How Your Computer Accesses the Internet through your Wi-Fi for Boats Router

By default, a router blocks any inbound traffic from the Internet to your computers except for replies to your outbound traffic. This section explains how a normal outbound connection works.

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing source and destination address and process information. Before forwarding your message to the remote computer, your router must modify the source information and must create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open Internet Explorer, beginning a browser session on your computer. Invisible to you, your operating system assigns a service number (port number) to every communication process running on your computer. In this example, let's say Windows assigns port number 5678 to this browser session.

2. You ask your browser to get a Web page from the Web server at www.example.com. and your computer composes a Web page request message with the following address and port information:

    - The source address is your computer's IP address.
    - The source port number is 5678, the browser session.
    - The destination address is the IP address of www.example.com, which your computer finds by asking a DNS server.
    - The destination port number is 80, the standard port number for a Web server process.
    - Your computer then sends this request message to your router.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the Web server at www.example.com.

4. Before sending the Web page request message to www.example.com, your router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):

    - The source address is replaced with your router's public IP address. This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.

- The source port number is changed to a number chosen by the router, such as 33333. This is necessary because two computers could independently be using the same session number.
- Your router then sends this request message through the Internet to the Web server at www.example.com.

5. The Web server at www.example.com composes a return message with the requested Web page data. The return message contains the following address and port information:

   - The source address is the IP address of www.example.com.
   - The source port number is 80, the standard port number for a Web server process.
   - The destination address is the public IP address of your router.
   - The destination port number is 33333.
   - The Web server then sends this reply message to your router.

6. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message, restoring the original address information replaced by NAT. The message now contains the following address and port information:

   - The source address is the IP address of www.example.com.
   - The source port number is 80, the standard port number for a Web server process.
   - The destination address is your computer's IP address.
   - The destination port number is 5678, the browser session that made the initial request.
7. Your router then sends this reply message to your computer, which displays the Web page from www.example.com.

8. When you finish your browser session, your router eventually senses a period of inactivity in the communications. Your router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

Allowing inbound traffic to local computers behind your router.

In the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. However, you might need to create exceptions to this rule for the following purposes:

- To allow remote computers on the Internet to access a server on your local network.
- To allow certain applications and games to work correctly when their replies are not recognized by your router.

Routers provide two features for creating these exceptions: *Port Forwarding* and *Port Triggering*.

Port Forwarding

Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature. A typical application of port forwarding can be shown by reversing the client-server relationship from our previous Web server example.

In this case, a remote computer's browser needs to access a Web server running on a computer in your local network. Using port forwarding, you can tell the router, "When you receive incoming traffic on port 80 (the standard port number for a Web server process), forward it to the local computer at 192.168.1.123."

The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens Internet Explorer and requests a Web page from www.example.com, which resolves to the public IP address of your router. The remote computer composes a Web page request message with the following destination information:

    - The destination address is the IP address of www.example.com, which is the address of your router.
    - The destination port number is 80, the standard port number for a Web server process.
    - The remote computer then sends this request message through the Internet to your router.

2. Your router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123.

    - Your router modifies the destination information in the request message.
    - The destination address is replaced with 192.168.1.123.
    - Your router then sends this request message to your local network.

3. Your Web server at 192.168.1.123 receives the request and composes a return message with the requested Web page data. Your Web server then sends this reply message to your router.

4. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the Web page from www.example.com.

5. To configure port forwarding, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or user groups or newsgroups.

Port Triggering

In the preceding example, requests are sent to a remote computer by your router from a particular service port number, and replies from the remote computer to your router are directed to that port number. If the remote server sends a reply back to a different port number, your router will not recognize it and will discard it. However, some application servers (such as FTP and IRC servers) send replies back to multiple port numbers. Using the port triggering function of your router, you can tell the router to open additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the router, "When you initiate a session with destination port 6667, you must also allow incoming traffic on port 113 to reach the originating computer."

Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program, beginning a chat session on your computer.

2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server.

4. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.

5. Noting your port triggering rule, and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.

6. The IRC server sends a return message to your router using the NAT-assigned source port (as in the previous example, let's say port 33333) as the destination

port. The IRC server also sends an “identify” message to your router with destination port 113.

7. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.

8. Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is an active session for port 113, associated with your computer. The router replaces the message’s destination IP address with your computer’s IP address and forwards the message to your computer.

9. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application, or user groups or newsgroups.