

Configuring Network Address Translation and Static Port Address Translation to Support an Internal Web Server

Document ID: 12905

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

- Background Information

Configure

- Network Diagram

- Configuration

Verify

Troubleshoot

Related Information

Introduction

Cisco IOS® Network Address Translation (NAT) is designed for IP address simplification and conservation. It enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a Cisco router that connects two networks together, and translates the private (inside local) addresses in the internal network to public addresses (outside local) before packets are forwarded to another network. As a part of this functionality, you can configure NAT to advertise only one address for the entire network to the outside world. This effectively hides the internal network from the world. Therefore, it provides additional security.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Background Information

One of the main features of NAT is static Port Address Translation (PAT), which is also referred to as "overload" in a Cisco IOS configuration. Static PAT is designed to allow one-to-one mapping between local and global addresses. A common use for static PAT is to allow Internet users from the public network to access a Web server located in the private network.

In order to get more information about NAT, refer to the NAT Technical Support pages.

This table shows the three blocks of IP address space available for private networks. Consult RFC 1918 for more details about these special networks.

IP Address Space	Class
10.0.0.0 – 10.255.255.255 (10/8 prefix)	Class A
172.16.0.0 – 172.31.255.255 (172.16/12 prefix)	Class B
192.168.0.0 – 192.168.255.255 (192.168/16 prefix)	Class C

Note: The first block is nothing but a single class A network number, while the second block is a set of 16 contiguous class B network numbers, and third block is a set of 256 contiguous class C network numbers.

In this example, the Internet Service Provider (ISP) assigns the DSL subscriber only a single IP address, 171.68.1.1/24. The assigned IP address is a registered unique IP address and is called an inside global address. This registered IP address is used by the entire private network to browse the Internet and also by Internet users that come from the public network to reach the Web server in the private network.

The private LAN, 192.168.0.0/24, is connected to the Ethernet interface of the NAT router. This private LAN contains several PCs and a Web server. The NAT router is configured to translate the unregistered IP addresses (inside local addresses) that come from these PCs to a single public IP address (inside global – 171.68.1.1) to browse the Internet.

IP address 192.168.0.5 (Web server) is an address in the private address space that cannot be routed to the Internet. The only visible IP address for public Internet users to reach the Web server is 171.68.1.1. Therefore, the NAT router is configured to perform a one-to-one mapping between IP address 171.68.1.1 port 80 (port 80 is used to browse the Internet) and 192.168.0.5 port 80. This mapping allows Internet users on the public side to have access to the internal Web server.

This network topology and sample configuration can be used for the Cisco 827, 1417, SOHO77, and 1700/2600/3600 ADSL WIC. As an example, the Cisco 827 is used in this document.

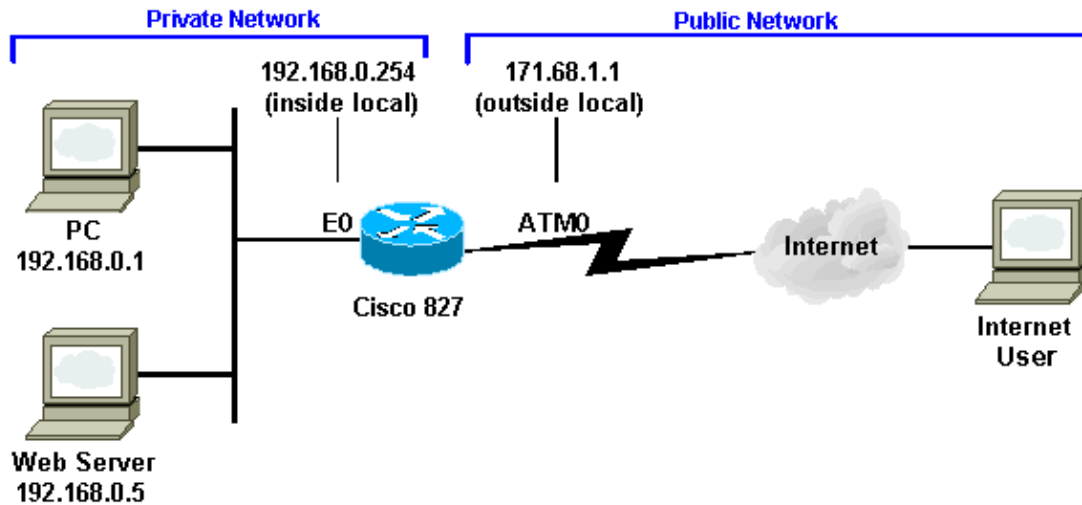
Configure

In this section, you are presented with the information you can use to configure the features described in this document.

