**Họ và tên: Ngô Tuấn Kiệt**

**MSSV: 21521034**

**Step 1: Verify Connectivity in the New Company Network**

First, test connectivity on the network as it is before configuring the ACLs. All hosts should be able to ping all other hosts.

PC-1 to Branch PC

**Text

Description automatically generated**

Một vài cái khác

A picture containing shape

Description automatically generated

### Step 2: Configure Standard and Extended ACLs per Requirements.

**ACL 1 Requirements**

o    Create ACL **101**.

o    Explicitly block FTP access to the Enterprise Web Server from the internet.

o    No ICMP traffic from the internet should be allowed to any hosts on HQ LAN 1

o    Allow all other traffic.

Text, letter

Description automatically generated

**ACL 2 Requirements**

o    Use ACL number **111**

o    No hosts on HQ LAN 1 should be able to access the Branch Server.

o    All other traffic should be permitted.

Text

Description automatically generated

**ACL 3: Requirements**

o    Create a named standard ACL. Use the name **vty\_block**. The name of your ACL must match this name exactly.

o    Only addresses from the HQ LAN 2 network should be able to access the VTY lines of the HQ router.

Text, letter

Description automatically generated

**ACL 4: Requirements**

o    Create a named extended ACL called **branch\_to\_hq**. The name of your ACL must match this name exactly.

o    No hosts on either of the Branch LANs should be allowed to access HQ LAN 1. Use one access list statement for each of the Branch LANs.

o    All other traffic should be allowed.

Text

Description automatically generated

### Step 3: Verify ACL Operation.

a.     Perform the following connectivity tests between devices in the topology. Note whether or not they are successful.

**Note**: Use the **show ip access-lists** command to verify ACL operation. Use the **clear access list counters**command to reset the match counters.

#### **Questions:**

Send a ping request from Branch PC to the Enterprise Web Server. Was it successful? Explain.

* Successful because it was permitted by ACL

Text

Description automatically generated

Which ACL statement permitted or denied the ping between these two devices? List the access list name or number, the router on which it was applied, and the specific line that the traffic matched.

//

* Branch(config-ext-nacl)#permit ip any any

//

* Branch(config-if)#ip access-group branch\_to\_hq out
* Branch\_to\_hq on the branch is permit ip any

Attempt to ping from PC-1 on the HQ LAN 1 to the Branch Server. Was it successful? Explain.



* Failed
* Deny by Branch access-list

Which ACL statement permitted or denied the ping between these two devices?

* Access-list 111 deny ….

Open a web browser on the External Server and attempt to bring up a web page stored on the Enterprise Web Server. Is it successful? Explain.

* The external server can access a webpage on Enterprise WebServer, the traffic is not blocked to the Enterprise Web Server.

Which ACL statement permitted or denied the ping between these two devices?

* Access-list 101 permit ip any any

b.     Test connections to an internal server from the internet.

#### **Questions:**

From the command line on the Internet User PC, attempt to make an FTP connection to the Branch Server. Is the FTP connection successful?



Which access list should be modified to prevent users from the Internet to make FTP connections to the Branch Server?

* Access-list 101 on HQ router

Which statement(s) should be added to the access list to deny this traffic?

* Deny tcp any host 192.168.2.45 eq 21