September 2008

AOS Quick Configuration Guide

Removing IP Unnumbered

Understanding IP Unnumbered

In a typical circuit configuration, a customer will be provided with two sets of IP addresses. A “WAN Block” allows the public interface of the router to communicate with the ISP. A “LAN Block” allows public devices to reside behind the router. Often times, to save IP addresses, an ISP will only assign a single block of IP addresses. They accomplish this by using IP Unnumbered. IP Unnumbered enables a public IP address to be assigned to the Ethernet port of the router and for the WAN port to utilize that IP when communicating with the outside world.

Figure 1 – Typical ISP

Figure 2 – IP Unnumbered

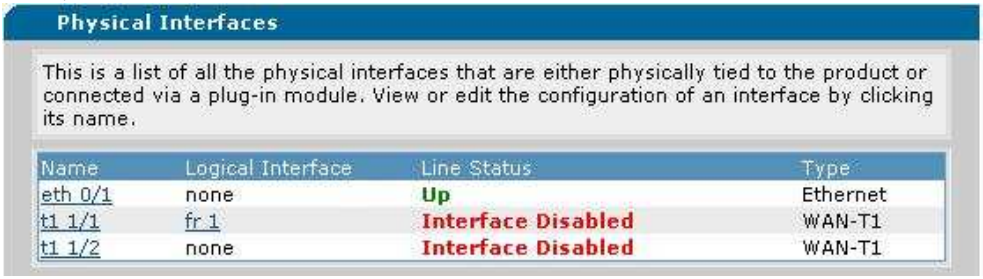
This guide will outline the steps required to remove IP Unnumbered from the router and assign private IP addresses to the internal LAN.

Removing IP Unnumbered

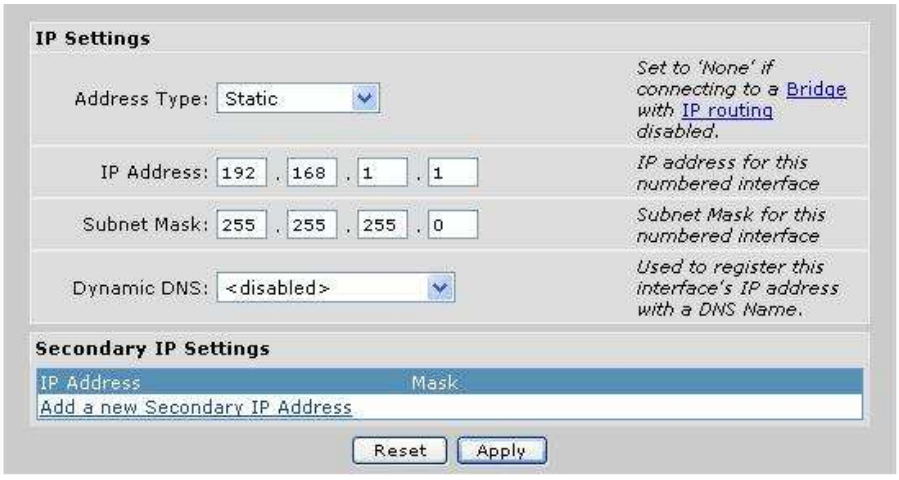
Removing IP Unnumbered in the GUI

First, navigate to “Physical Interfaces”

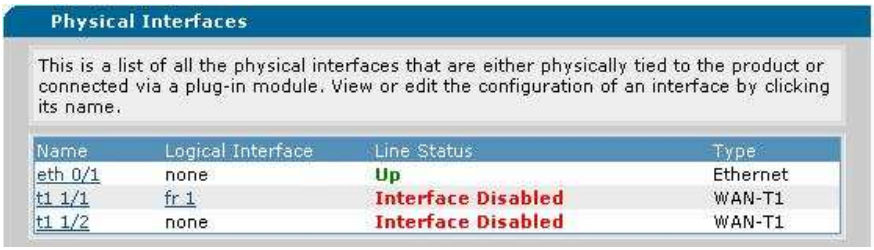
Next, click on the local Ethernet interface associated with the LAN.



