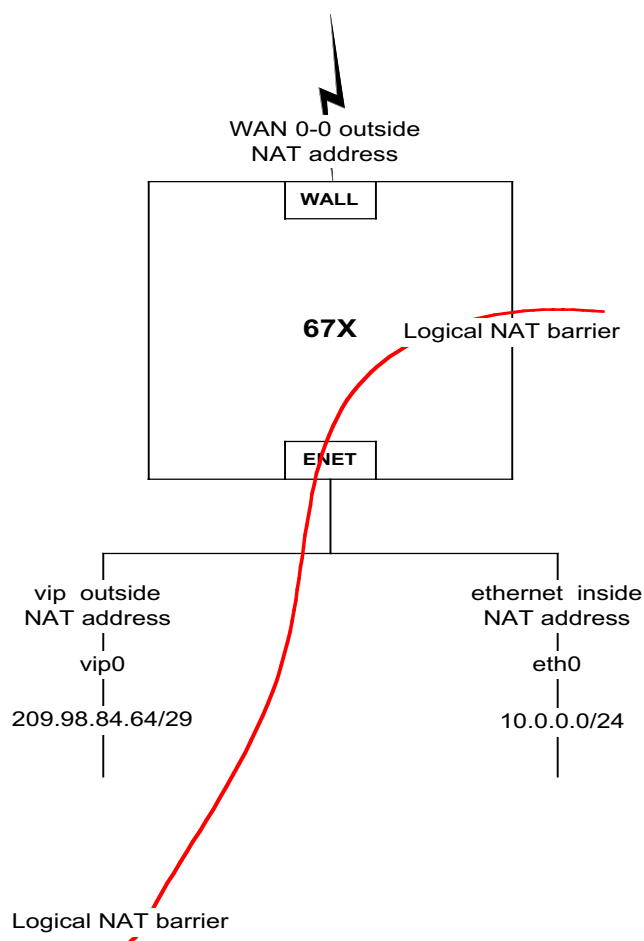


Effective Use of the VIP interfaces and NAT functionality in CBOS 2.4.3

Introduction

CBOS 2.4.3 provides a considerable amount of NAT and network interface functionality, which allows DSL subscribers to configure their networks to address a variety of needs. This document will examine some of the features and configuration requirements to benefit from this functionality. Also discussed are the top three configurations considered to be the most popular and applicable for the 6xx product family.

Public IP Server Network - Private IP Workstation Network



CBOS Commands

```
set ppp wan0-0 login username
set ppp wan0-0 password password
set ppp wan0-0 ipcp 0.0.0.0
set ppp restart enabled
set nat enabled
set int vip0 address 209.98.84.70
```

```
set int vip0 mask 255.255.255.248
set int vip0 outside
```

Many DSL subscribers want to run servers available to the outside world via their DSL connection and have leased public IP address space for this purpose from their Service Provider. Additionally, these subscribers would like to have a network of internal workstations to have access to these servers as well as the Internet.

Since these subscribers often have a limited number of public IP addresses NAT must be used to provide Internet access as well as access to the servers on the public address space. NAT enables the workstations to access the Internet via the external IP address assigned to the wan0-0 interface of this configuration. Packets coming from the network associated with eth0 will have the source address of the wan0-0 interface. Workstations on the eth0 network will be configured to reside within a range of RFC 1918 addresses¹. These addresses have been allocated by the Internet Engineering Task Force (IETF) for precisely this type of application. The default network for NAT configuration for the eth0 interface is 10.0.0.0/24.

Ideally, a block of addresses large enough to accommodate the servers requiring access from the Internet should be allocated. However, if over time the number of servers that require access from the Internet should increase beyond the size of the initial network, additional public IP addresses could be obtained from the Service Provider and configured for operation on the next available VIP interface. This is demonstrated in the following configuration example.

