Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Background Information](#)
[Configure](#)
[Network Diagram](#)
[Traffic Flow](#)
[Verify](#)
[Troubleshoot](#)
[Limitation](#)

Introduction

This document describes how to configure Network Address Translation (NAT) to enable communication between server and client which are on different network segments with overlapping IP space.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

> **Note**: This document applies to all Cisco routers and switches that run Cisco IOS.

Background Information

Purpose

Enable communication between a Server and clients on two separated network segments with overlapping IP Space (usually seen when a network merger happens).

Description

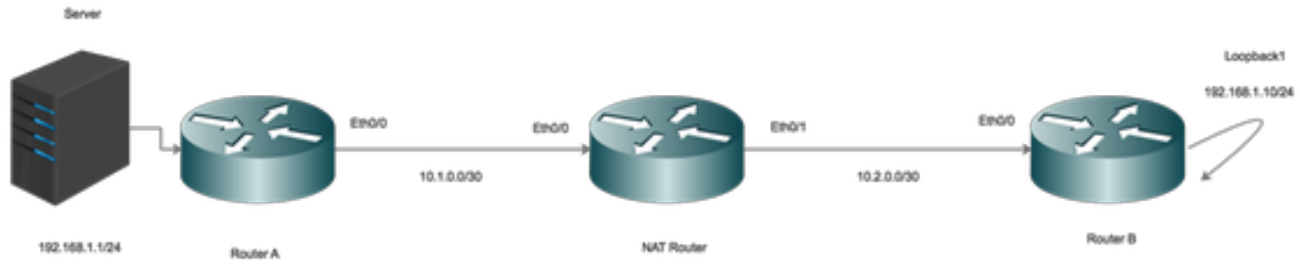
Two networks with same IP space are connected across Router A and Router B, (here we are

using loopbacks to simulate the connected network).

NAT router between Router A and Router B enables the communication between overlapping IP network space.

Configure

Network Diagram



Traffic Flow

- When the Clients initiate traffic to the global IP of Server, the traffic hits the NAT router and the traffic is forwarded to the Server, but when the traffic is returned back to NAT router, the Router fails to forward the traffic as the Server 192.168.1.1 is attached/known on inside interface.
- To fix this, Mask (NAT) the outside Source traffic as it traverses across the NAT router.
- Enable NAT on inside and outside interfaces.

Configure NAT to translate inside local to inside Global Address.

Now, configure NAT statements to translate the source of the clients as they hit the NAT outside interface.

Routing Configuration

Route for the Server. Note that the a specific route for the server is configured pointing towards LAN (Ethernet 0/0)

Route for the Client Network:

Verify

Use this section in order to confirm that your configuration works properly.

As seen, when a client initiates traffic (192.168.1.10) the NAT outside translates the Outside Global to Outside Local (10.100.2.10) and then routes the traffic towards NAT inside interface.

NAT inside interface now translates the destination (10.100.1.1) to inside local address (192.168.1.1) and traffic is moved towards the server.

The server has recieved traffic with source address of 10.100.2.10.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Limitation

In this setup, only the clients can initiate a connection and the connection will be successfull.

The traffic cannot originate from inside (from Server) as the NAT will fail, since there is no NAT entry on outside local to global translation table.