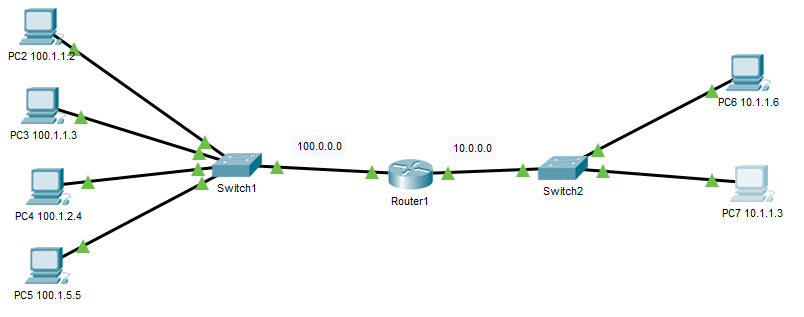
**Objectives**

Before running this lab, please read through Chapter 25 - *Basic 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 te textbook and slides cover.

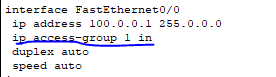
Up to now a properly configured network allows all packets to pass through routers. Creating an Access Control List allows us to limit/control which packets are permitted or denied. Again, the theory behind this operation is explained in the text.

**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. IMPORTANT: Update the router to add another port for later use.
4. Note that we are using a CLASS A network (10.x.x.x) – so our IP and subnet masks will be 255.0.0.0!
5. Configure the router’s ports for IP address 100.0.0.1 and 10.0.0.1.
6. Configure all PC’s – note that the gateway routers will be 100.0.0.1 and 10.0.0.1
7. Important: At this point ping from each PC to PCs on the other subnet so that you have full connectivity. If a ping fails debug the wrong IP address or gateway address.

**Part 2: Access Group Creation – Specific Address (no mask)**

1. Since there are no ACL’s all the pings work; all packets are allowed.
2. Let’s create our first access group.
   1. Enter global config mode on the Router.
   2. Enter **ip access-list standard 1** - we enter config-std nacl mode
   3. Enter **99 deny any** - a default row to deny all packets
   4. Enter **do show ip access-lists** *-* to verify that your ACL was created
   5. Examine the list – do you understand what you see?
3. While the access group is created, we need to enable it to a router port.
   1. Enter configuration mode for the port connected to Switch 1.
   2. Enter **ip access-group 1 in**
4. Look at the running configuration and verify that the port has access group 1 assigned.  
    
5. Now ping from the PC2 thru PC5 to PC6. It should fail. Why?
6. Let’s add a permit for one specific host:
   1. Enter **ip access-list standard 1**  -- we enter config-std nacl mode
   2. Enter **10 permit 100.1.1.2** -- we want this before row 99 – why?
   3. Enter **do show ip access-lists**  *--* you should seerows 10 and 99
   4. Ping from PC2 to PC6 - It should now work! (*you may have to ping twice*)  
      Ping from PC3 to PC6 - It should still fail.
7. Ping from PC6 to PC3 and watch what happens.   
   Why does the packet pass through going from right to left but fail returning left to right?
8. Let’s add a few more commands:
   1. **15 permit 100.1.1.3** - then test – does the ping work?
   2. **no 15 -** ping again, it shouldfail again
   3. **5 deny 100.1.2 -** ping PC4 to PC6 should work
   4. **do show ip access-lists -** see that that the commands sequence themselves
   5. ping PC2 to PC6 - it should fail because SEQ 5 denies the packet
   6. **no 5 -** deletes that deny command

