NAT Implementation with Load Balancing.

Ahmad Saad Khan, Akhilesh Akhade, Satyajit Bappanadu Manjunath, Tanay Pande

North Carolina State University.

Project URL: [**https://sites.google.com/a/ncsu.edu/loadbalancing/**](https://sites.google.com/a/ncsu.edu/loadbalancing/)

**Problem Description:**

We plan to implement a NAT for a list of servers with private IP address. The NAT will do IP and port address translation between a public IP address assigned to the NAT and the private IP addresses assigned to the server. All the servers in this scenario run video applications. Further we plan to implement load balancing for the incoming connections to the servers. We will demonstrate two techniques for load balancing – round robin and least rate. Particularly, we plan to demonstrate load balancing for a UDP connection.

**Platform and High Level Design:**

**Platform:** Linux kernel will be used to implement NAT functionality and Load Balancing. The testing will be done in NetLabs.

**Project Area:** Forwarding IP packets incoming to a server based on round robin and least rate approach. This will be done using Linux kernel.

**High level design:** The high level design of the system is shown in Figure 1.

**Components:**

1. Load balancing NAT using least rate (Kernel modules)

a) Destination NAT

b) Source NAT

1. Load balancing NAT using round robin (Kernel modules)

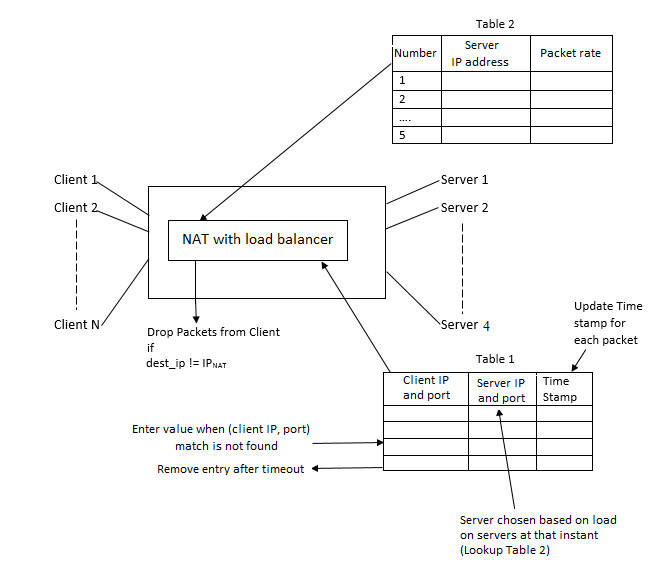
a) Destination NAT

b) Source NAT

1. Video servers
2. Clients

**Preliminary Design and Development Plan:**

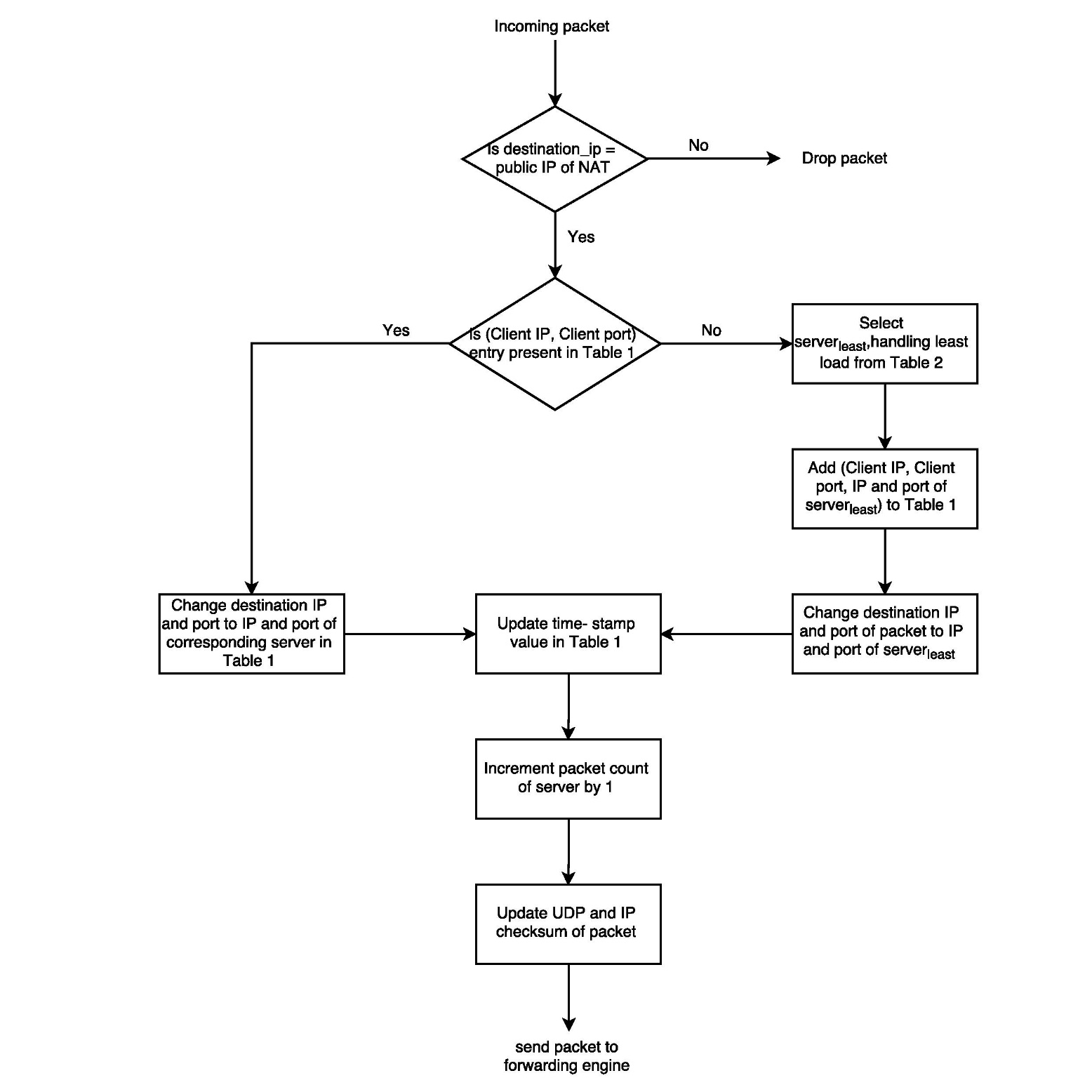
**High level design:**



Figure

**Component Development Phases:**

1. Load balancing NAT using least rate
2. Destination NAT



Figure

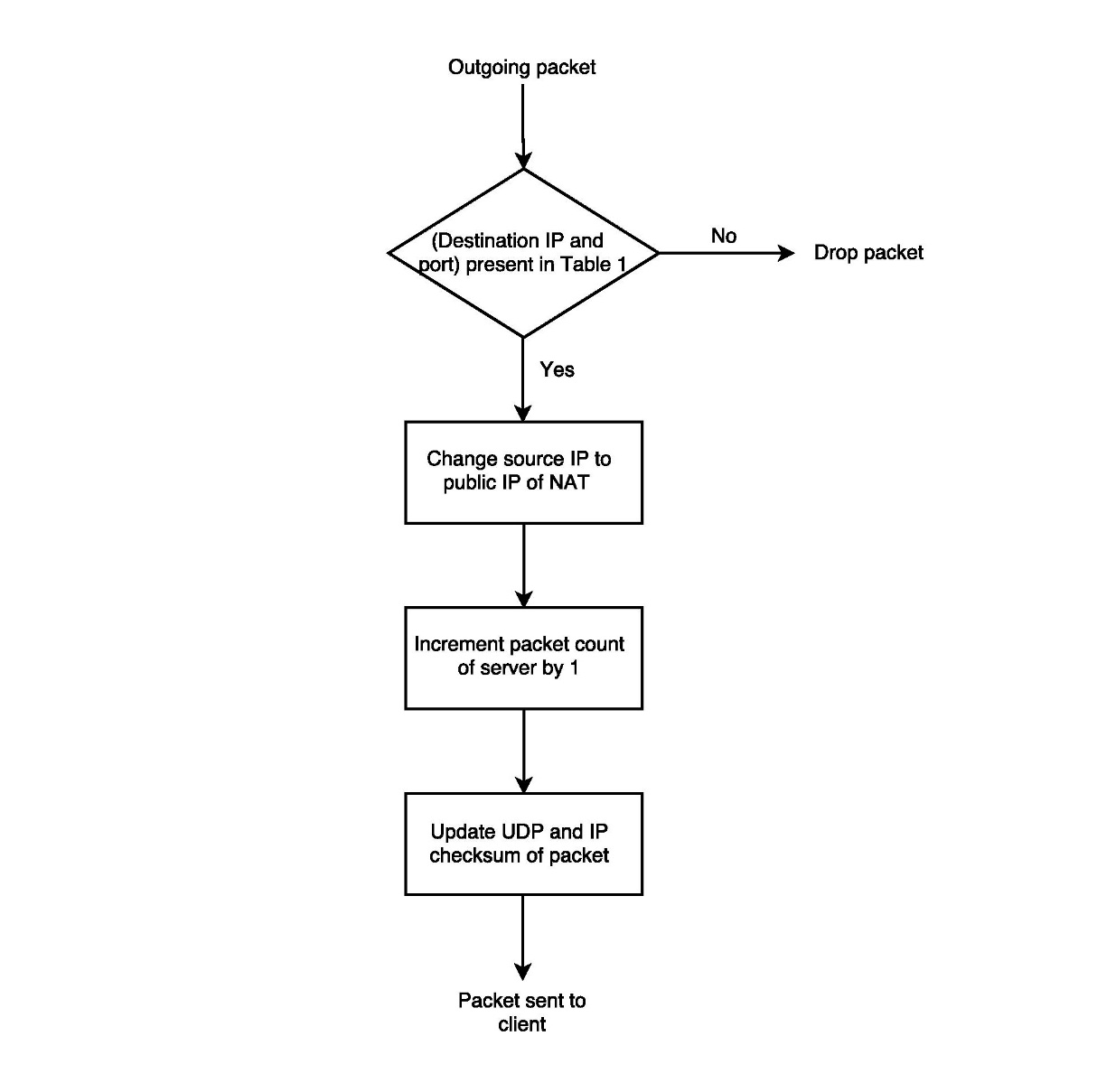
The load balancing NAT handles client requests by selecting the video server for a particular session. The selection of the server is based on the traffic handled by all the servers.

We maintain two tables Table 1 and Table 2. Table 1 consists of client IP, client port, server IP, server port and timestamp which is looked up to determine the server IP & server port for each packet based on its client IP and client port. If an entry is found, the packet’s destination address and port are changed to the corresponding (server IP, server port) at the PRE\_ROUTING hook. The UDP and IP checksums are re- calculated. The timestamp is updated for the particular (client IP, client port) entry in Table 1. The selection of the server in least rate approach is based on the traffic handled by all the servers. A server with the least traffic rate is selected for a new connection.

Table 2 consists of load rates of the servers. The rate at which each server processes a packet is updated every time an incoming/ outgoing packet arrives at NAT. For a new connection, the server with the least load is selected.

A chosen set of entries may be erased from Table 1 after a certain timeout period. This is determined by the timestamp.

