Lab 9: Access Control List, Network Address Translation

Student Name:...
Student No:...

Objectives:

- ✓ Practice access control list and Network Address Translation on Cisco Packet Tracer.

Content:

I. Access Control List

Access control lists (ACLs) provide a means to filter packets by allowing a user to permit or deny IP packets from crossing specified interfaces.

"Just imagine you come to a fair and see the guardian checking tickets. He only allows people with suitable tickets to enter. Well, an access list's function is same as that guardian"

(from http://www.9tut.com/access-list-tutorial)

Access lists filter network traffic by controlling whether packets are forwarded or blocked at the router's interfaces based on the criteria you specified within the access list.

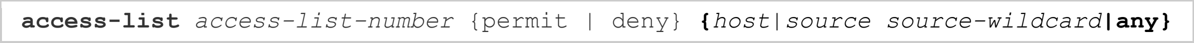
To use ACLs, the system administrator must first configure ACLs and then apply them to specific interfaces. There are 3 popular types of ACL: Standard, Extended and Named ACLs.

Access list type	**Range**
Standard	1-99, 1300-1999
Extended	100-199, 2000-2699

1. Standard IP Access List

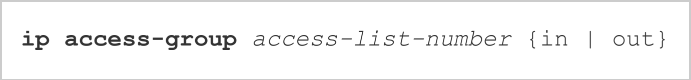
Standard IP lists (1-99) only check source addresses of all IP packets.

Configuration Syntax



```
access-list access-list-number {permit | deny} {host|source source-wildcard|any}
```

Apply ACL to an interface

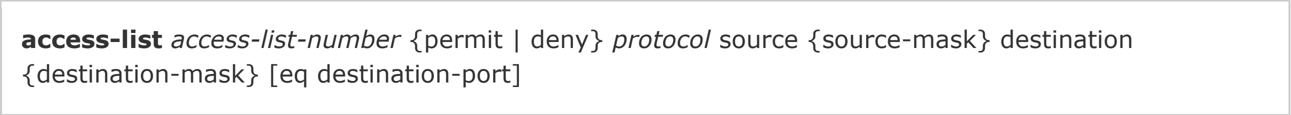


```
ip access-group access-list-number {in | out}
```

2. Extended IP Access List

Extended IP lists (100-199) check both source and destination addresses, specific UDP/TCP/IP protocols, and destination ports.

Configuration Syntax

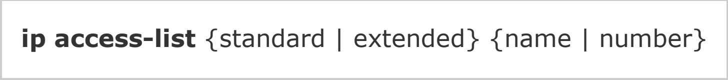


```
access-list access-list-number {permit | deny} protocol source {source-mask} destination
{destination-mask} [eq destination-port]
```

3. Named IP Access List

This allows standard and extended ACLs to be given names instead of numbers

Named IP Access List Configuration Syntax



```
ip access-list {standard | extended} {name | number}
```

Note: Where to place access list?

Standard IP access list should be placed close to destination.

Extended IP access lists should be placed close to the source.

Refer to these links to go into detail:

http://www.9tut.com/access-list-tutorial

http://www.9tut.com/access-list-tutorial/2

II. Network Address Translation

To help extend the life of the IPv4 addressing scheme while the newer IPv6 protocol is developed and deployed, many technologies have been developed. One of the most important of these is IP Network Address Translation. This technology allows a small number of public IP addresses to be shared by a large number of hosts using private addresses. This allows the global Internet to actually have far more hosts on it than its address space would normally support. At the same time, it provides some security benefits by making hosts more difficult to address directly by foreign machines on the public Internet.

Some facts should be considered when configuring and deploying NAT:

