SYMETRIX SOLUTIONS: TECH TIP

August 2014

Controlling Symetrix SymNet, Jupiter and Integrator Series Products over the Internet

Note: *All the information below applies to the* ***AirTools Voice Processor|2x and AirTools Multiband Processor|2m*** *as well. It does not apply to Express Cobra or CobraLink*

This document describes how to control Symetrix SymNet, Jupiter and Integrator Series Products over the Internet or other wide area network (WAN) using port forwarding. It discusses the necessary ports that need to be opened to enable access to SymNet, Jupiter and Integrator Series devices. It also discusses alternative ways of control and gives some general network background information.

Quick Summary of Required Port Forwarding

If you already have a good understanding of firewalls, port forwarding, and NAT and don't want to read this entire document, refer to the table below for a quick list the ports required to be enabled for remote control of Jupiter or Integrator Series products.

Usage	Protocol/Port	Notes
ControlNet Discovery	UDP 49216	Broadcast Packet used by Connection Wizard
ControlNet Control Data	UDP 49184	Controller changes, meter data, etc.
ControlNet String Data	UDP 49344	Channel names, etc.
SymNet Designer Communications	UDP 8000	Used for routine polling of device parameters, ARC programming, etc.
FTP control stream	TCP 21*	Passive FTP mode is used
FTP data stream	dynamic	Most firewalls automatically handle the data port without an explicit rule
Remote Terminal	48630	**Not recommended unless remote troubleshooting or remote control systems are required**

** Most routers and firewalls have a built-in rule for FTP. Whenever possible, this should be used instead of a manual rule for TCP port 21*

Refer to the table below for a quick list the ports required to be enabled for remote control of SymNet Composer products.

Usage	Protocol/Port	Notes
ControlNet Discovery	UDP 49216	Broadcast Packet used by Locate Hardware
ControlNet Control Data	UDP 49184	Controller changes, meter data, etc.
ControlNet String Data	UDP 49344	Channel names, etc.
SymNet Composer Communications	UDP 49472	Used for routine polling of device parameters, ARC programming, etc.
FTP control stream	TCP 21*	Passive FTP mode is used
FTP data stream	dynamic	Most firewalls automatically handle the data port without an explicit rule
Remote Terminal	48631	**Not recommended unless remote troubleshooting or remote control systems are required**

** Most routers and firewalls have a built-in rule for FTP. Whenever possible, this should be used instead of a manual rule for TCP port 21*

6408 216th Street SW | Mountlake Terrace, WA 98043 USA

T +1.425.778.7728 **F** +1.425.778.7727 | **www.symetrix.co**

Step-by-Step Instructions

Below are step-by-step directions for enabling and using port forwarding for a Jupiter or Integrator Series device.

1. Obtain the public/external IP address of the Symetrix device using a web site such as http://www.whatismyip.com or by contacting the ISP of the site.
2. Obtain the private/internal IP address of the Symetrix device by running the Connection Wizard with an on-site computer. The PC running the wizard must be on the same LAN as the Symetrix device.
3. If the Symetrix device is using DHCP to obtain its IP address, we recommend changing to a static IP address. This will ensure that its address remains the same, which is necessary for the port forwarding rules to work properly. Alternatively, most DHCP servers can be configured to permanently assign the same IP address to a given device using “reservations”.
4. On the site’s router or firewall, set up port forwarding rules from the public IP address to the private IP address. Create the rules for all ports listed above.
5. From off-site:

   SymNet Designer- Run the Connection Wizard (SymNet Designer) to find the device. On the Device Configuration page, click the Advanced button. Enter the Symetrix device’s public IP address in the Search IP Address Base. Enter 255.255.255.255 for the Search subnet mask. Press OK.

   SymNet Composer- Open the Locate Hardware. Enter the Symetrix device’s public IP address in the Search IP Address Base. Enter 255.255.255.255 for the Search subnet mask. Click Refresh List. Select unit and press Select Hardware Unit.
6. At this point, the Connection Wizard should be able to see the remote device. If so, select it and Finish the wizard.
7. You can now go on-line with the device just as if you were connected locally.

