnowledgment packets to synchronize sequence numbers and setup data transfer before actual data communication begins.
- TCP manages large data transfers by splitting a continuous data stream (many bytes of information) into separate IP-framed segments.
- TCP also manages message flow control by pre-specifying the number of bytes that may be sent before additional permission is required.
- TCP will multiplex messages to many recipients using port numbers to specify different destinations.
- TCP essentially increases reliability of the data transfer by assigning sequence numbers to data bytes and by using special flags to trigger other services. Sequence numbers help TCP assemble data in the correct order, discern duplicate data, and recover damaged or lost data bytes. For example, a sending TCP requires acknowledgment from a receiving TCP, and if not received within a timeout period, it causes the data to be sent again, helping to ensure its eventual delivery.

### The User-Datagram Protocol (UDP)

UDP provides an alternative transmission protocol to TCP and is generally used to send shorter messages without first establishing a connection between nodes. In this way, it is less reliable than TCP, but *quicker* for sending data. A UDP message is limited to 1500-20 (IPv4 Header)- 8 (UDP Header) or 1472 bytes maximum.

### The MACHine Address

While network routers/gateways use logically *assigned* 32-bit IP addresses and subnet masks to determine network destinations, a second unique hard-coded number inside every LAN device is called the **MAC address** (**Media Access Control** or **MACHine** address). While an IP address is logically assigned by the network IP and can change, the MAC address is a unique 48-bit (6 byte) number fixed into the device hardware and often expressed as 6 hexadecimal numbers separated by colons, like 00:01:07:B7:EB:6F.

The first three bytes of a MAC address identify the manufacturer of the device. Ethernet devices broadcast MAC addresses continuously on a network to let other devices know where to send/return a frame or packet. The router keeps track of where specific devices are located on its subnet by maintaining a list of MAC addresses associated with its LAN IP addresses, and it is the MAC address that allows a message to be delivered right to the device when the device location or logical IP address has changed.

---

### Example 1: Directly Connecting One Host PC to One Ethernet Device

---

- Requires a basic understanding of Ethernet static and dynamic IP addresses and the subnet mask.
- Requires knowledge for changing the IP Properties of a host computer's network interface adapter.
- May require knowledge for changing the IP address of a device if it doesn't have a default address set.

Direct connection is the simplest, most straight-forward and secure way to connect to an Ethernet device, as it involves the least number of steps and completely isolates the source and destination. But this is not a network connection, it only uses Ethernet to connect *one device to one host*. Direct connection will involve separately setting up the network interfaces of a host and an Ethernet device, with unique static IP addresses compatible with each other, then using a web browser of the host to communicate with the device (assuming the device supports web connection). Because it is often inconvenient to separate a host computer from its network when you change its address to a static IP address, this method is mainly used for test or configuration of a single Ethernet device apart from a network.

To talk between devices using Ethernet, each device must have a compatible IP address. For the host interface IP address, you have two options: if your computer only has a single wired Ethernet port, you must change that port's TCP/IP configuration and set it to a static IP address (refer to the TCP/IP Properties of its Network Configuration in Windows®), or you can add another wired network interface card to your host PC for exclusive connection to the device. For convenience sake, the latter option is preferred, as it doesn't affect your current wired network connection. But if your computer normally connects to the internet via WIFI, but also includes a wired Ethernet port, this will not normally be an issue as your WIFI internet connection can remain intact. But either option requires that you select two different IP addresses, one for each device, compatible with each other, as communication between two devices can only occur if both devices reside at addresses in the same address domain. Compatible IP addresses simply means the two addresses must share the same Network ID, but have different node ID's. The necessary steps for changing the TCP/IP configuration of the host computer will vary with your operating system. In general, on Windows® computers, you need to navigate to the Control Panel and change the settings of the network adapter with respect to disabling DHCP address assignment of the interface, setting it to a static IP address, and specifying a subnet mask. The steps to changing it at the device to connect should be covered in the device's manual, or it may already have a default IP address assignment. If your computer is part of your



company network, you may have to consult with your network administrator to temporarily change your TCP/IP configuration. Here are a couple of points about selecting two static IP addresses that are compatible:

- The Ethernet device to connect might already have a default static IP address assigned to it recorded in its documentation or stamped on its side label. Refer to this default IP address and its subnet mask, and reuse its network ID to set another static node address within its domain that you will assign to the host computer's wired network interface (both IP addresses must share the same subnet address or network ID but have different node ID numbers).
- The wired network interface of the host computer is most likely setup to obtain its IP address automatically using DHCP by default. This means if you set it to a static IP address, the computer will no longer be able to talk on your LAN or to your LAN router using that interface. Thus, it's often more convenient to install a second interface on the host computer and use that to create a dedicated private direct-connection to an Ethernet device.

But for either scenario, you must change the IP address of your host computer's network interface card to a compatible address in the address space of the Ethernet device you want to connect. For example, [Acromag Ethernet modules](#) include a default communication mode for web-setup that always uses IP address 128.1.1.100 with a subnet mask of 255.255.255.0. If I want to talk to this device, I would set my wired Ethernet interface to a similar address like 128.1.1.105. The node number you pick is any other number from 0-255, except 0, and 255. The first node number of 0 and the last node number of 255 are always reserved and 100 is already used by the Ethernet device, so you must pick a host address with its last octet set from 1-99, or 101-254 and it must also have the same subnet mask 255.255.255.0.

The three connection examples of this paper explains each way to connect to an [Acromag 989EN-4016 Ethernet I/O module](#), with each successive example reusing the prior. Beginning with Example 1 below which shows how to setup your computer's Ethernet adapter to communicate with a 989EN-4016 module set in its default communication mode, ultimately to configure it for DHCP address assignment outside of default mode, as required for Examples 2 and 3.

You can refer to [Acromag Application Note 8500-734](#) for more detailed information on making a direct connection to your Ethernet device using different versions of the Windows operating system at [www.acromag.com](http://www.acromag.com). An example procedure for doing this using a Windows 10 based computer is provided for reference below:

### **Change the IP Address of the Wired Ethernet Adapter on a Windows 10 Computer for Direct Connection**

You would normally only do this if you want to connect your computer to a single Ethernet device, perhaps to configure it for some application or set the device up for network communication, as for our example.

Example Ethernet Device: [Acromag 989EN-4016](#) (This device must be in its Default Mode, [see Manual](#))  
Default Mode IP Address: 128.1.1.100  
Default Mode Subnet Mask: 255.255.255.0

*Setup Required for Ethernet Adapter to talk to this device in its default mode:*

Disable DHCP Addressing      Disable Automatic IP Address Assignment (a common default)  
Set Static IP Address:        128.1.1.105 (Instead of 105, you could alternately choose from 1-99, or 101-254)  
Subnet Mask:                    255.255.255.0 (*set it identical to device*)



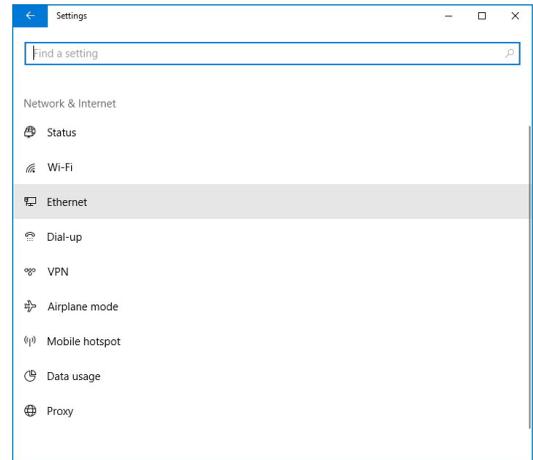
Setup Required for our Ethernet Device Outside of its Default Mode and for Examples 2 and 3:

IP Address: The LAN Device is set to use DHCP Address Assignment
Subnet Mask: 255.255.255.0 (set it identical to the adapter)

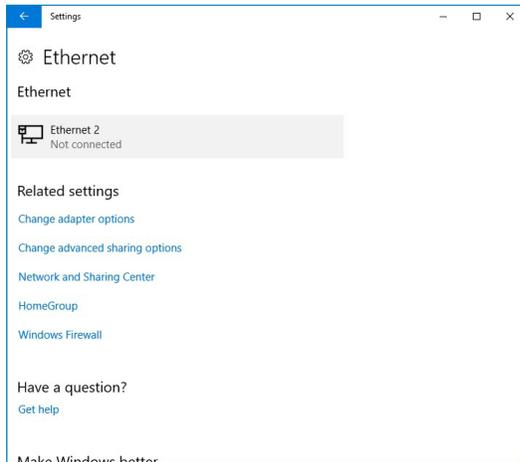
1. Disconnect your Windows 10 computer's wired Ethernet port from your network if your router is wired to your computer using this port by unplugging any Ethernet cable connection to it.

CAUTION: In changing the IP properties of your wired Ethernet adapter as follows, you will temporarily lose access to your existing network if made using this same interface.

2. On your Windows 10 computer, navigate to the Control Panel and select Settings (selecting the Gear icon after clicking the Start button in the lower left corner of your desktop will also get you to the Settings menu), choose "Network & Internet", then "Ethernet" as shown at right:



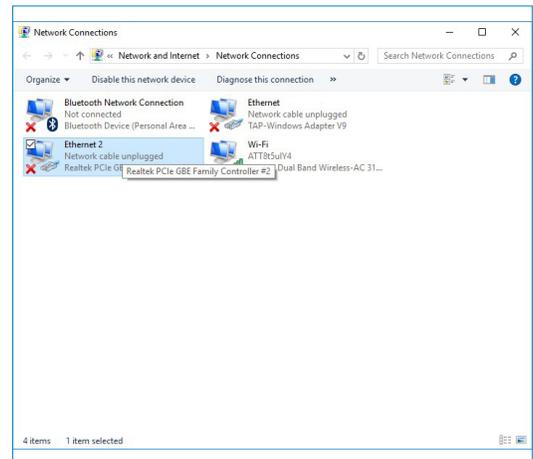
3. Your Ethernet adapter will be indicated similarly as shown below. Click to highlight your wired adapter, and then click to select "Network and Sharing Center" under Related settings.

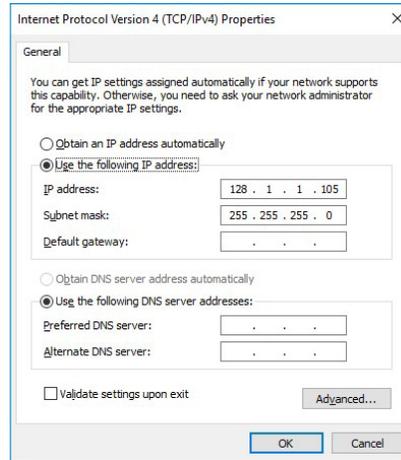
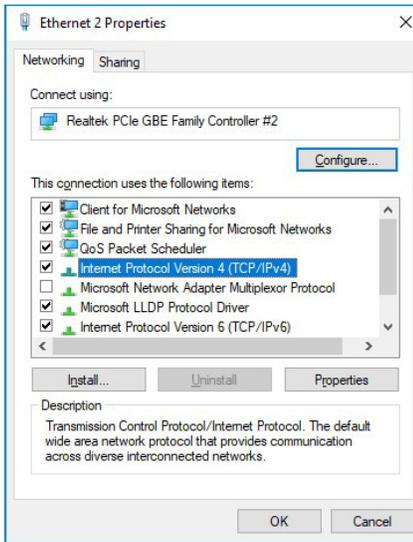


4. In the Network and Sharing Center, all your computer's network adapters will be listed similar to the screen below. If you happen to connect to the internet wirelessly via Wi-Fi, right click on the Wi-Fi adapter and select "Disable" to turn it off temporarily before continuing.

5. Right-click on your wired Ethernet adapter and select Properties to display the network properties list shown on the left below (the Ethernet properties of your adapter are listed with checks leading the properties that apply to it).

Click to highlight the item "Internet Protocol Version 4 (TCP/IPv4)" and then click the [Properties] button as shown below to display its IPv4 properties as shown in the screen to its right.





The computer's Ethernet adapter must be set to a unique static IP address in the same address domain as the 989EN-4016 default communication mode address of 128.1.1.100, and with a subnet mask set to 255.255.255.0. Thus, our choice for the adapter IP address simply requires that its first 3 octets equal 128.1.1 to match the module's first 3 octets, and the last octet can be anything from 1-254, except for 100 already used by the module (128.1.1.105 for this example).

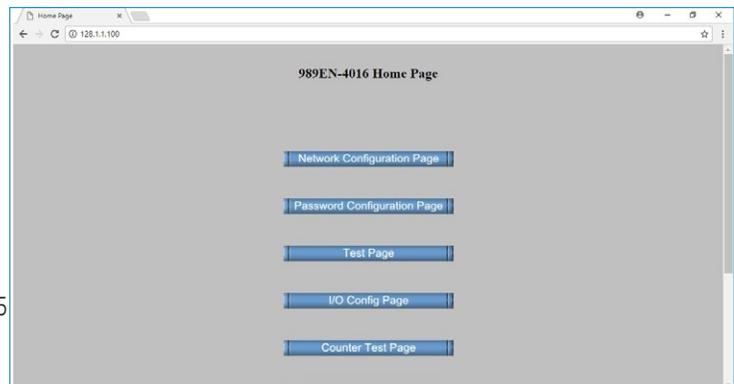
6. In the adapters IPv4 properties screen shown on the right above, click the button adjacent "Use the following IP address:", then enter IP address 128.1.1.105 into the IP address field as shown. Also enter 255.255.255.0 in the Subnet mask field and leave the Default Gateway and DNS settings alone, as they are not used when making a direct to device Ethernet connection. Click the [OK] button to save your changes.

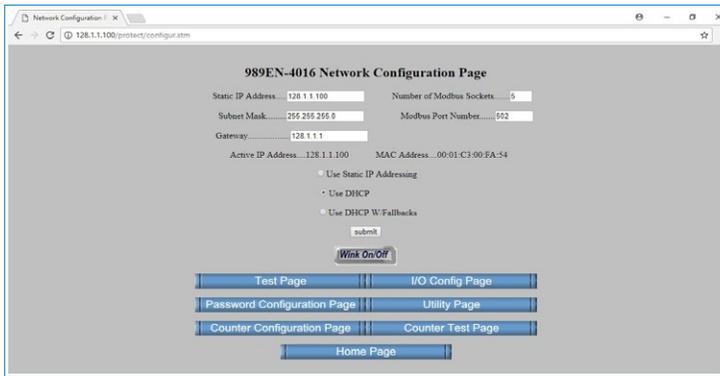
7. At this point, connect an Ethernet cable from the Ethernet port of your computer to the Ethernet port of the Acromag 989EN-4016 module and apply power to the module and place it in its default communication mode (refer to its instruction manual if needed). On your computer, load a web browser and type the address 128.1.1.100 into its web address field and press [Enter]. Your browser should then display the home page of the Acromag 989EN-4016 module as shown below:

The Home page is used to access other web pages of the module for configuring its network parameters, changing its password, and operating the module.

Because we intend to prepare this module for connection to a LAN in examples 2 and 3 of this paper, we need to select the Network Configuration Page (password required).

To access the Network Configuration Page, you will be prompted to enter a "User name:" and "Password:". The default settings are **User** and **password** respectively (Refer to the 989EN User Manual 8500-805 for more information). After entering the username and password, the 989EN will return the Network Configuration Page shown below.





Here, we need to set its Subnet Mask field to 255.255.255.0 and click to enable the option "Use DHCP" and direct the module to obtain its IP address automatically when we connect it to our LAN router with it outside of default mode.

After making the required changes, click on the [submit] button to write the changes to the module.

To this point, you have successfully connected your computer to an Ethernet module and have set the module up for reuse in the second and third examples of this paper.

### Making a LAN Connection to an Ethernet Device

Example 1 showed how to directly connect to an Ethernet device to test its operation or to accomplish device setup—this was not a network connection. In Example 2 that follows this section, we show how to connect the same device to a Local Area Network. Example 3 will cover remotely accessing this device over the internet.

To make a LAN connection, we need to access the home router's configuration console to setup a DHCP reservation to make our device IP address the same every time we access it on our network. But before walking jumping into Example 2, we need to explore a little more about IP addressing, sub-netting, and router operation.

### Public versus Private IP Addresses

Because we plan to connect our device to a router, it's now important to make a distinction between **public** and **private IP addresses**. A public IP address refers to the IP address used on the internet—this is essentially the address your ISP assigns to your router's WAN/internet port. Your router shares its public IP address among the different network devices connected to its LAN ports. On the other hand, a private IP address refers to the local IP addresses that are used behind the router that your LAN devices receive. As a rule, private IP addresses are separate from public addresses, cannot be routed to the internet, and are unique only on their own LAN. Public IP addresses are unique globally among the billions of LAN's that connect over the internet.

Public IP address space is managed globally by IANA (Internet Assigned Numbers Authority) using five Regional Internet Registries (RIR's) that administer IP addresses to guaranty they remain unique among billions of possible network devices on the public internet.

Each regional registry makes unique assignments to end users and other local internet registries operating in their territory, which may include your own Internet Service Provider (ISP). Your ISP or private network administrator assigns a public IP address to each public device connected to its network from a finite collection of IP addresses to which it subscribes from its Regional Internet Registry.

PRIVATE ADDRESS SPACE RESERVED BY IANA		
START ADDR	END ADDR	SIZE (NODES)
10.0.0.0	10.255.255.255	16777214
172.16.0.0	172.31.255.255	1048576
192.168.0.0	192.168.255.255	65534

These private LAN addresses cannot be routed on the public internet, effectively keeping your router's public IP address always different from any of its LAN IP addresses.



Private IP addresses are reserved for use behind a Network Address Translation (NAT) device (like your router). Your router will have a LAN IP address from one of these ranges, and your Ethernet devices will get similar IP address assignments in these ranges. While public IP addresses cannot be used by devices inside a home or business LAN (except by a router's WAN port), private IP addresses can be used many times by different LAN's without additional restrictions on sub-netting or address assignment.

Essentially, the internet is a Wide Area Network (WAN) of smaller inter-connected Local Area Networks (LAN's) that exchange information between network nodes using private IP addresses, but communicate network-to-network by passing data packets between routers/gateways using public IP addresses.

In addition to private IP addresses, be aware of some other IP address ranges reserved by IANA as follows:

- 0.0.0.0 to 0.255.255.255 are reserved and do nothing at present (these do not function on any network)
- 100.64.0.0 to 100.127.255.255 is for use between an ISP and subscribers using a carrier grade NAT.
- 127.0.0.0 to 127.255.255.255 is reserved for looping data back and specialized diagnostic functions.
- 169.254.0.0 to 169.254.255.255 is reserved for Automatic Private IP Addressing (APIPA)
- 224.0.0.0 to 255.255.255.255 is reserved for multi-casting (Class D 224-239) or future use (Class E 240-254)

Public or private, the numeric IP address of any device is *always unique on a network*—public IP addresses are unique globally on the internet and governed by IANA, while private IP addresses are unique on their own LAN and governed by the LAN (router/device). No two Ethernet devices on a network, public or private, may have the same IP address assignment on the same network at the same time.