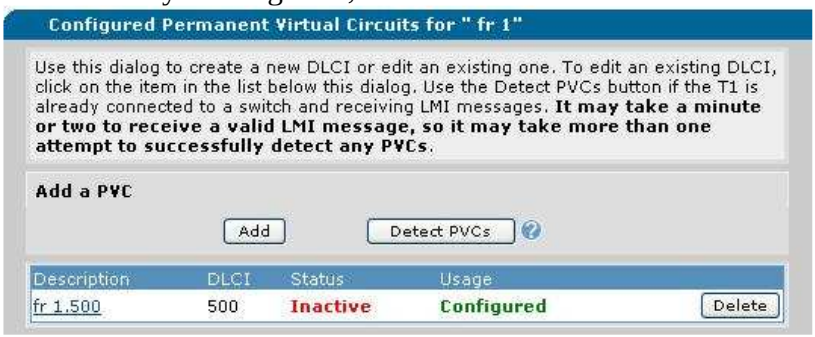
Now, change the local IP address to whatever private IP scheme is desired. Click “Apply”. After doing so, connectivity to the router will be lost until the IP address on the local PC is changed to the same subnet as the router.



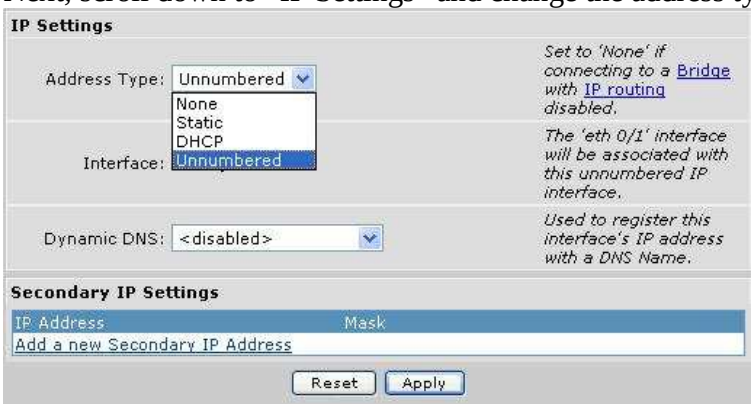
Next, navigate back to “Physical Interfaces” and click on the logical interface associated with the T1.



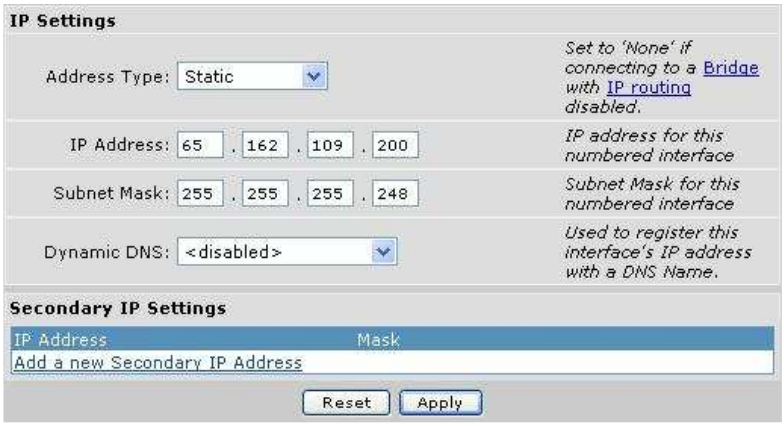
If frame-relay is being used, scroll down and click on the PVC that has been created.



Next, scroll down to “IP Settings” and change the address type from “Unnumbered” to “Static”.

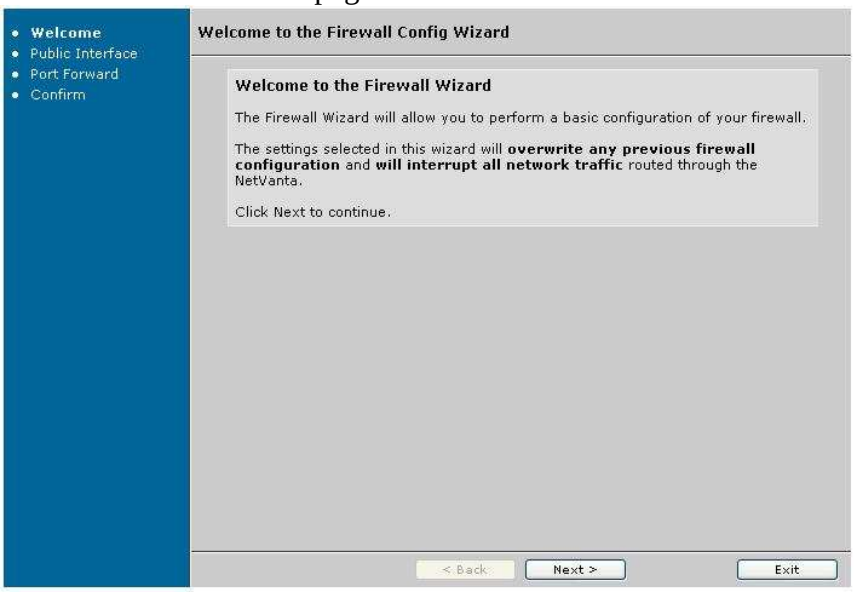


Next, set the IP address on the WAN interface that was previously assigned to the internal Ethernet interface.

