Lab 10: Extended ACLs

Or: *Keeping the hackers out of your workspace*

What You Will Do:

Work on separate equipment, but combine your skills & knowledge to:

1. Learn the standard procedure for clearing all configuration from a Cisco switch
2. Deploy one or more ACLs on suitable interface(s) in the correct direction (in/out)
3. Confirm & prove that the ACL meets the requirements of the pre-lab specs
4. Extra: Investigate the CLI and its ability to edit remarks in an ACL
5. Continue preparing and practising for the SBA. You will be **required** to:
   – SSH and Telnet to switches and routers;
   – capturing your *complete configs* and save them to a USB stick

Things that you will need to know or learn:

1. How to design, configure, and apply ACLs
2. URLs and addresses for testing the entire breadth of protocols

What you need to submit and when:

1. Pre-lab: **TWO PRINTED COPIES** of your ACLs, submitted within 5 mins of the official start time of your lab session. The ACLs should be clearly separated into 3 different sections.
2. Complete the in-lab part of the exercise (see below), **before** the end of your lab period.
3. Complete post-lab exercise and quiz on BrightSpace, **before** your next lab.

In-Lab Marks:

[1 mark] Show that your ACL is at least partially functional (some match counters incrementing)
[1 mark] Prove that your ACL fully meets all the security requirements, defined in the pre-lab

The pre-lab is worth **36%**, the in-lab is worth **28%**, and the post-lab is worth **36%** of this lab, even though the number of points may differ between the three parts.

Required Equipment:

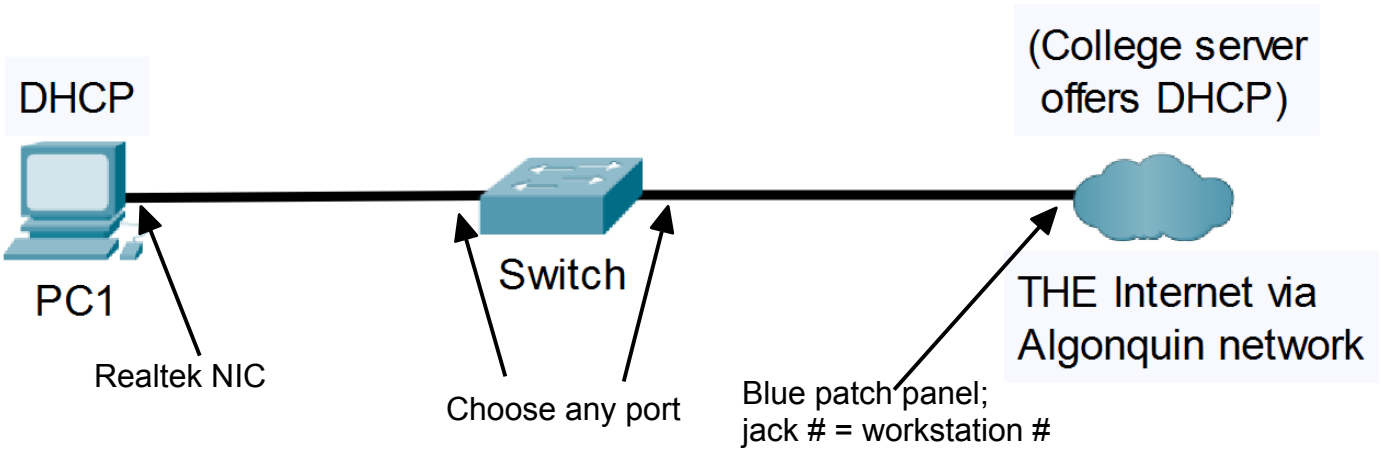
- A laptop and/or a USB memory stick to save results for post-lab questions
- **Hard-cover lab notebook**, for reference during **SBA** at the end of the course.

