

---

## CHAPTER 6

# Network Address Translation (NAT)

---

### 6.1 Introduction

NAT (Network Address Translation) is a method of mapping one or more IP addresses and/or service ports into different specified services. It allows the internal IP addresses of many computers on a 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.

### 6.2 NAT Setup

Usually you will use the router as a NAT-enabled router, where NAT stands for Network Address Translation. 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-enabled router translates the private network addresses to such a globally routeable IP address so that local hosts can communicate with the router and access the Internet. In the following, we explain NAT features for specific applications. 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.

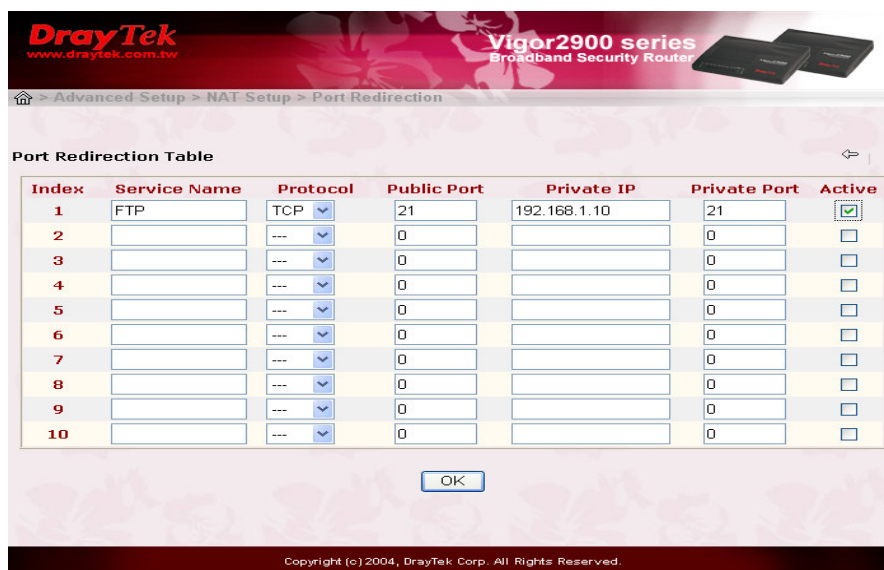
## NAT



### 6.3 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 to 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 an internal FTP server is exposed to the public domain. The internal FTP server is running on the local host addressed as 192.168.1.10.



As shown above, the **Port Redirection Table** provides 10 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.

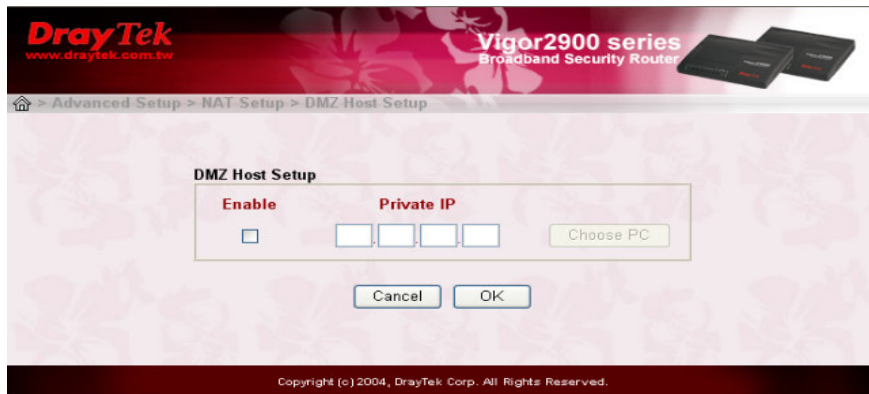
Click **OK**

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.

## 6.4 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.

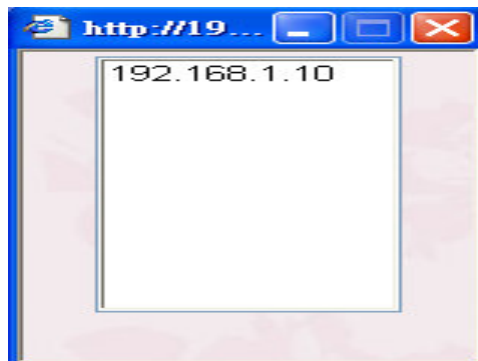
## NAT



**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 consisting of a list of private IP addresses of all hosts in your LAN network will automatically pop up. Select one private IP address in the list to be the DMZ host.