Ports and Protocols

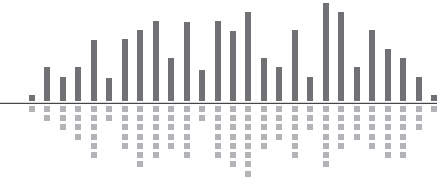
Jupiter and Integrator Series products use a variety of Ethernet ports and protocols for communication and control. All communications are Ethernet-based using the IP protocol. Both TCP/IP and UDP/IP connections are used. For a successful remote connection, all of the required ports must be available. The following sections describe each of the communication types used.

ControlNet (suite of protocols)

ControlNet is a suite of protocols designed by Symetrix for efficient low-overhead communication. It allows controlling and monitoring audio parameters and metering signals in real time. ControlNet also allows keeping string data such as channel names in sync between software applications and devices. There are 3 separate UDP-based protocols that make up the ControlNet suite: Discovery, Control Data, and String Data.

ControlNet Discovery

ControlNet Discovery is used to find or “discover” devices without knowing their IP addresses. It uses broadcast UDP packets. All connected devices respond to Discovery request and inform the requester of their name and IP address. Discovery is used in the Connection Wizard. In this case, the Connection Wizard running on the PC sends out the Discovery request, and the hardware devices respond. Discovery uses UDP port 49216 on the devices.



6408 216th Street SW | Mountlake Terrace, WA 98043 USA

T +1.425.778.7728 **F** +1.425.778.7727 | **www.symetrix.co**

SYMETRIX SOLUTIONS: TECH TIP

August 2014

ControlNet Control Data

Control Data packets are the workhorses of ControlNet. They are used to send and receive parameter changes and meter updates. When you move a fader or push a button in a Jupiter or Integrator Series GUI, the Control Data protocol makes the changes. Control Data uses UDP port 49152 on the devices.

ControlNet String Data

String Data packets are used to send text strings between devices and the GUI. They are used on the Automix Matrix 780 and other products to keep channel names, etc. in sync between the hardware and software. String Data uses UDP port 49344 on the devices.

FTP

FTP or File Transfer Protocol is a standard method used to transfer files between two devices. In the Jupiter and Integrator Series software, FTP is used primarily when transitioning between on- and off-line and upgrading firmware. For example, FTP is used to send your device file to the actual device for storage. Later, it can be retrieved from the device again using FTP. FTP uses TCP port 21 on the device for control. It also opens a second TCP port for data streaming. However, the second port is usually handled transparently by firewalls and routers.

SymNet Designer Protocol

The SymNet Designer protocol was created by Symetrix for controlling SymNet Audio Matrix devices. It allows full control over all aspects of a device. It is also used by Jupiter and Integrator Series for operations not supported by ControlNet such as saving presets, setting up external control, and programming ARC devices. This protocol also is used for routine polling of devices while on-line. The SymNet Designer protocol uses UDP port 8000 on the devices.

Remote Terminal

This protocol is typically used by AMX, Crestron, or other third party control systems. These controllers are almost always local to the device, so making them available over the Internet isn't required. However, this protocol can also be used for trouble-shooting, typically under the direction of tech support. Making this protocol available can allow this should the need arise. However, this is the least secure protocol, so caution is advised.

Port Forwarding

Port forwarding is the process of forwarding network traffic on specific ports destined for a public IP address to a private IP address. This allows certain types of traffic to be directed to the Jupiter or Integrator Series device, while other types can be sent to other equipment (for example, HTTP traffic to a web server). All the determination of which device receives each inbound network packet is based on the TCP/IP or UDP/IP destination port of the packet, hence the term "port forwarding". To control a Symetrix device, all the ports used by the Jupiter or Integrator Series software must be forwarded to the device.

The tables below show which ports need to be forwarded. There are three different versions with trade-offs between simplicity, security, and future compatibility.

Table 1: Minimal Port Forwarding, maximum security

This port list opens the fewest number of ports. This is the recommended setting for most users.

