CHAPTER 10
Network Address Translation (NAT)

10.1 Introduction

NAT is a method of mapping one or more IP addresses and/or service ports into different specified services, where NAT stands for Network Address Translation. It allows the internal IP addresses of many computers on a Local Area Network (LAN) to be translated to one public address, saving users' cost. It also plays a security role by obscuring the true IP addresses of important machines from potential hackers on the Internet. For convenience, we called a router having the NAT facility as a NAT-enabled router.

Usually you will use your Vigor router as a NAT-enabled router. The NAT-enabled router gets one (in Single ISP, PPPoE, PPPoA, MPoA) globally re-routeable IP addresses from the ISP and assigns private network IP addresses defined by RFC-1918 to local hosts. The NAT-enable router translates the private network IP addresses to such a globally routeable IP address so that local hosts can communicate with the router and access the Internet.

The following sections describe the web configuration for setting up the NAT facility, including specific configuration information and any limitation it has. One can find the entrance of this setting, as depicted in the following figure, after clicking the **NAT Setup** in the Advanced Setup of the main menu.

10.2 NAT Setup

Click **NAT Setup** to open the setup page. On the page, you will see the private IP

address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. Also, as stated before, the NAT facility can maps one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by using port mapping method. In the Vigor routers, we support three variants of port mapping methods: **Port Redirection**, **Open Ports**, and **DMZ host**.

Port Redirection: The packet is forwarded to a specific local host if the port number matches that defined in the table. A user can also translate the port to another port locally.

Open Ports: Similar to the Port Redirection, the Open Ports facility also support users to define a range of ports.

DMZ host: This opens up a single host completely. All incoming packets will be forwarded to the host with the local IP address you designated. The only exception is packets received in response to outgoing requests from

other local computers or incoming packets which match rules in the other two methods.

Herein, it should be noticed that, while you are using combinations of these three systems, there is a priority structure. That is, if a rule in one method co-incides with a rule in another method, then there is strict precedence. This leads to a predictable result and resolution of rule-conflict. The precedence is defined as follows.

Port Redirection > Open Ports > DMZ

***Example*:** If the port number of an incoming packet matches a rule specified in both **Port Redirection** and **Open Ports**, then the packet will be forwarded to the local address designated in **Port Redirection.**

Now, let us move on individual setting of these three port-mapping methods.

10.3 Configure Port Redirection Table

The **Port Redirection Table** may be used to expose internal servers to the public domain or open a specific port number for internal hosts. Internet hosts can use the WAN IP address to access internal network services, such as FTP, WWW, etc.

The following example shows how to expose an internal FTP server to the public domain. Assume that the internal FTP server is running on the local host with IP address of 192.168.1.10.

As shown below, the **Port Redirection Table** provides10 port-mapping entries for internal hosts.

