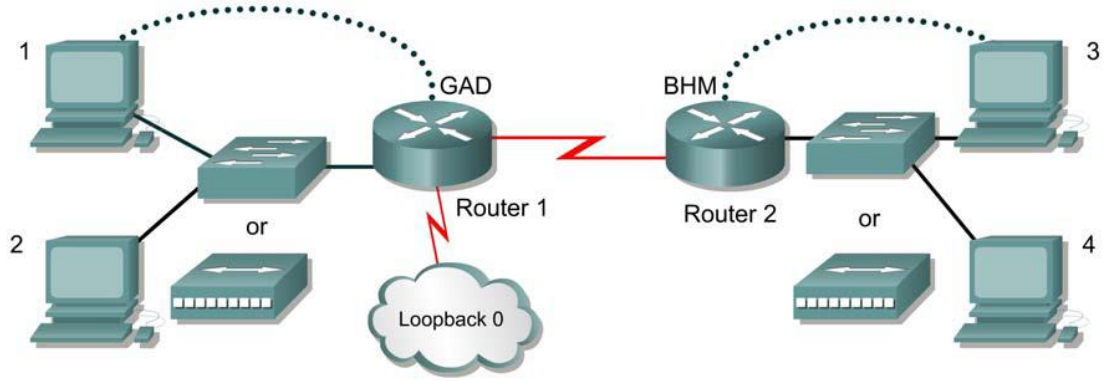
Lab – Topic 8

The answer sheet URL is posted on OLE. Please login to your OUHK Google Gmail account (gxxxxxxx@study.ouhk.edu.hk) and submit your answer online. Due date: Wed, 5 May 2021, 23:59

Lab 11.2.1b Standard ACLs



Router Name	Gigabit Ethernet 0/0 Address	Interface type	Serial 0/0/0 Address	Loopback0	Routing Protocol
GAD	192.168.1.1/24	DCE	192.168.2.1/24	172.16.1.1/24	RIP
BHM	192.168.3.1/24	DTE	192.168.2.2/24	-	RIP

Host	IP Address	Subnet Mask	Gateway
1	192.168.1.2	255.255.255.0	192.168.1.1
2	192.168.1.3	255.255.255.0	192.168.1.1
3	192.168.3.2	255.255.255.0	192.168.3.1
4	192.168.3.3	255.255.255.0	192.168.3.1

Objective

- Plan, configure, and apply a standard ACL to permit or deny specific traffic and test the ACL to determine if the desired result were achieved.

Background/Preparation

Setup a network similar to the diagram.

For users of CISCO router:

- **Note**: Go to the "Erasing and reloading the router" instructions. Perform those steps on all routers in this lab assignment before continuing.
- Start HyperTerminal session:
  1. Download putty.
  2. Choose "Serial" as the Connection type.
  3. Click "Open" button.

For users of CISCO Packet Tracer:

- Place two 2901 routes (with one HWIC-2T module installed on each route) as Router 1 and Router 2.

Lab – Topic 8

Scenario

The company home office in Gadsden (GAD) provides service to branch offices such as the Birmingham (BHM) office. These offices have some minor security and performance concerns. A Standard ACL needs to be implemented as a simple and effective tool to control traffic.

Infrastructure

Host #3 represents the kiosk station that needs to have its access limited to the local network.

Host #4 represents another host in the BHM office and the Loopback 0 interface on the GAD router represents the Internet.

Step 1 Basic Router Interaction

a. Interconnect the routers as shown in the diagram.

Step 2 Basic Configuration

a. Refer to the table on the first page and setup the router and host configurations including RIP configuration. Verify reachability by pinging all systems and routers from each system.

b. To simulate the Internet, add the following configuration to the GAD router.

```
GAD(config)#interface loopback0
GAD(config-if)#ip address 172.16.1.1 255.255.255.0
GAD(config-if)#exit
GAD(config)#router rip
GAD(config-router)#network 172.16.0.0
GAD(config-router)#^z
```

* ^z is the output when CTRL-Z is pressed.