## 6.5 Open Port Setup

The Vigor 2900 series of broadband security routers can support three variants of port mapping methods as follows:

**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.

While you are using combinations of these three systems, there is a priority structure; i.e. if a rule in one method co-incides with a rule in another method, then there is strict precedence, so that the result should be predictable. The precedence is defined as follows:

**Port Redirection > Open Ports > DMZ**

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

The following picture shows the **Open Ports Setup**. In the Vigor2900 series of broadband security routers, the **Open Ports** facility provides 10 entries for internal hosts.

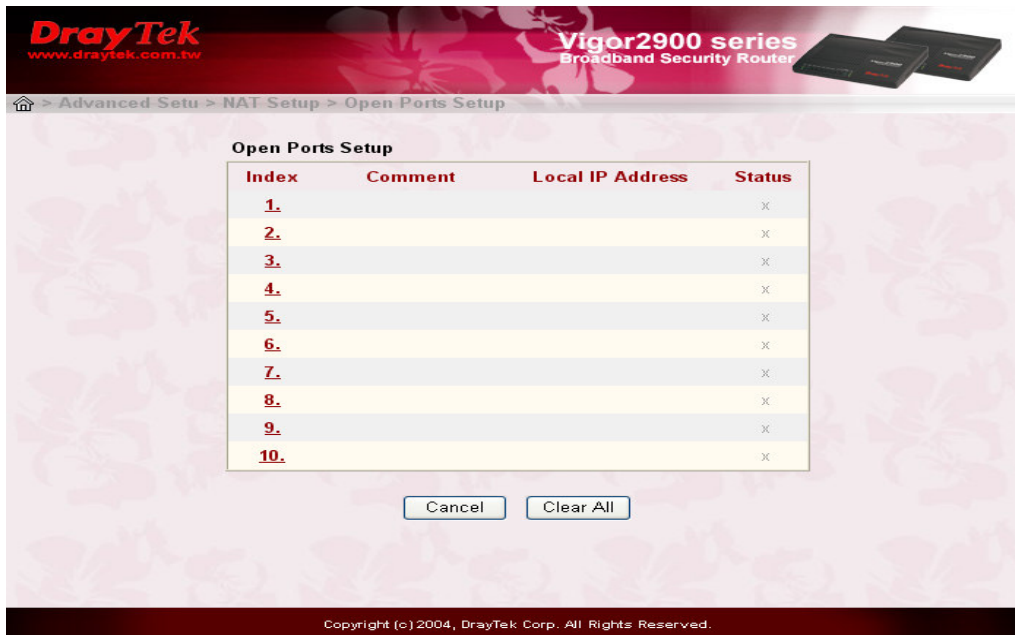
**Index:** Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.

**Comment:** Display the name for the specified network service.

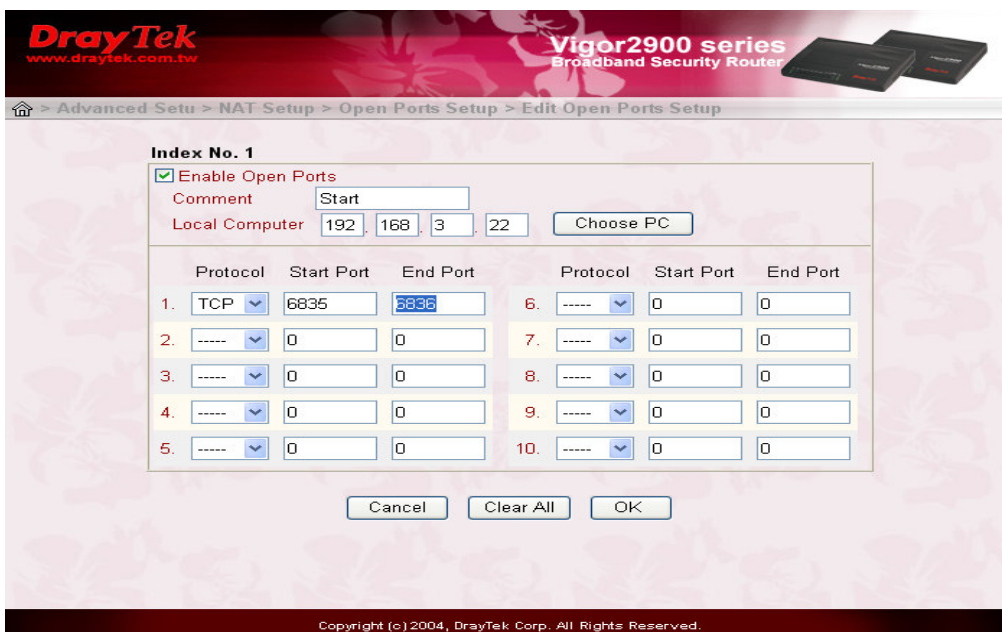
**Local IP Address:** Display the private IP address of the local host offering the service.