Usage	Protocol	Port
ControlNet Discovery	UDP	49216
ControlNet Control Data	UDP	49184
ControlNet String Data	UDP	49344
SymNet Communications	UDP	8000 49472
FTP	TCP	21*

6408 216th Street SW | Mountlake Terrace, WA 98043 USA

T +1.425.778.7728 **F** +1.425.778.7727 | **www.symetrix.co**

Table 2: Future-proof Port Forwarding

This port list opens additional ports that may be used in future versions of SymNet Designer devices.

Usage	Protocol	Port
ControlNet Discovery	UDP	49216-49247
ControlNet Control Data	UDP	49184-49215
ControlNet String Data	UDP	49344-49375
SymNet Designer Communications	UDP	8000
FTP	TCP	21*
Remote Terminal	UDP	48630

Table 3: Future-proof Port Forwarding

This port list opens additional ports that may be used in future versions of SymNet Composer devices.

Usage	Protocol	Port
ControlNet Discovery	UDP	49216-49247
ControlNet Control Data	UDP	49184-49215
ControlNet String Data	UDP	49344-49375
SymNet Composer Communications	UDP	49472
FTP	TCP	21*
Remote Terminal	UDP	48631

Table 4: Future-proof Port Forwarding

This port list opens additional ports that aren't needed, but requires the fewest rules, so is easiest to set-up.

Usage	Protocol	Port
ControlNet Suite	UDP	49184-49375
SymNet Communications	UDP	8000 49472
FTP	UDP	21*

** Most routers and firewalls have a built-in rule for FTP. Whenever possible, this should be used instead of a manual rule for TCP port 21*

Active vs. Passive FTP

To make an FTP connection, the server needs to know on which port to talk to.

In active FTP, which was designed before firewalls were common, client tells the server "this is the port you should talk to me on," and the server attempts to connect to that port. This is like client giving the server a phone number to call your computer at. The firewall blocks incoming calls, so you get an error when trying to open a connection because client never hears from the server.

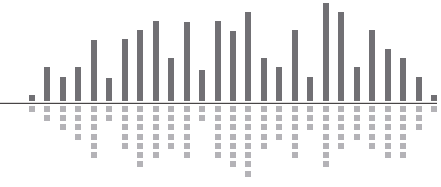
The client connects from a random unprivileged port (N > 1023) to the FTP server's command port, port 21. Then, the client starts listening to port N+1 and sends the FTP command PORT N+1 to the FTP server. The server will then connect back to the client's specified data port from its local data port, which is port 20.

From the server-side firewall's standpoint, to support active mode FTP the following communication channels need to be opened:

- FTP server's port 21 from anywhere (Client initiates connection)
- FTP server's port 21 to ports > 1023 (Server responds to client's control port)
- FTP server's port 20 to ports > 1023 (Server initiates data connection to client's data port)
- FTP server's port 20 from ports > 1023 (Client sends ACKs to server's data port)

In passive FTP, client asks the server to pick a port, and then connects to the server on that port. This is like client asking at what phone number it can call the server. Since client makes the call, the firewall allows it, and you are all set to transfer files.

The client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server. When opening an FTP connection, the client opens two random unprivileged ports locally (N > 1023 and N+1). The first port contacts the server on port 21, but instead of then issuing a PORT command and allowing the server to connect back to its data port, the client will issue the



PASV command. The result of this is that the server then opens a random unprivileged port (P > 1023) and sends P back to the client in response to the PASV command. The client then initiates the connection from port N+1 to port P on the server to transfer data.

From the server-side firewall's standpoint, to support passive mode FTP, the following communication channels need to be opened:

- FTP server's port 21 from anywhere (Client initiates connection)
- FTP server's port 21 to ports > 1023 (Server responds to client's control port)
- FTP server's ports > 1023 from anywhere (Client initiates data connection to random port specified by server)
- FTP server's ports > 1023 to remote ports > 1023 (Server sends ACKs (and data) to client's data port)

SymNet software operates in Passive Mode.