Step 3 Establish Access List Requirements

a. The kiosk station (host 3) needs to have its access limited to the local network. An ACL is needed to prevent traffic from this host from reaching any other networks. The access control list should block traffic from this host and not affect other traffic from this network. A standard IP ACL satisfies this requirement as it filters based on the source address to any destination.

What source address of the kiosk? _____

Step 4 Plan the Access List Requirements

a. It has been determined that this ACL will require 2 logical steps. Each of these steps can be accomplished with one statement each. As a planning tool, a text editor (Notepad on your PC) can be used to organize the logic and then write the list. In the text editor enter the logic by typing:

```
! stop traffic from host 3
! permit all other traffic
```

b. From this logic the actual ACL will be written. Using the tables below, document the information for each statement.

stop traffic from host 3			
Access-list #	Permit or deny	Source address	Wildcard mask
i.	ii.	iii.	iv.

permit all other traffic			
Access-list #	Permit or deny	Source address	Wildcard mask
v.	vi.	vii.	viii.

Note:

- access-list # can be any number from 1 to 99.
- wildcard mask is determine by subtracting the normal mask from 255.255.255.255.

c. What would be the result of not including a statement to permit all other source addresses?

_____

d. What would be the result of reversing the order of the 2 statements in the list?

_____

e. Why are both statements using the same ACL number?

_____

f. The final step in the planning process is to determine the best location for the access list and the direction the list should be applied. Examine the internetwork diagram and choose the appropriate interface and direction. Document this in the table below:

Router	Interface	Direction

Step 5 Write and Apply the ACL

a. Using the previously constructed logic and information of the access list, complete the commands in the text editor. The list syntax should look similar to:

```
! stop traffic from host 3
   access-list # deny address wildcard
! permit all other traffic
   access-list # permit address wildcard
```

b. Add to this text file the configuration statements to apply the list.

The configuration statements take the form of:

```
interface type #/#
ip access-group #{in, out}
```

c. Now the text file configuration needs to be applied to the router. Enter the configuration mode on the appropriate router and copy and paste the configuration. Observe the CLI display to ensure no errors were encountered.

Step 6 Verify the ACL

Now that the ACL is completed, the ACL needs to be confirmed and tested.

a. The first step is to check the list to see if it was configured properly on the router. To check the ACL logic use the **`show access-lists`** command. Record the output.

_____

_____

_____

Note:

- The source/source-wildcard of 0.0.0.0/255.255.255.255 means "any".
- The source/source-wildcard of 192.168.3.2/0.0.0.0 is the same as "host 192.168.3.2".

b. Next, verify that the access list was applied to the proper interface and in the correct direction. To do this, examine the interface with the **`show ip interface`** command. Look at the output from each interface and record the lists applied to the interface.

i. Interface _____

ii. Outgoing access list is _____

iii. Inbound access list is_____

c. Finally, test the functionality of the ACL by trying to send packets from the source host and verify that is to be permitted or denied as appropriate. In this case, ping will be used to test this. Check each [ ] if the ping test is success.

```
[  ] verify that host 3 CAN ping host 4
[  ] verify that host 3 CANNOT ping host 1
[  ] verify that host 3 CANNOT ping host 2
[  ] verify that host 3 CANNOT ping GAD g0/0
[  ] verify that host 3 CANNOT ping GAD LO0
[  ] verify that host 4 CAN ping host 1
[  ] verify that host 4 CAN ping host 2
[  ] verify that host 4 CAN ping GAD g0/0
[  ] verify that host 4 CAN ping GAD LO0
```

Step 7 Check Point: Send your screen capture to the instructor by email within the lab period.

