# Using Rumpus On Private Networks

Contents

Many networks are connected to the Internet using a single IP address, even though the network might link many computers. This is done to reduce connectivity costs and as an effective security measure, but it does present special problems when you are first setting up an FTP server.

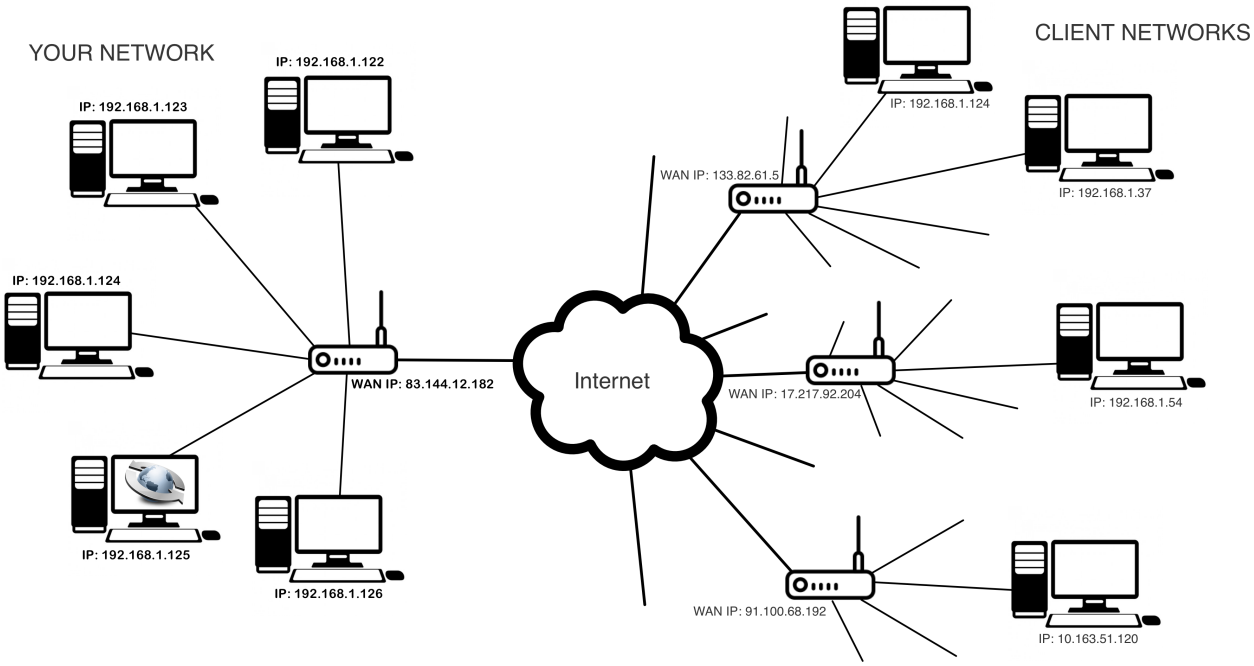
Networks configured this way typically use IP addresses that begin "192.168." on each local computer, although addresses that begin “172.16.” or “10.” can also be used. Addresses in this range are reserved for private (not directly Internet connected) use, and are not routable across the Internet. In other words, if the computers on your network have TCP/IP addresses that begin "192.168." (or “172.16.” or “10.”), then those addresses can be used only for local connections. No one on the Internet will be able to connect directly to any computer on your LAN.

Fortunately, it is still possible to run an FTP server and make it accessible to the outside Internet, using a common feature available in most routers called "Port Forwarding".

## How Port Forwarding Works

On a private network that is bridged to the Internet using a single “real” IP address, that address is assigned by your ISP to your router. Since that is the only Internet accessible address assigned to your LAN, that’s the address outside clients will use to connect.

Consider the following diagram, which represents a simplistic but helpful view of how the Internet is organized.



In the diagram, your network is on the left, while 4 clients who wish to connect to your server are shown on the right. Your Rumpus server is one of the computers on your network.

Notice that the computers on your network all have local IP addresses in the "192.168.1." range, and client networks have local clients assigned addresses in the same range. Local addresses in the assigned "LAN address ranges" are used on millions of networks across the Internet, which is why these addresses work just fine on your LAN, but can't possibly be routed across the Internet.