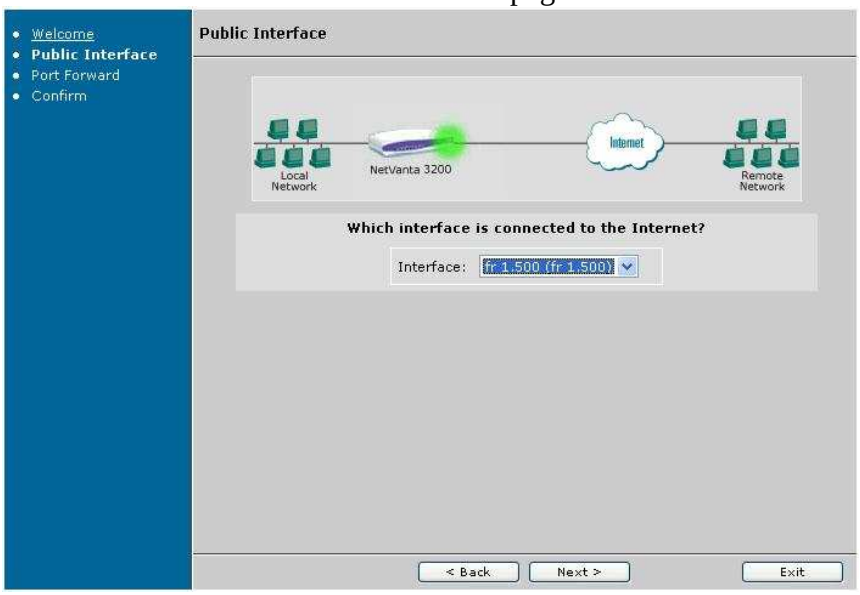


To complete the configuration, the firewall wizard must be run. Click on the “Firewall Wizard” link.

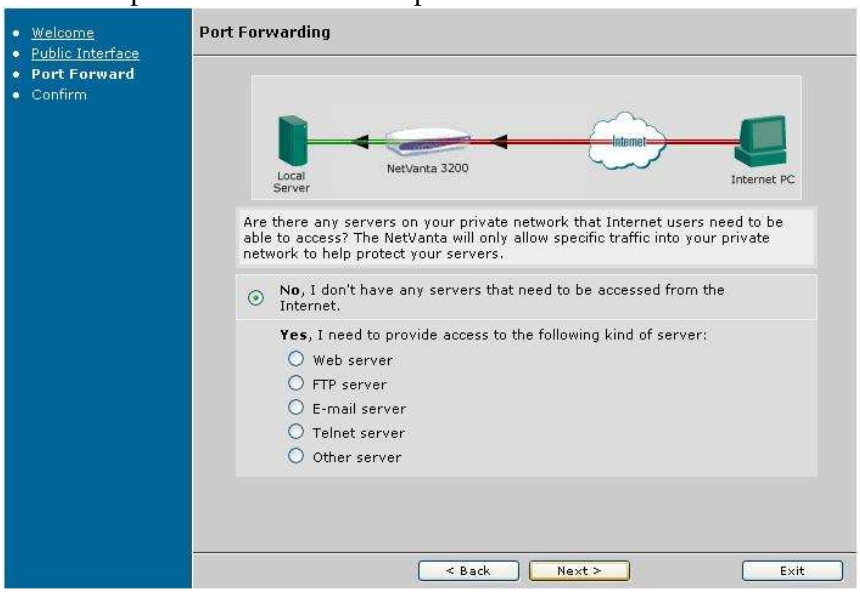
Click “Next” on the first page.



Select the WAN interface on the second page and click “Next”



Any port forwards can be initially configured using the next screen, but this is optional. Click “Next” to proceed to the final step.



Confirm the settings and click “Finish”. Clients with the correct settings on the internal network should now be able to access the internet.

Removing IP Unnumbered in the CLI

1. Identify the interface that is currently set to IP Unnumbered. If you are unsure, issue “show run” from the enable prompt to view the current configuration of the router. Also, note the IP address currently assigned to the Ethernet interface.