Since public IP addresses are unique and regional, that address can be traced back to its source location. For example, you could extract the source IP address from an email header and use that information to find the geographic location of the source (or at least its ISP). Of course, the address that is discerned is really the address of the router/gateway that connects to the device. Locating the LAN device itself would require additional information from the router. There are many free websites that can extract geographic detail from an IP address, such as [www.whatismyipaddress.com](http://www.whatismyipaddress.com). Online companies and their networks continually monitor IP activity and know you access their site, and sometimes restrict or grant access to website resources based on your location. Likewise, hackers can use these IP addresses to break into networks and sometimes take control of network devices. As such, other measures are taken to help ensure privacy and security (more on this later).

Normally your RG's public WAN port is dynamically addressed by your ISP, unless you pay up for a static public IP. Your home router typically assigns private IP addresses to its LAN devices dynamically using DHCP. The router/gateway allows the LAN devices to share its public WAN IP address using Network Address Translation (NAT) to communicate between networks, helping to preserve public IP address space. Communication sent between a private LAN address and a public WAN address is not permitted without passing through the intermediary RG (Router/Gateway or Residential Gateway). Dividing the total IP address space into public and private sets conserves address space, and using routers to gate access between the two sets is how billions of devices across the globe can talk together on the internet at the same time without bogging down the shared connection.

If you happen to set the destination IP address of a message packet to an address in another network, your message will be blocked by your RG—the externally bound message must be sent to the router/gateway to be forwarded properly, because each node of a network can only communicate directly with another node in its own address space (its own subnet).

### IP Addresses and Sub-Netting

Network nodes of an address domain only communicate directly with other nodes in the same address domain. Billions of conversations occur simultaneously on the internet by separating IP addresses into public and private address groups and gating communication between them. But how do very large networks handle many nodes needing to communicate at the same time? Large networks use sub-netting of their address space to divide themselves into smaller networks or communication groups and they use a subnet mask to do this. This division into independent communication groups is how simultaneous/parallel network chatter can work without becoming bogged by many nodes competing for shared communication media.

The term subnet refers to the contiguous string of IP addresses exclusive to the nodes of a group that share some common element for communication. Sub-netting address space helps separate larger numbers of nodes into smaller groups to allow them to communicate more efficiently. The subnet mask is another 32-bit number used to parse the IP address into two parts: a network address/ID and a node address/ID. This is done by logically AND'ing each bit of the two numbers, bit-by-bit, and the leading bits of the result correspond to the sub-network's address, and the trailing bits correspond to the node address space.

The first node address of a subnet (0) is the network ID and used to identify the subnet itself, while the last node address of a subnet is always used as a broadcast address to all nodes of that subnet--anything sent to the last IP address of a subnet is sent to every host on that subnet.



In general, sub-netting divides an IP address domain into three main block sizes or classes based on the 4 octets that make up an IPv4 address. A Class A subnet is any subnet that shares the first octet (8-bits) of the IP address (27=128 networks). A Class B subnet shares the first two octets of an IP address (214=16384 networks). A Class C subnet shares the first 3 octets of an IP address (221=2097152 networks).

CLASS	START-END ADDRESS	SUBNET MASK	NETWORKS	HOSTS/NETWORK	RESERVED ADDRESSES OF SPACE
Class A	0.0.0.0 -127.255.255.255	255.0.0.0	2 <sup>7</sup> -2= 126	2 <sup>24</sup> -2=16,777,214	10.0.0.0 – 10.255.255.255, 127.0.0.0 – 127.255.255.255
Class B	128.0.0.0 – 191.255.255.255	255.255.0.0	2 <sup>14</sup> -2= 6382	2 <sup>16</sup> -2=65,534 nodes	172.16.0.0 – 172.31.255.255
Class C	192.0.0.0 – 223.255.255.255	255.255.255.0	2 <sup>21</sup> -2= 2097150	2 <sup>8</sup> -2=254	192.168.0.0 – 192.168.255.255

For example, given an IP address of 192.168.1.100, its first octet of 192 tells you it is a Class C sub-network address with a 255.255.255.0 subnet mask. By using a logical AND applied bit-by-bit between the IP address and its subnet mask, we discern a network ID of 192.168.1.0 and a host on that network at address 192.168.1.100 (node 100). A Class C sub-network can accommodate up to 254 possible node addresses. Because the first and last IP node addresses are always used as a network ID number and broadcast address respectively, two is subtracted from the total possible unique node addresses that can be defined via the remaining octet. Compatible node addresses in this domain are of the form 192.168.1.x, with x being any number from 1-99, and 101-254.

Subnetting is used with public IP addresses and with private IP addresses. You generally can't modify your public subnet, but you can subnet your private IP addresses. For example, if we wanted to further divide a Class C sub-network of up to 254 network nodes into 14 parallel communication groups/subnets (then 4 more bits would be required to divide the private network domain). Thus, since the node portion only has 8 bits, its first 4 bits is required to identify each of the further divided sub-networks, we would use 11111111.11111111. 11111111.11110000" as our LAN subnet mask to further subdivide the Class C network into 14 sub-networks of up 14 possible nodes each (the maximum possible nodes has decreased from 254 to 14 networks x14 nodes each =196), but each parallel subnet can communicate more efficiently on its shared medium).

Remember that a binary host address with **all zeros** or **all ones** is invalid for use as a node number, as this corresponds to the first and last node address in a subnet. The first part of the subnet IP address with all 0's in the trailing portion is reserved as the sub-network address itself, while the first part of the subnet IP address with all 1's in the trailing portion (last node address) is reserved as a broadcast address for the entire sub-network.

### Named IP Addresses

Most often, you don't use numeric IP addresses in your web browser to access a subnet client, but a host name instead. The host name is easier to remember and often tells what the web site is about. But behind that name, the network needs a numeric IP address to locate the web site. **DNS** refers to the **Domain Name System** or **Domain Name Server** of the subnet used to associate an alphanumeric character string with its equivalent numeric IP address. The DNS is essentially a distributed database of domain names and their corresponding IP addresses for some segment of the domain name address space (its network ID) and it makes this information available for lookup to other clients called resolvers. For example, our DNS allows us to use "Acromag.com" as an IP address rather than a complicated number string like 122.168.1.5. If you don't already have a DNS server on your LAN, your ISP typically provides it for you, and its IP address is set inside your router by your ISP.

### Router Operation

Referring to the 7-layer OSI Network Model and its model of a stack of network protocols that operate on layers, message frames are generated and routed between LAN clients on Data Link Layer 2 using network switches. IP Packets are added at Network Layer 3 and routed to the internet using network routers, whose purpose is to link LAN clients together and connect/bridge them to the internet. Internet traffic only traverses between router/gateway devices. While all your Ethernet devices use private IP addresses hidden behind your router to communicate with other LAN devices connected to the same router, they share the router's public IP address applied at its WAN/internet port to communicate with remote devices outside the LAN (other public routers/gateways on the internet). The router's public IP address is usually assigned dynamically from a pool of public IP addresses that your ISP subscribes to, while the LAN devices connected to your router typically get their IP addresses dynamically from the router and use these addresses to forward packets between themselves. Your router may include a Wi-Fi channel to connect wireless LAN devices within range to the public internet too. Because the router acts like a gateway between LAN clients and the internet, your router is sometimes referred to as a Residential Gateway (RG). While its primary function is to send/receive frames/packets between nodes and between networks, your router has other functions that can be used to additionally analyze and filter packets, and even alter how messages are packaged for translating between networks.

If you connect a device with a private IP address directly to the internet, it becomes non-routable and no inter-network connection can be made to the device. The device must have its private IP address mapped to a working public address using a router, or its requests must be sent through another router or gateway with a valid public IP address. The router uses its public IP address to send network communication to the internet using a process called **Network Address Translation (NAT)** which maps private IP addresses of LAN devices to its public WAN IP address using a pre-defined port-forward number. Subsequent messages in an exchange continue to use the same port number. When a LAN client inside the network wants to connect to a WAN



client on the internet, it sends a connection request to the router at its Default Gateway IP address. The router dissects the internal connection request (SYNch request in TCP/IP) directed to the remote client, and changes that message's source address (return address) to the public IP address of the router's WAN port, so that any response will be returned from the remote WAN client right to the router IP address. It also makes a note in its NAT table that a connection with the remote client has been initiated from a local LAN client (which it specifically identifies the client using its private IP and MAC addresses). As traffic passes between LAN & WAN clients, NAT continues to swap the source addresses of messages in both directions with its own IP address on the same side (either its public or its private IP address) while keeping track of each data path by destination address and port assignment, without revealing the true end-point IP address of the sending client to either party. This enables the router to reverse the address change from a remote IP to a private IP address when data is received back. Essentially, no data packets cross between networks without a port number. The use of Port Numbers will be explained in later for gaining remote access.

The IP address typically stamped on the side label of a router is its private, non-routable, LAN IP address. This is the address that a LAN client of that router would use in its browser address bar to access that router's web console or configuration page. Its LAN clients will have similar addresses and any WAN packets directed to LAN addresses are blocked by the router. LAN IP addresses will range from 10.1.1.1 to 10.255.255.254, 172.16.1.1 to 172.31.255.254, or from 192.168.1.1 to 192.168.255.254, and **will not be recognized outside of the LAN**, as they are set aside in IPV4 for private use only by IANA. Because the IP address is logically assigned to a device and subject to change, it is the device MAC address that permanently identifies the client, and the router keeps track of IP and MAC address associations to ensure message delivery.

When a response comes back from a remote client to the router (via SYNch ACKnowledgement in TCP/IP), the router looks up the private LAN client using its NAT table, and when it finds a match, it changes the incoming response message's destination address from its own public IP address to that of the LAN client and forwards the message to the device. The router continues to transparently swap the private sending and public receiving addresses as packets travel back and forth between the LAN and WAN networks. When the connection is terminated, the router removes the connection note from its NAT table and it does all this transparently as you surf.

### Packet Routing

*Before a message can be delivered, a client name must be resolved to an IP address (DNS query), then to a device MAC address (ARP request), then inserted into a frame/packet for delivery.*

In any TCP/IP or UDP/IP protocol suite, if a client needs to send a data frame to another client, it first needs the numeric destination IP address and may need to query its DNS (Domain Name Service) if the address is in the form of a name. To find the numeric IP address of a named destination, the client issues a DNS query to its DNS server. The local DNS server checks its records to see if it finds a matching IP address in its local database for the named host. If it doesn't find a match, it queries another "higher-level" DNS server, and the process repeats itself down the line until one DNS server ultimately finds a matching IP address for the host name. That DNS server responds to the client with a DNS reply that includes the numeric IP address of the named remote host/website. Of course, as that DNS reply passes back through the gauntlet of DNS servers to get back to the local DNS server, it becomes a new domain name record in each DNS server's database on the way back.

Finally, after resolving a named client to its equivalent numeric IP address via DNS record, a node also needs to find the device-specific MAC address of the destination client, because the IP address is only a logical address under control of the network and can change from time to time, the fixed MAC address of the client is required to ensure delivery to the right client. The network **Address Resolution Protocol (ARP)** determines how the node of a subnet will associate a logical network IP address with a unique MAC address.

The router examines the numeric IP address against its subnet mask to discern the destination network ID and determine if it has the same network ID as its own (local), or an entirely different network ID (remote).

### For Local Delivery within the Same Network LAN

For a local destination, it will broadcast an ARP request on its own subnet to get the MAC address of the local device at the numeric IP address. Every other LAN client examines the IP address in the broadcasted ARP request, and the one client that finds it matches its own IP address returns an ARP reply along with its MAC address. With both the destination IP and MAC addresses, the sending client frames his message for direct unicast delivery to the local destination and attaches his own source IP and MAC addresses.

### For Remote Delivery between Different Network LAN's

For a remote destination, the sending client can't easily discern the remote MAC address, so it creates a packet, attaches the destination IP address, and sends it to its local RG (Router/Gateway) instead because it can't send it directly to an address outside of its own address domain without being blocked. RG's inter-connect and move packets between LAN's and having received a message from a LAN client, the router examines the destination IP address in the message packet and refers to its internal forwarding table. If it finds a matching route to the remote destination, the RG sends the packet along the route to the destination. But if the local router does not discern a route (as it hasn't learned it yet), it forwards the packet to its defined gateway, and the



lookup process repeats itself at various linked network RG's until one public RG finds a matching route for the destination IP address in its own LAN. That router then determines the MAC address at that destination IP address of its LAN and swaps the source address of the packet with its own IP address and forwards it to the LAN destination (note that swapping source addresses is one way the router hides an IP address to protect a client).

---

### **Example 2: Connecting an Ethernet Device to a Local Area Network**

---

Unlike the direct-to-device connection of Example 1, Example 2 is no longer private since it connects the device to a LAN router--this is a network connection. But connecting a device to your network is a little more complicated than making a corporate connection, because you are the administrator of your network and you must control your router. You need the address of your device to maintain the same address when connected to your network so that you can use that address repeatedly to access it at any time.

Example 1 used a static IP address assignment to talk to the device in its default communication mode. Connecting to a corporate network may also use a static address assignment set inside the device, because corporate administrators have greater control of their larger network's enterprise or business class router. However, most small home RG's want dynamic control of IP address assignment and setting a static address may not work, as the router will not discover its MAC address when you connect it to a LAN port. In this instance, you need to set the device to use DHCP IP address assignment and take additional steps to direct the router DHCP to give the same address assignment to the device every time it powers up. This way, the router will automatically connect to it and discover its MAC address, allowing you to direct the router to make the same assignment every time.

In a nutshell, to connect an Ethernet device to a LAN network, you need to accomplish the following:

1. Connection Scenario 2 requires that Connection Scenario 1 be completed for your device.
2. You must determine the LAN IP address of your router, and its username/password or access code (refer to its side label information). You need this to change your router's default configuration.
3. You must connect your Ethernet device to a LAN port of your router, or through an Ethernet switch that is connected to your LAN router.
4. You must access your router's configuration console at its IP address from a web browser of the LAN and enter its username/password or access code to make changes to its configuration. Once inside the router, you will view the address it has assigned to your device via DHCP, then direct the router to reserve that address each time it connects to your device.

#### **Prepare the Device for Network Connection**

For this example, you have already set your device to acquire its IP address via DHCP and it has its subnet mask set to 255.255.255.0 (This was done in Example 1). For this example, an Acromag 989EN-4016 module has been setup for connection to my LAN.

#### **Determine Your Router IP Address, Username/Password or Access Code**

Your router has a default private (local) IP address assigned that you can use to access its configuration console from a computer on your LAN. It's usually the same address for router models of the same brand.

Routers use LAN addresses that have been reserved for their use by IANA and fall into these ranges:

- 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

Your home router will have an IP address in one of these ranges. You can usually find this on its side label or in its documentation. This is the LAN IP address of your router's configuration console and it is static. For example, IP address 192.168.1.1 is one of the most common default gateway addresses used by wireless routers/gateways and ADSL modems. These addresses and their derivatives cannot be routed on public networks, ensuring that your router and any of its LAN devices will never have the same IP address. Refer to your own router and take a moment to find and record this address, plus anything noted as an Access Code, or default username/password.

If you can't get to your router or have lost its documentation, you could also retrieve this IP address by referring to the Gateway Address returned after using the Windows command prompt utility **"ipconfig" or "ipconfig/all"** on a computer connected to the LAN router.

Additionally, if you do not know the username/password defaults of your router, you could use a web search engine to help find them if you know the brand/model of your router and have not already changed its defaults.



Using ipconfig on the Windows Command Prompt to Retrieve your Gateway Address

For Windows computers, you can navigate to the Windows Command Prompt utility and type "ipconfig" or "ipconfig/all" and press [Enter] to retrieve a list of IP properties like the following:

```

Command Prompt
C:\Users\bcybu>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : attlocal.net
    IPv6 Address. . . . . : 2600:1702:950:d9e0::7b5
    Link-local IPv6 Address . . . . . : fe80::31d0:d615:75c0:ae80%15
    IPv4 Address. . . . . : 192.168.1.70
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

```

The LAN IP address of your router is indicated as the Default Gateway for your Ethernet Adapter. The router IP address will look something like 192.168.x.x, 172.16.x.x, or 10.x.x.x (Apple routers). Note that 192.168.1.254 is the default gateway indicated in our example above. Its subnet mask is also indicated (255.255.255.0). If you can get to the side label of your router, you can verify that the same IP address is indicated there. Since most home routers also function as DHCP servers, the same address would be listed as the IP address of the DHCP server.

*Note, if "ipconfig" or "ipconfig/all" returns a DHCP server address like "169.254.x.x", this is a Windows APIPA address that usually means the server is permanently or temporarily unavailable, or the network connection is not working properly. Receipt of this address may trigger the client to temporarily configure itself with an address from 169.254.0.1 to 169.254.255.254, and subnet mask 255.255.0.0, until the DHCP server becomes available (the Windows APIPA service rechecks periodically until the DHCP replaces its APIPA address with a valid IP address).*

Different router brands have default usernames and passwords set for router reconfiguration. Some brands may instead use a unique Access Code for reconfiguration (this code is on its label or in its documentation). You will need this information to make changes to router parameters necessary to connect your device to your router LAN. Here are some default IP addresses, Usernames, and Passwords of familiar brands (assuming you have not changed your username & password defaults):

ROUTER	IP ADDRESS	USERNAME	PASSWORD
ATT (Pace)	192.168.1.254	NA (Use Access Code)	NA (Use Access Code)
3COM, BenQ, US Robotics, Linksys	192.168.1.1	admin	admin
Belkin, SMC	192.168.2.1	admin	admin
D-Link, Sitecom	192.168.0.1	admin	admin
Netgear	192.168.0.1	admin	password
Thomson	192.168.1.254	user	user

You can always use a web search engine to find your defaults and there are web sites that can retrieve the defaults for your brand/model, such as 19216811.wiki. If you have changed your password/username and forgotten the settings, you may have to reset your router or modem to revert it back to



its default settings (typically this means you hold down its reset button for ~10 seconds to reset it to factory defaults).

Once you have identified your router's IP address and any access code or username/password, you can use it to log into the router configuration console after you connect your device to your router.