Security Considerations

By setting up port forwarding for a Symetrix device, you are making it visible on the global Internet, opening up potential security issues. However, you do have one measure of security, the so-called "security by obscurity". Unless someone else knows the IP address and listening ports of your device, it can't connect to it. This isn't foolproof, but does reduce the risk of hacking.

Another aspect of security by obscurity is that the Symetrix-specific protocols described here aren't well known. Hackers tend to concentrate on familiar protocols such as HTTP, FTP, and Telnet. Of course if you were paying attention above, you noticed that Jupiter and Integrator Series devices use FTP. This is probably the biggest security risk. The FTP connection does require a valid user-name/password combination, so this provides some protection.

To further minimize security risks, you can set up your port forwarding rules to allow only connection from a specific IP address. For example, if you always access the device from a corporate PC which has a static IP address, you can limit connection to just that (public) IP address. Keep in mind that this would prevent you from accessing the device from home, or a WiFi hotspot on the road.

Symetrix offers hardware-based security, which covers the ability to connect and control a device with the Symetrix software. This should definitely be turned on for a device visible on the Internet. However, even though this prevents connection from the Symetrix software by securing the SymNet Designer protocol, it doesn't protect other protocols such as ControlNet and Remote Terminal. In particular Remote Terminal is unsecured and has the power to do serious damage to a device.

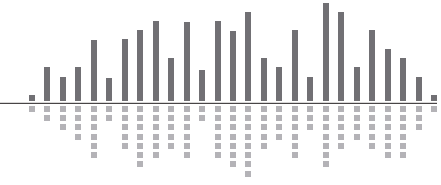
Probably the best way to ensure security is to use a VPN connection, as described below.

Testing and Trouble-shooting

After setting up port forwarding for remote access, use these guidelines to test and trouble-shoot the connection. The primary tool for testing is the Connection Wizard. Ideally there should be someone on site to make any required changes.

1. Run the Connection Wizard and try to locate your device. If it appears, ControlNet Discovery is working properly. If not, verify you are using the correct external IP address (in the Advanced dialog box) and that the port forwarding rule for Discovery is properly configured and enabled.

2. If you can discover your device, push the Flash Device button. If someone locally can verify the front panel LEDs are flashing, communications are working properly. If not, verify a port forwarding rule for UDP port 8000 to the private IP address of the Symetrix device is properly configured and enabled. If no one is available locally to visually verify the flashing LEDs, it is possible to determine if this works from the application. After pressing the Flash Device button, note how long it takes before you can click on other buttons. If control returns within 1-2 seconds, it is working. If it takes 10 seconds or more, it isn't working. Some versions of the Wizard will indicate success of the command directly with a pop-up "balloon" message.



6408 216th Street SW | Mountlake Terrace, WA 98043 USA

T +1.425.778.7728 **F** +1.425.778.7727 | **www.symetrix.co**

3. Press the Properties button. This will use FTP to read the device properties. If the Device Properties dialog comes up within a few seconds, FTP is working properly.
4. Try going on-line with the device. If the above three steps work, you should be able to go on-line. If you aren't able to, see the discussion of latency below.

Latency Issues

When controlling a SymNet, Jupiter or Integrator Series device over a local area network, packets typically travel between the PC and the device in a few milliseconds. However, over the Internet the latency is much larger, often hundreds of milliseconds. Most of the protocols used in Symetrix devices are relatively insensitive to increased latency, with the only affect being slower response to changes. However, the SymNet protocol requires a response to every command and assumes a low latency connection. If there is a problem with latency, you may find you can connect to a device initially, but it drops off-line shortly thereafter.

To fix this, there is a registry setting available to tell the software to "wait longer" before giving up on SymNet commands. The setting is called "ConnTimeout" and is located in HKEY_CURRENT_USER\Software\Symetrix\<Product Name and Version>\Connection (note that <Product Name and Version> are specific the software you are using, e.g. "ZoneMix 760 2.5". The default value is 50 (milliseconds). If you are having trouble staying on-line or know your latency is significantly longer than 50 ms, increase this value. Be sure to make all changes while the SymNet, Jupiter or Integrator Series software is not running.

