NAT (Network Address Translation)

Technology Primer v1.1c

. Why do I need NAT?
. How does NAT work?
. Our NAT with Built-in Application Router Layers
. When NAT needs Virtual Servers!
. UPnP makes everything NATural!
. To Get Going

Introduction : The Internet & NAT

The Internet has grown faster and larger than anyone could have imagined! It is increasingly a requirement for small businesses and homes to connect to the Internet. The explosive growth of the Internet, along with security and administrative requirements, has spurred the increasing use of Network Address Translation, or NAT in short.

NAT is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address. This allows home users and small businesses to connect their network to the Internet cheaply and efficiently.

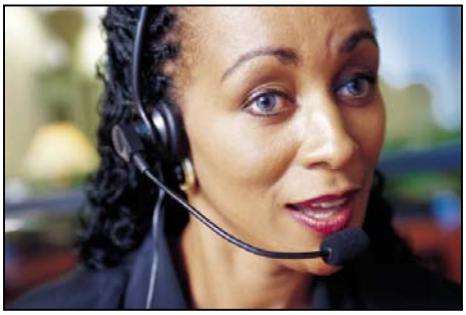
Why do I need NAT?

For a computer to communicate with other computers on the Internet, it must have an IP address (IP stands for Internet Protocol). An IP address is a unique 32-bit number that identifies the location of your computer on the network and it functions like your postal address to provide a means so that mails and parcels can be delivered to you.

The current scheme of IP addressing (IPv4) provides a theoretical maximum of 4,294,967,296 unique addresses (2^{32}), and everyone had thought it to be plentiful to meet any need. Yet, its scarcity is increasingly apparent with the unprecedented growth of the Internet and home, campus and business networks. The solution, which is a complete overhaul of the present IP addressing scheme to IPv6, will take years to materialize. Therefore, the world has to tackle a very real and imminent problem in the mean time, and this is where NAT comes into the picture.

Network Address Translation lets a single, unique IP address, represent a group of computers in a private (or local) network to the Internet (or public network). This takes place by means of a gateway device, like a router, that manages any information transaction between the two networks.

Another key reason for using NAT is the added security inherent in its implementation. By nature of its working, Network Address Translation ensures that a computer on an external network cannot connect to your computer unless your computer has initiated the contact.



We can think of NAT with the example of the receptionist in a large office. Given instructions by you not to forward any calls to you unless you request it, you would give to your clients the office's main number of the receptionist. Hence, each time you expect a call from a potential client, you would tell the receptionist to put her through.

When that client calls the main number and tells the receptionist that she is looking for you, the receptionist would then lookup the telephone directory for your name and the extension where she may forward the caller. In like manner, NAT functions as a simple and convenient means to sieve out unsolicited connections and requests from the public network. The computers within the private network thus remain "invisible" from the Internet and cannot be directly accessed. Thus, this is why NAT becomes spoken of as a firewall.

How does NAT work?

Network Address Translation works in several ways but we shall discuss Dynamic NAT with Port Address Translation, sometimes also referred to as NAPT – Network Address Port Translation. The basic purpose of NAT is to multiplex traffic from the internal network and present it to the Internet as if it was coming from a single computer having only one IP address. Using Dynamic NAT with Port Address Translation, each computer on the private network is translated by the gateway device to the same IP address, but with a different port number assignment as illustrated in Figure 1:

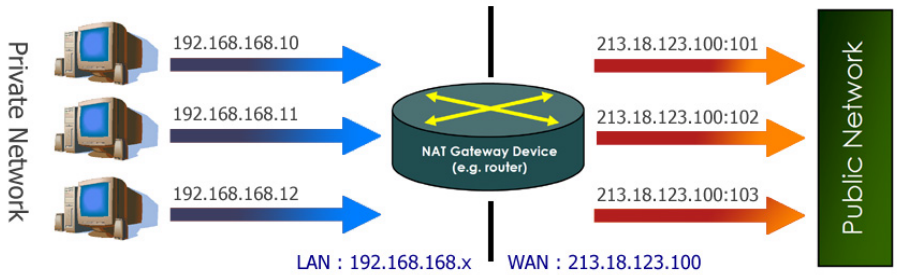


Figure 1 : Network Address Translation

In an everyday situation when you operate the PC at your work desk for regular web-surfing, your computer (the client) on the internal network contacts another computer on the Internet by sending out IP packets destined for that machine (the host). Each IP packet sent from your computer would be labeled with a header containing the source and destination addresses and unique port numbers so as to get these packets to their destination:

Source Address	Source Port	Destination Address	Destination Port

This combination of numbers completely defines a single TCP/IP connection. The addresses specify your PC and the web server at each end, and the two port numbers ensure that each connection between the two computers can be uniquely identified.