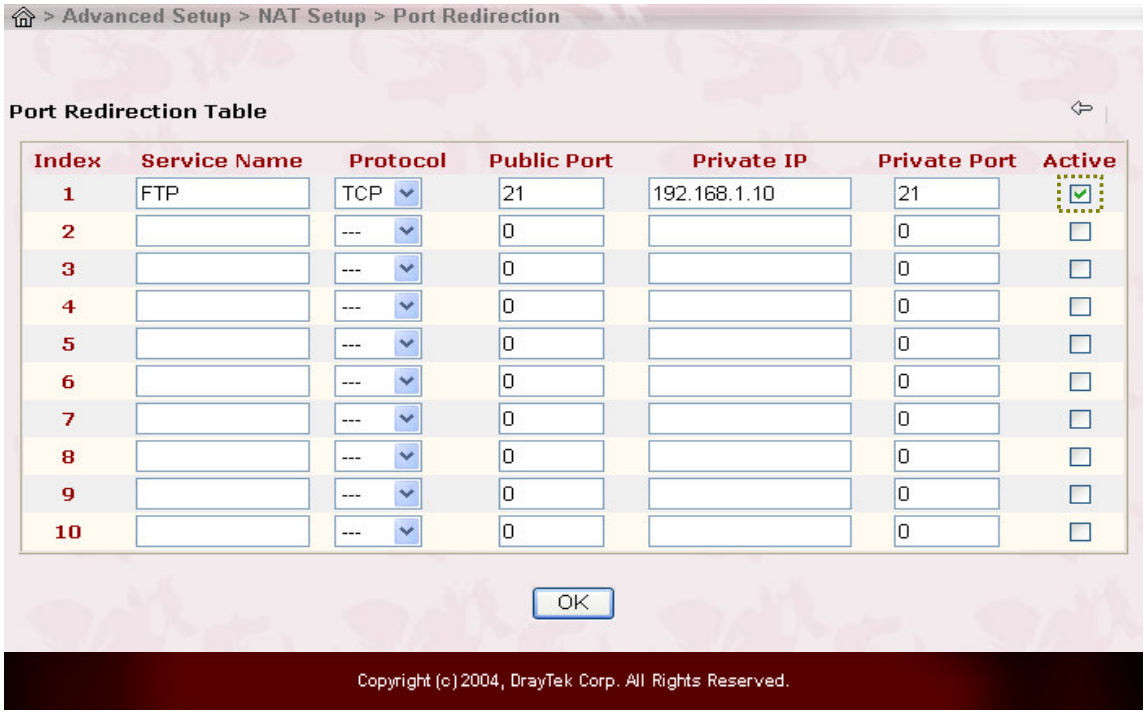
Service Name: Specify the name for the specific network service.

Protocol: Specify the transport layer protocol (TCP or UDP).

Public Port: Specify which port should be redirected to the internal host.

Private IP: Specify the private IP address of the internal host offering the service.

Private Port: Specify the private port number of the service offered by the internal host.



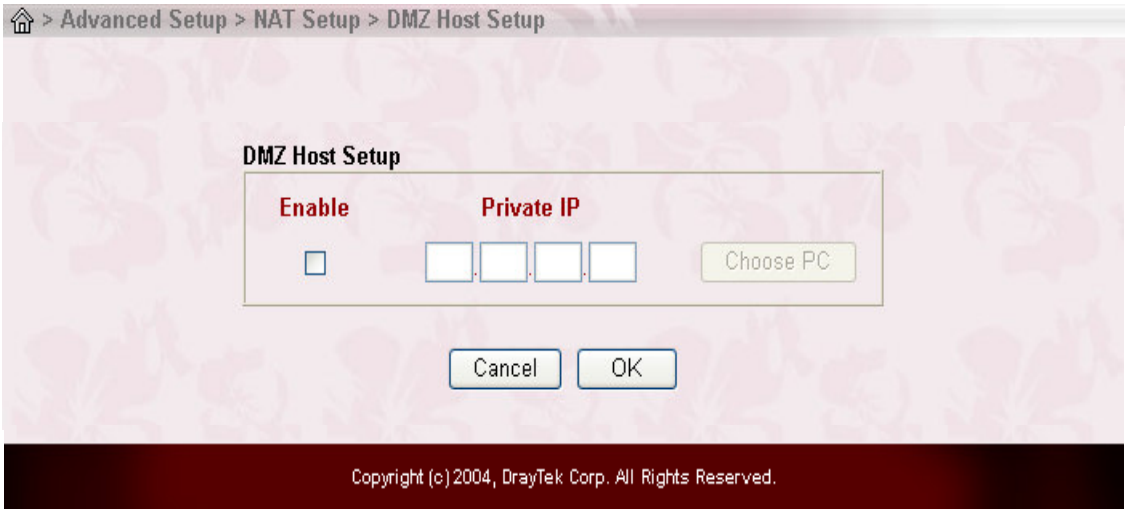
Active: Check here to activate the port-mapping entry.

Click **OK**

Note that the port forwarding can only be applied to external users only - i.e incoming traffic. The Internet users behind your LAN can not access your external public IP address and come back in; the internal users shall access the server on its local private IP address, or you can set up an alias in a Windows hosts file. Please only redirect the ports you know you have to forward rather than forward all ports. Otherwise, the intrinsic firewall type security of NAT facility will be influenced.

