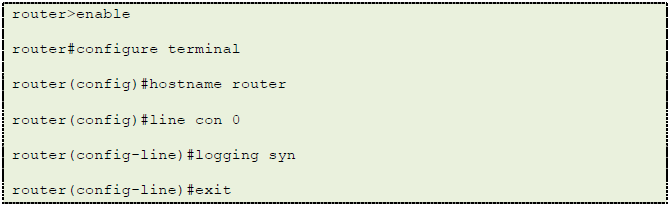
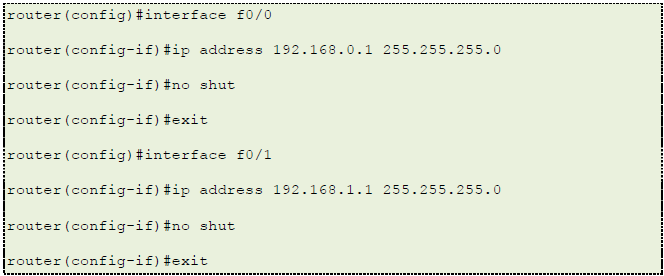
# **Lab 4: Cisco Router ACL Configuration**

Type the following commands to configure R1 (tip - use the up-arrow key to recall previously-entered commands):

**Entering configuration mode and configuring individual line:**

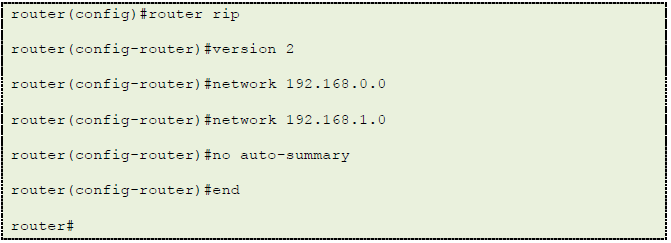


**Configuring interfaces connected to C1, C2, and C3:**



**Configuring Routing Information Protocol (RIP):**

*RIP* is the dynamic routing protocol used in ARPANET, the original Internet. RIP calculates how long route packets take by comparing the number of hops the packet requires to reach its destination. RIP maintains a routing table on each router that is kept accurate by sending routing update messages regularly and whenever the network topology changes.



You can also find detailed descriptions of each command.

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig24.png

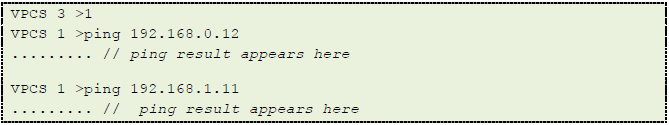
Typing the ‘?’ key at the prompt will give you a list of all commands that you can use in current state.

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig25.png

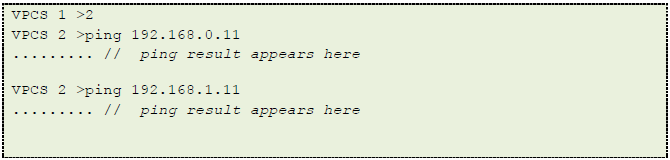
Typing a command followed by the ‘?’ character will give you details on the parameters of the command.

**Step 10**

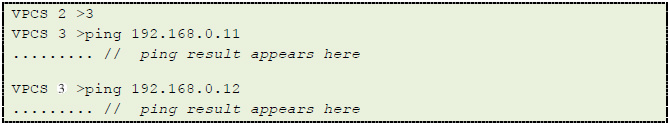
Go to the VPCS window. Type “1” to switch to **vpcs1**. Ping **vpcs2** (192.168.0.12) using the command below. If you have successfully configured everything, you will see connectivity from **vpcs1**, through the router to **vpcs2**, then to **vpcs3**.



Try the following commands to ping from **vpcs2** to **vpcs1** and **vpcs3**.



Try the following commands to ping from **vpcs3** to **vpcs1** and **vpcs2**.



The following commands may be useful in verifying virtual PC configuration. Command “show” displays the configuration of all virtual PCs.