Connect the Device to Your Router

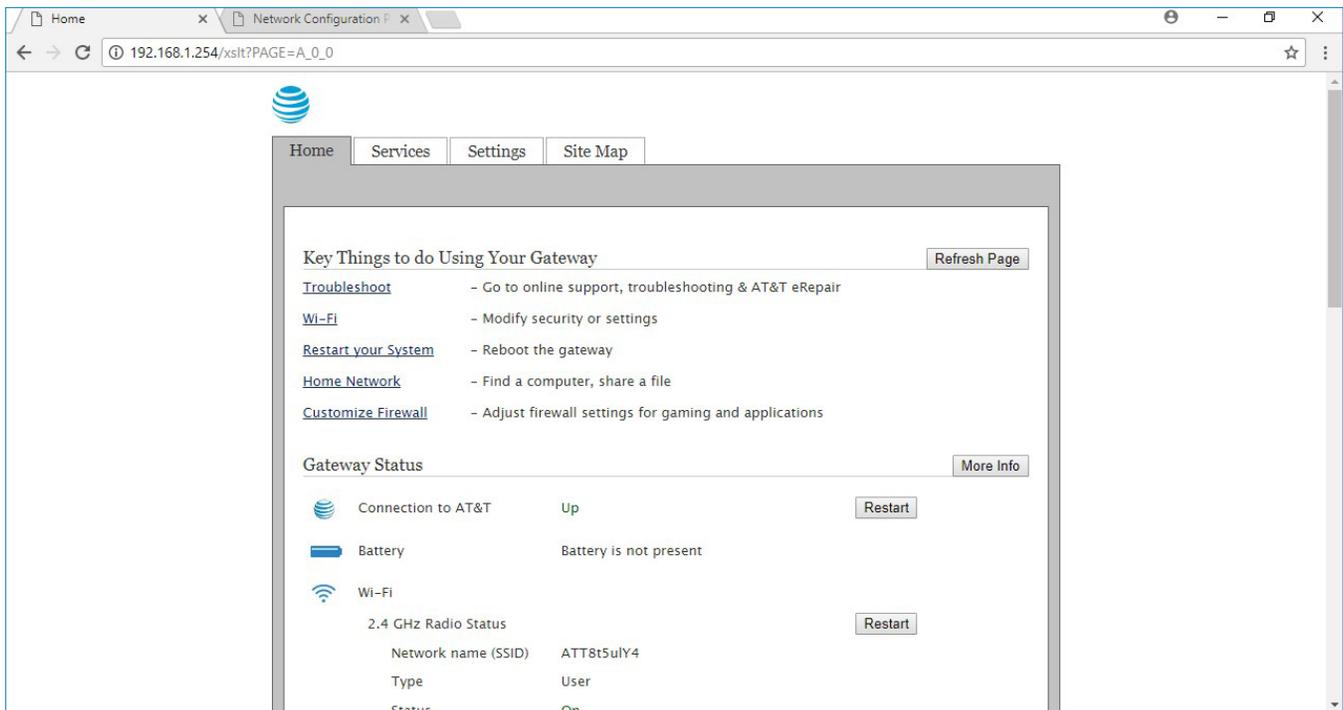
Use an Ethernet cable to connect your Ethernet device to a LAN port of your router, or through an Ethernet switch that is connected to your LAN router. Make sure your device is powered. For this example, the ISP is ATT UVerse and ATT has provided a Pace model 5268AC router which connects to a powered Acromag 989EN-4016 module at LAN port 1.

Log into Your Router at its LAN IP Address to Make a DHCP Reservation for Your Device

You need to use your router to set it up to fix the IP address it assigns to your Ethernet device so that you can use that same address to access it on your network every time.

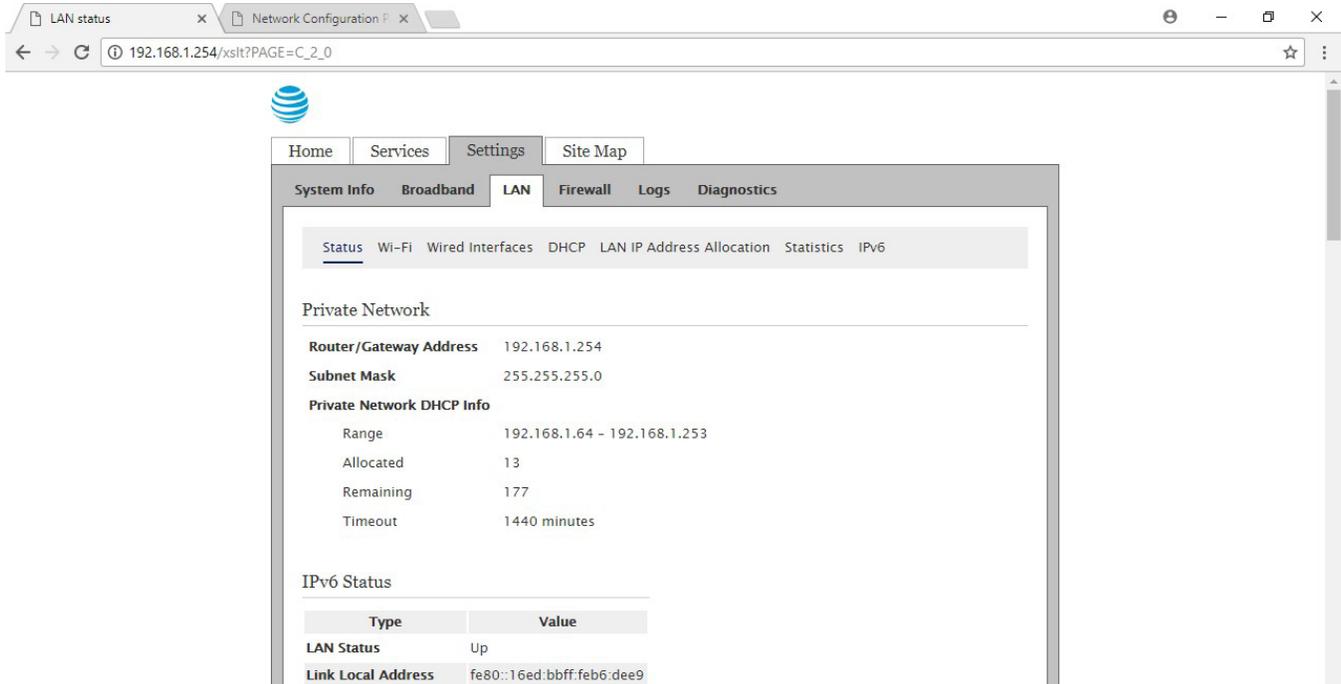
By now, you should realize that your home router handles many network functions: it works as a gateway, a firewall, a DNS, and a DHCP address server. For some routers, it should not surprise you that it even wants to control IP address assignment, and if you try to preset your Ethernet device to a static IP address of your own choosing, your router may not "discover" it. In this case, you must set your device to get its IP address from the router via DHCP, which allows the router to automatically "see" it and associate its internal MAC address with an IP address. Then, once you can see your device through the router, you can direct the router to serve the same IP address each time it connects to your device and every time your device powers up. This is referred to as a DHCP reservation, which is simply another option to static addressing that you can use to reserve an IP address for a computer on your LAN such that it always receives the same address. You need its address to be constant so that you can consistently use that address to access your device from a computer on your LAN.

For my example router, on its side label is its LAN IP address 192.168.1.254 along with a special access code (instead of a username/password). From a computer on my LAN, I direct its web browser to the LAN IP address of my router at 192.168.1.254 and the router home page is displayed as shown below:



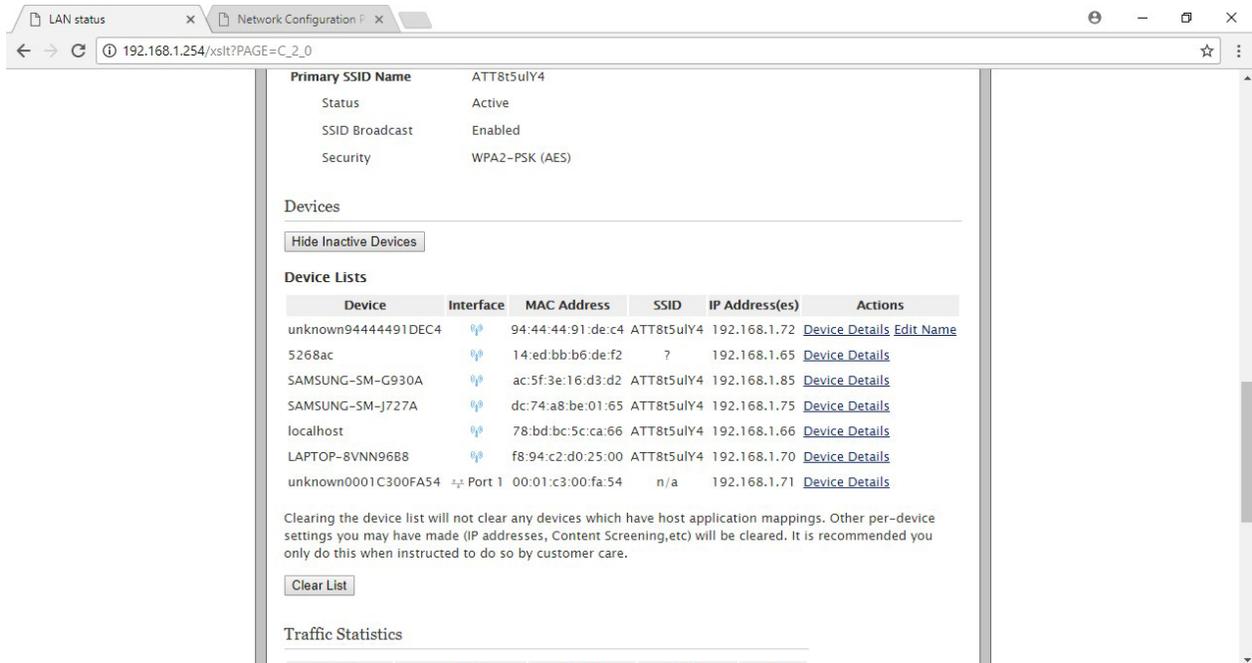


Remember that I need to find out the address my router DHCP has assigned to the Acromag 989EN-4016 Ethernet module I have connected to it. For my router, this information is displayed in more than one area. I click through the Settings tab to the LAN tab to display the following:



Note the LAN page above indicates that the router's DHCP will assign addresses in the range 192.168-1.64 through 192.168.1.253 (its address domain), the router has already allocated 13 addresses, and the router has capacity for 177 more devices.

I'm ultimately looking for a place to view the IP address that my router DHCP has assigned to my device (my device must be connected to the router and powered up). I scroll down the LAN page to view the IP addresses of all connected LAN devices as shown below:

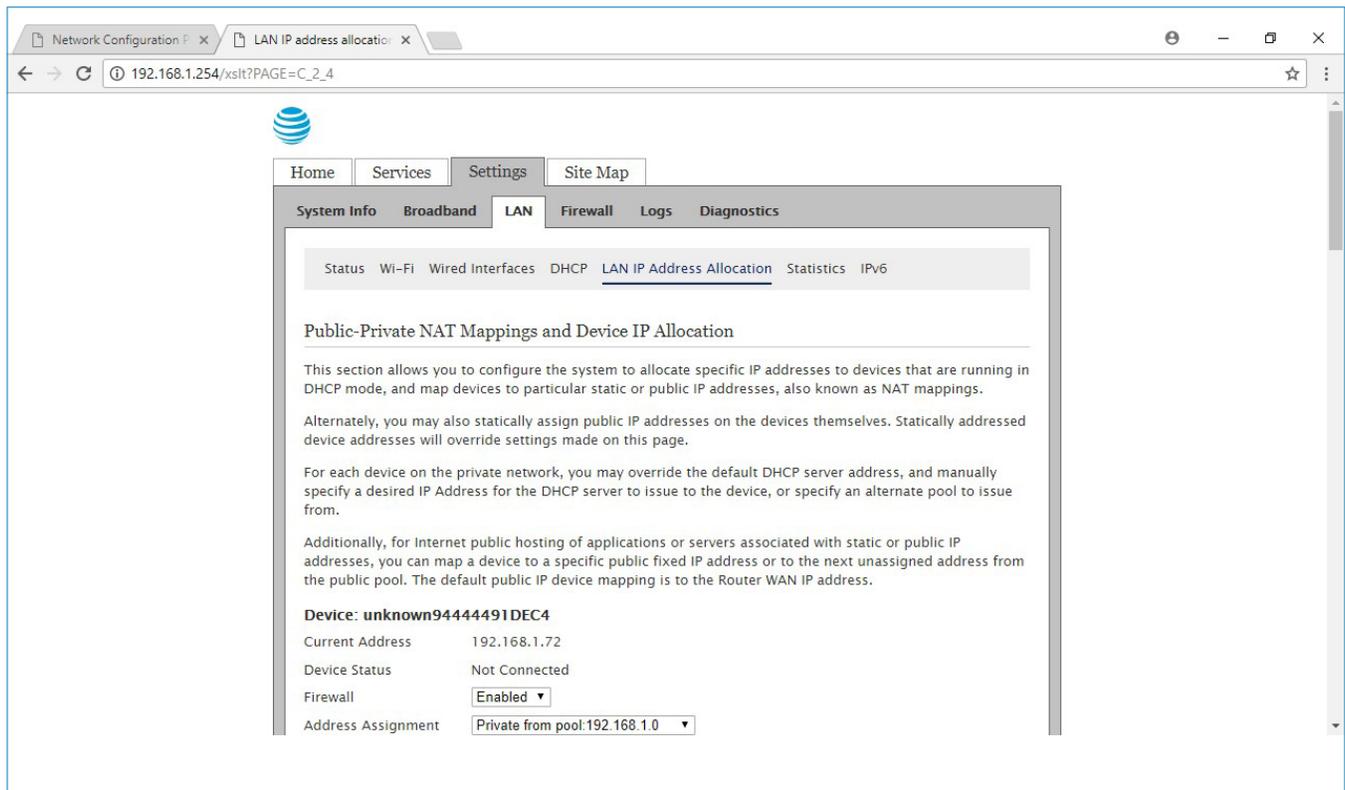




I'm looking for the IP address of my Acromag 989EN-4016 module. As I view the Device List of this page, I can see that the router has detected a device denoted by "unknown0001C300FA54" and those digits correspond to the digits of my module's MAC address (the MAC address of my device is indicated on its side label). This verifies that the router is properly connected to my module (because it sees its MAC address) and my module has been correctly configured for LAN communication and is powered-up. Here I determine that the router DHCP has assigned IP address 192.168.1.71 to the module.

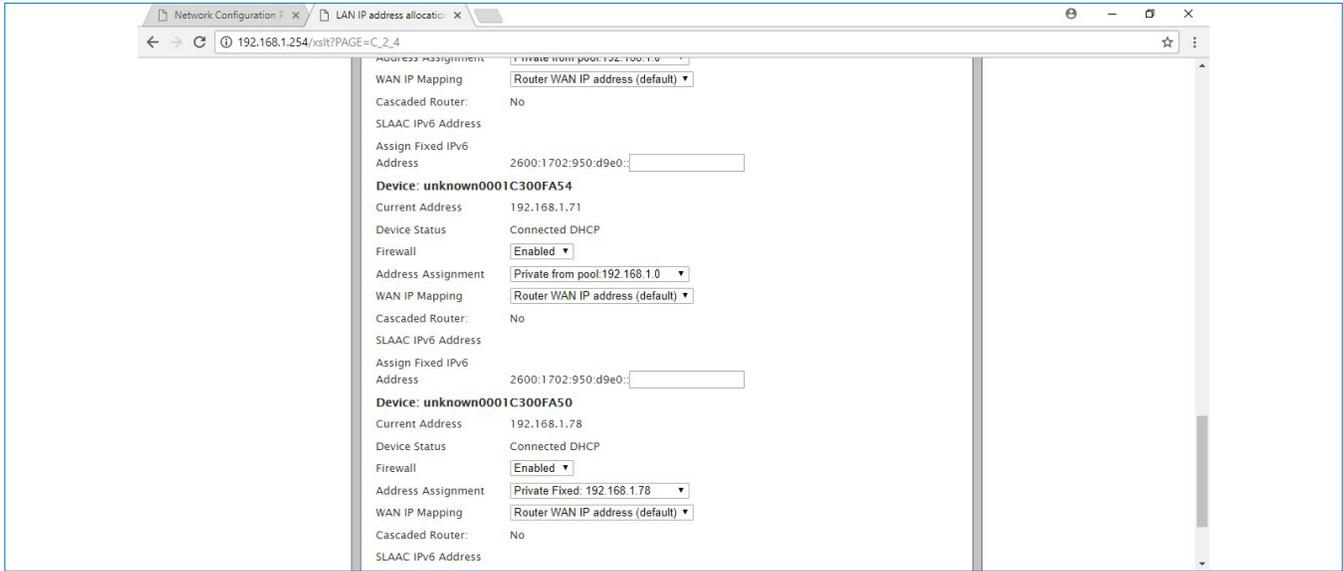
At this point, if I set a LAN web browser to address 192.168.1.71, I will view my module's home page. However, to be able to consistently access my module at this same address every time, I have to make the router DHCP use that same assignment every time my device powers up and connects to it. That is, I want to make a DHCP reservation of address 192.168.1.71 inside my router.

Explore to find the screen used to fix the DHCP IP address assignment to the module. The terminology used by ATT for DHCP Reservation is different, but the "LAN IP Address Allocation" tab shown below sounds related. Your router may also loosely refer to these terms and you will sometimes have to follow the router screens very closely to make sure you are where you want to be. So for my example, I click through to the "LAN IP Address Allocation" sub-menu under Settings > LAN > to display the following screen:

