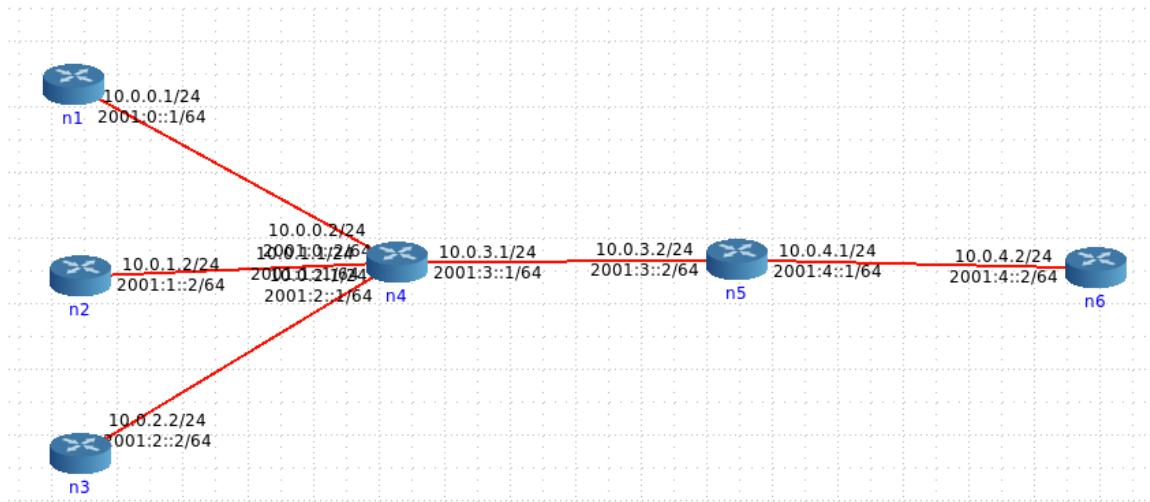


## Firewall Section (10pts)



Useful commands:

- Flush the filter table: `iptables -F`
- Flush the NAT table: `iptables -F -t NAT`
- List the rules in the filter table: `iptables -L`
- List the rules in the filter table with #packet, #bytes matching each rule: `iptables -L -n -v`
- Change the default policy of the INPUT chain of the filter table to DROP: `iptables -P INPUT DROP`

Use IPTTables (<http://www.netfilter.org/projects/iptables/index.html>) to apply the following rules **at n4** to the network below.

For each question, provide a list of firewall rules to apply at n4. Associate rules with each of the requirements above. Please provide screenshots and make each expand to the width of the page.

Example:

1. a. `iptables -A .... etc.`

- 1) (3pts) Drop 50% of all ICMP packets **from n2** (lookup and use the iptables statistics option)
  - Show the iptables command you used?
  - Use ping command to ping from n2 to n6 for 120 seconds. Show the following:
    - Show iptable counts to see # of packet drops corresponding to this rule
      - You can use the command "iptables -L -n -v"

- ii. Show ping statistics reflecting the loss (lost packets should roughly match matched packets count in i.1)
  - c. Reset iptables by flushing the rules as indicated in the “useful commands” section
- 2) (4pts) Imagine n5 is a server that you are running and that n1, n2, and n3 are clients. Node n1 is an attacker who is using hping3 to run a UDP flooding attack against you. Nodes n2 and n3 are good nodes
- a. Set the link between n4 and n5 to be 2Mbps.
  - b. Run a TCP iperf server on node n5: iperf -s -i 1
  - c. Try to run an iperf TCP client from node n2 to node n5. Set client to send 1mbps of data (-b option) for 1 minute (-t option).
    - i. iperf -c 10.0.4.1 -i 1 -b 1M -t 60
  - d. What throughput does iperf report?
  - e. Now, use hping3 to run a SYN flood attack from node n2 to node n6
  - f. Repeat c, d
  - g. Now add a firewall rule **at node n4** to drop all packets coming in from n1. What rule did you add?
  - h. Repeat c, d. If your rule works you should get same throughput as your first run.
- 3) (3pts) Imagine that nodes n1 and n2 are running the same server: nc -k -l 12345. Nodes n5 and n6 are both running “nc” clients and we want to load balance connections between n1 and n2.
- a. Assume nc clients on both n5 and n6 initially send traffic to node n1.
  - b. Use a combination of DNAT and NAT (you can also use the statistics option from 1) to change traffic from n5 so it goes to n2 instead. Ensure bidirectional traffic is possible.
  - c. Use any combination of screenshots to convince me that your solution works.
  - d. Provide the iptables commands you used.
  - e. Show the output of “iptables -L -n -v”, the output of “iptables -t NAT -L -n -v”, and the output of “iptables -t mangle -L -n -v”.