ACLs

- Configure an ACL (standard named) on your 2800’s and 3750 to:
  - allow SSH access from a host of your choice (your home IP?)
  - allow SSH access from host: 144.38.192.40
  - allow SSH access from host: 209.33.215.102
  - deny SSH from all other locations
  - Apply that to your vty’s
  - Prove that SSH works by SSHing in from your home IP (or ssh.cs.dixie.edu), then trying it from a not permitted IP and make sure you get denied on all 3 devices.
  - prove that your ACL is working by showing the output from “show access-list XX” (where XX is your name) showing the deny/permit is working and matching packets on all 3 devices.
  - copy the outputs of the above line to a text file for uploading.

- Configure another ACL (standard numbered) on your three devices:
  - Allow source IPs of: 204.17.177.8, 204.17.177.3
  - Deny all others.
  - Apply that standard numbered to your NTP to limit the IPs NTP can query.
  - Configure another NTP server on your three devices for: 198.60.22.240
  - prove that your ACL is working by showing the output from “show access-list XX” (where XX is your number) showing the deny is working and matching packets on all three devices.
  - copy the output of the command in the line above for all three devices to a text file for uploading.

- Configure the following ACLs (on both of your 2800s) using extended named:
  - Configure ACLs for your VM Networks as follows:
  - Permit VM Services of SSH/FTP/HTTP to be accessed from 144.38.0.0/16, 209.33.192.0/18, and another single IP of your choice (your home IP?)
  - Disallow http access from traffic coming from any IP to your VM Network
  - Disallow ftp access from traffic coming from any IP to your VM Network
  - Permit dns lookups to 204.17.177.11 and 204.17.177.21 from your VM IP (TCP AND UDP).
  - Disallow dns lookups from your VM IP to anywhere else (TCP and UDP)
  - Permit all other
  - Apply the above ACL to your VM interface on your 2800. Which way should you apply it? Think it through.
  - Prove that your ACL works by trying to lookup DNS from 8.8.8.8 and 204.17.177.11 from your VMs. Only 204.17.177.11 should work. Also make sure SSH is being denied from non-approve IPs to your VMs.
  - copy the output from the “show access-list XX” for this portion to prove that it works and is permitting/denying appropriate things.

- Create another ACL (or two) on your 3750 using extended named
  - Allow icmp (pings) from 144.38.0.0/16, 209.33.215.102, and your home IP to your public /27 network.
  - Disallow icmp (ping) from anywhere to your public /27 network
  - Disallow your public /27 network from serving DNS (udp/tcp) AND NTP.
  - Permit all other
  - Apply the above ACL(s) to your uplink SVI interface on your 3750.
  - copy the output from the “show access-list XX” for this portion after proving that your ACL works and is permitting/denying appropriate things.

To pass off

Upload copies of [show run] from EACH of your three devices, and “show access-list XX” outputs in separate text files to Canvas by due date and time listed in Canvas.