References and Resources:

- Slide decks on ACLs
- Post-Lab 9 exercise on extended ACLs
- Old versions of Firefox: https://www.mozilla.org/en-US/firefox/releases/

Updates and Extra commands (added 11:30am 14/Nov/2022):
– on our switches, ACLs may only be placed **in**bound on interfaces
– after obtaining an IP address on VLAN 1, do "logging console 5"
– append the keyword "log" to every ACE in order that match counters get updated
– for http/https: Google invented QUIC which runs over UDP (May 2021 - RFC 8999-9002)
– add the college DNS to your permitted traffic: the IP for T108 resembles 10.50.254.21

Topology and Addressing Diagram



Device	Interface	Address	Gateway
Switch (student 1)	TBD by student		Provided via DHCP
	VLAN 1 – DHCP	How will you show this?	
PC1 (student 1)	Realtek NIC	How will you show this?	Provided via DHCP
Repeated by partner, for twice the experience & twice the practice!			

Complete General Setup

Task 1: Cable the Network

(You know what to do)

Task 2: Clear the Switch

The equipment in our lab is used by *many* students, so we'll follow *standard procedure* to ensure the switch is cleared of any config. It's just a few commands, so quick & easy to do.

Step 1. Connect to the console port of the switch. Note the cabling arrangement graciously provided by our dept technician. (Don't forget to thank him some time!)
Step 2. Issue two commands to clear the config: **erase startup-config** **delete vlan.dat**
Step 3. Reboot the switch ("reload"); don't save the config
Step 4. When you get back the CLI, ignore VLAN config: **vtp mode transparent**

Task 3: Configure basic *settings for PCs*

With the switch working and the PC connected to via the college network, configure the Realtek NIC for DHCP addressing. Do not proceed to the next task until you've confirmed *from a CMD window* that the PC has obtained all the necessary settings from DHCP.

You'll need to **NOTE THE ALGONQUIN DNS IP ADDRESS** and add it to your ACL.

Task 4: Configure basic services on the Switch

A switch is mostly "invisible" to traffic passing through it. For this lab, however, we'd like to have some additional testing capabilities so we'll configure it with telnet, SSH, HTTP, and HTTPS. For that, the switch will need to obtain an address via DHCP from the college network.

Step 1. Configure basic settings on the switch, exactly the same as you have been doing for routers in all previous labs. To save time, you can use 1024 or 2048 bit RSA.

Step 2. For interface VLAN 1, set the IPv4 address to DHCP: **`ip address dhcp`**
Wait a few moments, and then you should see an Information message confirming the IP address. You **need to know this address** for later steps and tasks!
Q. In the "Method" column of **`sh ip int br`**, how was the IP address assigned?

Step 3. With the successful IP address on Vlan 1, reduce the amount of messages you'll get on the console: **logging console 5**

Step 4. Assuming you've completed step 1 completely and correctly, confirm that you can telnet and SSH to the switch from the PC. Troubleshoot as necessary.

Step 5. Configure an HTTP and HTTPS server: **ip http server ip http secure-server**

Step 6. Using a browser on the PC, navigate to http://x.x.x.x (where x.x.x.x = switch IP) and then https://x.x.x.x It doesn't matter what page or message you get, as long as it's not a timeout you're guaranteed you're getting through to the switch.

Task 5: Confirm full connectivity to the internet

Before applying any ACL, it's important to make sure everything is working properly. You'll want to test all the protocols allowed for the Networking Student: bootup, browsing, accessing NetLab (booking page), ping + traceroute to NetLab, and FTP. For today, we'll skip verifying email.

Step 1. Test DHCP with the CMD commands: **ipconfig /release ipconfig /renew**

Step 2. Test NTP: right click on the time at the bottom right corner of the screen, choose Adjust Date/Time, click "Sync now". It *not successful*, see last page.

Step 3. Confirm you can browse freely on the internet, including the NetLab booking page.

Step 4. Ping & traceroute: for ICMP, please note that Algonquin only permits a destination of NetLab; all other destinations are blocked and packets are silently discarded.

Step 5. For telnet & SSH: you can test a connection to SDF.org. If you get a login prompt, it means you've successfully connected (even if you can't actually login).