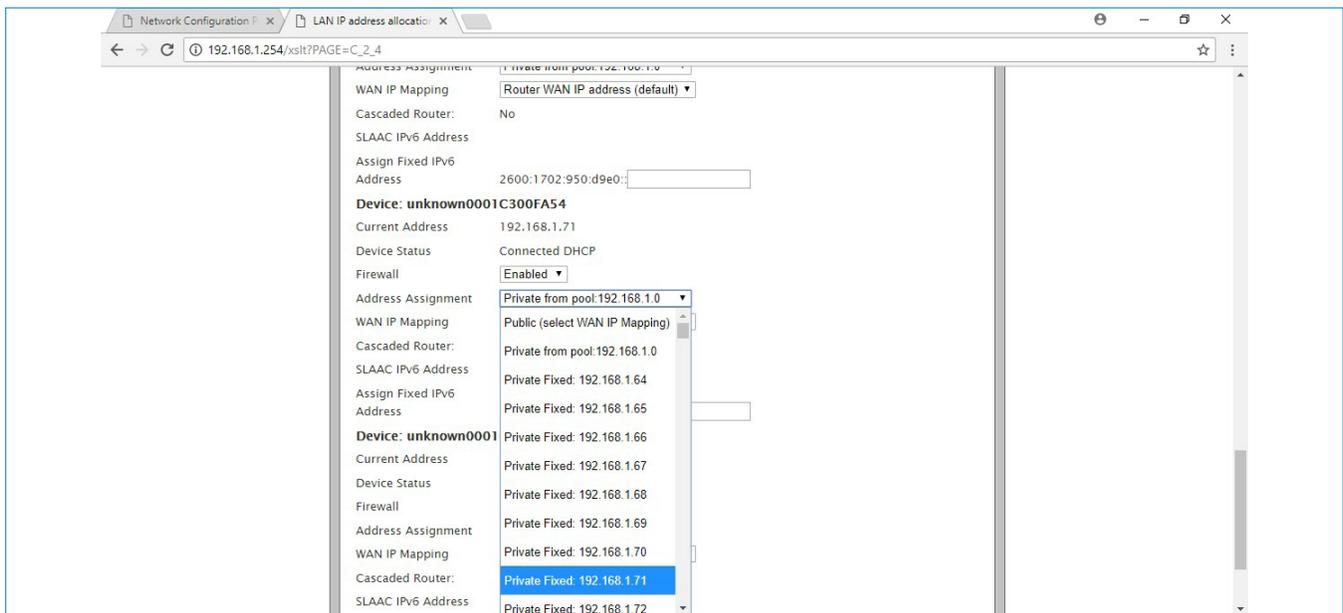


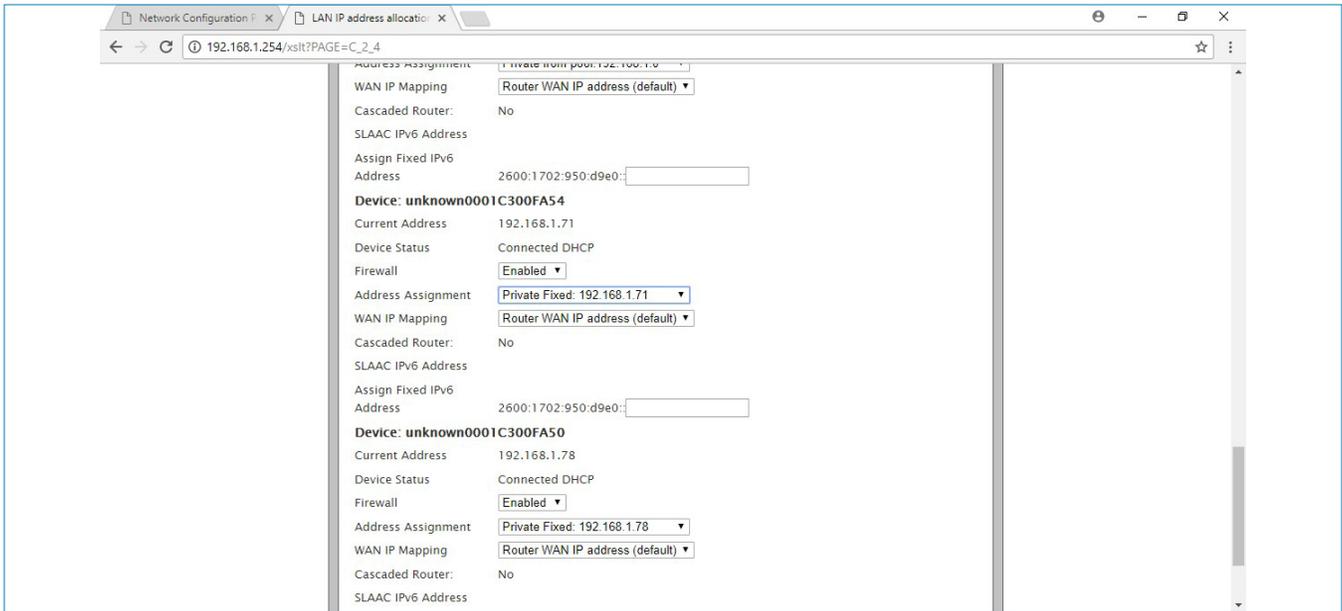


If I scroll down this page, I can review a list of each device connected to my LAN (all the devices that the router DHCP has assigned an address to). Some devices will have recognizable device names, and others may simply refer to “unknown” paired with MAC address digits in the Device line. I scroll down to find my module denoted by **unknown0001C300FA54** at IP address **192.168.1.71** as shown in the following screen (the MAC address is noted on the side label of my module). If I didn’t find my device on this list, it may not have been properly preset to get its IP address via DHCP, or it may not be connected to my router or powered-up. With the device identified on this list, I want to direct the router to fix its address to the IP address it has already assigned via DHCP.

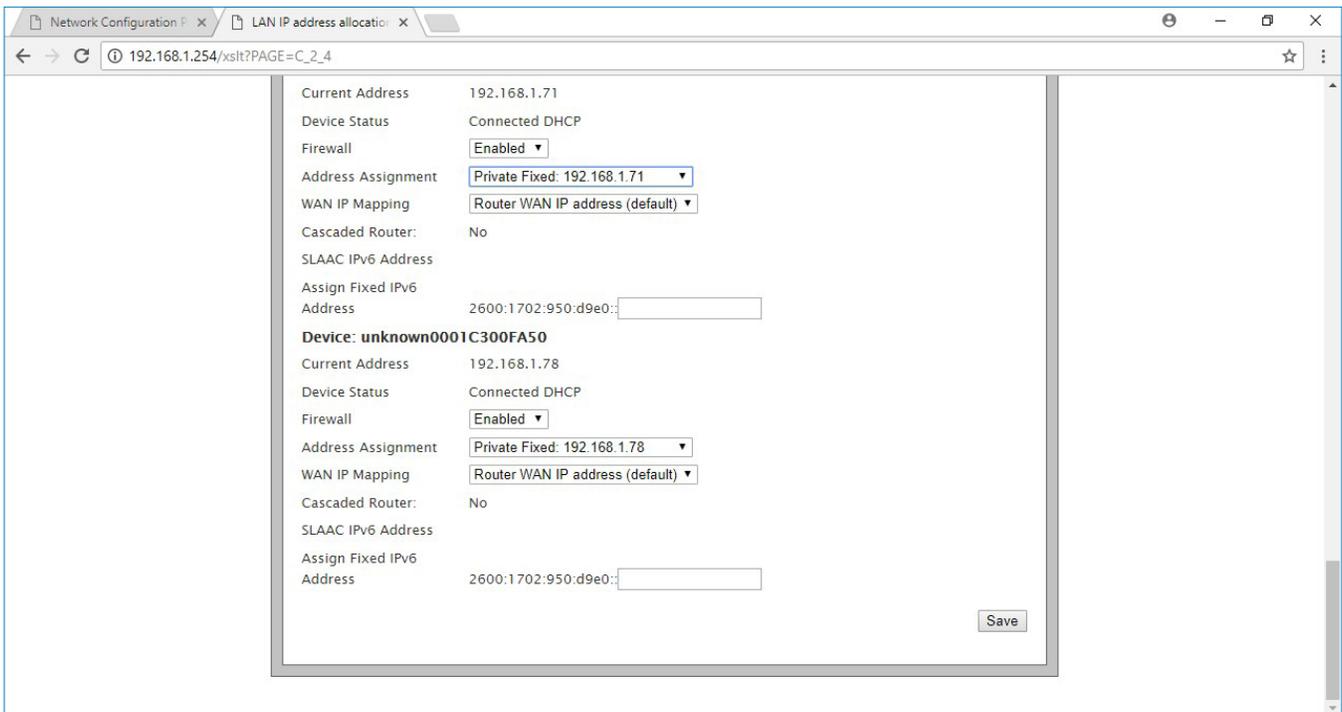


For device **unknown0001C300FA54**, I click the down arrow to the right of the “Address Assignment” field and select **Private Fixed 192.168.1.71** as shown below:

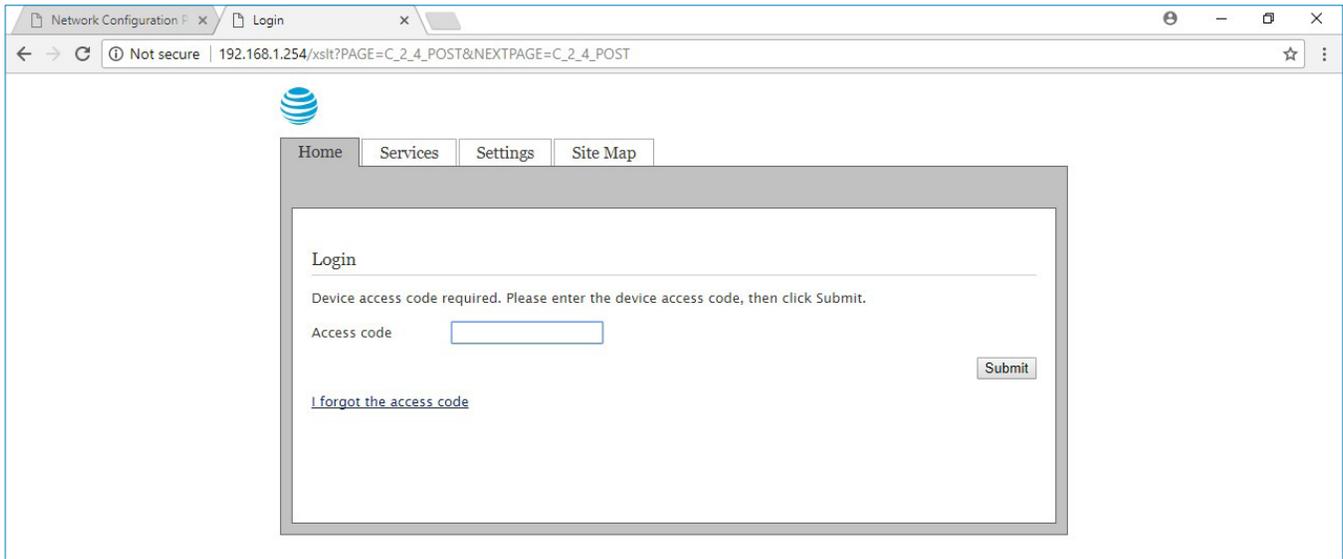




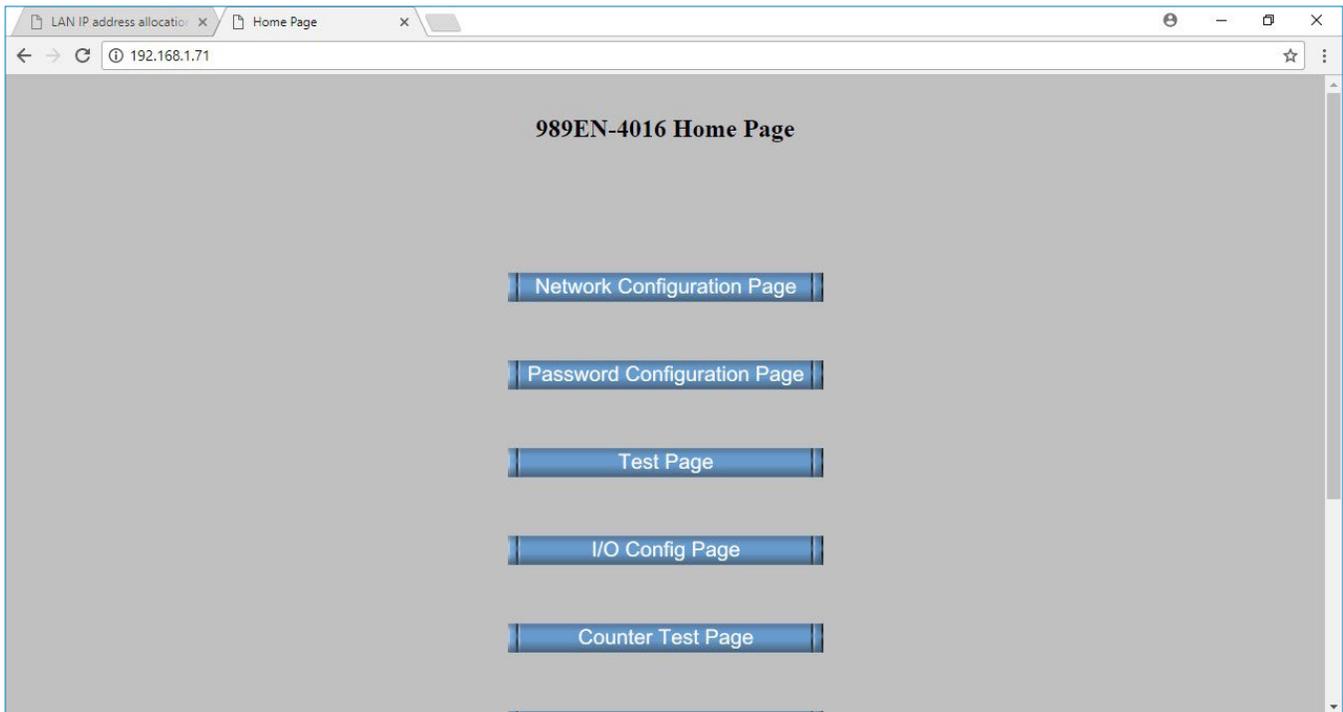
Next, I scroll down to the bottom of this page and click the [Save] button to save my DHCP Address Reservation of IP address 192.168.1.71.



After I click the [Save] button, the router will prompt me for the special access code (or username/password on other routers) in order to save my router changes as follows:



So I type the router's access code into this field and click the **[Submit]** button, and my DHCP reservation is made. Every time I reconnect or repower the module on this network, this router DHCP will give it IP address 192.168.1.71 (the router has associated its MAC address with this IP address). Now I can use a web browser on any computer of this LAN and reach the Home page of the module at IP address 192.168.1.71 as shown below:



To review, the key to making this LAN connection with this router was to realize that rather than simply discerning the router's address domain and picking a compatible static IP address assignment for the device (discussed below), the device had to use DHCP addressing with this router, then be viewed through the router to see what IP address assignment the router DHCP gave it, and then direct the router to make the same assignment every time my device connects. This was done because this router never connects to the device if it is manually preset to a static IP address. Your router may act differently, but doing it the way illustrated has an added advantage of avoiding potential error in picking your own IP address and indirectly verifies the device is connected and powered-up.



**Optional – Setting a Static IP Address in the Device You Want to Connect to your Home Network**

You cannot access your device on your network reliably if its IP address changes. Many home routers, including the router of Example 2, do not support statically addressed LAN devices and we had to utilize a form of DHCP reservation in the router to give the device an address that doesn't change. If your router does support statically addressed LAN devices, you could optionally set your device to utilize a static IP address as follows:

Refer to the LAN subnet mask to extract the node address portion of your network. Most often this is a Class C network with a subnet mask of 255.255.255.0 which would allow up to 254 network devices (the device IP addresses typically look like 192.168.x.x). One strategy for setting a unique static address inside your device would be to add 10 to the node address portion of your Default Gateway IP address to obtain another unique address in its address domain. For example, if your Default Gateway was 192.168.1.1 and your Subnet Mask was 255.255.255.0, your new static address assignment could use 192.168.1.11, or similar if the resultant address happens to already be in use by another device on the LAN. Remember when setting another node number, you cannot use the first node number (0) or the last node number (255), but only another unique number from 1-254 that's not already used on the LAN (different from your router IP address).

In Example 1 the device itself was setup for a router that does not allow LAN devices to be statically preset and had to use DHCP addressing instead. For other routers that support static IP address assignment, in Example 1, on its Network Configuration Page, instead of telling the device to Use DHCP, select Use Static IP Addressing and replace the static IP Address with a compatible IP address in the LAN domain. Refer to the documentation for your router to determine if you need to set any other parameters inside the router for static IP addressing of your device.

Now network connecting my device to my LAN is great if I only need network access from the same network. But if I need to access it from a remote computer on a different network (like remotely from my computer at work), then I would have to implement a Port Forward to its IP address on my LAN. That is, to port forward, I use the public IP address of my router's WAN port along with a port number that I assign to the private LAN IP address of my device inside the router. Unfortunately, it gets even more complicated at this point, as you will likely have to pay for additional services and/or a static public IP address to accomplish port forwarding on your home network. In addition to obtaining a static public IP address, you may want to add the services of a Virtual Private Network (VPN). A third connection example shows how to remotely connect to an Ethernet device that is connected to a home LAN (Example 3 reuses the same device of Examples 1 and 2).

**Contrast Example 2 for Making a home LAN Connection with Making a Corporate LAN Connection**

If you happen to be connecting your device to a corporate network, the process will be much easier, as you can simply consult with your network administrator to obtain an unused static IP address within your corporate address domain that can be set aside for your device (i.e. you want to select an unused domain address that shares the same corporate network ID). Your network administrator typically has a pool of static IP addresses to pick from and can select or reserve one for your device without also stepping on other node addresses that are being used by other corporate LAN clients. Your corporate network administrator generally has greater control over corporate or business class router operation and may even allow you to set a static IP address in your device that your network administrator reserves for you (rather than using DHCP reservation as demonstrated in Example 2 for a home LAN connection). Then, with your device connected to an Ethernet port of your corporate LAN, or to an Ethernet switch connected to your corporate LAN, you simply use a web browser at a computer inside your LAN directed to the static IP address reserved by your network administrator for your device. Example 1 setup the device for home LAN connection in Example 2, but for corporate network connection, you typically would change your device from using DHCP address assignment to using a fixed static IP address that your network administrator provides for you.



---

### Example 3: Remotely Accessing an Ethernet Device Connected to Your LAN

---

#### Connecting to an Ethernet Device

This section covers the third scenario of remotely accessing an Ethernet device. Remote access reuses the information and the device of Examples 1 and 2, but adds Port Forwarding from a static public IP address, and potentially the services of a VPN (Virtual Private Network).

Using the internet to remotely access your device can be very complex and usually involves the purchase of additional services. Background information for making the connection is presented first, followed by an example. If you read all the background information, you should have enough information to make the connection yourself, and much of this information can be extrapolated to other Ethernet device connections of your home network.

#### How Public Clients Talk to Private Clients?

Nothing passes between the LAN and WAN without passing through the router's gateway and the router also masks source addresses from recipients, it additionally uses a port number assignment to link public and private messages between clients. Subsequent messages between clients of different networks use the same port number to keep the messages between themselves and no data packet can be exchanged without a port number.

Thus, remote access of an Ethernet device can only be accomplished via port forwarding in the router between the public WAN and private LAN client, and this section shows how to achieve that.

Once remote access to a device is properly setup, then from a remote web browser of another network, you simply enter your LAN router's public IP address followed by a port number that you select and separated by a colon ":" to remotely access your device on your LAN (like <http://107.211.235.76:59926>).

The following example reuses the information and device of Example 1 and 2 which setup a Acromag 989EN-4012 Ethernet module on a home LAN. Example 3 adds remote access to this module over the internet. Please review section 1 and 2 before picking up here. But before we walk through our third example for setting up remote access to an Ethernet device, we need to cover some additional network terminology

#### Before You Start - Your Public IP Address Must be Static

*Recall that a static IP address is an address that is fixed and does not change. Most ISP's block ports to dynamically assigned public IP addresses and a static public IP is required to open ports. Unless you already pay for a static IP address or have leased a small bank of static IP addresses, you must consult with your ISP before attempting to follow Example 3 of this document.*

By default, residential Internet Service Providers (ISP's) assign public IP addresses dynamically to a router's WAN port, meaning that it can change from time to time. In fact, your public IP address today may be assigned to another client tomorrow and reassignment is normally out of your control. In addition, by default, most ISP's block ports of residential clients and clients that have a dynamically assigned IP address. For security reasons, they do not want to open ports at IP addresses that can be reassigned to other customers and they block port access to prevent residential customers from hosting web servers, which consumes their bandwidth. Their service is structured to make you pay for the privilege of remotely accessing an Ethernet device hosted on your home network, which requires that port(s) be opened. Your avenue to opening ports of your public IP address is to pay for static public IP addresses. But in addition to paying for a static public IP address, you may still need to separately request that port(s) be opened at that IP address by your ISP. Typically, your ISP will ask you for more money for several static IP addresses that they would be willing to open ports for, or they may request that you pay for a premium level of service to enable remote access (which will ultimately specify a static public IP address). This will be true even if you happen to notice that your public IP never seems to change (this was the case for my own public IP address from my ISP, see below).