The Delicate Art Performed

The NAT device (e.g. NMCBR140) sitting as your router device would change the Source address on every outgoing packet to the one public address given by your Internet Service Provider (ISP). By using a port mapping table, your NAT router device dynamically remembers and keeps track of how it renumbered the Source ports for the client's outgoing packets, which therefore relates the client's real local information (i.e. the local IP address, source port and its translated source port number, destination address and destination port).

Subsequently, when the reply packets come back, the NAT router device is able to reverse the process and route them back to the correct clients. It would be interesting to note that when a web server on the Internet responds to a client computer within the private network, the packets arriving at the NAT router will all have the same Destination Address, but its Destination Port number would be the Source Port number previously assigned by the NAT.

The NAT router device looks in its port mapping table to determine which "real" client address and port number a packet is destined for, and replaces these numbers before passing the packet on to the local client. This ensures that your computer will know how to relate pieces of disparate information back to the correct connection.

Because the port mapping table relates complete connection information - source and destination address and port numbers - it is possible to validate any or all of this information before

passing incoming packets back to the client. This checking helps to provide effective firewall protection against Internet-launched attacks on the private network.

With this method, each computer can also have multiple connections opened concurrently – which is an everyday scenario whenever you visit multiple web pages through several browser windows at the same time. Despite the large number of connections that may originate from many local computers or multiple browsers in one computer, it would appear from the web server's point of view that the packets arrived from the NAT router.

These steps are carried out transparently such that neither your computer on the private network nor the Internet host is aware of them – certainly a beauty of the NAT magic.

Our NAT with built-in Application Router Layers

The NAT router devices have built-in application gateway layers that will transparently handle unique applications like your FTP client, mIRC, Net2Phone, IPSec and PPTP packets – allowing you to enjoy hassle-free operation of these applications within the private network.

Even when several PCs within the private network initiate sessions with external parties, the NAT router intelligently manages the unique data packets from these supported client applications, and it will remember the correct initiator to return their designated packets. Hence, with our engineers working hard behind the scenes to make sure your favourite applications function without a hitch, you free yourself to address other pertinent issues at your work.

When NAT needs Virtual Servers!

Up till now, we have got you up to speed on how connections and requests initiated from within your private network are handled. In specific circumstances when you are required to build a web-server within your private network, so that computers from elsewhere on the Internet may have access, you will then need to let them initiate connections. How do we accomplish this easily? This is when the Virtual Servers (based on Port and IP Forwarding and De-Militarized Zone) feature in the router (eg. NMCBR140) comes in useful.

Virtual Servers based on Port Forwarding

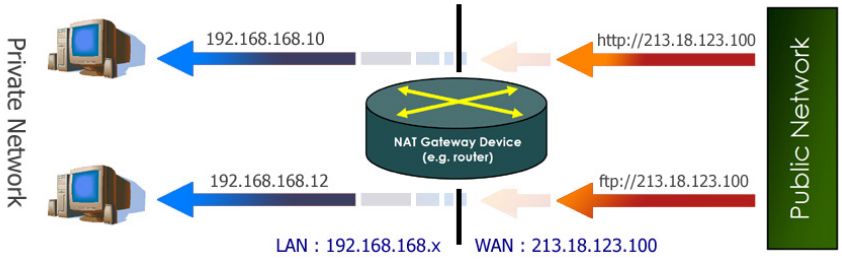


Figure 2 : Virtual Server based on Port Forwarding

By accessing the intuitive configuration menu on the router devices to set up Port Forwarding, you will be able to deploy an Internet web-server or a FTP (File Transfer Protocol) server within your private network. For the example illustrated in Figure 2, knowing the TCP port of your intended application (HTTP web-servers use TCP Port 80 by default) and your ISP assigned IP address, we can define a Virtual Server at Port 80, to be forwarded to 192.168.168.10. Once implemented, all "http://213.18.123.100" requests will be forwarded to the computer with 192.168.168.10 IP address. If you wish to host another FTP server in your private network on a computer with an IP address of 192.168.168.12; you will then need to define a Virtual Server at TCP Port 21 (used by FTP by default) to be forwarded to 192.168.168.12.