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig29.png

Command “ping” can be used to check if a virtual PC is connected to the network. Using the [Lab Setup Diagram](https://www.up.ist.psu.edu/documentation/IST554/Cisco_ACL.php#diagram) in this document, determine if your networks are connected to the router. Start at Cloud 1, ping the router interface before the router, ping the router interface after the router and ping Cloud 2.

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig30.png

**Task 3 - Configure Access Control List and Test**

In this scenario, you are the Network Administrator and the Intrusion Detection System Analyst calls you at 3:00 am. He is receiving attack traffic from a machine. It seems C2 has been infected with malware and needs to be cut off from the network. You will set an access control list on the interface to stop all traffic from the infected host while allowing traffic from the uninfected host to continue. Then, you get to go back to bed.

**Step 1**

Begin to configure and deploy the ACL by opening the Router console:

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig31.png

This command is only needed if you closed down the terminal and reopened a new one:

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig32.png

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig33.png

This command creates an extended access list named 101 and puts you in a position to edit that list:

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig34.png

This command denies all traffic between the infected host and the host we wish to protect:

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig35.png

This command allows traffic between all other hosts and the machine we wish to protect. The access list starts at the top of the list and continues till it finds a rule that applies to the packet it is examining and then stops looking. So, adding this permit rule at the end allows any traffic not affected by the deny rule to continue:

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig36.png

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig37.png

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig38.png

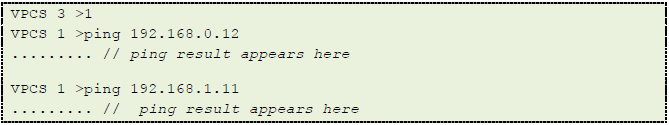
This command applies the access list we prepared to the inbound traffic of the interface closest to the infected host.

https://www.up.ist.psu.edu/documentation/ist554/cisco_acl/Fig39.png

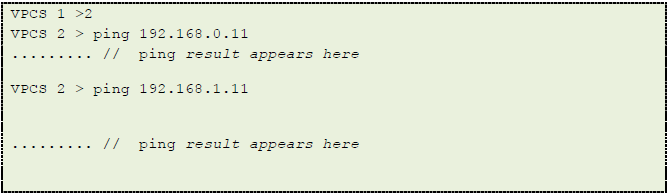
This set of commands will create a list of rules that will deny access between the infected system while permitting traffic with the uninfected system.

**Step 2**

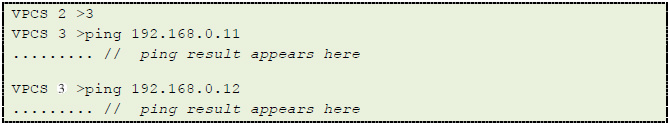
Test the ACL. Return to the VPCS screen. Type “1” to switch to **vpcs1**. Ping **vpcs2** (192.168.0.12) using the command below. You will see connectivity from **vpcs1**, through the router to **vpcs2**, then to **vpc3**.



Try the following commands to show connectivity from **vpcs2** to **vpcs1** and **vpcs3**:



Try the following commands to show connectivity from **vpcs3** to **vpcs1** and **vpcs2**:



If the access list is working properly, there should be connectivity between all of the hosts except 192.168.0.12 and 192.168.1.11.

**Links:**

Official Cisco Guide   
[Official Cisco Guide](http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml)  
Cisco Access Control Lists Tutorial Videos   
Part 1   
[Cisco Access Control Lists Tutorial Video (PART 1)](http://www.youtube.com/watch?v=jHW_Bv8VN94)  
Part 2   
[Cisco Access Control Lists Tutorial Video (PART 2)](http://www.youtube.com/watch?v=AOhSJZfPlYs)  
Part 3   
[Cisco Access Control Lists Tutorial Video (PART 3)](http://www.youtube.com/watch?v=WckaVR3FkGU)

**Report:**

Clearly state your results of this project. You are expected to hand in a report in the following format:

* A Cover Page (including lab title) with your name or team name
* A Table of Contents with page numbers
* Use double-spaced type for convenient grading.
* Number each page, size 12 font, single column.
* Save the Microsoft Word document with your name or team name in the title. Upload the document into the appropriate dropbox.

The report should include all sections listed below with each section covering all of the topics described below. You do not need to itemize each topic. Take screenshots, if necessary.