But after you pay your ISP for a static public IP address, you typically receive a small bank of static IP addresses (typically a bank of 8), and your IP addresses will be known. Although you may think that you only need one static public IP address, having more than one gives you greater freedom in setting up your LAN. For example, you could choose to give your host device its own IP address separate from your LAN router, helping to protect other LAN devices from being hacked. Most installations will need at least three IP addresses anyway: one for the network address, one for WI-FI, and one for a broadcast address. For my example that follows, my ISP wanted an extra \$15/month to provide five usable static IP's that they would be willing to open ports for (five useable static IP addresses from eight provided).

**My Example:** *When I started out to enable remote access, I was initially encouraged to find that my ISP public IP address already appeared to be static and never seemed to change. Subsequent research suggested that the only events that might prompt a change in my IP address are typically service-call related, like swapping my gateway for upgraded equipment, or if my technician changes my service port at their terminals. But when I proceeded to set a port forward to my application using that IP address, I discovered that no matter what I did, my ports were being blocked at my public IP address. I called my ISP customer service, told them what I was trying to do, and asked the technician to open ports on my IP. The first technician I spoke to remotely accessed my router and did this for me while I was on the phone. However, after hanging up, I noted that when I used my web-browser, I would receive numerous security errors and warnings, rendering the browser nearly impossible to use (and my email stopped working).*



*I called my ISP back and told them what was happening and a second representative thanked me for reporting this incident and he remotely accessed my router (their first technician was not supposed to open ports at my IP address).*

*The second technician also offered that they could help me get remote access if I were to pay for a static IP address bank for an additional \$15/month. I said no thanks and hung up. I also reset my router to help alleviate security issues, although I think my ISP remotely closed my ports during the second call. But still, my web-browser acted strangely and seemed to work intermittently. I called my ISP again the next day, told them what had transpired, and what I was originally trying to accomplish, and after being bounced around to several different people, I was passed up the ladder to another technician that offered if I paid for premium technical support, they could help me setup remote access, and it would only be another \$15/month. Frustrated at this point, I refused the upgrade. But after more research, I found out that I cannot achieve remote access with my ISP without ultimately paying them for a small bank of static IP addresses, which they would be willing to open ports for. I also discovered that during this brief episode of having my ports open, I had acquired some type of browser hijack malware, and it could not be removed using my malware software. I also noted its path was tied to my web browser, so I uninstalled my browser and deleted its remnant folders/files to finally get rid of it. I also investigated adding a VPN service, since it appeared that I may have acquired this virus while my ports were opened briefly.*

#### **TIP: How to Find Your Public IP Address**

There are many ways to find your public IP address if you don't already know it. You could ask your ISP, or you could use your router's LAN IP address to access its configuration console and review this information (you already used your router's configuration console in the Example 2). Your router's web console has at least one page where your public IP address will be indicated.

But even easier than asking your ISP or using your router's LAN interface, your public IP can be found quite easily from a computer inside your LAN. Simply direct the web browser of a LAN computer to [WhatsMyIPAddress.com](http://WhatsMyIPAddress.com) to retrieve the public IP address of your internet connection and both your IPv4 and IPv6 IP address will be indicated. There are many other free sites that will return your public IP address, like [howtofindmyipaddress.com](http://howtofindmyipaddress.com).

In addition to paying your ISP for a static IP bank that they can open ports for, you have two other services that you might consider (these will be explained later):

- (Recommended) Because open IP ports pose a unique security risk to you, you should consider subscribing to a VPN service (your ISP may also offer this service with static IP addresses). Be aware that some VPN services are more Port-Forward friendly than others (more on this later).
- (Optional) You may want to purchase a Dynamic DNS host name to make your numeric public IP something more meaningful and memorable (even if you already have a Dynamic DNS service, your ISP will be reluctant to open ports for the dynamically assigned numeric IP address it will link to).

#### **Port Forwarding, Port Mapping, or Virtual Server**

Every TCP or UDP packet contains a source IP address, plus a **source port number**, a destination IP address and a **destination port number**. The combination of IP address and port number form a remote communication **socket**.

We already stated that a LAN router blocks public messages directed to private IP addresses, such that public messages must instead be directed to the router's WAN port with a port number to be delivered to specific LAN client. Likewise, outgoing messages from a LAN client to a public/internet client must be directed to the router IP address along with a port number. The router NAT receives these messages and swaps its own LAN IP address with the message source IP address in the datagram packet header as it is in transit across the router gateway, then forwards the packet to the specific client associated with that port number. Essentially NOTHING passes between networks in either direction without reference to its port number. As a web address, the port number normally follows the IP address for specific port assignments, or it may be dropped from the IP address for a standard default port number (like port 80 for http messages).

This behavior of the router/gateway NAT (Network Address Translation) that steers external communication with a port number to a specific LAN client or clients associated with the same port number (socket) is referred to as **Port Forwarding, Port Mapping, and Virtual Server**. Its purpose is to make a LAN client accessible to a remote computer of the internet, even though client IP addresses are isolated from each other by their routers. Port forwarding is commonly used for game server communication, or remote access to private security cameras, sometimes for voice over IP, and for downloading large server files (FTP). It works remotely the same as if done locally using private LAN IP addresses between clients of the same LAN.

Port number associations inside your router can only be made between IP addresses that do not change. This means that your public IP must be static, and your device IP must also have an address that doesn't change. Further, your ISP must not block ports at your public IP address.

The port number itself is an unsigned 16-bit integer (0-65535) that is inserted into a TCP or UDP network packet header. Any TCP or UDP connection requests sent to your router must include this service port number, which defines its logical connection inside the LAN where the router should direct the incoming message. In any subsequent exchange, the remote client includes the same port number in its response to continue to direct the router to the



right LAN client. Because of NAT, the remote client never knows the specific IP address of the LAN client or vice-versa, as source addresses are swapped with the IP address of the LAN router on the destination side. You can port forward a single port number or range of port numbers to a single LAN IP address or range of LAN IP addresses, and all incoming connection requests that specify the same port number(s) are forwarded to the same LAN client(s). IANA has reserved some port numbers for common default network functions and others for private use.

For example, some routers enable remote access to their LAN IP address configuration console using default port 8080, such that combining it with the router's public IP address from a remote web browser (<http://X.X.X.X:8080>) can access it the same as a local LAN client using its private LAN IP address.

HTTP refers to HyperText Transfer Protocol and is the protocol used on the internet which specifies how messages are formatted and transmitted, and which directs web servers and browsers how to respond to messages. An example default is port 80, which is reserved for web-servers of a LAN (the servers that process HTTP messages). An inbound message to the router's public IP address with Port 80 would direct the router to forward that message to the LAN IP addresses that handle web-server clients. Likewise, when you use your browser to view a web page on the internet, it uses port 80 to connect to the outside world. But because 80 is a well-known default port for web traffic, it does not need to be included with the IP address for remote access. Other defaults include, port 3389 for connection to a Remote Desktop, and port 21 for connection to an FTP server.

**CAUTION:** *Your router NAT is your first line of defense to help prevent hacking by the method it uses to isolate source IP addresses from destination clients. But once you forward a port, you have at least one open port or internet socket that can be exploited for nefarious purposes if left open to inbound connection requests. Internet criminals often attempt to open communication with well-known ports to gain control or build a lateral path to other clients inside a network (for example, remotely accessed network printers are one weak port of entry for internet criminals).*

You are not restricted to using standard port number assignments, but can create your own for your own unique services. Even though standard port numbers exist for common services, your network may not include the services they correspond to. Of course, external clients may have certain expectations with standard numbers, such that you should be careful about reassigning well-known ports to other services. In most cases, your home RG is leased by your ISP and they typically alter its internal program to limit what you can do and they often block port forwarding by default. As such, solutions for remote access can get quite creative. For example, if your ISP blocks remote access to your router's admin interface by blocking reference to port 8080, then you could port forward a port number to another LAN device instead that might allow you to use its web browser to access the configuration console of your router using the router's LAN IP address.

Every router has its own software and terminology for port forwarding and this may vary from model to model. Generally, you will find the router's LAN IP address written on the side of the unit and you may need to explore its configuration console menus to search for inferences to port forwarding, such as port mapping, pin-holes, virtual server, etc. While its setup will vary from router to router, it generally involves the following steps:

- Log into your Router at its LAN IP address to reach its admin console from a LAN browser.
- Navigate to its User Application/Port Forwarding/Virtual Server configuration page. You will need the console username and password to get here. You will need the LAN IP address of your device and a port number not already being used (typically 49152 to 65535).
- Add your Port Forward rule to the router as required, then test that your port(s) forward correctly using an online port checker like that at [YouGetSignal.com](http://YouGetSignal.com).

You should be aware of another type of Port Forward called **UPnP Port Forward (Universal Plug 'n' Play)**. This works the same as Port Forwarding, except instead of you or a network administrator having to set the mapping up inside the router, software inside a network LAN client automatically sets the NAT router to forward WAN traffic to itself (LAN client). This is how some UPnP compliant devices join themselves to a network without you or your network administrator's intervention via other special router configuration. It's also how some VPN services install their software on your network. Many routers enable UPnP by default, but some older equipment might require you to manually enable it. If your router does not support UPnP, then you will have no option but to manually setup Port Forwarding via your router's configuration console. And just as some routers disable remote management, some routers keep UPnP turned off for security reasons.

### Port Number

A port number is a 16-bit unsigned integer ranging from 0 to 65535. Both the TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) transport layer protocols include source and destination port numbers in their packet headers to directly target nodes of different networks. Since remote access requires communication between different networks, you must also use a port number to accomplish remote access of your Ethernet device. Your router links messages with a port number to specific LAN client(s) and NOTHING may be exchanged between networks without reference to some port number.



The port numbers used by public network clients to access applications or services of private IP networks are divided into three ranges as follows (see <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>):

- 1. Well-known ports from 0 to 1023** – These are reserved for common system or root processes and applications that can be run by privileged users, such as: 80=Hypertext Transfer Protocol/HTTP for world-wide web clients, 110=Post Office Protocol Version 3/POP3, 25=Simple Mail Transfer Protocol/SMTP, etc.
- 2. Registered ports from 1024 to 49151** – These are reserved for private use of TCP applications and assigned by the Internet Assigned Numbers Authority/IANA. These applications normally run as ordinary programs and may be accessed by unprivileged users.
- 3. Dynamic or private range ports from 49152 to 65535** – You can assign these for use by any LAN client to open communication with any WAN client via the Transmission Control Protocol/TCP or User Datagram Protocol/UDP.

The standard or well-known port numbers from 0-1023 specify default levels of service that people use for well-known types of communication. For example, port 80 is the default port number for web (http) servers and web hosts will listen for port 80 messages. Remember that nothing crosses a network between clients without a port number. But when you surf the internet and access various web servers on other networks, you don't normally include this port number after their IP address (like <http://107.211.232.77:80> or <http://acromag:80>). This is because the web service you are trying to access has been implemented for the standard port number, which allows you to drop having to specify that port in your browser address line. You are not restricted to using standard numbers, and can assign your own. However, any remote messages to IP addresses at user-defined ports will have to include the ":port\_number" after the web IP address (or host name).

*We have already used the router's LAN IP address to access its configuration console in Example 2. Some routers additionally have a default port number assignment of 8080 to remotely access their administration interface (typically you separately enable this if you want to take advantage of it). The remote management Web Access from WAN feature of some routers is one instance of Port Forwarding. You must be careful if you choose to enable remote configuration of your router, as this open port is potentially an open door for hackers to invade your network router and foul your control over network devices. You could explore changing the default port number of your router's web interface to something else (likewise for any other default ports that are open that you want to protect). When using port numbers, it is recommended that you never open all ports on your router and most ISP's block all ports by default unless you pay for extra services which allow you to open ports on your static public IP address. Additionally, it's always good practice to install up-to-date virus protection software on all LAN client(s), as well as make use of built-in router firewall protection.*

Port 25 is a standard port which mail servers listen on and most ISP's block inbound and outbound port 25 traffic to stop spammers from penetrating their client networks. As you can reason, this would make running a mail server off your home network difficult, if not impossible. Likewise, many ISP's also block traffic on port 80 to stop viruses like Nimda from slowing down their networks and infecting their client's computers. Because your ISP may be blocking port 25 and port 80 traffic, you will need to take special measures to open these ports (and others) if you need this type of remote access. For my example, because my ISP account also includes a satellite TV service which already uses port 80, I could not use standard Port 80 to host the web server of the 989EN-4016 module in my port forward definition, and I had to select my own port number, which works exactly the same way except that I must include the port number after my public web address (like [www.107.211.232.75:65535](http://www.107.211.232.75:65535)).

### Virtual Private Network (VPN) – A Recommended Option for Increased Security with Open Ports

**VPN or Virtual Private Network** is a third-party intermediary service that allows you to conceal your identity (LAN IP address) from remote clients of a Wide-Area-Network (WAN) and that will encrypt all your traffic.

Why might remote access need a VPN service? In the preceding section, we stated that open ports on a LAN can be a welcome mat for hackers to invade your network, and net criminals are known to routinely open communication with "known" ports to gain control and build lateral paths to LAN clients inside a network.

Not convinced? You should know that it's quite easy for anyone to determine if your public IP address has any open ports. There are numerous web sites that allow you to enter a public IP address and a port number, to check to see if it is open. But even if you don't know the port number to check, other sites will scan ports in a wide range that you specify and return a listing of all open ports (for example, <http://www.ipfingerprints.com/portscan.php> will scan an IP address for any open ports).

Recall that a router swaps source IP addresses for messages that cross its border with its own address to help keep source and destination IP addresses hidden from each other. Your public IP address can be a problem in that it can approximate your computer's location and potentially expose you or your network to hacking. You could employ a proxy server to further help conceal your IP address. A **proxy server** is just an intermediary server that acts as a gateway between your LAN and a larger WAN network like the internet that helps conceal your IP address further. This is good, but a better and even more secure option to communicate over the internet and conceal your IP address can be done using a **VPN** (Virtual Private Network). The VPN is similar to a proxy server, except that a VPN additionally encrypts all of your traffic as traffic is routed through the intermediary VPN server.



A VPN is a third-party service that you subscribe to (usually online for a small fee). Once you have a VPN account, your VPN is setup to turn ON whenever you go online, or it may require you to log into it after going online. Typically, you connect to the public internet through your ISP the same way you do now, but then initiate a VPN connection to a VPN provider's server using their client software. You continue to communicate to remote clients just as you do for local clients of your LAN. The VPN intermediary helps you remain anonymous by shielding your browsing activity from others when using public Wi-Fi and can even enable navigation around access-blocks of region-restricted or censored web sites. VPN's are most often utilized by large corporations to allow their remote users or branch offices to more securely access corporate applications and resources. A VPN works by providing a temporary IP address or "alias" that masks your actual public IP address from every web site or email server you connect to by using dedicated connections in combination with tunneling protocols that use data encryption.

Still, all your internet traffic passes through your ISP servers and can be viewed by your ISP at any time. When you use a VPN, you connect through your ISP to another intermediary VPN server that uses another IP address and encrypts all your traffic creating a secure VPN tunnel. Because VPN services use specific port numbers to direct traffic through their servers, the VPN port number of a datagram can reveal it as a VPN connection to your ISP even if they don't recognize the end destination of the VPN packet.

There are many web sites that allow you to enter a public IP address and locate its geographic source (like [whatismyip.com/whatismyip.net](http://whatismyip.com/whatismyip.net)). But if that IP address has been hidden by a VPN service, a query of it using an IP finding web site will return the location of the VPN it is using, not the location of the originating source--some VPN services allow you to direct which server source location to mimic to further conceal your real location when you surf.

**TIP:** *Geolocation of a public IP address refers to the identification or estimation of the approximate geographic location of an internet-connected computer (or at least the location of its ISP terminal). This is great for helping to identify the source location of an email for example. A great site to geo-locate your own IP address is [www.whatismyip.net](http://www.whatismyip.net) or [www.whatismyip.com](http://www.whatismyip.com). Try this for your public IP (from a terminal on your LAN) to check your public IP—does the location indicated match your own? If you want to check any other IP, you can go to [www.iplocation.net](http://www.iplocation.net) and enter any public IP address in the field to geo locate it. Note that if the source you are locating is using a VPN service, you will be returned the VPN server location, not the actual source location. Some VPN services allow their clients to choose the source location of their servers such that you can make your data messages appear to be sourced from a far-off location relative to your own. Network computers that are linked to a router share the same public IP address and private IP addresses are untracked and unrestricted. Sites like [WhatsMyIPaddress.com](http://WhatsMyIPaddress.com) cannot geographically locate a user's computer by their private IP address. You can examine the type of IP address in the header of an unsolicited email to help you determine the origin of an email (is it local or remote), but its true origin can be referenced by looking in the earliest received email header of a thread.*

### **Dynamic DNS Service (One Option for Added Convenience)**

*Do not confuse a Dynamic DNS domain name with a static public IP address.*

Dynamic DNS (DDNS) refers to a service you can subscribe to that allows you to create a unique, easier to remember domain name, that you can use to access a network in place of a numeric public IP address. Even if your public IP address is dynamically assigned (subject to change), DDNS uses special software to alias your current IP address assignment to a fixed domain name that doesn't change. Some DDNS services may charge a small monthly fee for your domain name, and some offer this as a free service with purchase of their equipment (it is an included option for some routers). For example, assume that you use a DDNS service and specify a domain name "mynetworkathome1.net". This allows you to enter **<http://mynetworkathome.net:portnumber>** into a remote web browser to access a service on your LAN that is mapped to that port number (for example, **<http://mynetworkathome.net:8080>** could access your router's web interface remotely if you have enabled remote management and your router supports registered port number 8080).

Up front, we said that to get remote access to an Ethernet device, you must pay for a static public IP address. With a static public IP address, you can use the same numeric IP address to accomplish remote access from anywhere on the internet, except that it's often inconvenient to remember a numeric IP address, and you might want to make it more meaningful by creating a named web address that signifies its service. This might lead you to believe that you can simply subscribe to a Dynamic Domain Name service to obtain a "static" domain name that doesn't change, but this would not offer the same benefit of a static numeric IP address. This is because even though DDNS makes your numeric IP address appear static, your ISP will be reluctant to open ports at the dynamically assigned public IP address it may be assigned to—for reliable remote access of a LAN client, you must additionally associate it with a static numeric public IP address.

Devices that attach to your home LAN most often get their IP address dynamically from your home router, while your home router's WAN port gets its public IP address dynamically from your ISP. This means that your public IP address is subject to change, and to setup remote access to a device over the internet, you must have a public IP address that does not change. In the second example of Connection Scenario 2, we showed how you used a DHCP reservation feature of the router to direct the router set the same IP address to your device inside your network (great), but remote access requires that you additionally pay to lease a fixed public IP address from your ISP, like business customers do. A changing public IP address will make it difficult for you to maintain reliable remote access and your ISP will not want to open ports at a dynamically assigned numeric IP address in order to accomplish remote access, even if you note that your IP address doesn't seem to change.



Behind every web address is a numeric IP address. Your custom DDNS domain name is always subject to availability when you set it up, but you use that in place of your numeric IP address for remote access. Your domain is unique on the internet, and never changes (a name like yourhomnetwork1.net or ??). This is true even if your public IP address is not static—your DynDNS service automatically associates yourhomenetowrk1.net with your public WAN IP address at any given time by simply assigning it to your LAN router, or running its client software on a computer connected to your LAN, or installing it in a NAS server on your LAN (Network Attached Storage server). Your router may already have this as a built-in option and the simplest way to implement would be to set it up via the router's configuration console.