Virtual Servers based on IP Forwarding ***exclusive!***

"I understand that most NAT router products only support Port-forwarding, what if I have subscribed to a range of IP addresses from the ISP, how else can I set up such servers within my private network?" In this case, you cannot buy just any ordinary product, but you will NEED a product like NMCBR140 that supports IP forwarding! Exclusive to Netmax, the router will forward all Internet requests as you defined the Virtual Server based on IP forwarding, regardless of the application's TCP port, to a mapped host on the private network.

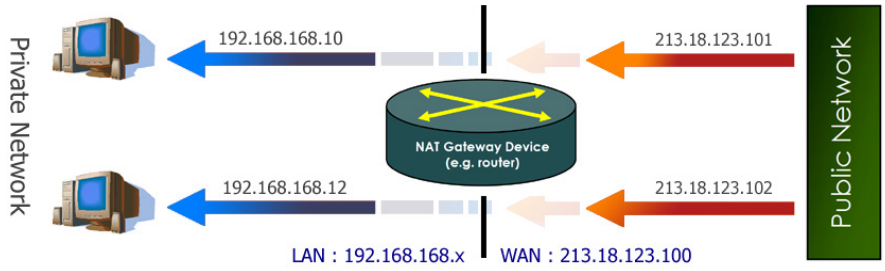


Figure 3 : Virtual Server based on IP Forwarding

As illustrated above in Figure 3, assuming you subscribed to the range of IP addresses from 213.18.123.100 to 213.18.123.102, the following can be configured: while 213.18.123.100 is assigned to your NAT gateway device, you may choose to map the public IP 213.18.123.101 to the private IP 192.168.168.10, and another from 213.18.123.102 to 192.168.168.12.

Virtual Servers based on De-Militarized Zone (DMZ)

The last of these interesting implementations of Virtual Servers is the De-Militarized Zone, or DMZ in short. Without having to set (or know) the application's port, you may let the router direct all unresolved Internet requests to a particular computer assigned a specific IP address – known as the DMZ host.

This final set up puts the computer "outside" of the NAT firewall and provides transparent, unrestricted access to it, making it suitable for applications-testing purposes, etc.

An NAT router device such as the user-friendly NMCBR140, with its support of Virtual Servers (IP and Port Forwarding, DMZ), makes it a comprehensive and indispensable network management product. It makes possible the set up of secure private networks, but yet allows selected applications to be initiated from within.

UPnP makes everything NATural!

Still, with computer networks pervading campuses, small offices and especially the homes, the presence of NAT simply "breaks" many compelling new home PC networking experiences. Applications such as multi-player games, real-time communications, and other peer-to-peer services, that people increasingly want to use, run into hiccups when they use private address on the Internet, or attempt simultaneous use of the same port number.

Application routers like those built into the routers provide means for existing programs with known ports to pass through the NAT. As the list of programs with specific port requirement expands, frequent firmware updates do not appear to be a viable long-term solution. Also, the manual configuration of a NAT gateway device requires the user to know the port in which a particular application uses – which amounts to fair efforts for proper administration. Therefore, the router supports Universal Plug and Play (UPnP) so that our customers can enjoy the benefits of NAT without having to worry about elaborate configuration procedures.

More than Virtual Servers, Universal Plug and Play (UPnP) was conceived as the architecture for pervasive peer-to-peer network connectivity of PCs and intelligent devices or appliances, particularly within the home. With UPnP, devices announce their presence and capabilities on a network. In the PC realm, this allows UPnP-enabled devices to recognize each other, communicate with each other, negotiate ports, and allow UPnP applications to work transparently with no configuration needed.

Transversing the NAT-transversal problem

Choosing a UPnP-enabled NAT gateway device, like the NMCBR140, will ensure a painless network setup for multi-player gaming, peer-to-peer connections, and real time communications. UPnP-enabled applications can automatically manage the router within operating systems like Microsoft Windows ME/XP that features Universal Plug and Play.

