

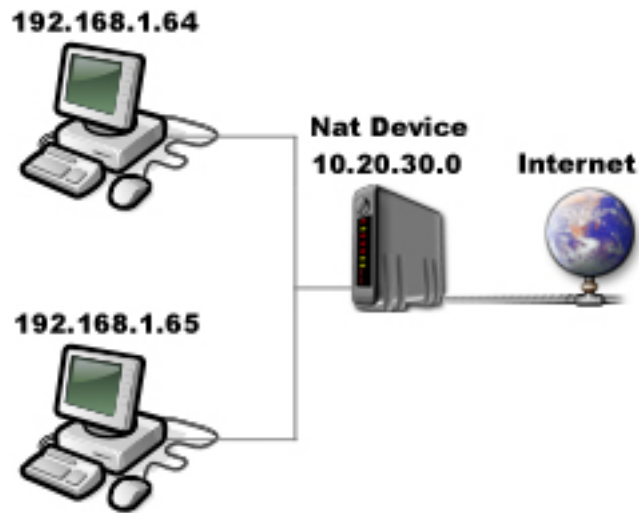
NAT problems and UPNP

by SuperBonBon

1. NAT

NAT (Network Address Translation) is becoming widely used with the lack of IP addresses and the increase of broadband ADSL modem use on the internet. Unfortunately NAT is a recurrent problem with FTP servers and often breaks the server usability. The result is that unless you configure your NAT device yourself, you'll have no chance to make your FTP server work correctly.

Here is a typical network scheme with a NAT ADSL router:



Network schema

2. Problem with NAT and FTP ?

The only problem with NAT is that you cannot receive incoming connections on your server as long as your device is not configured correctly.

There is two methods to start a data transfer (for directory listing and file transfer) between

an FTP client and server:

- **PORT** : Port command is issued by the client and instructs the server where (which port) it will need to connect to initiate the file data transfer.
- **PASV** : Pasv command is the opposite of **PORT**, it instructs the client where (what port) the server will allow the client to connect to initiate the file data transfert.

The problem is that the **PASV** mode cannot work if the server is using an unconfigured NAT device and the **PORT** mode cannot work if the client is using a NAT device that blocks all incoming ports. Now imagine the following network scenario :

We have one client and one FTP server, each one behind an unconfigured NAT device, assuming that only the server listening port is configured on the server's network NAT device (otherwise the client won't even be able to connect ...):



Network schema

- **PASV scenario :**

The client issues a **PASV** command, the server response instructs the client that it can connect to port 14536

```
Client Command : PASV
Server Response : 227 Entering Passive Mode (10,20,30,40,57,1).
```

When the client tries to connect to the address provided by the server, the connection will fail since the NAT device on the server side is not configured to forward data for port 14536 on the local network for the host IP 192.168.1.65

NAT problems and UPNP

The result is that the FTP server is unusable since the connection cannot be established. The usual reaction from the end user is to use the PORT command, let's take a look.

- PORT scenario :

The client issues a PORT command to instruct the server that it can connect to 14536 port on the FTP client machine for the data transfert.

```
Client Command : PORT 50,60,70,80,57,1
Server Response : 200 PORT command successful.
```

When the client will try to start a file transfert the server will try to establish the data connection, which will fail since the NAT device on the client side is not configured to forward data for port 14536 on local network for the host IP 192.168.2.34

The final result : no connection can be established, as long as at least one NAT device is correctly configured to forward data on a certain port of a certain host on the internal network. Usually the client will never configure its NAT device.

The only solution is to correctly configure the NAT device on the server network, most of the time the server administrator (simple home user) is not even aware of this problem. Also, the manual configuration of a NAT device is painful :

- Change your server IP address ? Don't forget to change the mapping in your NAT device !
- Change your server port ? Yet another reconfiguration of the device.
- Finally, don't do any configuration error or nothing will work, since testing PASV mode from your local network is usually impossible.

3. Another problem with NAT

Networks using a NAT device use an external IP address for internet access as you can see it on the first and second schema.

The main problem with this is that sometimes the server will not (or is not configured to) detect the external IP address and will use the internal IP in its PASV response.

```
Client Command : PASV
Server Response : 227 Entering Passive Mode (192,168,1,65,57,1).
```

You just guessed the answer, the server will not work in pasv mode, since the client will try to connect to the server's internal network IP.

The same story occurs on the other side when the client will send its internal IP address in a

PORT command :

```
Client Command : PORT 192,168,2,34,57,1
Server Response : 200 PORT command successful.
```

Same result, it's impossible to connect the hosts for the data transfer.

4. NAT problem solution

JAFS is the first to provide an UPNP (Universal Plug And Play) feature on the Java platform to send remote orders to your UPNP enabled modem so that the NAT port mapping is done automatically, no need to bother with NAT configurations, everything is handled automatically and you can make sure that your server will be effectively **available from the internet**.

JAFS checks the mapping status each xx mins (user defined setting), you can stop your device and restart it, the mapping will be redone automatically, and your server will be available again, no need to restart it.

To enable UPNP you will need:

- A UPNP enabled device (most of the new ADSL router modems have UPNP support)
- The device must implement the UPNP *InternetGatewayDevice WANIPConnection* service specification. Setup JAFS to support UPNP, start it and you will be told if your device supports it or not.
- Make sure that the UPNP support is switched on, since some NAT device vendors factory settings are default to off. Check your UPNP device manual for more informations to switch on UPNP.

Finally you'll need to add a [NAT mapper](#) UPNP driver to your desired network interface. The driver class name to [specify](#) is `net.sbbi.jafs.nat.UPNPNatPortsMapper`. Here is a small XML config example with UPNP NAT driver enabled:

```
<jafs-service xmlns="http://www.sbbi.net/jafs/1.0/jafs-service" ... >
  <network-interfaces>
    <network-interface id="default" name="eth0" fw-host-name="www.mycompany.com">
      <fw-nat-ports-mapper class-name="net.sbbi.jafs.nat.UPNPNatPortsMapper"
        mappings-monitoring-time="10"/>
    </network-interface>
    ...
  </network-interfaces>
  ...
</jafs-service>
```

NAT problems and UPNP

You can find more informations about network interfaces and nat mappers configuration [here](#).

The problem with the PORT command on the client side still remains, JAFS cannot do anything about this, but UPNP support for FTP clients is starting to appear (the first UPNP enabled FTP client has been released in 2003). Such support will fix this remaining problem.

5. External IP address problem solution

For this problem there is no real easy solution, you'll need to configure JAFS correctly. The [fw-host-name](#) network interface service configuration parameter is **very** important since it will be returned by PASV commands. If you have no firewall, the [host-name](#) will be used to return the IP in PASV commands.

Warning:

Setting a value such as "localhost" will cause functional problems from the internet since IP 127.0.0.1 will be returned by a PASV command.

If you plan to allow internet access to your server set a value with a correct host name (such as [www.mycompany.com](#)) that will return a correct external IP address.

For the client side problem, JAFS detects if an internal IP address (PORT 192,168,1,33,57,1, PORT 127,0,0,1,57,1 ...) of the FTP client's network is used in the PORT command and rejects it if such a scheme occurs.