UNIVERSITY OF INFORMATION TECHNOLOGY – VNU-HCM
FACULTY OF COMPUTER NETWORKS AND COMMUNICATIONS

5. ACCESS CONTROL LIST

NETWORKING TECHNOLOGIES– v1.2025

A. OVERVIEW

1. Learning objective

Students will demonstrate practical in implementing Access Control List (ACL) technologies through direct configuration and testing exercises. Students will configure standard and extended ACLs on routers and switches, establish proper placement strategies for optimal network security, and implement traffic filtering policies to control network access.

Through guided practice scenarios and troubleshooting exercises, students will apply ACL configuration commands to create functional security architectures, verify traffic filtering behavior between network segments, and diagnose common implementation issues using appropriate diagnostic tools and packet analysis techniques. Students will document their ACL configurations, demonstrate proper security implementation procedures, and successfully complete practical assessments that validate their ability to deploy ACL solutions for network security and traffic management in real network environments.

2. Practice Environment

- Networking simulation with Cisco Packet Tracer.

B. LAB TASKS

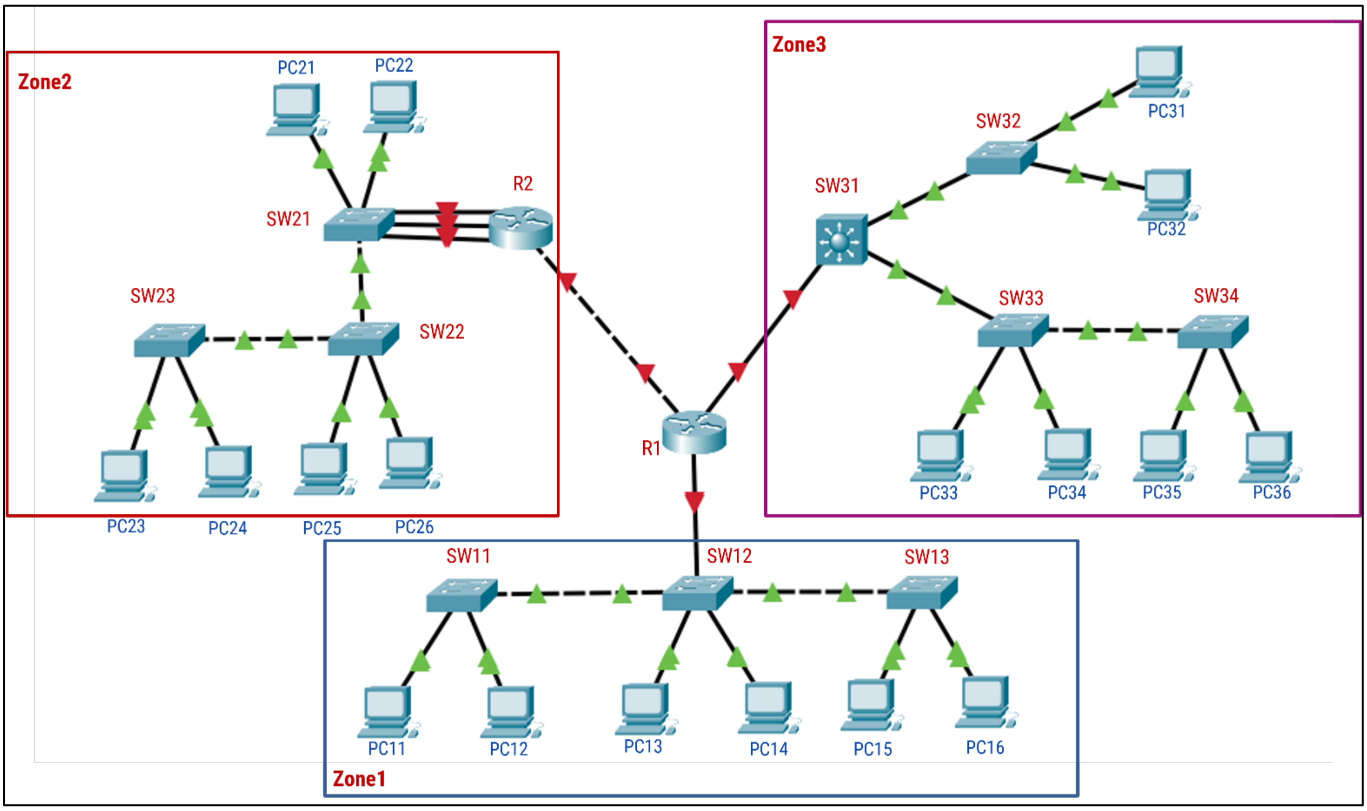

Figure 1: The network topology for Task 1

Giving the network topology as Figure 1 above (previous lab).

Zone 1 has 4 VLANs:

- VLAN 10: 192.168.0.0/24 PC11, PC13, PC15
- VLAN 11: 192.168.1.0/24 PC12
- VLAN 12: 192.168.2.0/24 PC14
- VLAN 13: 192.168.3.0/24 PC16

Zone 2 has 3 VLANs:

- VLAN 20: 172.20.0/16 PC21, PC22, PC23, PC25
- VLAN 21: 192.21.0.0/16 PC24
- VLAN 22: 192.22.0.0/16 PC26

Zone 3 (network: 192.168.8.0/24) has 5 VLANs:

- VLAN 31: PC31, PC33, PC35
- VLAN 32: PC32
- VLAN 33:
- VLAN 34:
- VLAN 35: PC36

Requirements:

1. Assign IP to devices, configure VLAN, and inter-VLAN routing *(Completed in lab 4).*
2. Routing for 3 zones: Zone 1, Zone 2, and Zone 3 *(Completed in lab 4).*
3. Configure an ACL on router R1 to deny all traffic from PC21 (Zone2) to PC11 (Zone1), but allow all other traffic.
4. Create an ACL on router R2 that blocks HTTP traffic (port 80) from any device in Zone2 to any device in Zone3, while allowing all other protocols.
5. Design and implement ACLs on routers R1 and R2 with these requirements:
   - Zone1 devices can only access Zone3 devices using SSH (port 22).
   - Zone2 devices cannot access Zone1 at all.
   - Zone3 devices can freely communicate with Zone1 but only HTTP/HTTPS with Zone2
6. PC26 (Zone 2) cannot ping PC16 (Zone 1), but PC16 can ping PC26.

C. REQUIREMENTS

You are expected to complete all tasks in section B (Lab tasks). Advanced tasks are optional, and you could get bonus points for completing those tasks.

Your submission must meet the following requirements:

- You need to submit a **detailed lab report in .docx** *(Word Document)* format, **using the report template** provided on the UIT Courses website.
- A report written in English is required.
- When it comes to **programming tasks** *(require you to write an application or script),* please attach all source-code and executable files (if any) in your submission. Please also list the important code snippets followed by explanations and screenshots when running your application in your report. Simply attaching code without any explanation will not receive points.
- Submit work you are proud of – don't be sloppy and lazy!

  Your submissions must be your own. You are free to discuss with other classmates to find the solution. However, copying reports is prohibited, even if only a part of your report. Both reports of the owner and the copier will be rejected. Please remember to cite any source of the material (website, book,…) that influences your solution.

Notice: Combine your lab report and all related files into a single **ZIP file (.zip)**, name it as follow:

StudentID_ReportLabX.zip