Your UPnP-enabled router will be automatically recognized through its Ethernet connection when attached to your Windows XP machine. It will work in conjunction with Windows so that when a UPnP application like Microsoft Messenger runs, any ports required by the software can be released and the negotiations handled cleanly and automatically through the NAT router device (also referred to as IGD, short for Internet Gateway Device).

For example, when a video/audio communication is started in Microsoft Windows Messenger, it will open a UDP port (audio) or a TCP port (video) dynamically as it requires. The application would use UPnP to change the NAT Port Forwarding (Virtual Server) parameters automatically so that the

connections may transverse the NAT. Without you noticing, UPnP enables the automatic learning of public IP address, enumeration of existing port mappings, the addition/removal of port mappings and assignment of lease times to mappings on the IGD.

All these takes place so that your favourite UPnP-enabled programs continue to work across the fortified firewall settings. You will discover that your UPnP-aware instant messaging software is now able to painlessly establish file transfers, hook you up on a voice chat or even conduct a video-conference across the company's network firewall! Most of all, *gasps* multiplayer gaming can be allowed to transcend local network boundaries!

A well-conceived approach to link up your private network to the Internet will ensure a seamless yet secure platform whereby business transactions may take place. It will shield confidential and private data from malicious hackers, but still enable unrestricted day-to-day data communications for your network.

To sum up, with an NAT gateway device like NMCBR140 set up and running, you can have a peace of mind enjoying its efficient and transparent operation between the private network and the Internet.

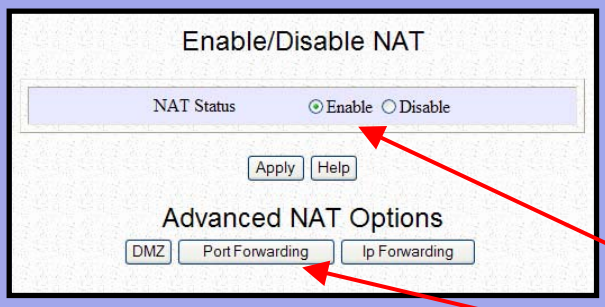
To Get Going

Now that we have a good overview of the technologies that gives us a more fruitful computing experience, let us take a peek at how a few easy steps can bring us a long way to make these technologies work for us. Check out the walkthrough guides below:

Example 1: Enabling NAT with Virtual Server (Port Forwarding)

Within your private LAN, you'll like to run a HTTP web-server (using known default Port 80) on a computer with IP address 192.168.168.99, so that PCs from outside the LAN may access it. This may be accomplished in two easy steps.

1

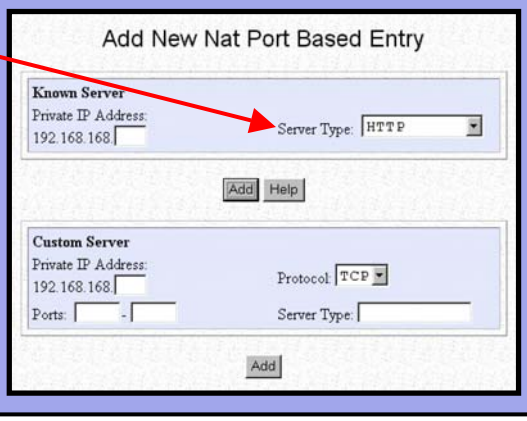


Step right in! From within the NetPassage's browser-based configuration menu, you can take advantage of the increased security by simply clicking the "Enable" radio button.

2

To set up Virtual Server based on Port-Forwarding. Hit the "Port Forwarding" button under "Advanced NAT Options" and then "Add" on the next screen to be brought to the "Add New Port Based Entry" configuration.

The drop-down menu of "Server Type" allows you to pick a gateway for common applications like HTTP, FTP, POP3 or NetMeeting (this example, choose HTTP).