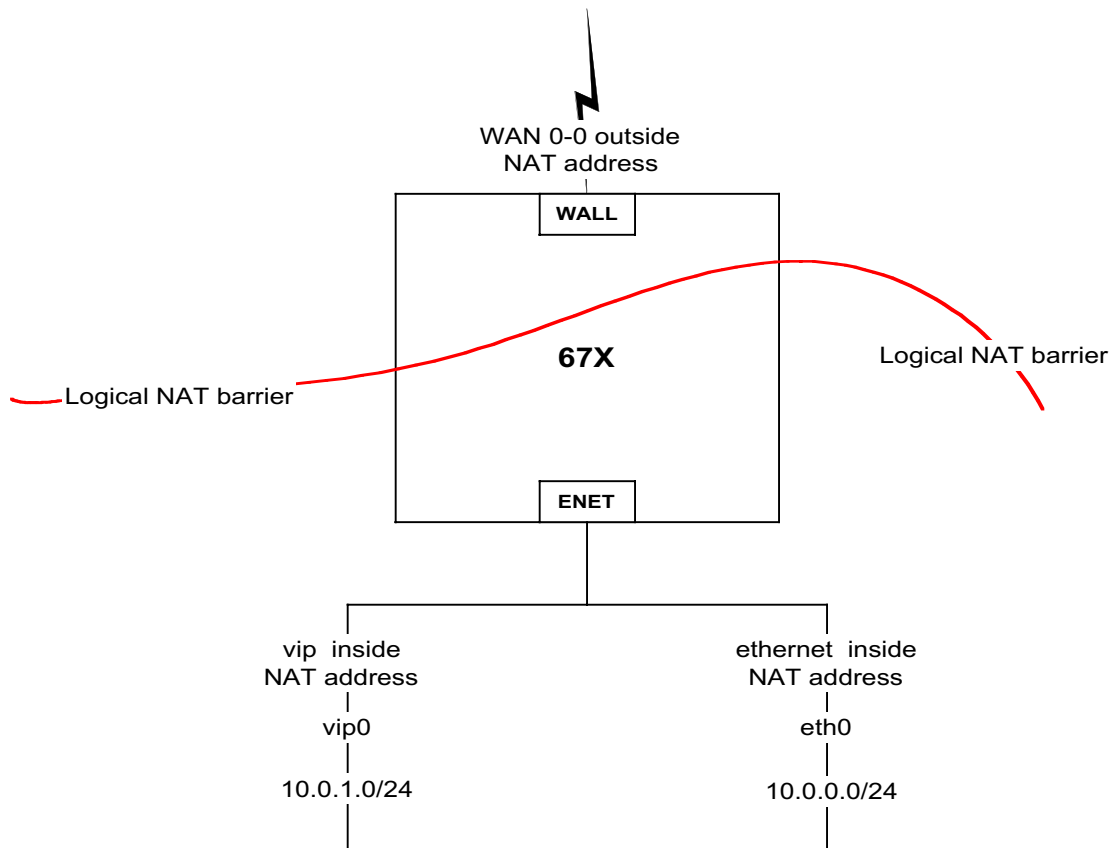
```
set int vip1 address 209.98.98.0
set int vip1 mask 255.255.255.0
set int vip1 outside
```

There may be times when a subscriber may want to make an application available on the network associated with the eth0 interface to hosts on the outside network. The following example demonstrates a NAT entry for FTP, that will allow an application to be statically mapped from vip0(outside) to a host on the eth0(inside) interface.

```
set nat entry add 10.0.0.2 21 209.98.84.65 21 tcp
```

By segmenting hosts within a network in this fashion, connectivity effectively realized between the servers on the public IP address space, from hosts on the Internet and from within the local network.

All NAT - No Public IP Configuration



CBOS Commands

```
set ppp wan0-0 login username
set ppp wan0-0 password password
set ppp wan0-0 ipcp 0.0.0.0
set ppp restart enabled
set nat enabled
set int vip0 address 10.0.1.1
set int vip0 mask 255.255.255.0
set int vip0 inside
```

Many DSL subscribers are primarily interested in having Internet access for workstations with little or no need to host services or to accept incoming connections. For these subscribers NAT connectivity provides a very convenient means of facilitating this type of access.

Additionally, the vip interface mechanisms provide a flexible means of segmenting the network into separate broadcast domains and routing between them. Servers and work-groups can be placed into networks associated with the different vip interfaces. As long as the vip interface is defined as being inside from a NAT perspective, traffic destined for these separate networks is routed via the 6xx without requiring NAT between inside interfaces.

Undoubtedly, there will be occasions where a subscriber will want to allow inbound connections to hosts on the internal networks. When these occasions arise, the Port Address Translation (PAT) feature within CBOS can be utilized to map inbound connections from the Internet to the designated host on the inside segment.

The following is a sample NAT entry that will allow HTTP to be statically mapped from wan0-0 to a host on the vip0(inside) interface. Note the use of the global 0.0.0.0 address wildcard to accommodate the dynamic allocation of addresses via IPCP.