To measure the latency between your PC and the Symetrix device, you can use the "ping" command from a command prompt. The command "ping <public IP addr>" will tell you the round-trip delay. We recommend using a value slightly larger than the reported maximum round-trip time.

Note that the actual bandwidth of the connection (megabits per second) is less important than the latency for the responsiveness of a remote connection. As long as the latency is low (i.e. < 30 ms), the responsiveness can be very good even with a relatively slow 1 Mbit/second connection.

Special Cases

Controlling Multiple SymNet, Jupiter or Integrator Series Devices at the Same Site

SymNet, Jupiter and Integrator Series devices don't support controlling multiple units with the same public IP address via port forwarding. It is possible to discover multiple units behind the same public address, but connecting requires a dedicated public IP address for each device. If multiple public IP addresses are used, you should set up duplicate port-forwarding rules for each device/public IP address pair. Each set of rules would map a single public IP address to a single private IP address for a Symetrix device.

Another option is to use a VPN connection, as described in **Other Control Methods.**

Site Contains an Externally Accessible FTP Server

If a site contains an FTP server accessible from the outside world, the firewall may already have a rule set-up to forward FTP traffic to the FTP server. This presents a problem in that FTP traffic from Jupiter or Integrator Series software will be sent to the FTP server instead of the device. To resolve this, you can either a) use multiple public IP addresses or b) use multiple port numbers for FTP.

In the first option, the FTP server and the Symetrix devices would each have their own public IP address. Then the firewall would have two separate rules for FTP and forward FTP traffic appropriately based on the public IP address. This is the most straight-forward solution, but may require contacting the site's ISP to arrange for the additional public IP address(es).

The second option is to change the port number used for FTP for one of the devices. FTP typically uses TCP port 21, but most FTP servers can be configured to listen on other port numbers. Jupiter and Integrator Series devices currently don't support ports other than 21 for FTP, so the change must be made to the FTP server. After this is done, FTP users will need to specify this new port number for their connection, typically done by adding ":<port>" after the URL. For example, if the previous URL for FTP was ftp.mysite.com and the new port number was 10021, the new URL would be ftp.mysite.com:10021.

6408 216th Street SW | Mountlake Terrace, WA 98043 USA

T +1.425.778.7728 **F** +1.425.778.7727 | **www.symetrix.co**

Other Control Methods

In addition to the port forwarding method described above, there are a few other options for remote control of Jupiter or Integrator Series products.

Virtual Private Network (VPN)

If you can establish a VPN connection to the remote site, you should be able to connect to and control a Jupiter or Integrator Series device without any other set-up. As long as the VPN allows the network traffic listed above (which is generally the case by default), it should work just as if you were local.

After establishing the VPN connection, run the Connection Wizard. On the "Select Network Adapter" screen, you should see an option for your VPN under Network Adapters. Select this and continue.

The main advantages of this method are simpler set-up and configuration, improved security, and ability to access multiple Symetrix devices at the same site. The main disadvantage is the overhead of creating the VPN account, and potential security risks of a site giving an outside contractor VPN access to their internal network.

Static NAT

Also called "one-to-one NAT", this method sets up a simple one-to-one mapping of a public and private IP address. Basically, any traffic destined for a particular public IP address is sent to a particular private IP address regardless of port. Using this method has the advantage of being easier to set-up since individual ports need not be configured. The disadvantage is increased security risks since all traffic will now be sent to the device. It also likely requires a dedicated static public IP address for the device, as opposed to port forwarding which allows sharing a public IP address with other equipment on site.

Remote Control of a Local PC

An entirely different approach is to maintain a PC on site with the SymNet, Jupiter or Integrator Series device and then simply access and control that PC remotely (aka remote desktop). This reduces the problem to establishing a remote control connection, which is a very common task. This method is outside the scope of this discussion. But in brief, there are a variety of methods for establishing remote connections including web-based tools such as LogMeIn.com, GoToMyPC.com, the built-in Windows Remote Desktop, free tools such as VNC, and commercial products such as PC Anywhere. Some web conferencing solutions also include remote control features.