1. Source NAT



Figure

All outgoing packets from the video server are forwarded to the particular client which initiated the request. The source address of the packet from the video server is mapped to the public address of the NAT and the source port is mapped to the public port of NAT at the POST-ROUTING hook. The UDP and IP checksums are updated. The packet rate corresponding to the particular server is updated.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Client IP address** | **Client port** | **Server IP address** | **Server port** | **Timestamp** |
| 192.168.1.3 | 1700 | 192.168.2.1 | 2500 | 10/02/2015 4:30 PM |
| 192.168.1.5 | 1800 | 192.168.2.4 | 2100 | 10/02/2015 4:33 PM |
| 192.168.1.5 | 1900 | 192.168.2.1 | 2600 | 10/02/2015 4:32 PM |
| … |  |  |  |  |
| … |  |  |  |  |

Table

|  |  |
| --- | --- |
| **Server IP address** | **Packet rate** |
| 192.168.2.4 | 70 |
| 192.168.2.1 | 50 |
| 192.168.2.2 | 0 |
| 192.168.2.3 | 0 |
| 192.168.2.5 | 0 |

Table

1. Load balancing NAT using round robin
2. Destination NAT

The load balancing NAT handles client requests by selecting the video server for a particular session. The selection of server will be done based on round robin fashion.

Further we maintain a table that consists of client IP, client port, server IP, server port and timestamp which is looked up to determine the server IP and server port for each packet based on its client IP and client port. If an entry is found, the packet’s destination address and port are changed to the corresponding server IP, server port at the PRE\_ROUTING hook. The UDP and IP checksums are re- calculated, the timestamp is updated for the particular client IP, and client port entry in the table. Else, a new entry is added for the particular client IP and client port. The server is selected based on round robin approach. A timestamp is added for the particular connection. The packet rate corresponding to the particular server is updated in Table 2.

1. Source NAT

All outgoing packets from the video server are forwarded to the particular client which initiated the request. The source address of the packet from the video server is mapped to the public address of the NAT and the source port is mapped to the public port of NAT at the POST-ROUTING hook. The UDP and IP checksums are updated. The packet rate corresponding to the particular server is updated.

1. Video servers

These are machines with identical video files. The IP addresses of the servers are private to the internal network

1. Clients

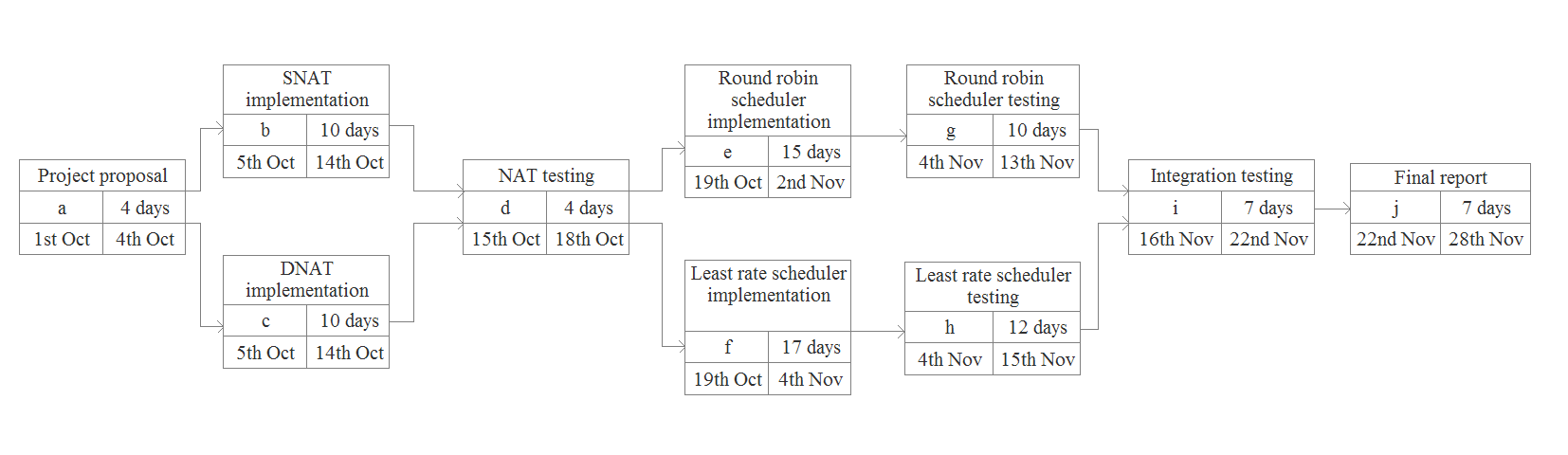
These are machines which request for a particular video file from the servers. The requests are directed to the public IP of the NAT.