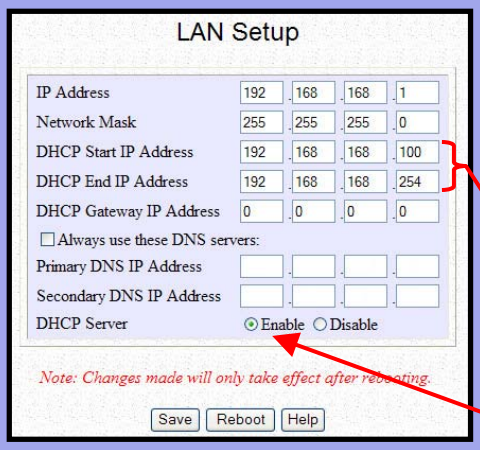


Key in an appropriate IP address for that "Known Server" you plan to be running (in this example, 192.168.168.99). It's this easy. *(Refer to Example 1a for related information pertaining to fixed & dynamic IP addressing)*

Example 1a: A Mix of Fixed and Dynamic IP addressing!

Surely, this is not an uncommon situation. You have configured your router to point to a publicly accessible HTTP server that resides within your private LAN. At the same time, you have to manage and keep a healthy group of users comprising workstations and mobile roadwarriors. Hence, you will need to allocate a fixed IP address for the HTTP server (e.g. 192.168.168.99), while leaving the rest of the workstations and notebook PCs to automatically obtain IP addresses from the DHCP server.

The only catch is this: you will need to tell the DHCP server, in this case the one built-in with your router, to reserve that particular fixed IP. This ENSURES that the DHCP server will not lease 192.168.168.99 to other PCs, which will render your HTTP server inaccessible. Here's how we do it in 3 simple steps:



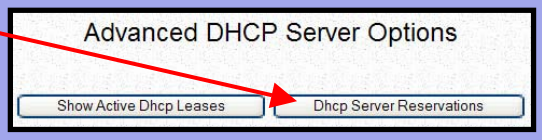
1

First step! Go into the "LAN Setup" menu in your router's web-browser configuration.

While ensuring that the IP address to be reserved does not lie in the range you are about to define for the "DHCP Start IP Address" and "DHCP End IP Address", you may choose any number from 1 to 254. (In this case 192.168.168.99 is outside of the allocated range). Finally, simply click "Enable" DHCP Server, "Save" and then "Reboot".

2

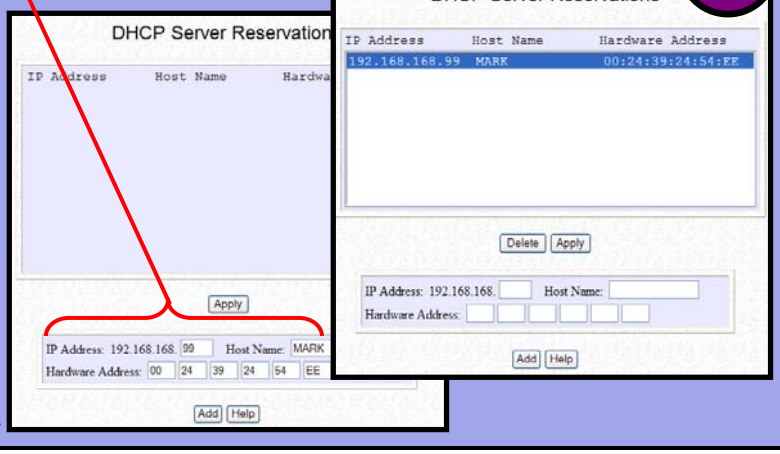
For step 2, within the LAN Setup screen, scroll down to click on "DHCP Server Reservations" under the "Advanced DHCP Server Options".



3

For this example, key in 192.168.168.99 as the IP to reserve. You will also need to key in the Host Name and Hardware Address corresponding to the machine you intend to run as the HTTP server. Then hit the "Add" button.

The entry will be added like the figure on the right.



Example 2: Enabling NAT with Virtual Server (IP Forwarding)

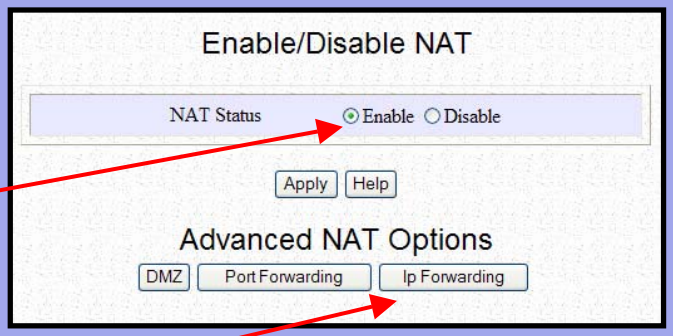
exclusive!