10.4 DMZ Host Setup

Click **DMZ Host Setup** to open the setup page, as shown below. The DMZ Host setting allows a defined internal user to be exposed to the Internet in order to use some special purpose applications such as Netmeeting or Internet Games etc. Each item in the setup page is described below.



Enable: Check to enable the DMZ Host function.

Private IP: Enter the private IP address of the DMZ host.

Choose PC: Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.

10.5 Open Port Setup

The following picture shows the **Open Ports Setup**. In Vigor routers, the **Open Ports** facility provides 10 entries for internal hosts.

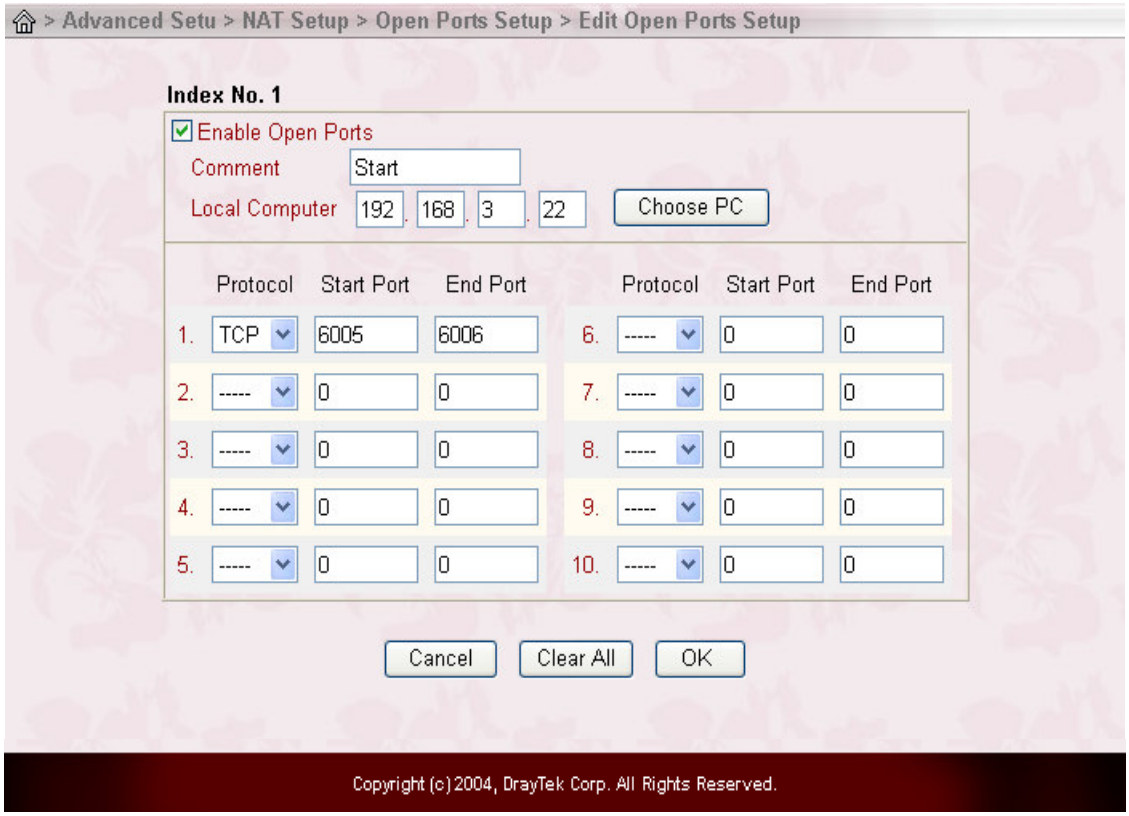
Index: Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.

Comment: Display the name for the specified network service.

Local IP Address: Display the private IP address of the local host offering the service.

Status: Display the state for the corresponding entry. We use X or V to represent the *Inactive* or *Active* state.

As stated above, after you click one index number, say index No. 1, in the above figure, you will see the following setup page for the entry with index No. 1. Further, each entry (loc al host) can specify 10 port -ranges for diverse services. More details for individual items in the setup page are described below.