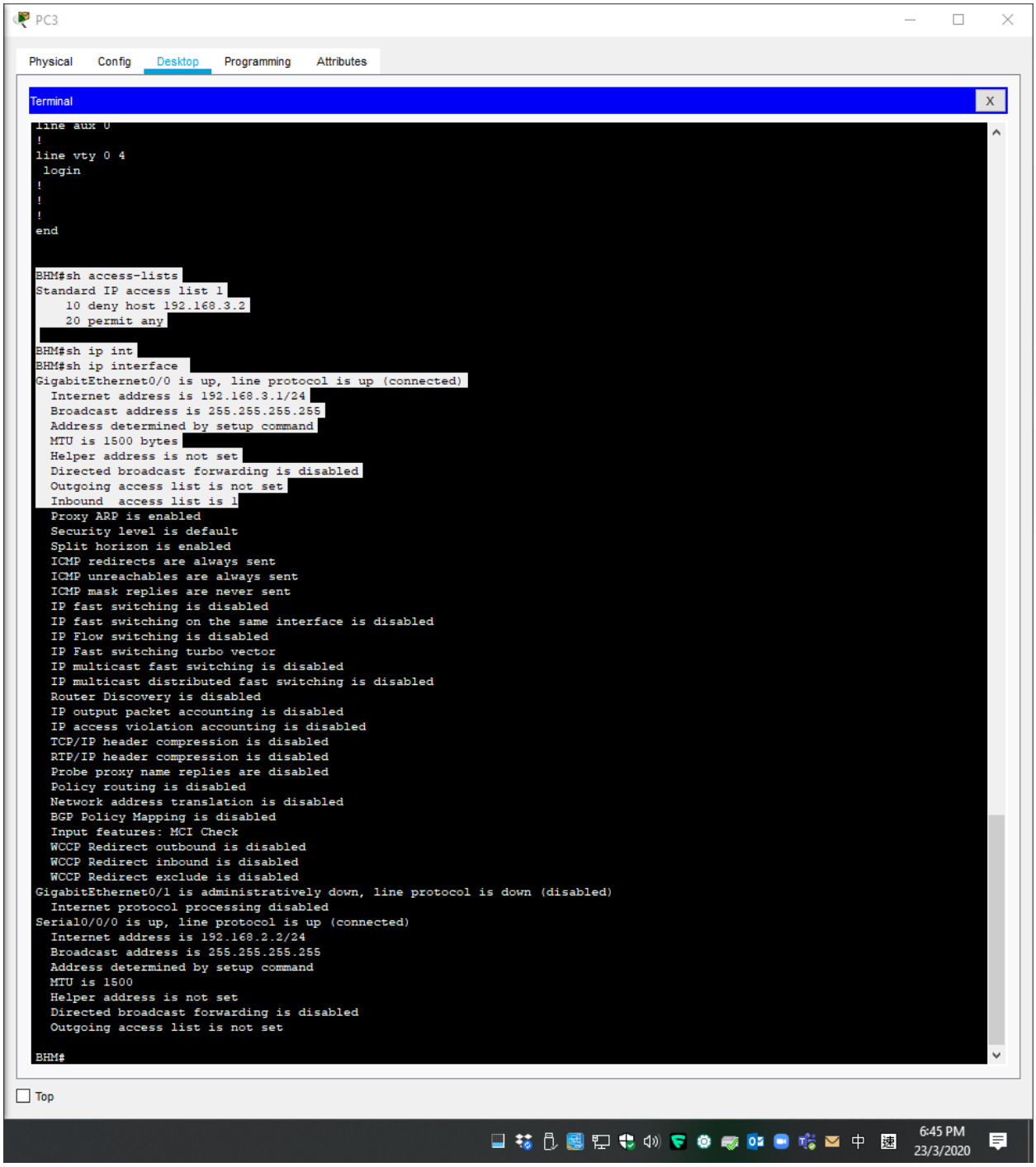
a. Take one screen capture with the following items. (Sample capture is on next page).

I. CLI of the routers showing the prompt and the output on Step 6 (a) and (b).
II. ~~The Computer name and Domain~~.
III. The date and time of your capture.

b. Save the screen capture to a Word file with filename “your_8_digit_student_number-topic8.docx”. (Eg. **12345678-topic8.docx**).