Step 6. For FTP: again connect to SDF.org. Use the standard anonymous FTP credentials: account: anonymous password: {your-email}

Task 6: Deploy your ACL

Here's where you get to test your ACL. Enter the ACL and then confirm proper operation on your chosen interface. The ACE counters should increment as a result of network activity.
FOR THE SWITCHES IN LAB T108: ACLs can only be applied "in"; append "**log**" to every ACE.

Step 1. Using your pre-lab sheet as a reference, configure the "Networking Student" ACL.

Step 2. Apply the ACL to your best guess of the right interface(s) and the right direction.

Step 3. Re-run the tests from the previous section. After each one, check the ACE counters by showing the access-lists. You've chosen the wrong interface or the wrong direction if none of the counters increments, or you can no longer access the internet. Individual ACEs are likely incorrect if you see the final "deny all" counter increasing instead of the expected individual protocol ACE.

You should be at one of the two checkpoints by this point in time. Check point demos can be done as a pair of students, assuming you both worked on the final solution!!

CHECK POINT #1: Demo that at least some of your counters are incrementing correctly.
While waiting to do your demo, continue working on correcting your ACL!

CHECK POINT #2: Demo that your ACL is completely correct by showing that all your counters are incrementing correctly (ignoring email).
While waiting to do your demo, continue working on the extra challenges.

Task 7A: [Extra Challenge] ACLs and accessing services on the switch

Your ACL is in effect, allowing or blocking traffic and counting every single packet passing through. But what about packets that go *to* the switch? Check out whether your arrangement for the ACL sees & counts these packets.

Step 1. Test telnet, SSH, HTTP, and HTTPS to the switch. Remember, any sort of a response other than a timeout means you're getting through (from a networking standpoint). Check the ACE counters to confirm they're incrementing as expected.
Step 2. If you can't get through on any of these protocols, can you think of a way to change the location and/or direction of your ACL so that you can access the switch?

Task 7B: [Extra Challenge] Modifying Remarks in a Cisco ACL

Hopefully you had at least one, and ideally many **remark** statements in your original ACL. In this task, you'll explore your ability to add, modify, and delete remark statements from an existing ACL. Think about it: what network do you think exists that hasn't changed, or hasn't had users moved, etc? The comments/documentation for an ACL will always need updating!

Step 1. Find all the ways possible to display an ACL with the remark statements.
Step 2. Can you add a remark with a line number? Try it!
Step 3. Can you insert a remark part way into an existing ACL? Try it!
Step 4. Find as many ways as possible to modify an existing remark.
Step 5. Can you delete a remark by repeating the entire line with "no" in front? Try it!
Step 6. Find as many ways as you can to change

Q. What is the reason the slide deck (a) suggests using a text editor, and (b) outlines the method of copy & paste for editing remarks?

Task 8: Backups and Clearing the equipment

All steps in this task will be **required for the SBA**. Please make sure you can make a backup! Then be sure your equipment is cleared of all config before de-cabling and powering down:

`show startup-config` If the startup-exists, then: `erase startup-config`

And for good measure because this is a switch:

```
delete vlan.dat
```

Congratulations! You're a safer surfer now that you're protected by ACLs! :-)

Fixing the hiccup with NTP in T108

There appears to be some difficulties accessing the default MS-Win NTP server, time.windows.com. Even from home, it took over a minute to get a successful update.

A better option is the National Research Council (NRC Canada) NTP server. It's located at time.nrc.ca. To change Win10 to use this server:

- open Control Panel (may need to choose: view by *Small icons*)
- click Date and Time, choose the tab Internet Time
- click Change Settings; ensure *Synchronize with an internet time server option* is selected
- even though it looks like a drop-down list, go ahead and type: time.nrc.ca
- click Update now and look carefully (it may say Fail and yet also say that it sync'd the time)
- If that doesn't work, try the internal Algonquin NTP server at 10.254.21.21
- If at least one attempt is successful, it should create some matches on your NTP ACE when you click *Update now* (though it may take several clicks on the lab PCs).