### Firewall Protection

Because open ports do invite hacking, you should be aware that your router usually includes some default “firewall” protection schemes already enabled to help curb nefarious access. This should make sense to you because you know that all communication between networks must pass through the router gateway before being received by a client. Thus, routers add firewall features that help mitigate access in both directions and allow you to establish rules and restrictions for traffic flow between LAN clients and external public WAN clients of the internet.

A **Firewall** is an entity that operates between networks, usually as part of a network gateway or router, which enforces default rules and others that a network administrator can set for restricting and filtering traffic flow between networks. The router already blocks direct transmission/reception between private LAN addresses and public WAN addresses using NAT to swap message source addresses with its own IP address to protect clients. It also includes firewall features that allow you to set higher-level rules for access in either direction to increase client security. For example, a firewall may utilize *stateful* packet inspection, which enables the firewall to assess traffic in context, and only allows incoming traffic it knows is a legitimate response to an internal network request, allowing that data to be received and data not requested to be blocked. Likewise, for data sent out to an external client, it may only wait for a response packet for a preset amount of gate time, after which the firewall will block incoming traffic. A firewall may also use ingress packet filtering to ensure that inbound packets are really from the networks they indicate and blocks packets from outside the network that may be using a spoofed source address inside the LAN, preventing a WAN node from impersonating a LAN node to gain access, typically done with intent to steal data, hijack web browsers, spread malware, or bypass access controls. A spoofed packet is simply an IP packet sent from a WAN node that impersonates a valid LAN client.

### Example 3: Using Port Forwarding to Remotely Access a LAN Device on a Home Network

Example 3 outlines how to implement a port forward to connect to a device remotely and gives an example of remotely connecting to an Acromag 989EN-4016 Ethernet module connected to a Pace Model 5268ac home router provided by my ISP. You can extend much of this instruction to other Ethernet devices that you may wish to access remotely. For example, maybe you have a NAS device at home (Network Attached Storage) and wish to access some files on it remotely, or a Sling box for streaming media, or a surveillance camera for home security, or perhaps you host a game server for online gaming. In short, this is a simplified review of what must be done to remotely connect to an Ethernet device:

- You need to fix the public IP address of your home router/gateway WAN port to a static IP address (this will typically require a service upgrade to accomplish) unless you already pay for or lease a static IP address like most corporate networks do. Consult with your ISP to upgrade a dynamic public IP address to a static IP address. Most ISP's will block ports to standard issue dynamically assigned IP addresses.
- You must complete Connection Examples 1 and 2.
- You must select a port number to assign to your device to use for remote access.
- Similar to Example 2, you must log into your router's configuration console from a LAN computer, but setup a TCP port forward to your application device's IP address.

**IMPORTANT:** Use port forwarding with caution to prevent potentially nefarious access to devices on your home network. You should consider adding a VPN service to increase protection.

### Get a Static Public IP Address

Before you begin, if your public IP is not leased or already static, you must request a static public IP address for your home RG to allow your ISP to open ports on it and so that the same IP address can be reused remotely at any time. **This requires that you minimally purchase a static IP from your ISP.** You may also need to separately request that your port be opened to accomplish remote access (consult with your ISP about why you need a static IP). For security reasons, you should consider adding a VPN service to your network to access your device (you may consult with your ISP or select a third-party VPN service for your network).

Once you have a static public IP and your ports are open, the setup of remote access is all done inside your router using its configuration console to configure port forwarding to create a bridge between your WAN public IP address and your LAN private IP address.

Note that in addition to a static public IP address, your LAN device IP address must have an assignment that does not change. Most home router/gateways will not talk to devices that are not setup to get their IP address via DHCP. Rather than setting a static IP address in the device, you utilize a DHCP reservation in your router to automatically assign the same IP address to the device every time it is connected (This was done in Example 2).



It seems that most ISP's do not provide manuals for their routers, as was the case in my example. I am able to use a search engine to find the instructions for my RG, which also includes some instructions for higher level control like implementing a port forward. You can do the same for your own router and the manual may also indicate your router's default username/password.

### Connect Your Device to Your LAN Router

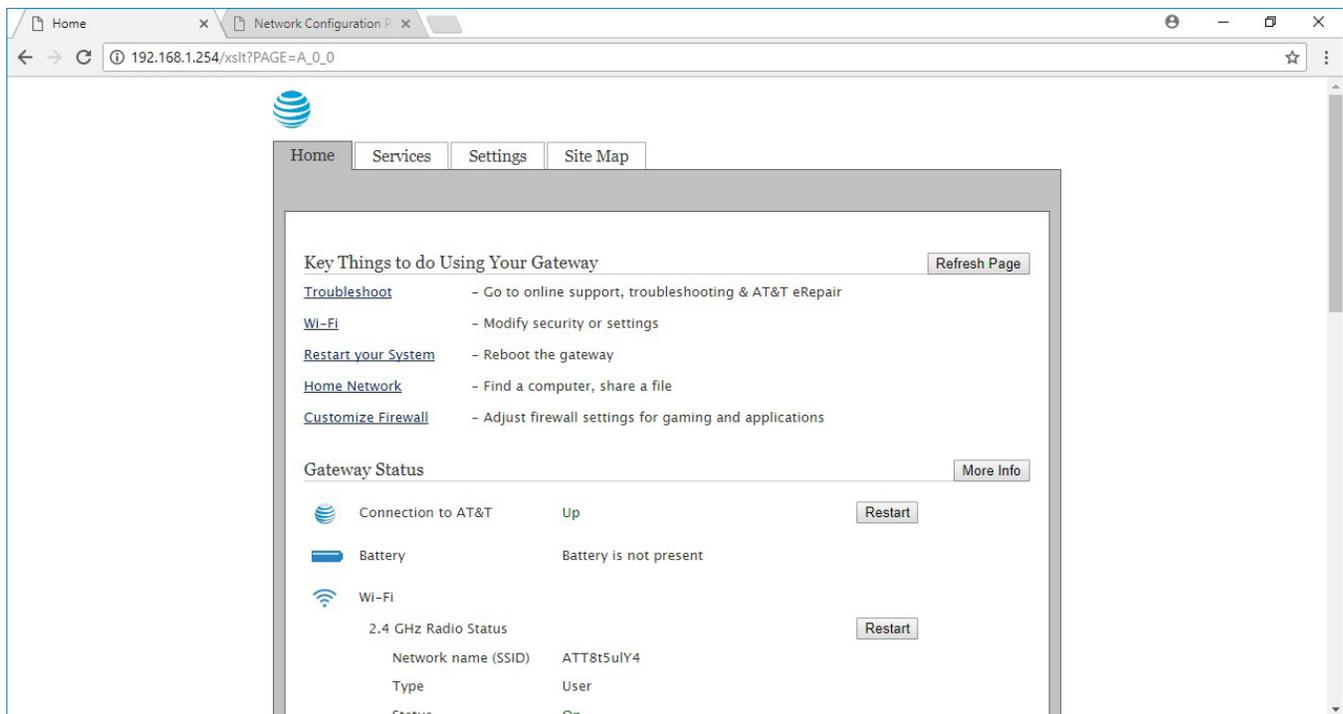
That is, your device is connected to your LAN router and you can already access it using a web browser on a computer of your LAN directed to its LAN IP address (as was demonstrated in Examples 1 and 2). For the 989EN-4012 module of our example, it is set to get its IP address via DHCP and has a subnet mask set to 255.255.255.0 (Example 1). A DHCP reservation was made inside the router to assign the same IP address to the 989EN-4012 already connected to the router. The device can be accessed using a local LAN web browser directed at device IP address 192.168.1.71 (Example 2).

### Pick a Port Number to Assign to your Device

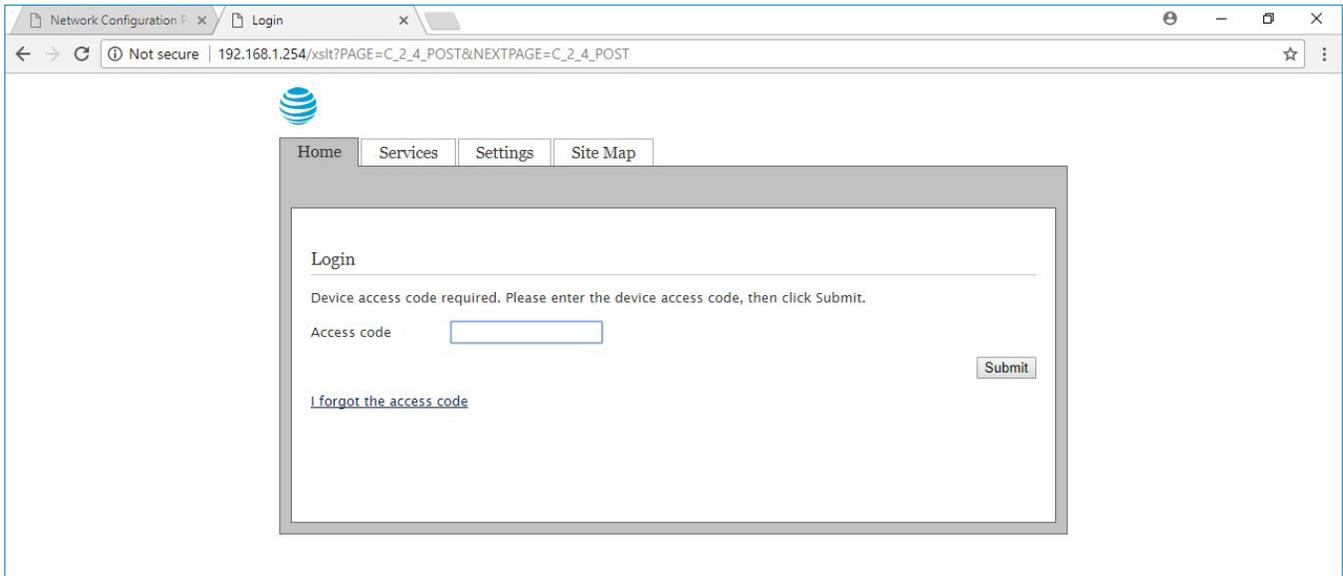
I recommend a user-configured port number in range 49152 to 65535 to assign for remote access. You can pick any number you want if it is not already used by another application. For this example, I will use port number 59925.

### Log into Your Router/Gateway at its LAN IP Address and Configure Port Forwarding

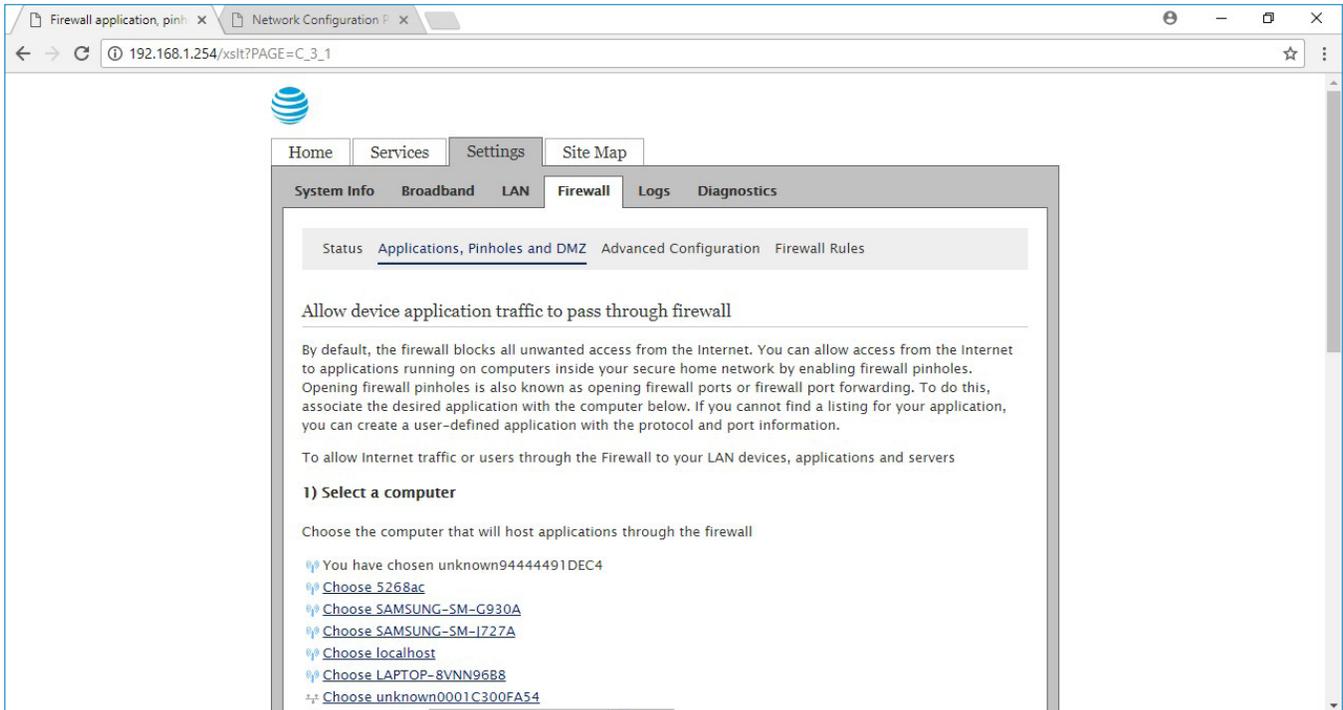
For my example, the router side label indicates IP address 192.168.1.254 and a special access code (instead of a username/password). Note that my router's IP address is a Class C address with capacity to address up to 254 nodes in my home (most common type used for small home networks). As such, all my LAN devices will have similar IP addresses assigned by DHCP in the same address domain (i.e. IP addresses will look like 192.168.1.x). To setup a Port Forward for adding remote access, from a computer on my LAN, I direct its web browser to the LAN IP address of my router at 192.168.1.254 and the router home page is displayed as shown below:



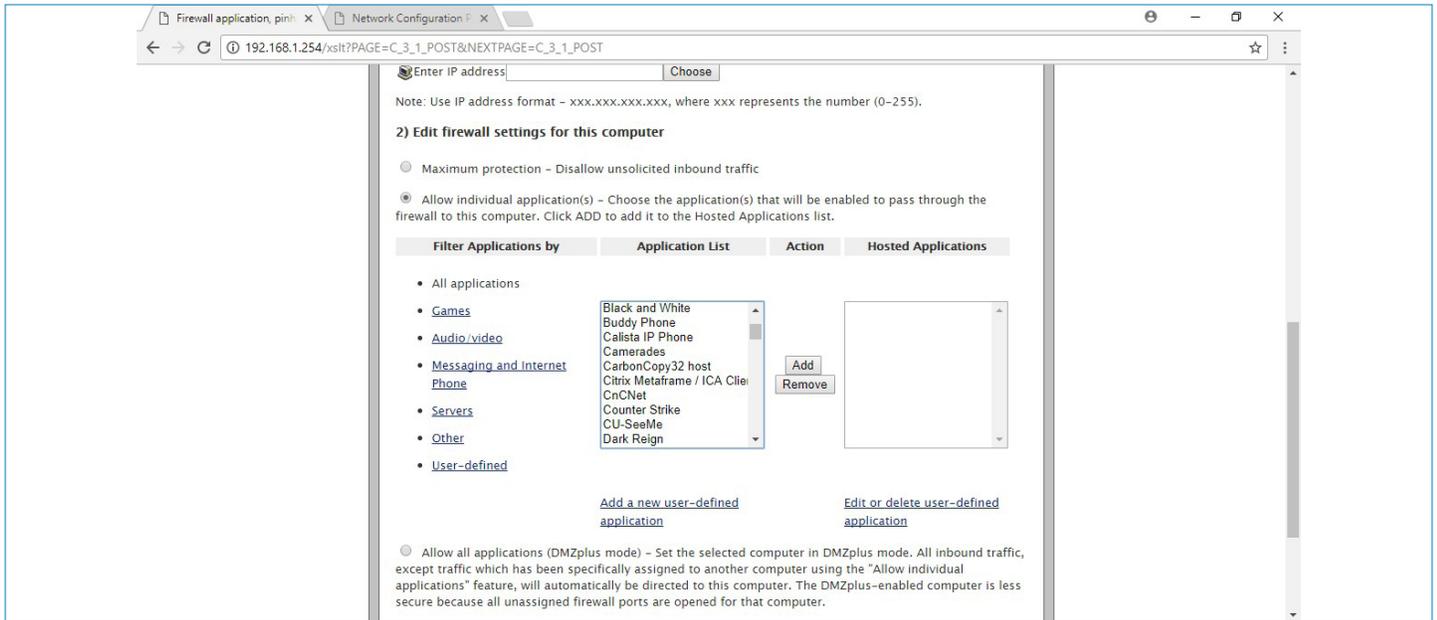
From the router home page, I'm looking for something that resembles Port Forwarding and my router's terminology may be different, so I click to the Settings tab and the router returns a prompt requesting its access code as follows (my access code was indicated on the side label of the router):



Once I enter my router access code, I am logged into my router. I need to find the port forwarding section--this page might be labeled **Port Forwarding**, Applications, Gaming, Firewall, Virtual server, or Protected Setup. If you can't find this page, try looking under "Advanced Settings". Exploring under the Settings tab, I select "Firewall" where I see Applications, Pinholes, and DMZ". Remember that I am trying to port forward to an application that I will specify (my 989EN). As was evident for Example 2 where I wanted to find DHCP reservation, the terminology used by my router for port forwarding is different, and your router terminology will vary--you will have to read closely to discern where you may configure a port forward application for your router. In my router, I select the sub-menu "Applications, pinholes, and DMZ" where I will be able to setup my application.