**Per Member Responsibilities:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Modules** | Ahmad | Akhilesh | Tanay | Satyajit |
| SNAT | ✓ |  |  |  |
| DNAT |  |  | ✓ |  |
| RR Scheduling |  |  | ✓ | ✓ |
| Least Rate Scheduling | ✓ | ✓ |  |  |
| Testing RR |  |  | ✓ | ✓ |
| Testing Least Rate | ✓ | ✓ |  |  |
| Erasing Entry from Table & Testing |  | ✓ |  | ✓ |
| End to End Testing | ✓ | ✓ | ✓ | ✓ |
| Final report | ✓ | ✓ | ✓ | ✓ |

Table

**Timeline:**



Figure

**Verification and Validation Plan:**

**Test Application:**

We will download video application from the servers. To test the functioning of the NAT and the two load balancing techniques, we will run wireshark on the NAT box, clients and servers and capture the packets flowing.

**Test Plan:**

We will run four video servers having private IP addresses in the subnet 192.168.0.0/29. The servers will be connected to the client through a NAT. We will perform the following tests to verify the functioning of the system.

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Test | Expected Outcome | Conclusion |
| 1 | From a client, ping to the NAT public IP. | The DNAT changes the destination IP & port address of the incoming packet from the client. The SNAT will reverse this change. The client will feel like it is communicating with the NAT public IP address. This we will check by wireshark captures on the client and the NAT box. | NAT is working properly. |
| 2 | Give ping requests with varying rates from 6 clients to the NAT public IP with round robin module. | The 1st client connects to the 1st server. 2nd client to 2nd server….. 5th client to 5th server…. 6th client to 6th server. This can be confirmed through a wireshark capture. | Round Robin Is working properly. |
| 3 | Give ping requests with varying rates from 6 clients to the NAT public IP with least rate module. | The client with the least rate has the maximum number of connections. This can be confirmed through wireshark capture. | Least Rate is working properly. |
| 4 | Do pings from 6 clients to the NAT IP in RR Scheduling. Stop the Ping from one of the clients for time = timeout and start ping from the same client again to the NAT IP. | The client after timeout connects to the 3rd server. | The connection timeout is working properly. |

Table

**Demo Playbook:**

|  |  |  |
| --- | --- | --- |
| Test | Expected Outcome | Conclusion |
| We shall run videos of different data rates on the 4 servers. (If necessary, we will limit the bandwidth of the links from the 4 servers to the NAT to see the difference. Note that the BW of all 4 servers will be same.) We will connect 6-8 clients to the servers. | We expect round robin to show buffering of the video and in some cases even dropping of packets (if the bandwidth we limited is such that it is less than the total output rate of videos.) We expect a better performance in least rate method. Also, in least rate method, we expect to see more number of connections to the server with least video quality through wireshark capture. | Least rate connection shows better performance than round robin in case of load balancing on the servers. |

Table

**References:**

[1] P. Srisuresh and K. Egevang, Traditional IP Network Address Translator (Traditional NAT). IETF RFC 3022, Jan, 2001.

[2] J. Postel, User Datagram Protocol. IETF RFC 768, Aug, 1980.

[3] Load Balancing Scheduling Methods Explained:

<http://loadbalancerblog.com/blog/2013/06/load-balancing-scheduling-methods-explained>

[4] Load Balancing – Least Connections:

<https://www.citrix.com/blogs/2010/09/02/load-balancing-least-connections/>

[5] P. Srisuresh and M. Holdrege, IP Network Address Translator (NAT) Terminology and Considerations. IETF RFC 2663, August, 1999.

[6] F. Audet, Ed. and C. Jennings, Network Address Translation (NAT) Behavioral Requirements for Unicast UDP. IETF RFC 4787, Jan, 2007.