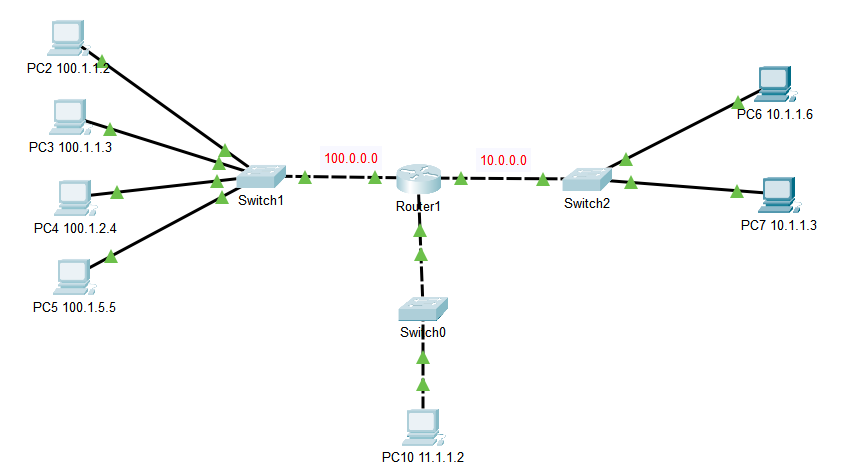
**Part 3: Access Group Creation – Using masks**

1. Ensure that all sequences except 99 have been deleted from access list #1.   
   Enter **do show ip access-lists.** IfACL 1 has any entries besides “99 DENY ANY” delete the sequences via the NO command.
2. Now add a permit for all addresses that have 100.1.1 as their first 3 bytes   
   (addresses 100.1.1.2 and 100.1.1.3).
   1. **ip access-list standard 1**
   2. **10 permit 100.1.1.0 0.0.0.255** -- note the mask
   3. **do show ip access-lists** *--* do you see the mask?
   4. Ping PC2 to PC6 and PC3 to PC6 -- these should work  
      Ping PC4 to PC6 and PC5 to PC6 -- these should fail
3. Now add a permit for all addresses that have 100.1. as their first 2 bytes (PC2-PC5).
   1. ***20 permit 100.1.0.0 0.0.255.255*** -- note the mask
   2. “*show ip access-lists” --* do you see the mask?
   3. Ping from PC2-PC5 to PC6 -- all pings should work

**Part 4: ACL List logic**

1. At this point PC2-PC5 are all permitted.
2. Add a deny for PC3 at sequence 50.
   1. **50 deny 100.1.1.3**
   2. **Do show ip access-lists** *(*note: you may see different matches)
3. Ping PC3 to PC6 – Why didn’t the deny work?
4. Change the sequence of the deny.
   1. **no 50** - delete that entry
   2. **5 deny 100.1.1.3**
   3. **do show ip access-lists**
5. Ping PC3 to PC6 – Why does it work now?

**Part 5: Create and Configure an Output ACL**

1. Now add subnet – 11.0.0.0/24 with a switch and PC. Configure IP addresses, subnet masks, default gateways, and router ports. When complete you should be able ping from PC2, PC4 and PC5 to PC10. (Packets from PC3 should be denied by ACL 1.)   
     
   
2. From Global Config Mode:
   1. **ip access-list standard 2**
   2. **99 permit any**
   3. **50 deny 100.1.2.4**
3. Move to specific configuration mode for the port with new subnet (ex: “int g0/0/0”)
4. Enter  **ip access-group 2 out** *- Note that we specify OUT (not IN)*
5. Ping from PC4 to PC10 fails, but from PC4 to PC6 works.

**Part 6: Create and Configure a New ACL List**

Create a standard ACL – number 10. You will create the list but don’t configure to any port. Read through the requirements below carefully. Follow the logic.

* 1. Block all IP addresses not specified below.
  2. Block all from network 9.x.x.x except 9.2.3.4
  3. Always allow from 200.200.55.7
  4. Block from 33.7.5.2
  5. Block all from 192.168.x.x except 192.168.6.x
  6. Allow any from 220.x.x.x except 220.100.x.x

**Part 7: Lab Completion**

1. Open a textbox and include all new commands introduced in module 10.
2. Save your packet file as Lab10a-Lastname and submit via iLearn.