You have several IP addresses (e.g. 213.18.123.101 and 213.18.123.102) subscribed from your ISP and within your private LAN, you have an HTTP server running at 192.168.168.10, and a FTP server at 192.168.168.12.

You can forward all data packets for 213.18.123.101 to the HTTP server on your private network at 192.168.168.10 by following two simple steps.

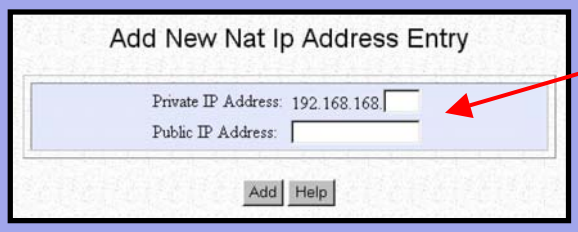
1

Again, like before, ensure that the NAT Status reflects "Enable" from within the router's browser-based configuration menu.



Hit the "Ip Forwarding" button under "Advanced NAT Options" and you will be brought to the following screen.

2



Therefore, for this example, you will key in "213.18.213.101" for the Public IP Address, and "192.168.168.10" for the HTTP server. Then click the "Add" button.

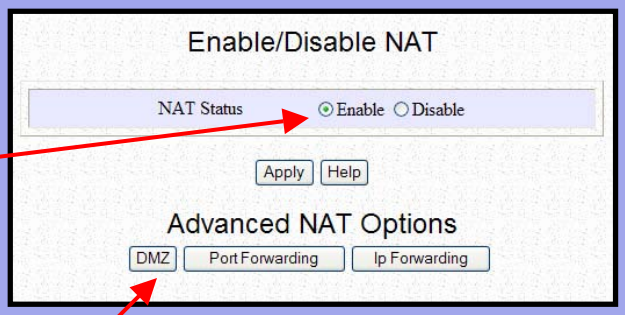
For the case of the FTP server you are running in this example, type "213.18.213.102" for the Public IP Address, and "192.168.168.12" and then click the "Add" button. It's done! You have successfully configured your router to have IP Forwarding based Virtual Server!

Example 3: Enabling NAT with De-Militarized Zone (DMZ)

As a network administrator, you have a computer with IP 192.168.168.45 and you wish to test a particular application that requires direct, unrestricted access both in and out of your private network. In this case, you may decide to enable DMZ which effectively puts the computer (running the application) "outside" the NAT firewall.

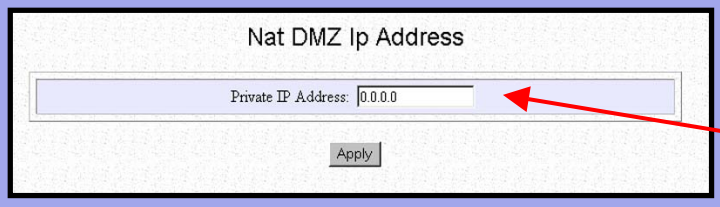
1

Once more, ensure that the NAT Status reflects "Enable" from within the router's browser-based configuration menu.



To configure the DMZ, first click on the "DMZ" button under the "Advanced NAT Options" afterwhich you'll be led to the following screen.

2



Now, it is as simple as keying in the computer's private IP address, 192.168.168.45. Then hit the "Apply" button.

In three short walk-throughs, we have covered a few common networking scenarios you may encounter. For the next example, we want to address a common, but relatively more troublesome circumstance when your favourite multiplayer game is faced with a secure firewall that is too great for it to scale on its own.

Example 4: Getting the Errant Game to Work with NAT

All work and no play makes Jack a dull boy. Even though most of your cutting-edge games should work well even behind a secure firewall, there are more than a handful of network games that will need you to exercise some effort before they'll actually work. Sometimes, the process may get rather involved when the application is not UPnP-compliant.