Note: In order to find additional information on the commands used in this document, refer to the IOS Command Lookup tool (registered customers only) .

Network Diagram

This document uses this network setup.



Configuration

Cisco 827

Current Configuration:

```
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
!
hostname 827
!
ip subnet-zero
no ip domain-lookup
!
bridge irb
!
interface Ethernet0
ip address 192.168.0.254 255.255.255.0
ip nat inside

!--- This is the inside local IP address and it is a private IP address.

!
interface ATM0
no ip address
no atm ilmi-keepalive
pvc 0/35
encapsulation aal5snap
!
bundle-enable
dsl operating-mode auto
bridge-group 1
!
interface BVI1
ip address 171.68.1.1 255.255.255.240
ip nat outside

!--- This is the inside global IP address.
!--- This is your public IP address and it is provided to you by your ISP.

!
ip nat inside source list 1 interface BVI1 overload

!--- This statement makes the router perform PAT for all the
!--- End Stations behind the Ethernet interface that uses
```

```

!--- private IP addresses defined in access list #1.

ip nat inside source static tcp 192.168.0.5 80 171.68.1.1 80 extendable

!--- This statement performs the static address translation for the Web server.
!--- With this statement, users that try to reach 171.68.1.1 port 80 (www) are
!--- automatically redirected to 192.168.0.5 port 80 (www). In this case
!--- it is the Web server.

ip classless
ip route 0.0.0.0 0.0.0.0 171.68.1.254

!--- IP address 171.68.1.254 is the next hop IP address, also
!--- called the default gateway.
!--- Your ISP can tell you what IP address to configure as the next hop address.

!
access-list 1 permit 192.168.0.0 0.0.0.255

!--- This access list defines the private network
!--- that is network address translated.

bridge 1 protocol ieee
bridge 1 route ip
!
end

```

Verify

From the **show ip nat translation** command output, the `Inside local` is the configured IP address assigned to the Web server on the inside network. Notice that 192.168.0.5 is an address in the private address space that cannot be routed to the Internet. The `Inside global` is the IP address of the inside host, which is the Web server, as it appears to the outside network. This address is the one known to people who try to access the Web server from the Internet.

The `Outside local` is the IP address of the outside host as it appears to the inside network. It is not necessarily a legitimate address. But, it is allocated from an address space that can be routed on the inside.

The `Outside global` address is the IP address assigned to a host on the outside network by the owner of the host. The address is allocated from an address or network space that can be globally routed.

Notice that the address 171.68.1.1 with port number 80 (HTTP) translates to 192.168.0.5 port 80, and vice versa. Therefore, Internet users can browse the Web server even though the Web server is on a private network with a private IP address.

In order to get more information about how to troubleshoot NAT, refer to the [Verifying NAT Operation and Basic NAT Troubleshooting](#).

```

827#
827#show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
tcp 171.68.1.1:80      192.168.0.5:80   ---                ---
tcp 171.68.1.1:80      192.168.0.5:80   198.133.219.1:11000 198.133.219.1:11000
827#

```

Troubleshoot

In order to troubleshoot address translation, you can issue the **term mon** and **debug ip nat detailed** commands on the router to see if the address translates correctly. The visible IP address for outside users to reach the Web server is 171.68.1.1. For example, users from the public side of the Internet who try to reach 171.68.1.1 port 80 (www) are automatically redirected to 192.168.0.5 port 80 (www), which in this case is the Web server.

```
827#term mon
827#debug ip nat detailed
IP NAT detailed debugging is on
827#
03:29:49: NAT: creating portlist proto 6 globaladdr 171.68.1.1
03:29:49: NAT: Allocated Port for 192.168.0.5 -> 171.68.1.1: wanted 80 got 80
03:29:49: NAT: o: tcp (198.133.219.1, 11000) -> (171.68.1.1, 80) [0]
<... snipped ...>
```

Related Information

- [Cisco DSL Technology Support Information](#)
- [Product Support Information](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Apr 09, 2007

Document ID: 12905
