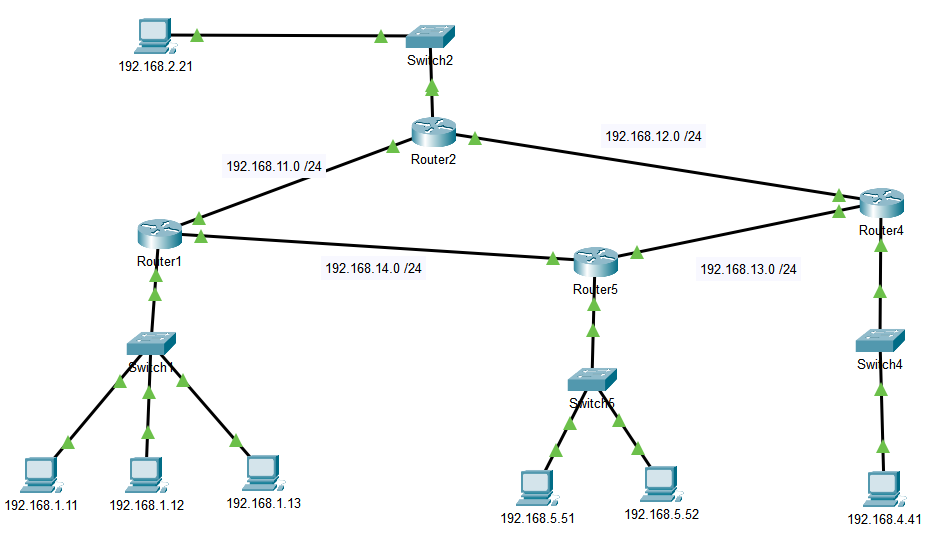
Before running this lab, please read through Chapter 26 – *Advanced* *IPv4 Access Control Lists* in the 100-105 textbook, and make sure you understand the concepts in the slide deck. The point of the lab isn’t to teach you new material; it’s to reinforce what the textbook and slides cover.

This lab refers to PC based on the last byte of their IP address. For example, PC**21** is the PC with IP address 192.168.2.**21.**

**Part 1: Initial Topology**

**Step 1: Create and Configure the initial topology**

1. In Packet Tracer turn simulation on – click on the SHOW NONE to clear the list, then click on EDIT FILTERS so you only filter ICMP frames
2. Create the below topology.  
   
3. Configure all PC’s with IP addresses, subnet masks, and default gateways. Configure all routers with IP addresses.
4. Create a STATIC ROUTE on R1 so that packets destined for 192.168.4.0 go through R2.
5. Create a STATIC ROUTE on R4 so that packets destined for 192.168.1.0 go through R5.
6. Configure RIP v2 on all routers

At this point all PC’s should be able to ping each other. Pinging from PC11 to PC41 should take the upper route (R1 – R2 – R4) and return via the bottom route (R4 – R5 – R1).

**Part 2: Extended ACL’s**

Number your ACL’s 1xy where x is the router number (1,2,3,4,5) and y is the port you will assign it to. For example, ACL 152 will be on router 5 assigned to port 2.

1. Router 1
   1. Block packets from PC11 to subnet 192.168.5.0 (use a mask)
   2. Block packets from subnet 192.168.1.0 (use a mask) to 192.168.2.21
2. Open a text box and enter the ACL subcommands to accomplish the following:  
   1. Block TCP packets to subnet 192.168.5.0 (use a mask)
   2. Block all IP packets from port 80
   3. Block all IP packets from 192.168.5.51

**Lab Completion**

1. Open a textbox and include all new commands introduced in the first section of module 11.
2. Save your packet file as Lab11a-Lastname and submit via iLearn.