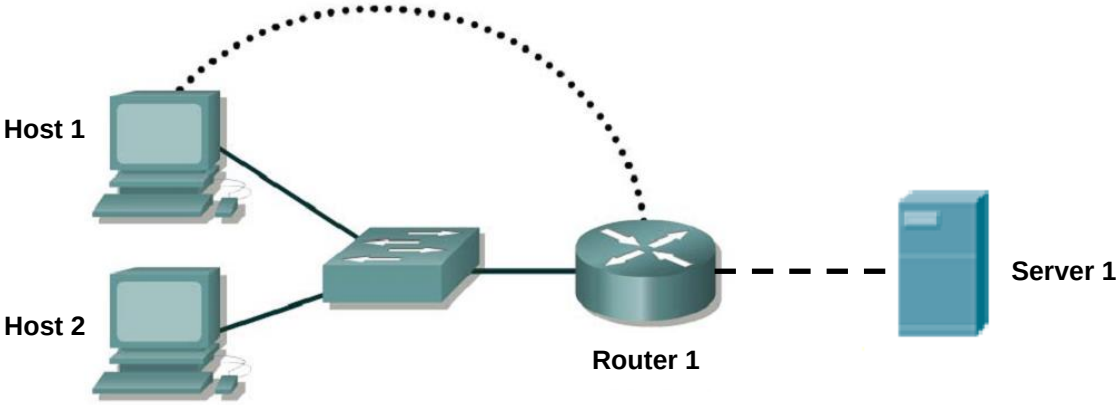
c. Email your saved file to thluk@ouhk.edu.hk (subject: **topic 8**).

Lab – Topic 8


PC3
Physical
Config
Desktop
Programming
Attributes
Terminal
line aux 0
!
line vty 0 4
login
!
!
!
end
BHM#sh access-lists
Standard IP access list 1
10 deny host 192.168.3.2
20 permit any
BHM#sh ip int
BHM#sh ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 192.168.3.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is 1
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
GigabitEthernet0/1 is administratively down, line protocol is down (disabled)
Internet protocol processing disabled
Serial0/0/0 is up, line protocol is up (connected)
Internet address is 192.168.2.2/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
BHM#
Top
6:45 PM
23/3/2020

Lab – Topic 8

Lab 11.2.2a Configuring Extended Access Lists



Router Designation	Router Name	Gigabit Ethernet 0/0 Address	Gigabit Ethernet 0/1 Address
Router 1	GAD	192.168.1.1/24	192.168.2.1/24

Host	IP Address	Subnet Mask	Gateway
Host 1	192.168.1.2	255.255.255.0	192.168.1.1
Host 2	192.168.1.3	255.255.255.0	192.168.1.1
Server 1	192.168.2.2	255.255.255.0	192.168.2.1

Objective

- Configure, and apply an extended ACL to permit or deny specific traffic.
- Test the ACL to determine if the desired results were achieved.

Background/Preparation

Cable a network similar to the one in the diagram.

Step 1 Configure the GAD router

a. On the GAD router, enter the global configuration mode and configure the hostname as shown in the chart. Then configure the Gigabit Ethernet interfaces on the router according to the chart.

Step 2 Configure the hosts on the Ethernet segments

Step 3 Save the configuration information from the privileged EXEC command mode

```
GAD#copy running-config startup-config
```

Step 4 Confirm connectivity by pinging the default gateway from both hosts and the server.

a. If the pings are not successful, correct the configuration and repeat until they are successful.

Step 5 Connect to the Server 1 using Web browser

a. From a host, connect to the Server 1 using a Web browser to ensure that the Web server function is active.

Step 6 Prevent access to HTTP (port 80) from the Ethernet interface hosts

a. Create an access list that will prevent Web browsing access to the Server 1 from the 192.168.1.0 network.

b. At the router configuration prompt type the following commands:

```
GAD(config)#access-list 101 deny tcp 192.168.1.0 0.0.0.255 any eq 80
GAD(config)#access-list 101 permit ip any any
```

c. Why is the second statement needed? _____

Step 7 Apply the access list to the interface

a. At the GigabitEthernet 0/0 interface mode prompt type:

```
GAD(config-if)#ip access-group 101 in
```

Step 8 Ping the server from the hosts

a. Were these pings successful? _____

b. If they were, why? _____

Step 9 Connect to the Server 1 using the web browser

Was the browser able to connect? _____

Upon completion of the previous steps, logoff by typing **exit**. Turn the router off.