Enable Open Ports: Check to enable the Open Port function for this entry.

Comment: Specify the name for the defined network service.

Local Computer: Enter the private IP address of the local host.

Choose PC: Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select one appropriate IP address of the local host in the list.

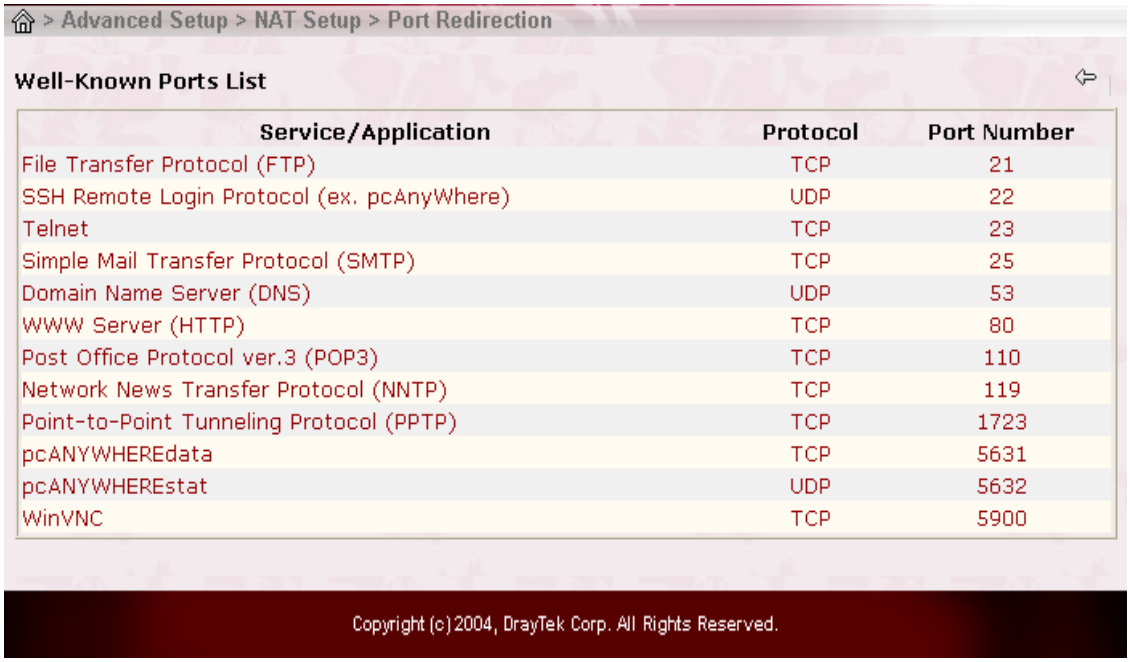
Protocol: Specify the transport layer protocol. It could be TCP, UDP, or NONE for selection.

Start Port: Specify the starting port number of the service offered by the local host.

End Port: Specify the ending port number of the service offered by the local host.