An obvious disadvantage of this method is that a PC must be accessible on site. If it is not feasible to dedicate a PC for this purpose, it may be possible to pre-arrange this for specific incidents.

Appendix A: Private (Internal) vs. Public (External) IP addresses

Each computer running on a local area network will have a unique IP address. This consists of 4 numbers between 0-255 separated by dots, e.g. 192.168.100.1. In addition, other Ethernet devices such as routers, printers, servers, and Symetrix hardware also have IP addresses. This is the private IP address, also sometimes referred to as the internal IP address. It is the address on the local area network. However, often many or all computers on a LAN share the same connection to the internet. Therefore, to the outside world, all the computers on the LAN may appear to have the same IP address. This is their public IP address, also sometimes referred to as the external IP address.

To determine your private IP address, open a command prompt (Start->Run, then type cmd and hit OK.). Then type IPCONFIG. Alternatively, in Windows XP, go to Start->Settings->Network Connections. Double-click on Local Area Connection and click the Support tab. The private IP address usually begins with 192.168, 172.16-31, or 10.

6408 216th Street SW | Mountlake Terrace, WA 98043 USA

T +1.425.778.7728 **F** +1.425.778.7727 | **www.symetrix.co**

An easy way to determine your public IP address is to use a web site such as http://www.whatismyip.com. You will most likely find that the private and public IP addresses differ. A public IP address will never begin with 192.168, 172.16-31, 169.254, or 10.

When connecting to a device over the internet, you will need to use its public IP address for all communications. A properly configured router or firewall will then forward the data to the appropriate private IP address. This port mapping is typically done via a web browser interface to the router. The specific settings differ by router, so consult the router documentation.

Appendix B: More on Ports - Source vs. Destination and UDP vs. TCP

This section provides a little more background information on the topic of ports in IP communications.

Source Port vs. Destination Port

In the above discussion, we've only discussed a single port value. In reality, every packet contains two different port numbers, a source port and a destination port. Just as a packet is sent from a source IP address to a destination IP address, it is also sent from a source port number to a destination port number. All the ports listed in the tables above are the destination ports for communications flowing from the software to the Symetrix device. Keep in mind that when the device responds, the source and destination ports are reversed, just as the source and destination IP addresses are reversed.

We have discussed only destination ports since typically that is all that is required when setting up firewall/router rules. Generally the firewall/router doesn't care what is source port is for inbound traffic, it is just looking for a specific destination port in order to decide what to do with the packet.

UDP vs. TCP

UDP stands for User Datagram Protocol and TCP stands for Transport Control Protocol. They are both protocols that sit above IP (Internet Protocol), so either can be routed over the Internet.

Because of this, you may sometimes see them referred to as UDP/IP and TCP/IP, making it more explicit that they are based on IP. UDP is a simpler, lower overhead protocol that can send "one off" messages. In contrast, TCP is a more complicated protocol that first establishes a connection, and then sends data, maintaining the connection until it is no longer needed. One is not better or worse than the other, they are just different tools for different jobs. Integrator Series devices use a combination of UDP and TCP communications, as do many other applications.

Both UDP and TCP use a port numbers in the range of 0-65535. But these port numbers are completely separate between UDP and TCP, which can be a point of confusion. The key point for Integrator Series application is to make sure you select UDP or TCP as indicated when setting up firewall/router rules. If you get this wrong, it won't work! Everything is IDP except for FTP, which uses TCP. As mentioned above, firewall/routers often have pre-defined rules specifically for FTP since this is such a common protocol. In this case, a pre-defined rule should always be used instead of a manual rule for TCP port 21.

References for Further Reading

http://en.wikipedia.org/wiki/Port_forwarding

http://en.wikipedia.org/wiki/Network_address_translation

http://www.tcpipguide.com/

6408 216th Street SW | Mountlake Terrace, WA 98043 USA

T +1.425.778.7728 **F** +1.425.778.7727 | **www.symetrix.co**