Computer Networks 1

ACCESS CONTROL LIST

Names: .....
Student No: .....

Objectives

- Understanding Access Control List concepts and its usage
- Practising configuring Access Control List on Cisco Packet Tracer.

Content and Practice

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.

4. Wildcard Mask

Wildcard masks are used with access lists to specify a host, network or part of a network.

The zeros and ones in a wildcard determine whether the corresponding bits in the IP address should be checked or ignored for ACL purposes.

You have been familiar with “network mask” (netmask) concept. For example, the network 192.168.1.0/24 has the network mask 255.255.255.0.

Wildcard mask is the inversion of network mask. For example, consider network 172.23.16.0/20, its network mask is 255.255.240.0. This network mask is converted into wildcard mask by converting all bits 0 to 1 and all bits 1 to 0.

255 = 1111 1111 -> convert into 0000 0000

240 = 1111 0000 -> convert into 0000 1111

0 = 0000 0000 -> convert into 1111 1111

Therefore 255.255.240.0 can be written in wildcard mask as 0000000.00000000.00001111.11111111 = 0.0.15.255

Remember, for the wildcard mask, 1′s are **I DON’T CARE**, and 0′s are **I CARE**.

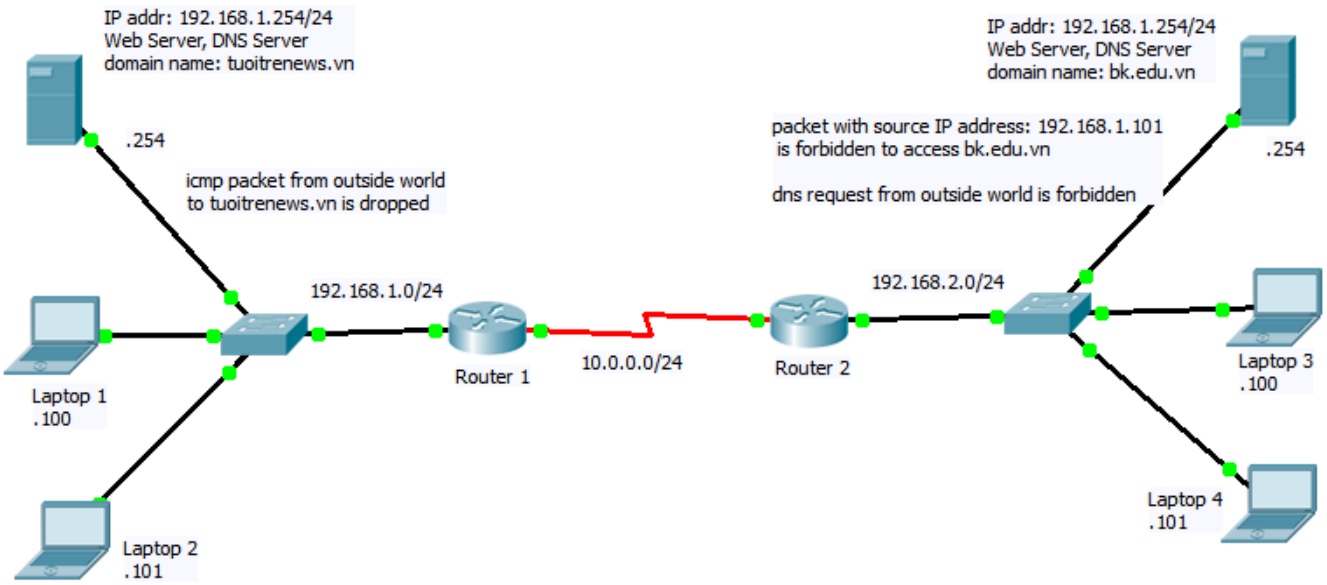
Refer to these links to go into detail:

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

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

II. Practice

Network topology on Cisco Packet Tracer:



The computers and routers' IP addresses, web servers and DNS servers have been 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. Ensure every host and server is reachable from others:
   - Ping from laptop 2 to server bk.edu.vn.
   - From command line of laptop 2, enter the command: nslookup bk.edu.vn 192.168.2.254
   - Open web browser on laptop 2, access to server bk.edu.vn
   - Ping from laptop 3 to server tuoitrenews.vn.
3. Configure Router 2 so that packet with source IP address: 192.168.1.101 is forbidden to access bk.edu.vn (hint: use *standard ip access list*)
4. Configure Router 1 so that ICMP packet from outside world could not reach tuoitrenews.vn server. (hint: use *extended ip access list*)

5. Configure Router 2 so that dns request from outside world to server 192.168.2.254 is forbidden.
6. Ensure all configurationsc are right:
    - Ping from laptop 2 to server bk.edu.vn: **fail**
    - Ping from laptop 1 to server bk.edu.vn: **successful**
    - From command line of laptop 1, enter the command: nslookup bk.edu.vn 192.168.2.254: **successful**
    - Open web browser on laptop 2, access to server bk.edu.vn: **fail**
    - Open web browser on laptop 1, access to server bk.edu.vn: **successful**
    - Ping from laptop 3 to server tuoitrenews.vn: **fail**
    - Open web browser on laptop 3, access to server tuoitrenews.vn: **successful**

III. Submission

Complete all tasks in section II, then submit Lab11_<student_code>.pkt onto Sakai.