10.6 Well-known Port Number List

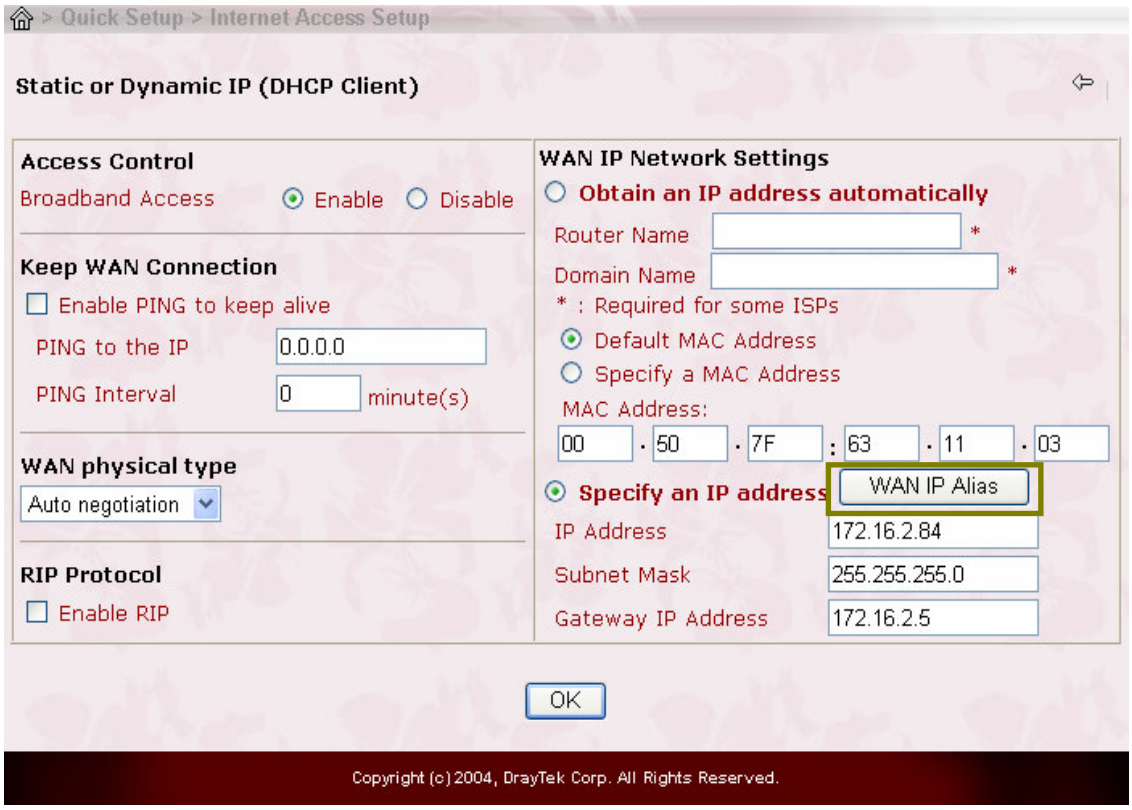
This page provides some well-known port numbers for your reference.



10.7 Multi-NAT Setup

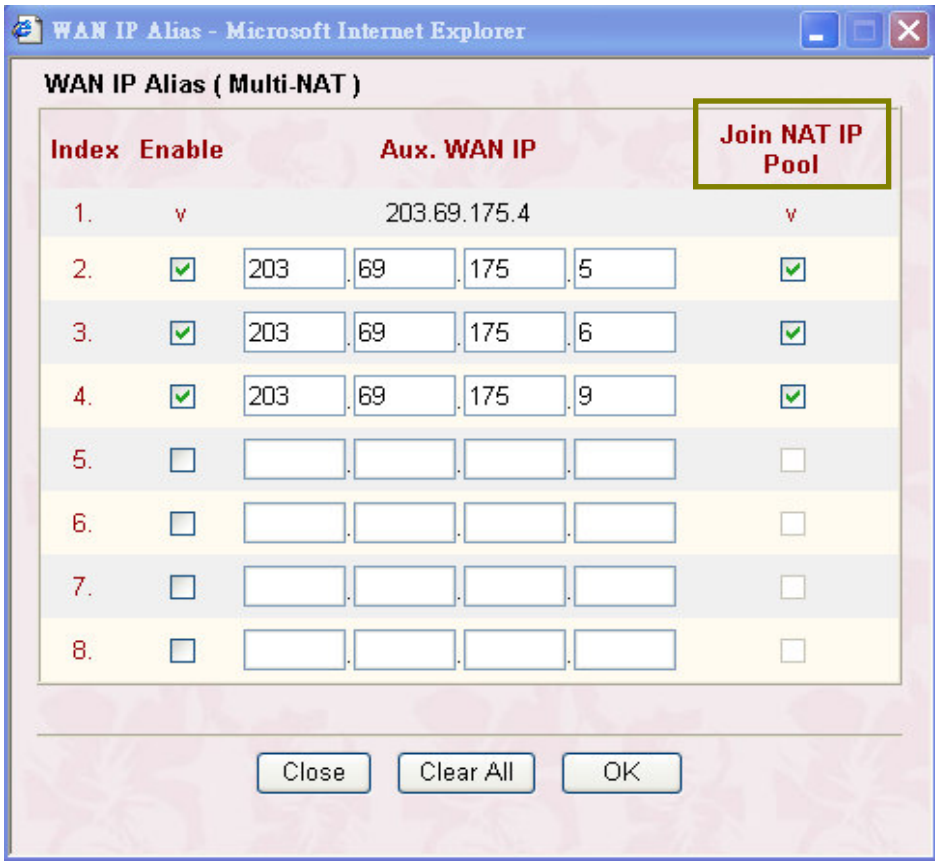
If you have a group of static IP addresses, then you can use the Multi-NAT features to set up multiple DMZ hosts or multiple open ports hosts in your Vigor routers. The following session shows you how to setup Multi-NAT feature.