2. Navigate to the Ethernet interface and set it to the private IP that you wish to use. Once you enter this command, you will lose connectivity to the router if you are telnetted in. At this point, you will need to change your PC to an IP address in the same subnet as your new Ethernet IP before you can re-establish connectivity.

Syntax: **ip address** *<A.B.C.D> <Subnet Mask>*
EX: (config-eth 0/1)# **ip address 192.168.1.1 255.255.255.0**

3. Navigate to public interface that is currently set to IP Unnumbered. This interface must be set to the IP address that was formerly assigned to the Ethernet interface.

   Syntax: **ip address** *<A.B.C.D> <Subnet Mask>*
   EX: (config-fr 1.500)# **ip address 65.162.109.200 255.255.255.248**

4. At this point, the router has the correct IP addresses assigned to it. Now, firewall rules must be created in order to use NAT (Network Address Translation). Exit to the global config prompt and issue the following commands:

   Create the access list to match all outbound traffic for NAT

   Syntax: **ip access-list extended** *<ACL Name>*
   EX: (config)# **ip access-list extended matchall**

   Set the ACL to match all IP traffic.

   Syntax: **permit** *<protocol type> <source host or subnet> <destination host or subnet>*
   EX: (config-ext-nacl)# **permit ip any any**

   Create the Public firewall policy for the WAN interface. It will remain empty for the time being.

   Syntax: **ip policy-class** *<Policy Name>*
   Ex: (config)# **ip policy-class Public**

   Create the Private firewall policy for the LAN interface.

   Syntax: **ip policy-class** *<Policy Name>*
   EX: (config)# **ip policy-class Private**

   Create the NAT within the Private firewall policy to NAT all outbound traffic.

   Syntax: **nat source list** *<ACL Name>* **address** *<WAN IP>* ***overload***
   EX: (config-policy-class)# **nat source list matchall address 65.162.109.200 overload**

5. Next, navigate to the LAN and WAN interfaces of the router and assign the appropriate firewall policy to each.

   Syntax: **access-policy** *<Policy Name>*
   EX: (config-fr 1.500)# **access-policy Public**
   Syntax: **access-policy** *<Policy Name>*
   EX: (config-eth 0/1)# **access-policy Private**

6. Finally, from the global configuration prompt of the router, enable the firewall.

   Syntax: **ip firewall**
   EX: (config)# **ip firewall**

At this point, with valid DNS settings and a default gateway of the router, a PC on the inside should be able to reach the internet.

Command Summary Table

	Command	Description
Step 1	(config-eth 0/1)# **ip address** <A.B.C.D> <Subnet Mask>	Change the IP address of the LAN interface to a private IP.
Step 2	(config-fr 1.500)# **ip address** <A.B.C.D> <Subnet Mask>	Change the IP address of the WAN interface to the public IP formerly assigned to the LAN interface.
Step 3	(config)# **ip access-list extended** <*ACL name*>	Create an ACL to match all traffic for NAT.
Step 4	(config-ext-nacl)# **permit** <*protocol type*> <*source host or subnet*> <*destination host or subnet*>	Define the ACL to match all traffic that will be NATted outbound.
Step 5	(config)# **ip policy-class** <*policy name*>	Create a Public and Private policy for firewall rules to be applied to.
Step 6	(config-policy-class)# **nat source list** <*ACL name*> **address** <*WAN interface IP*> **overload**	Create a NAT statement within the private policy class to allow privately addressed traffic to get out.
Step 7	(config-eth 0/1)# **access-policy** <*policy name*>	Apply the Private policy to the local Ethernet interface.
Step 8	(config-fr 1.500)# **access-policy** <*policy name*>	Apply the Public policy to the WAN interface
Step 9	(config)# **ip firewall**	Specify the ports that will be forwarded to the previously specified server.

Example configuration

(config-eth 0/1)# **ip address 192.168.1.1 255.255.255.0**
(config-eth 0/1)# **interface fr 1.500**
(config-fr 1.500)# **ip address 65.162.109.200 255.255.255.248**
(config-fr 1.500)# **exit**
(config)# **ip access-list extended matchall**
(config-ext-nacl)# **permit ip any any**
(config-ext-nacl)# **ip policy-class Private**
(config-policy-class)# **nat source list matchall address 65.162.109.200 overload**
(config-policy-class)# **ip policy-class Public**
(config-policy-class)# **interface eth 0/1**
(config-eth 0/1)# **access-policy Private**
(config-eth 0/1)# **interface fr 1.500**
(config-fr 1.500)# **access-policy Public**
(config-fr 1.500)# **exit**
(config)# **ip firewall**