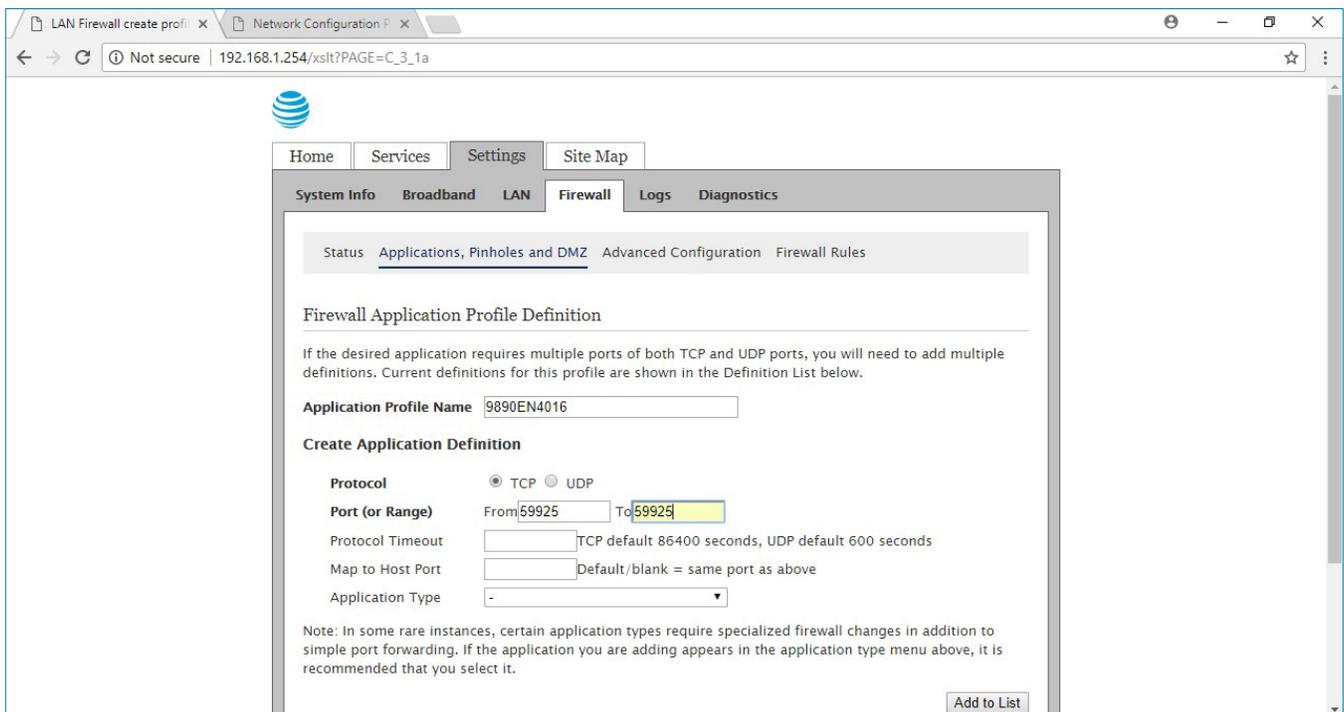


Under "1) Select a Computer", I click to select my 989EN device name denoted "unknown0001C300FA54". Note that my device did not have a host name so the router used unknown paired with the digits of its MAC address to denote it.



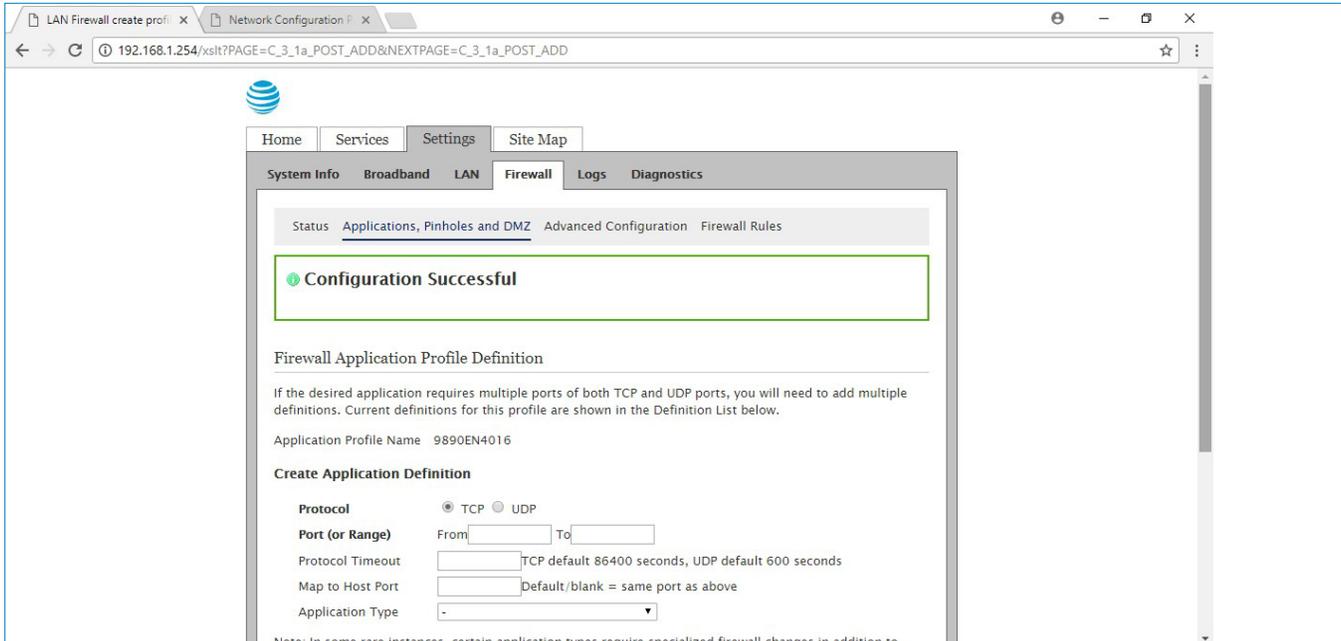
After selecting the device **Edit Firewall settings for this computer**, I select "Allow individual application(s)" as shown above. Note that some gaming applications are already available on the Application List, but I'm planning to create a new application that I have denoted "9890EN4016".

Next, I click on the field below the Application List denoted **Add a new user-defined application** to display the Application Profile Definition screen shown below. You should name your application with something meaningful to you and you must specify its protocol as TCP or UDP (if both, you must create separate applications in this router). For the "port From" and "port To" fields you will enter a port number between 1 and 65535, but keep in mind that most of the lower numbers are already reserved for other well-known services, like email or web-server. To help you select a number, some routers have a drop-down menu with pre-configured port number assignments of well-known applications. If your intended application is already listed, select that port number, or another number from the range it specifies. Otherwise, set a different port number not already reserved as in my example.

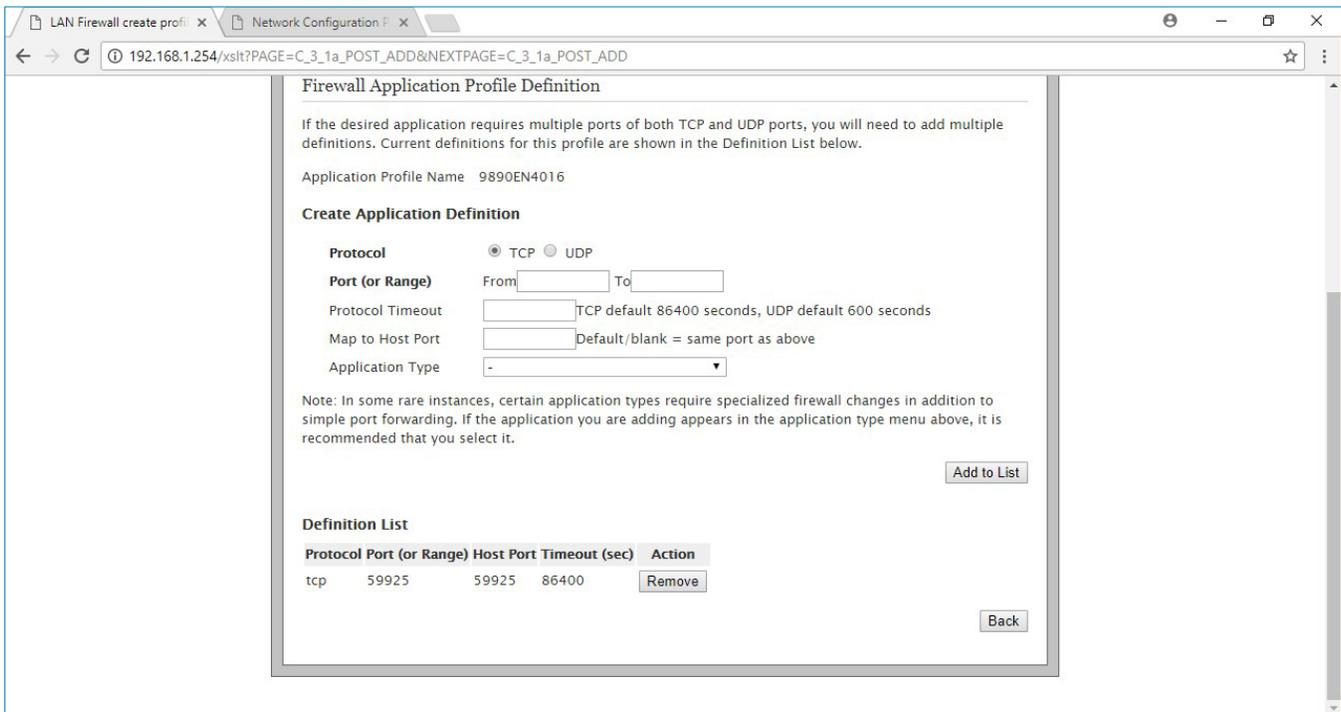




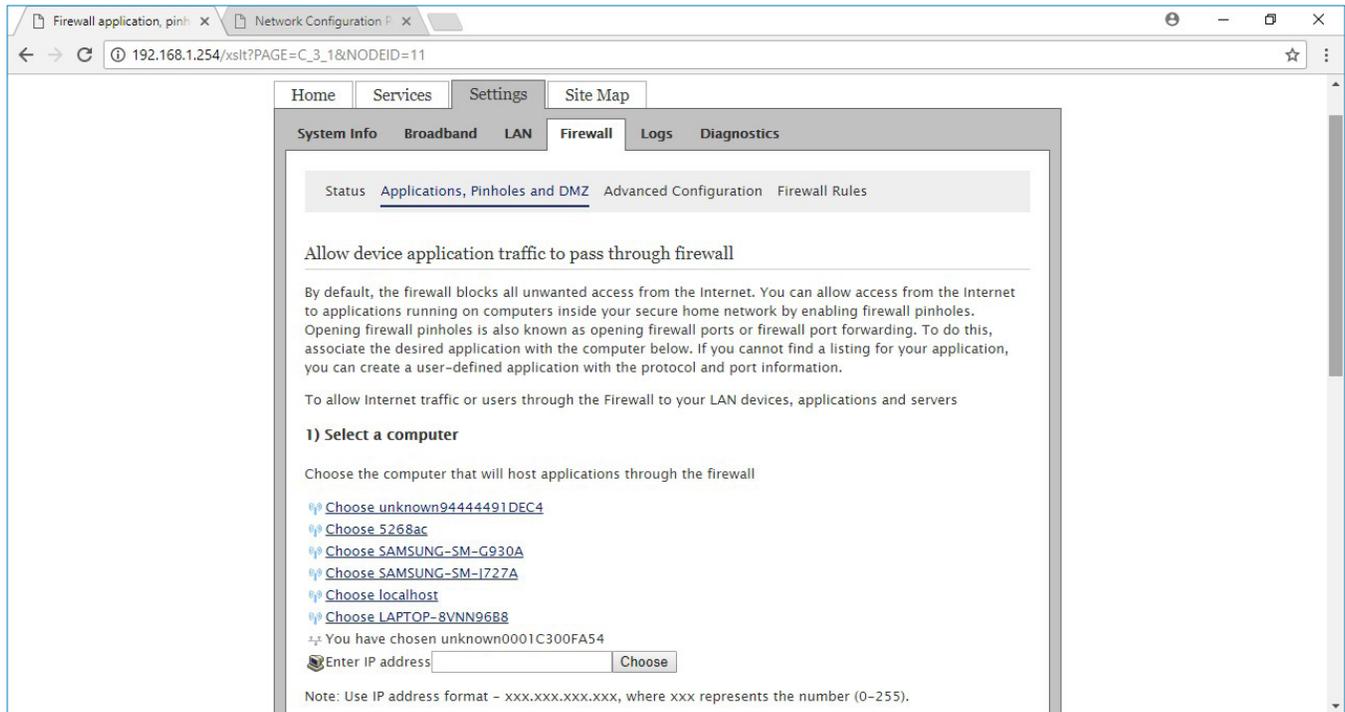
In this window I type my Application Name "9890EN4016" in the Application Profile Name field, set its Protocol to TCP, and I enter my Port number "59925" in the Port From and To fields as shown above (be sure to select a port number that is not already being used, typically in the range 49152 to 65535). The Protocol Timeout, Map to Host Port, and Application Type fields can be left empty and they will be set to defaults. Next I click the [Add to List] button in the bottom right hand corner and "Configuration Successful" is returned as shown below:



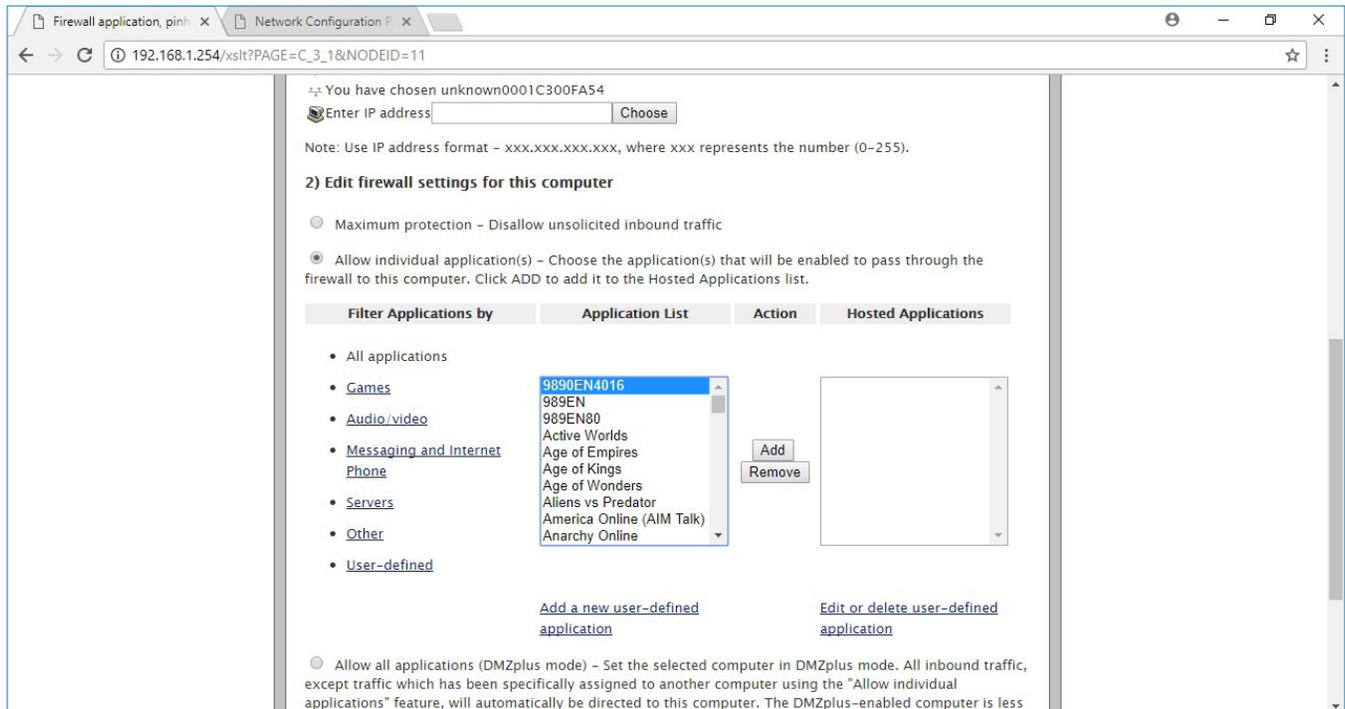
My new TCP application is now listed at the bottom of this screen as as shown below:



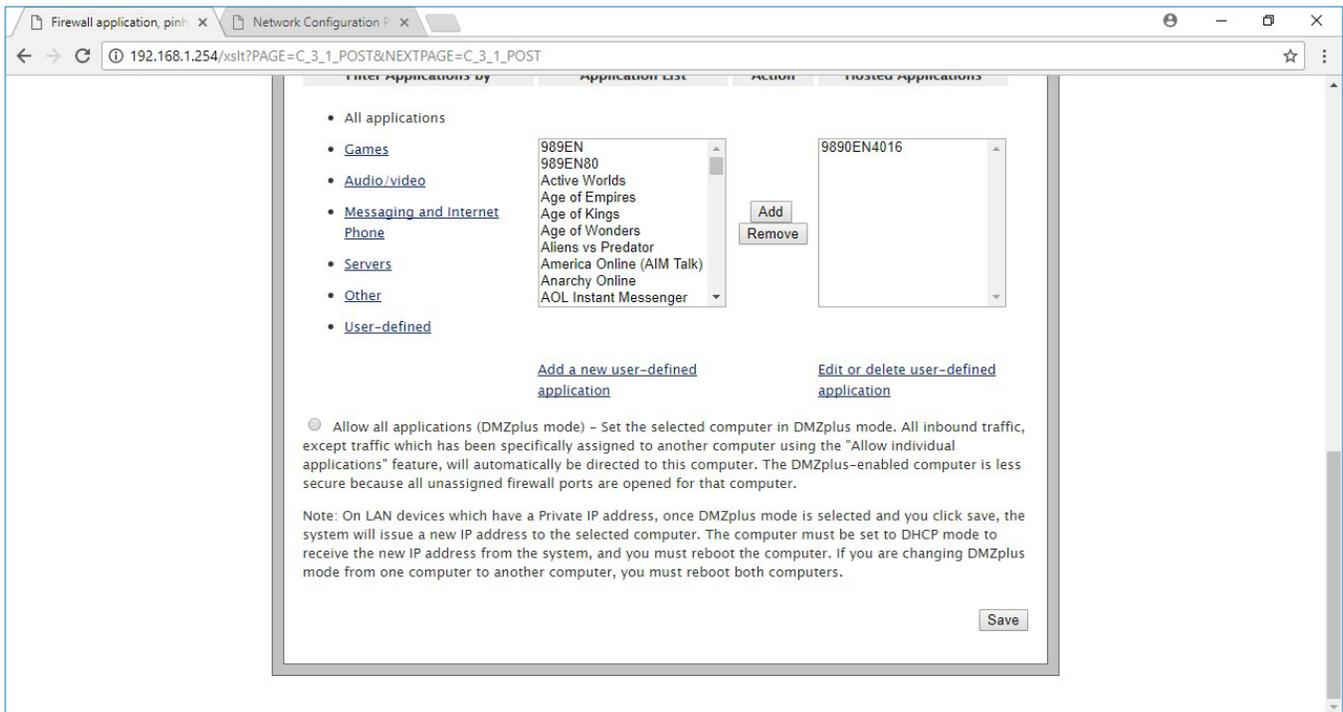
Now I click the [Back] button in the lower right-hand corner and I am returned to the Firewall-Applications... menu shown below. I need to reselect my computer "unknown0001C300FA54" in "1) Select a computer".