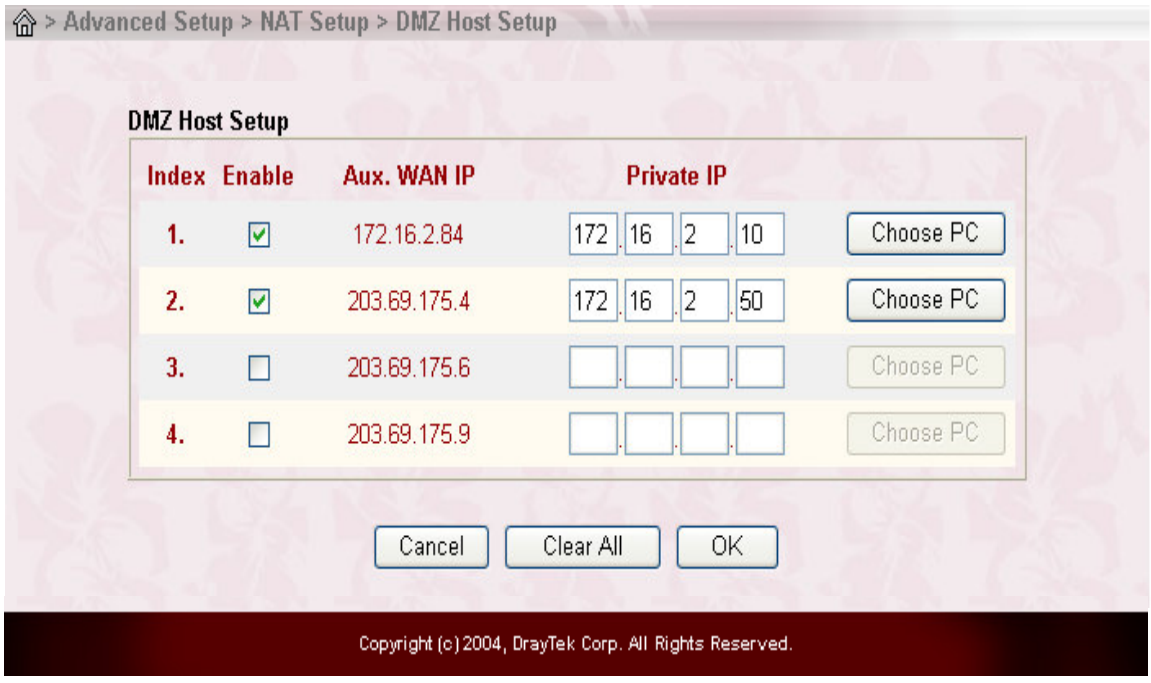
To achieve it, you should find the path to click the button of **WAN IP Alias**. The path is Main Menu→**Quick Setup**→**Internet Access Setup**. Herein, you will see the following page.