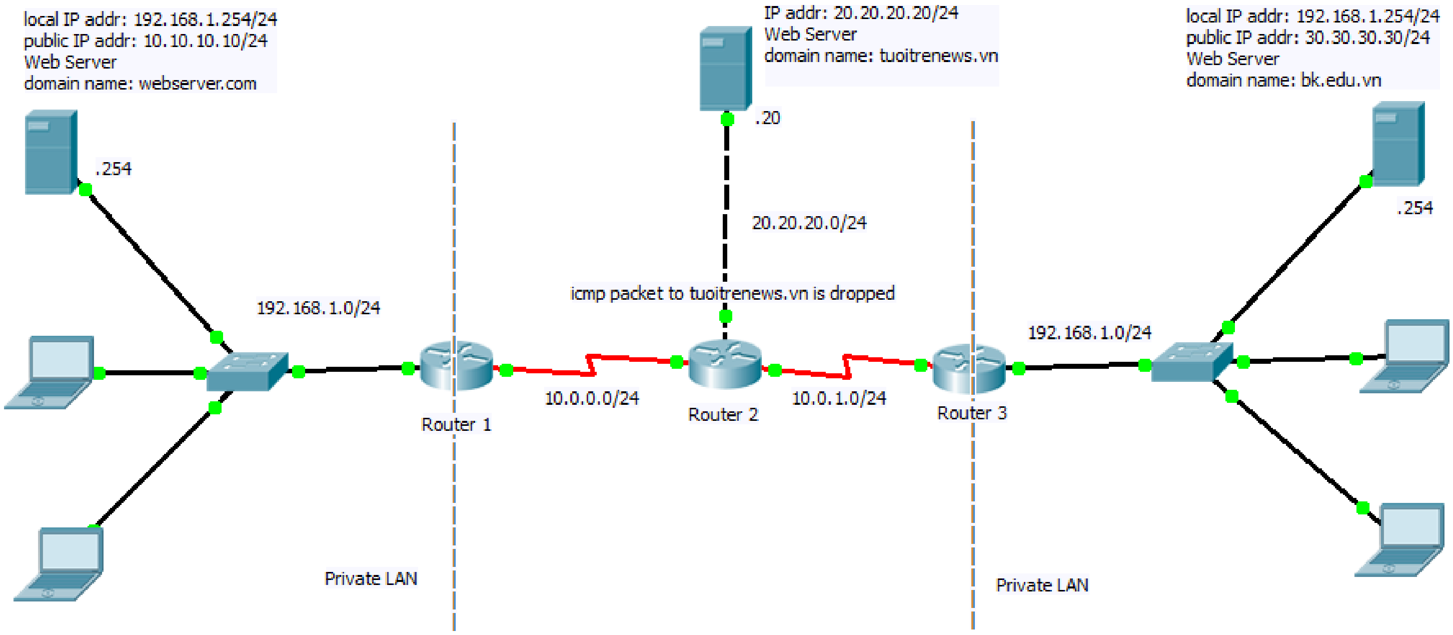
1. Define NAT inside and outside interfaces.
   - Do users exist off multiple interfaces?
   - Are there multiple interfaces going to the internet?
2. Define what you're trying to accomplish with NAT.
   - Are you trying to allow internal users to access the internet?
   - Are you trying to allow the internet to access internal devices (such as a mail server or web server)?
   - Are you trying to redirect TCP traffic to another TCP port or address?
   - Are you using NAT during a network transition (for example, you changed a server's IP address and until you can update all the clients you want the non-updated clients to be able to access the server using the original IP address as well as allow the updated clients to access the server using the new address)?
   - Are you using NAT to allow overlapping networks to communicate?
3. Configure NAT in order to accomplish what you defined above. Based on what you defined in step 2, you need determine which of the following features to use:
   - Static NAT
   - Dynamic NAT
   - Overloading
   - Any combination of the above
4. Verify the NAT operation.

For deeper insight and configuration, refer to:

http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html

III. Practice:

Network topology on Cisco Packet Tracer:


local IP addr: 192.168.1.254/24
public IP addr: 10.10.10.10/24
Web Server
domain name: webserver.com
.254
192.168.1.0/24
Private LAN
Router 1
10.0.0.0/24
IP addr: 20.20.20.20/24
Web Server
domain name: tuoitrenews.vn
.20
20.20.20.0/24
icmp packet to tuoitrenews.vn is dropped
Router 2
10.0.1.0/24
Router 3
local IP addr: 192.168.1.254/24
public IP addr: 30.30.30.30/24
Web Server
domain name: bk.edu.vn
.254
192.168.1.0/24
Private LAN

The computers and routers’ IP addresses, web servers and DNS servers have bee already configured.

Requirements:

1. Configure routing information for Router 1, 2, 3, using RIP. Do not advertise network 192.168.1.0 in RIP.
2. Configure NAT for Router 1 and Router 3 so that each laptop could access tuoitrenews.vn, which is the web server at 20.20.20.20.
3. Configure NAT for Router 1 and Router 3 so that each laptop could access all web servers.
4. Configure Router 2 so that ICMP packet could not reach tuoitrenews.vn server.

IV. Submission

Complete the practice in section III and submit Lab9_<student_code>.pkt onto Sakai.