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

## NAT



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 (local host) can specify 10 port-ranges for diverse services. More details for individual items in the setup page are described below.



## NAT

**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.

## 6.6 Well-known Port Number List

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



The screenshot shows the configuration interface for a DrayTek Vigor2900 series Broadband Security Router. The page title is "Well-Known Ports List". The table below lists various services and their corresponding protocols and port numbers.

Service/Application	Protocol	Port Number
File Transfer Protocol (FTP)	TCP	21
SSH Remote Login Protocol (ex. pcAnywhere)	UDP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (DNS)	UDP	53
WWW Server (HTTP)	TCP	80
Post Office Protocol ver.3 (POP3)	TCP	110
Network News Transfer Protocol (NNTP)	TCP	119
Point-to-Point Tunneling Protocol (PPTP)	TCP	1723
pcANYWHEREdata	TCP	5631
pcANYWHEREstat	UDP	5632
WinVNC	TCP	5900

Copyright (c) 2004, DrayTek Corp. All Rights Reserved.

## 6.7 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 the Vigor 2900 series of broadband security routers. The following session will show 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.

The screenshot shows the configuration page for the Vigor2900 series Broadband Security Router. The page is titled "Static or Dynamic IP (DHCP Client)" and is part of the "Quick Setup > Internet Access Setup" menu. The page is divided into several sections:

- Access Control:** Broadband Access is set to "Enable".
- Keep WAN Connection:** "Enable PING to keep alive" is unchecked. PING to the IP is set to "0.0.0.0" and PING Interval is set to "0" minute(s).
- WAN physical type:** Set to "Auto negotiation".
- RIP Protocol:** "Enable RIP" is unchecked.
- WAN IP Network Settings:**
  - "Obtain an IP address automatically" is selected.
  - Router Name: "vigor2900"
  - Domain Name: (empty)
  - \* : Required for some ISPs
  - "Specify a MAC Address" is selected.
  - MAC Address: 00 . 50 . 7F : 38 . 49 . 5F
  - "Specify an IP address" is selected, and the "WAN IP Alias" button is highlighted with a red box.
  - IP Address: 172.16.2.136
  - Subnet Mask: 255.255.255.0
  - Gateway IP Address: 172.16.2.6

An "OK" button is located at the bottom of the configuration area. The footer of the page reads "Copyright (c) 2004, DrayTek Corp. All Rights Reserved."

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 check this check box, then the local user can not use this IP.



## NAT

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	203.69.175.4	v
2.	<input checked="" type="checkbox"/>	203.69.175.5	<input checked="" type="checkbox"/>
3.	<input checked="" type="checkbox"/>	203.69.175.6	<input checked="" type="checkbox"/>
4.	<input checked="" type="checkbox"/>	203.69.175.9	<input checked="" type="checkbox"/>
5.	<input type="checkbox"/>		<input type="checkbox"/>
6.	<input type="checkbox"/>		<input type="checkbox"/>
7.	<input type="checkbox"/>		<input type="checkbox"/>
8.	<input type="checkbox"/>		<input type="checkbox"/>

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

Index	Enable	Aux. WAN IP	Private IP	Choose PC
1.	<input checked="" type="checkbox"/>	192.168.100.50	192.168.1.10	Choose PC
2.	<input checked="" type="checkbox"/>	203.69.175.5	192.168.1.25	Choose PC
3.	<input type="checkbox"/>	203.69.175.6		Choose PC
4.	<input type="checkbox"/>	203.69.175.9		Choose PC

# NAT

The screenshot shows the configuration interface for a DrayTek Vigor2900 series Broadband Security Router. The breadcrumb navigation is: **Advanced Setu > NAT Setup > Open Ports Setup > Edit Open Ports Setup**. The page title is **Index No. 1**. The **Enable Open Ports** checkbox is checked. The **WAN IP** dropdown menu is open, showing a list of IP addresses: 203.69.175.4, 203.69.175.5, 203.69.175.6, and 203.69.175.9. The **Local Computer** field is empty. Below these fields is a table for configuring open ports:

	Protocol	Start Port	End Port	Protocol	Start Port	End Port	
1.	----	0	0	6.	----	0	0
2.	----	0	0	7.	----	0	0
3.	----	0	0	8.	----	0	0
4.	----	0	0	9.	----	0	0
5.	----	0	0	10.	----	0	0

At the bottom of the configuration area are three buttons: **Cancel**, **Clear All**, and **OK**. The footer text reads: **Copyright (c) 2004, DrayTek Corp. All Rights Reserved.**