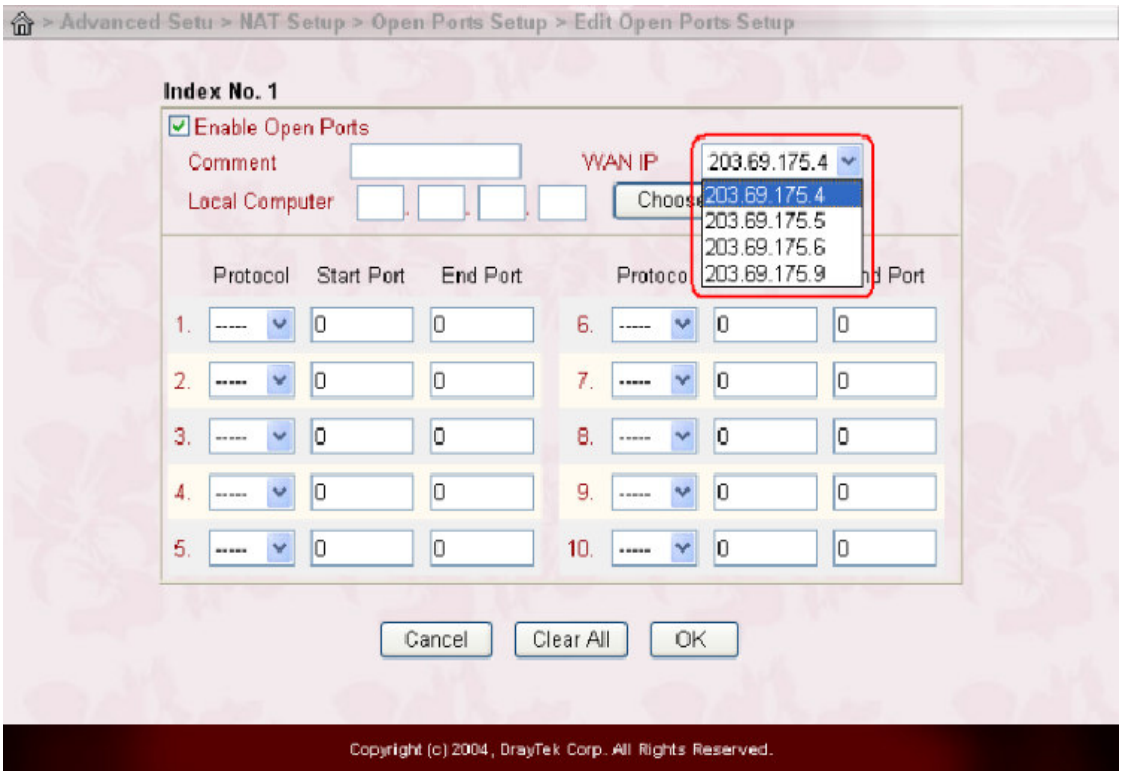


When you click the **WAN IP Alias** button, it will open a window for you to input your public IPs, as shown below. The **Join NAT IP Pool** check box indicates that the local user can use this IP to connect to the Internet. If you do not chick this check box, then the local user can not use this IP address.

After you set up the **WAN IP Alias**, then you can setup multiple DMZ and/or multiple open ports, as shown below.


WAN IP Alias - Microsoft Internet Explorer
WAN IP Alias (Multi-NAT)
Index
Enable
Aux. WAN IP
Join NAT IP Pool
1.
v
203.69.175.4
v
2.
203.69.175.5
3.
203.69.175.6
4.
203.69.175.9
5.
6.
7.
8.
Close
Clear All
OK


> Advanced Setup > NAT Setup > DMZ Host Setup
DMZ Host Setup
Index
Enable
Aux. WAN IP
Private IP
1.
172.16.2.84
172.16.2.10
Choose PC
2.
203.69.175.4
172.16.2.50
Choose PC
3.
203.69.175.6
Choose PC
4.
203.69.175.9
Choose PC
Cancel
Clear All
OK
Copyright (c) 2004, DrayTek Corp. All Rights Reserved.


> Advanced Setu > NAT Setup > Open Ports Setup > Edit Open Ports Setup
Index No. 1
Enable Open Ports
Comment
WAN IP
203.69.175.4
Local Computer
Choose
203.69.175.4
203.69.175.5
203.69.175.6
203.69.175.9
Protocol
Start Port
End Port
Protoco
nd Port
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
Cancel
Clear All
OK
Copyright (c) 2004, DrayTek Corp. All Rights Reserved.