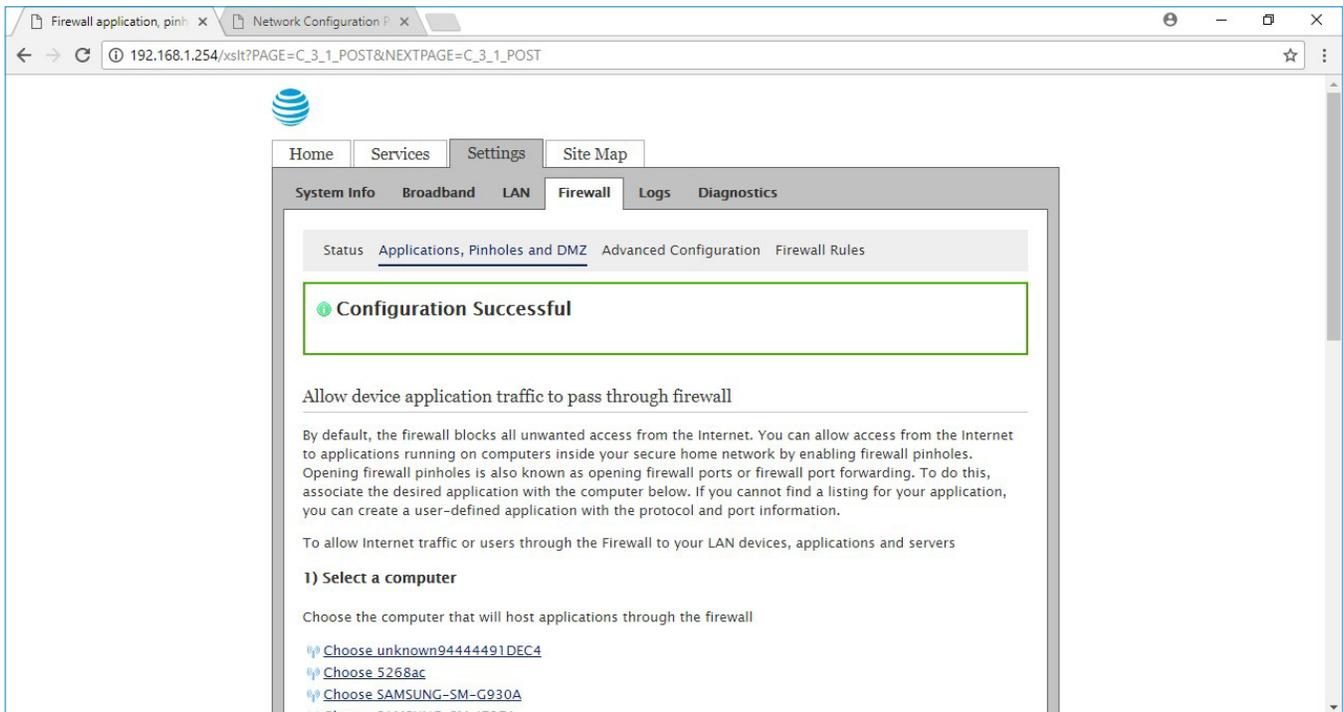
Under "2) Edit Firewall settings for this computer", my new application **9890EN4012** is listed in the Application List. Select the "Allow individual application(s)" option again and click to highlight application **9890EN4012** as shown below:



I want to move application 9890EN4012 to the "Hosted Applications" list by clicking the [Add] button to the right of the Application List, and the screen will look like this with 9890EN4016 listed as a Hosted Application:

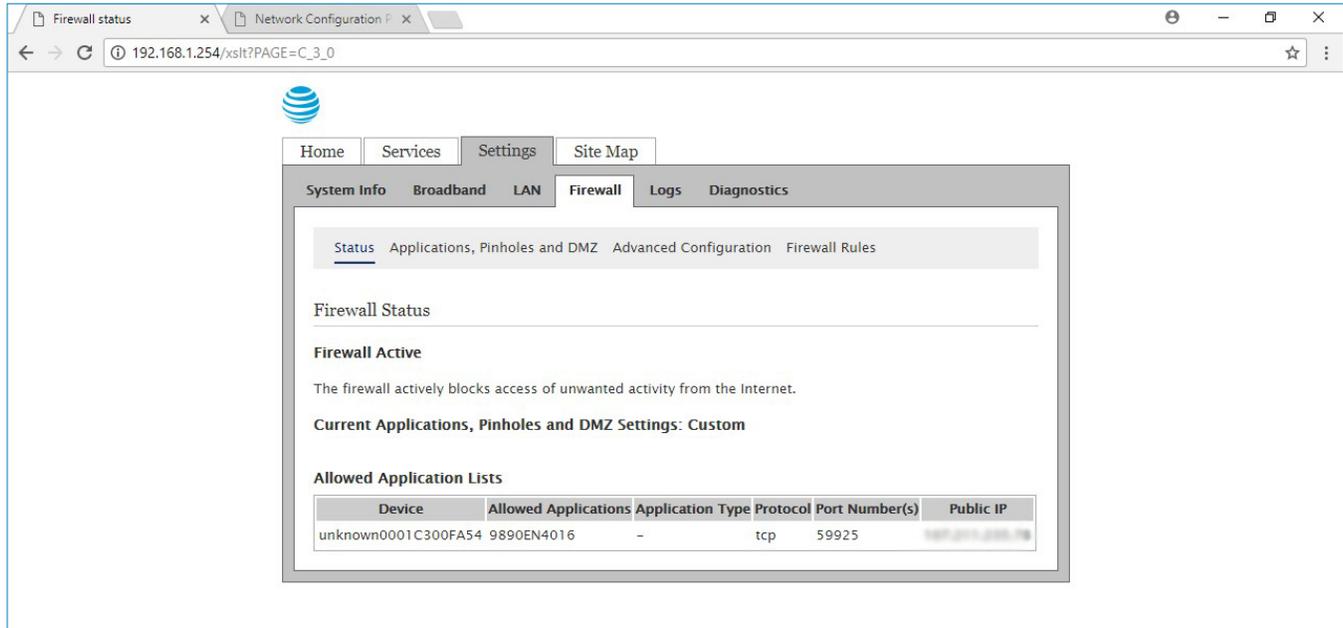


To save my changes to the router, I click the [Save] button in the lower right-hand corner and the Configuration Successful message appears at the top of the screen as shown below:





My new application is also visible under the Firewall > Status sub-menu as shown below:



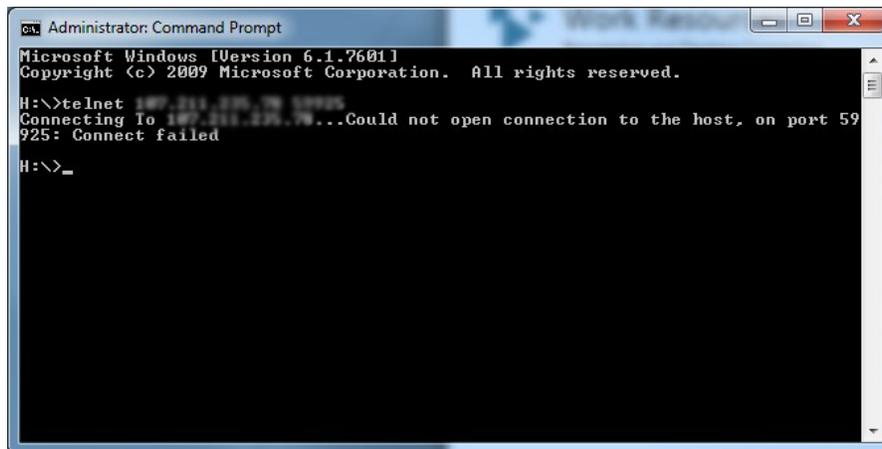
My port forward of port number 59925 will now allow me to remotely access the Home page of the Acromag 9894012 module if I type my IP address (or DDNS hostname) followed by “:59925” in a remote browser address field (http://IPaddress:59925 for my example). Note that you cannot normally access an internal server using an external IP address unless your router supports NAT loopback or reverse NAT. Most routers, including my own, do not support NAT loopback, preventing me from accessing the application from a browser of the same LAN using <http://publicIPaddress:59925>. This form is intended for remote access only--local LAN access requires that I use its private LAN IP address of 192.168.1.71 to access its embedded web Home page instead.

Of course, your router may be different than my own, but its setup of Port Forwarding will be similar. If this doesn't work for your application, your ISP is likely blocking the port. You can test if ports are open using an online port checker like that found at <http://YouGetSignal.com>. A message will appear, notifying you if your port is blocked by a firewall or ISP.

### Test to See If Your Port is OPEN

You can test your router's port forward rule using a port checker available online at [YouGetSignal.com](http://YouGetSignal.com). Here you simply specify the public IP address of your router and the port number mapped to your device's static IP address and click "Check". If your rule works, you will receive a message like Port X is open on (your IP address here).

Another useful utility to test for OPEN ports is telnet. Some computers have the telnet utility installed and you can go to your Windows® Command prompt, type "telnet publicIPaddress portnumber" and it will let you know if your port is open (at the Windows command prompt I enter "telnet 192.168.1.254 59926", see example below which indicates that my port is blocked).



Can I ping my public IP address? The application just demonstrated is a TCP application, and if you attempt to ping it from a remote location, it will not work, as the ping utility is an ICMP application. Instead, you should use Telnet from a Windows command line prompt, or a port checker like <http://YouGetSignal.com> to test your remote connection.

### Contrast Example 3 with Achieving Remote Access on a Corporate Network

For access to a device connected to a corporate network, remote access will be easier for you. Typically, you consult with your network administrator to obtain an unused static IP address that you can set inside your device. For example, Acromag leases a group of public static IP addresses for various devices/servers of our corporate network. As a demo, we have a 989EN-4012 Ethernet module like the one used in the examples of this paper already setup on 24-hour power and used for remote access via domain name 989.acromag.com. This module has a static LAN IP address of 10.1.1.162. We have added a DNS entry that connects the domain name 989.acromag.com to one of our public static IP addresses (versus using a third-party dynamic DNS service). At this IP address, a server computer is listening on default web port 80 that is connected to the 989EN-4012. Our router NAT has been preset to map remote WAN communication directed to 989.acromag.com to the internal 989EN-4012 Ethernet demo module at its LAN IP address 10.1.1.162 (versus using a port number and numeric public IP address).

Example 3 of this paper illustrated how to achieve remote access over the internet to an Ethernet device connected to a home router. Another approach to remotely access a device would be to port forward to a LAN computer and use that computer's web browser to access the network device using its LAN IP address (not recommended). Be aware that some business, professional, and enterprise versions of the Windows Operation system include built-in provisions for achieving Remote Access (Windows v7, v8, v10 Business, Professional, Enterprise, and Ultimate, but not Windows 10 Home). There is a Remote Desktop App available from the Windows Store that you can use to connect to another PC at a different location on another network under these supported operating systems, and it allows you to utilize that computer's local apps, files, and network resources just as if you were sitting in front of that computer. A description of how to use this feature is beyond the scope of this paper. It will involve the same principles of Port Forwarding illustrated in Example 3, and it will utilize registered TCP port number 3389, which Microsoft reserves for a Remote Desktop Connection or Terminal Services Client. A network client enabled for remote access will listen on this port for remote clients. The Windows Remote Access APP conveniently takes care of creating the port forward for you from a higher level so that you don't have to setup port forwarding inside your router as illustrated in Example 3 of this paper. But its use is still subject to the same operation constraints in that the port must be opened by your ISP or Network Administrator, its public IP address must be static, and the LAN IP address of the device must not change (it must be static or set to the same address by DHCP reservation). I do not recommend this method because it potentially exposes all the computer's resources, including its stored information to hackers. It is more appropriate on an enterprise level network where virus/malware and firewall protection are stronger—most useful perhaps if you need to work from home.



---

## Glossary

---

- Addressing Method : An Ethernet device's Addressing Method refers to how it obtains an IP address when it joins an IP network: It may use Static assignment inside the device or automatic DHCP (Dynamic Host Configuration Protocol) assignment upon joining the network. If not statically assigned, or dynamically assigned by DHCP, a device could specify "protocol", which grants permission to the reigning application protocol to assign it an IP address.
- DHCP refers to Dynamic Host Configuration Protocol which is one means of assigning IP addresses to network devices automatically (as opposed to static IP address assignment inside the device itself).
- DHCP server is the hardware responsible for dynamically passing out LAN IP addresses to Ethernet devices connected to a LAN network and is a service typically built into your home router. A device setup for dynamic addressing can have a different IP address every time it connects to the network, and sometimes, its IP address may change while it is still connected.
- Domain Name Server is the DNS IP Address that refers to the device used on the LAN to relate symbolic host names to actual numeric IP addresses. Note that some networks may have more than one Domain Name Server. Your ISP normally provides a DNS service to your router.
- Ethernet is the IEEE 802.3 protocol standard which defines a system of interconnecting multiple devices to form a Local Area Network (LAN) for communicating and sharing information and resources.
- Gateway Address is the IP address of the device a LAN node uses to send a packet outside of its sub-network. For example, a TCP/IP LAN could have two routers, one configured as a router to other "internal" TCP/IP network(s) and one setup as a gateway to the internet. If a subnet does not use a separate gateway and a LAN device asks for a gateway address, you can usually set it to an unused IP address within its address domain, or to the IP address of the LAN router, as gateway functionality is often integrated with router functionality in a single RG device.
- Gateway is a device used to regulate traffic between two different networks, while a Router is a device used to regulate traffic between similar networks. These terms are often used interchangeably for the same device and their message routing functions are often integrated into one device (Residential Gateway or Router/Gateway).
- Host Name is the fixed alphanumeric name assigned to a client if its numeric IP address happens to be assigned dynamically using DHCP (it's an easy to remember alias option for a complicated numeric IP assignment). ARP refers to the Address Resolution Protocol used on an Ethernet network whose purpose is to resolve the device-specific MAC addresses associated with logical IP addresses. If a network host wants to send data to another local host, it broadcasts an ARP request to the entire LAN. If the received ARP request IP address matches one in its own TCP/IP stack, a client returns an ARP reply which informs the sender of its own MAC address, which allows the sender to forward its unicast packet to its destination client.
- Host, Client, Computer, Node, Server, and LAN Device refer to any Ethernet device connected to a network, and any device that may have its own IP address.
- IANA is an acronym for Internet Assigned Numbers Authority, a non-government, internet-specific organization that assigns and allocates IP addresses to keep the numbers unique across the globe.
- IANA or Internet Assigned Numbers Authority is a governing body comprised of five Regional Internet Registries (RIR's) that administer public IP addresses to guaranty an address remains unique among billions of possible networks spanning the globe. Each regional registry is responsible for unique assignment of IP addresses to end users and other local internet registries that operate in their designated regions, and this includes your own Internet Service Provider (ISP). Your ISP or private network administrator assigns a public IP address to each router/gateway device of its network from a finite collection of public IP addresses to which it subscribes from its Regional Internet Registry.
- IP Address is a unique 32-bit ID number temporarily assigned to each Ethernet device interconnected on an IP network. It is usually expressed in dotted decimal format as 4 groups of 8-bit integers (octets) from 0 to 255, with a decimal placed between octets (for IPv4 addresses).
- IP refers to Internet Protocol and is the mechanism used on an Ethernet network to transport messages between nodes which include how they are addressed.
- Local or Private IP Addresses refer to the addresses used behind a router that LAN devices receive. Any IP address is unique on its own network, but IANA has specific private address ranges reserved for LAN use that cannot be routed on the internet.
- MAC address refers to the 48-bit MACHine address uniquely hard-coded into every Ethernet device. Routers use the IP address to locate a device, but the MAC address to specifically identify the device. In practice, you could say the IP address is used for messages sent between routers/gateways, but the IP address and MAC address is used between routers/gateways and their LAN clients. The network router will associate the fixed device MAC address with a unique and temporary IP address that it controls, either using static IP address assignment, or via a named DHCP server that automatically make this association dynamically as the device is connected to the network.



- Port Number is a 16-bit numeric designator that a router uses to associate a WAN message with a specific LAN device/server.
- Public IP Address refers to the IP address used on the internet--the address your ISP assigns to your router's WAN/internet port is a public IP address. Public IP addresses are unique globally among the billions of LAN's that connect over the internet. Public IP address space is kept separate from private IP address space and public addresses cannot be routed inside home or business network LAN's.
- Router is a hardware device used to interconnect LAN devices, and to connect different networks. It is responsible for moving packets between network clients and between networks. The terms Gateway and Router are often used interchangeably to refer to your Residential Gateway (RG).
- Static IP address is an IP address assignment that is fixed inside the device itself and doesn't change during operation. This should not be confused with addresses that act static, and instead are set by DHCP reservation in the DHCP server (which is usually integrated into the router of small networks).
- Subnet is a contiguous string of IP addresses exclusive to nodes of a group that share some common element for independent communication. Subnets are formed using a 32-bit Subnet Mask to sub-divide network IP address domains into two or more sub-networks by bit-wise AND 'ing mask bits with IP address bits, such that the leading bits of the logical result correspond to the network address (network ID corresponding to the most significant bits flagged by binary 1's in the mask). The remaining mask bits correspond to the host address space which determines how many devices may connect to the sub-network (its set bit value minus 2). Sub-netting larger networks into smaller groups allows them to more efficiently communicate independently at the same time.
- Subnet Mask is a second 32-bit number used to sub-divide the IP address into two or more network groups by a logical AND combination between each IP address and corresponding mask bit. The result discerns the network address/ID from its node address space. The leading bits of the network ID are flagged by set (1) bits in the mask, and its trailing bits are clear (0) for the node ID or host address space. The maximum value of the trailing bits minus 2 determine the largest number of devices that may connect to the sub-network identified (first/zero and last/all 1's node address numbers are always reserved).
- TCP is the Transmission Control Protocol of the transport layer of an Ethernet network that makes host-host communication possible by establishing host-client connections, imposing flow-control, synchronizing sequence numbers, segmenting large amounts of data, providing error recovery and retry, and multiplexing IP addresses to specific sockets (a socket refers to a port number combined with an IP address). TCP seeks to ensure messages are delivered and processed in the same order they are sent and uses SYNch requests & ACKnowledgement messages to establish a connection before sending data.
- TCP/IP or UDP/IP Stack refers to the complete set of networking protocols required to manage communication on a network and although only its two principal protocols are commonly indicated in its acronym, the reference to stack refers to all the protocols that are required to communicate on an Ethernet network. This stack of "software" uses the concept of groups of protocols at various layers that operate on a message that passes up/down the stack through adjacent layers with each layer doing its part for transmitting/receiving that message. Traditionally the OSI Model is said to have a seven-layer stack, while the modern Internet reference model or TCP/IP stack has four layers.
- UDP or User-Datagram Protocol is another transport layer protocol that is connectionless and does not include the error recovery mechanism of TCP and does not guaranty message delivery, but is faster with less overhead as it has little error checking and no retry mechanism.



---

## Conclusion

If you have made it through this paper, you should be able to accomplish remote access to your device from a computer of another network over the internet. While your implementation of remote access may differ from our example, particularly for different routers and different internet service providers, no matter how you achieve it, it will ultimately involve some form of port forwarding, and open ports at a static public IP address. This often requires paying for extra services and can lower your network security. Proceed with caution and be cognizant that opening ports on your router can allow unauthorized access to your device (and possibly other devices of your network). Use strong passwords and up to date malware and security software. It is a good idea to disable remote access and port forwarding in your router when you don't need to use it. Also, consider adding a VPN service with remote access. All things considered, you may be content with simply achieving local network access of your device as described in this paper.

---

## About Acromag

Acromag is a multi-million-dollar international corporation that combines more than 60 years of process monitoring and control experience with a solid background in high-tech computer design.

We are focused on developing industrial I/O solutions that provide the best long-term value in the industry. A complete line of industrial I/O products including process instruments, signal conditioning equipment, data acquisition boards, distributed I/O modules, and network communication devices are available. Industries served include manufacturing, water services, power generation, mining, defense, and transportation.

Acromag I/O is ideal for a broad range of monitoring and control operations where controllers communicate with instrumentation on the plant floor or in the field.

Author: Bruce Cyburt, Senior Design Engineer, Acromag, Inc., February 20, 2018