In the area of multiplayer gaming, let's walk through a particular example of setting up a PC, for example, with IP address 192.168.168.110, to play Half Life Counterstrike (earlier than v1.30)! After quick research from the Internet, it is known that the game uses the following source ports:

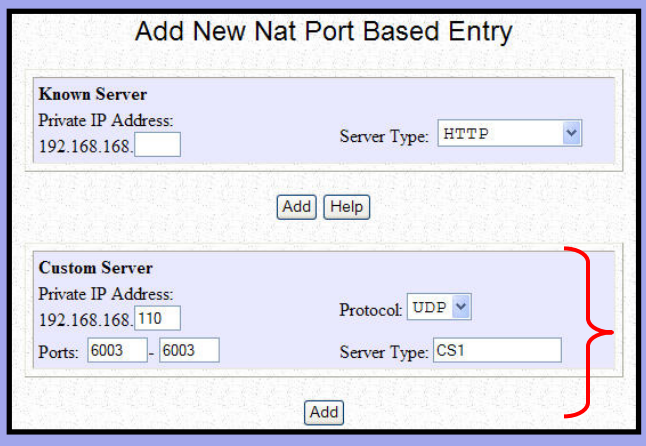
UDP 6003, UDP 7002, UDP 27010, UDP 27015, UDP 27025

This means we will have to configure your NAT firewall to forward data with these port addresses to a specific IP address within the network. It's not difficult, just 4 steps and you should be blasting away!

1

Check that NAT Status reflects "Enable", and then click on "Port Forwarding" and "Add" on the next screen to be brought to the "Add New Nat Port Based Entry" configuration menu.

2



In this case, we would consider the Counterstrike application you'd be running as a custom server.

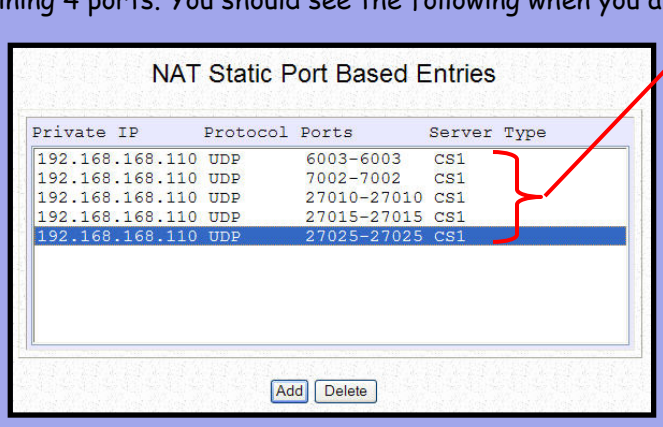
Under Private IP Address, put in the machine's IP address "192.168.168.110", select "UDP" as the protocol and plug in "6003" – "6003" as the Ports range. A possible name for the Server Type is "CS1". Hit the "Add" button.

Continued on the next page…

… continued from previous page.

3

To complete the set up, simply repeat steps 1 and 2 for each of the remaining 4 ports. You should see the following when you are done.



Whew!

Important Note: The port numbers as indicated in this example may change depending on the software developer. You should verify the port numbers directly with the relevant helpdesks whenever possible. A good resource citing common applications' port usage can be found at: www.practicallynetworked.com/sharing/app_port_list.htm

As you may already have tasted the tedium of manual settings, we shall look at the set up of Universal Plug and Play on your Windows OS and the NAT gateway so that your future network management job may be greatly simplified.

Example 5: UPnP coming to our rescue - Setting it up!

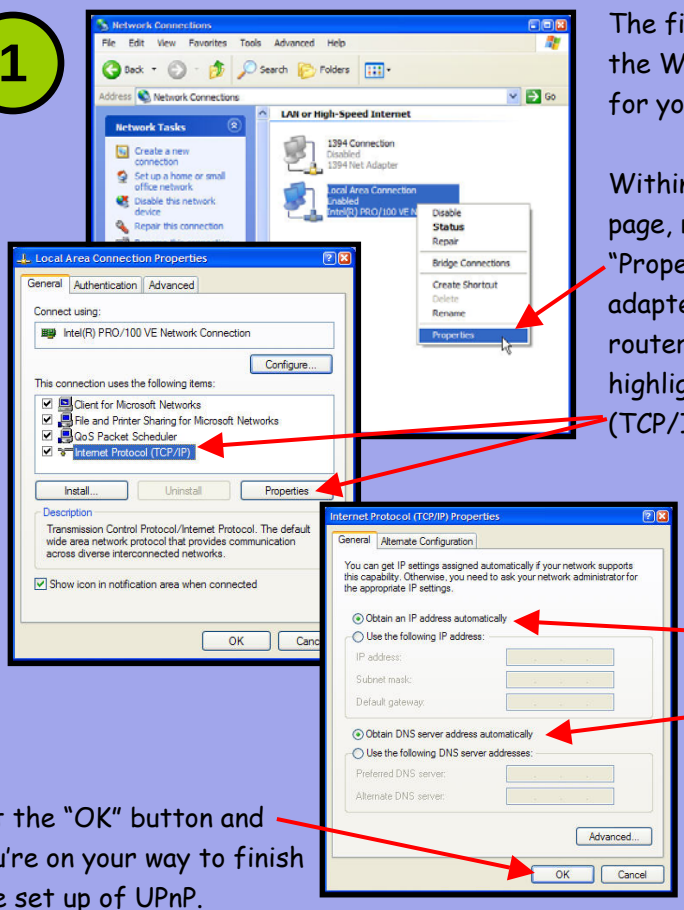
feature!