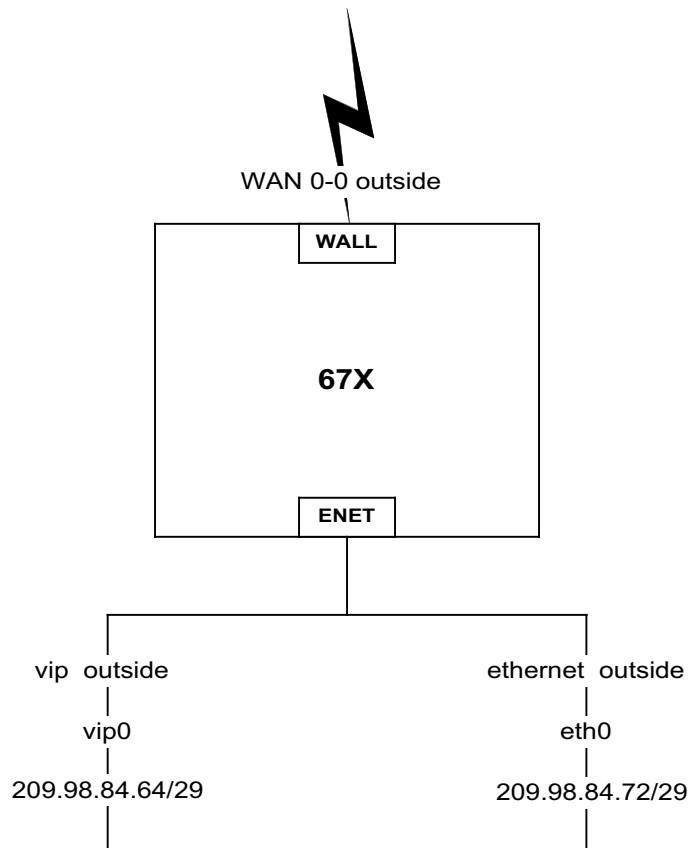
```
cbos# set nat entry add 10.0.1.3 80 0.0.0.0 80 tcp
```

An additional NAT entry that will allow FTP to be statically mapped from wan0-0 to a host on the eth0(inside) interface. Again, note the use of the global 0.0.0.0 address wildcard to accommodate the dynamic allocation of addresses via IPCP.

```
set nat entry add 10.0.0.2 21 0.0.0.0 21 tcp
```

Comprehensive documentation regarding the PAT capabilities of the Cisco 6xx platform can be found on the Cisco web site.ⁱⁱ

No NAT - Entirely Public IP Configuration



CBOS Commands

```
set ppp wan0-0 login username
set ppp wan0-0 password password
set ppp wan0-0 ipcp 0.0.0.0
set ppp restart enabled
set int vip0 address 209.98.84.70
set int vip0 mask 255.255.255.248
set int vip0 outside
set int vip1 address 209.98.84.70
set int vip1 mask 255.255.255.248
set int vip1 outside
```

Some subscribers have a significant quantity of public address space and would like to make it all available for use within their network. Both for use by servers which are publicly accessible via the Internet and Workstations, which may run certain applications which require public IP addresses.

The configuration detailed above illustrates the ability of the vip interface to support this type of configuration as well as route between these network segments.

Operational Notes

Here are a few things to keep in mind when using some of these features on the 6xx family of products.

VIP Configuration

When setting the address and the mask on the vip interfaces the changes are not reflected until the next reboot of the 6xx device. Configuration elements can be added and changed prior to the reboot but changes will not be reflected until the next reboot. Where applicable CBOS will inform the user that these changes will not take place until the next reboot.

NAT Configuration of TFTP and Telnet

If NAT entries are created through the wan0-0 interface for the telnet service users will not be able to telnet into the 6xx in order to administrate it via the wan0-0 interface. Additionally, if NAT entries are created for TFTP, users will not be able to tftp software images to the 6xx device via the wan0-0 interface. Users should exercise care when creating NAT entries for these services.

Summary

The vip interface functionality in CBOS provides a considerable amount of operational flexibility. When used in conjunction with the NAT and PAT feature sets, a wide variety of configuration scenarios can be accommodated. By strictly enforcing the NAT boundaries users can effectively segment their networks both internally and externally, providing a means to effectively grow their networks.

ⁱ <http://www.ietf.org/rfc/rfc1918.txt>

ⁱⁱ Comprehensive documentation regarding NAT and the PAT capabilities of the Cisco 6xx family can be found at the following URL's.

Understanding Port Address Translation on the Cisco 600

<http://www.cisco.com/warp/public/794/600pat.html>

Cisco Broadband Operating System (CBOS)

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/c600s/cbos/index.htm