Clients on external networks can actually only connect to your router, in the example above represented by the Internet-routable address "83.144.12.182". This is an important point... Outside clients can not connect to your Rumpus server on the LAN-only address "192.168.1.125", but can connect to the router at "83.144.12.182".

So how do you get outside clients connected to the Rumpus server? The purpose of port forwarding is to tell your router, "When you receive a connection from an outside client, connect them to the local server running on '192.168.1.125'."

## Configuring Your Router

Specific setup procedures will vary depending on the router, so the following instructions are fairly general. If you have detailed questions about configuring port forwarding on your router, contact the router manufacturer.

Open the router setup software, or setup URL if your router is configured by Web browser. Go to the "Port Forwarding" setup area. This is also sometimes called "Virtual Servers", “Pinholes”, "Port Mapping", "Inbound Port Mapping" or "Relays". Here, you can specify the needed connection mappings for individual ports.

The necessary ports will depend on your Rumpus settings. Open the "Get Connected" window in Rumpus (on a Windows server, click the "Get Connected" button, on a Mac server, choose "Get Connected" from the "Help" menu) and flip the the "From Outside Your LAN tab. There, Rumpus will list the required ports for each service you have enabled.

It is usually best to start with Web (HTTP) access, by default on port 80. Rather than worry about the entire list, get port forwarding configured for that port first, test it from outside your network, and get clients connected via Web browser. Once you've gotten that working, it should be relatively easy to complete the same procedure for the other needed ports.

Of course, security restrictions on the required ports put in place on the router or on an external firewall need to be lifted as well.

## Rumpus Setup

The last step is to tell Rumpus what the router's "real" IP address is. In Rumpus, open the Network Settings window and select the “Basics” tab. Enter the IP address of the router into the "External Network IP Address" field.

Next, open the FTP Settings window and flip to the “Basics” tab. The "Allow Router To Perform Data Connection Address Mappings" will need to be set correctly for your router. Start with the option enabled, and have an outside user attempt to connect via FTP to your server. If outside FTP clients are unable to transfer files, try disabling the the option.

## On Networks With A Dynamic IP Address

When possible it is best to supply an IP address, not a domain name, in the "External Network IP Address" field, because Rumpus must provide an address, not a name, when telling clients to establish passive connections. However, you may supply a domain name that maps to the address if you wish. This allows you to use Rumpus even when your Rumpus network address is dynamic. If the network address assigned to the server can change, and your ISP updates the domain name so that it always points to the correct address, then enter the domain name instead of the address. Each time it is needed, Rumpus will look up the address by the domain name, allowing FTP services to continue working even after your dynamic IP address is reset.

## Testing And Troubleshooting Your Server

After setting up Rumpus and your router, have someone outside your network use an FTP client to connect to your server. We strongly recommend that you test FTP with a dedicated FTP client as well as the Web File Manager using a standard Web browser. An FTP client will provide you with much better diagnostic information and various connection options not available in Web browsers.

If users are able to make a connection (in the FTP client, open the "Transcript Window" and watch for connection activity) but can't get directory listings or transfer files, you are halfway there. Port 21 is correctly forwarded and Rumpus is accepting connections, but data connections can't be established. Most FTP clients allow you to choose between "Active Mode" and "Passive Mode" connections. Try both to see where the problem lies. In Fetch, for example, the option is called "Use passive mode transfers" and is on the "Firewalls" tab of the main Preferences window.

If "Active Mode" connections don't work, check your router and firewall, and have the client do the same. In this case, the server is unable to open a connection with the client on port 20, the defined FTP data port. Many client networks will have firewalls that block incoming connections on this port (and many others), so Active Mode connections may not be possible. Most clients, including Web browsers, therefore default to Passive Mode connections.

If "Passive Mode" connections don't work, then the problem is either your port forwarding setup for ports 3000 through 3008 (the upper bound may be different, as described above) or there is a firewall that is denying connections from the client to the server on these ports. Check your router's port forwarding setup for this port range, make sure that the maximum number of simultaneous users is set in Rumpus so that the forwarded range is correct, and check to make sure there isn't another firewall or router on your network blocking these ports. Also, have your client ask their network administrator or ISP if their network is restricted from making connections to these ports.

If you are still having problems, send an e-mail to "support@maxum.com". Please send the address of your server (or rather, of the router that forwards to your server) and a sample username and password. Maxum Technical Support staff will be happy to attempt to connect to your server, and check to see if it is accessible from the Internet.