You've gone through the harrowing experience of manually opening ports in your NAT firewall for umpteen games purchased. Each software requires different ports to be opened, and the developers don't always reveal the ports used or it differs from versions to versions.

To make matters worse, applications like instant messaging software sometimes attempt to open ports in an adhoc basis, to establish peer-to-peer connections like file transfer, voice conversation or video conferencing. You simply can't work around these unless you abolish the security of your firewall, or go UPnP!

Using the UPnP-enabled routers, a UPnP-enabled operating system like Windows XP, and a suitable UPnP-enabled software application like Microsoft's MSN Messenger, you will be pleased with the experience. Let us take a look at how UPnP may be set up.

1



The first steps here involve getting the Windows operating system ready for your UPnP-enabled router.

Within XP's "Network Connections" page, right-click and select "Properties" under the network adapter you use to connect to the router. On the next dialog box, highlight "Internet Protocol (TCP/IP)" and click on "Properties".

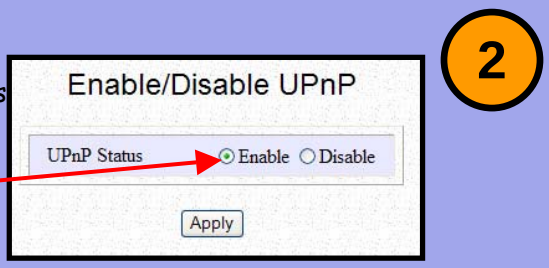
Then for the next page appearing, ensure that the settings are "Obtain an IP address automatically" as well as "Obtain DNS server address automatically", to let the router handle such allocations for you.

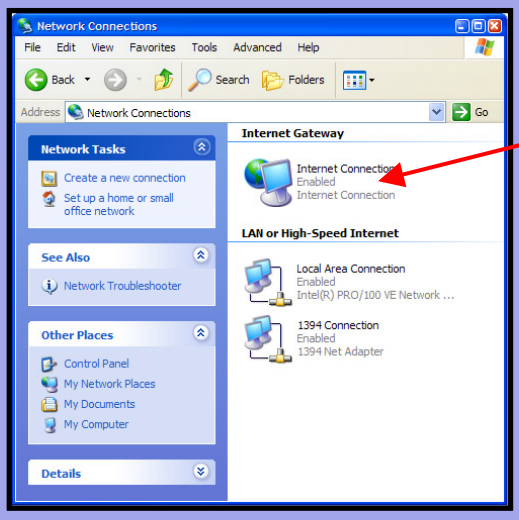
Hit the "OK" button and you're on your way to finish the set up of UPnP.

Continued on the next page...

… continued from previous page.

To finish up, you gotta jump to your router's UPnP menu. It cannot get easier from here, simply click the "Enable" radiobox and hit the "Apply" button. Viola!





To verify your set up, within your "Network Connections" page, you will notice a new item "Internet Connection" enabled under a new category "Internet Gateway".

Congratulations on your successful configuration of Universal Plug and Play! ☺

You may also go within its "Properties" page to change the detailed settings of the UPnP services in use.

Important Note: Always keep your Windows up to date with the latest security patches and fixes available at Microsoft's Windows Update site.

Keeping in mind our mission statement to deliver solutions that exceed your expectations, you will discover that the routers are designed for unparalleled ease-of-use, yet without compromising security and the powerful feature-set that will satisfy the most demanding network administrator.