SKILLScomp
Skills competitions for VET development

Co-funded by the European Union

Networking Academy

WYŻSZA SZKOŁA INFORMATYKI i ZARZĄDZANIA
z siedzibą w Rzeszowie

Professional Skills Competition

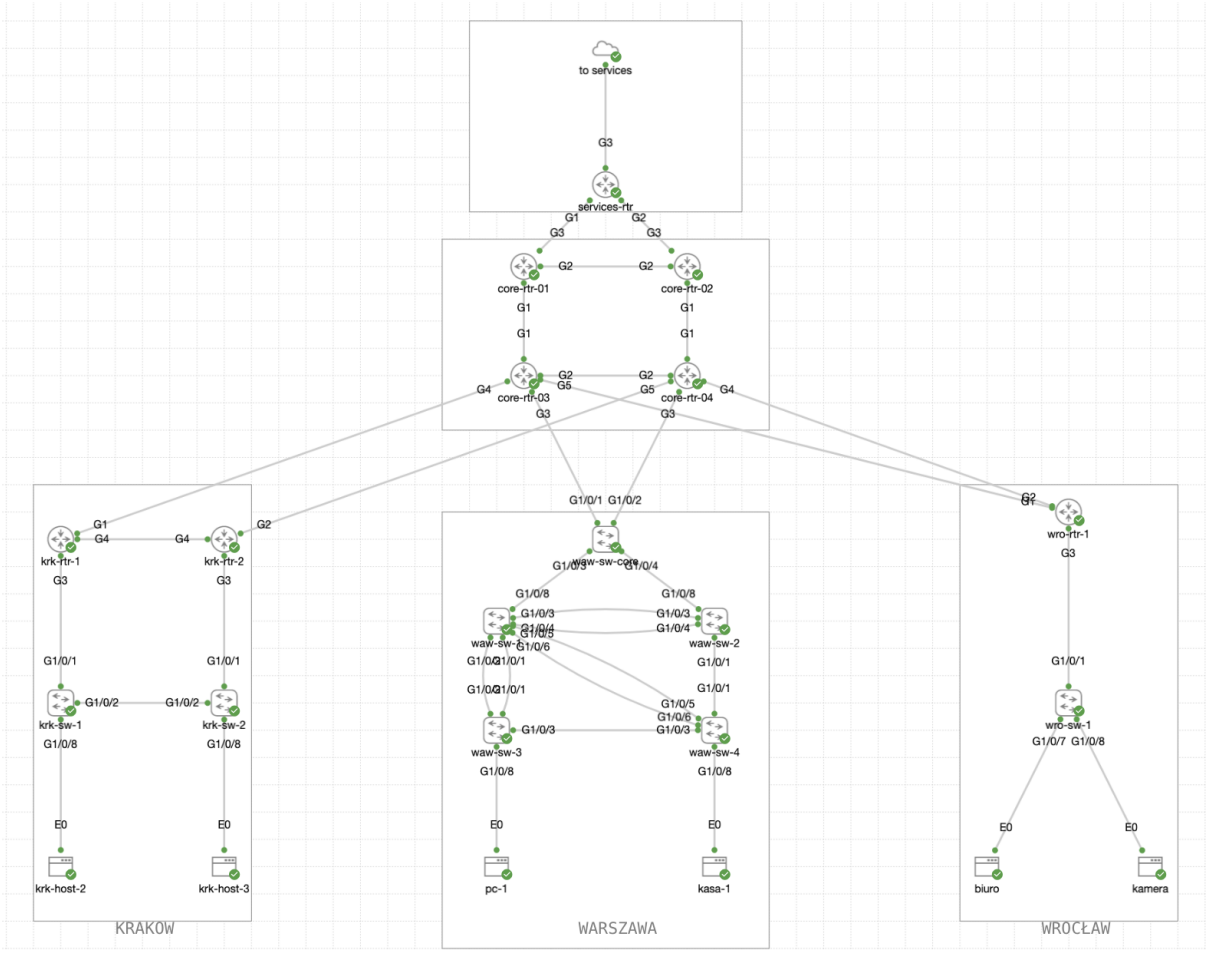
Network Systems Management

--- FINALE ---

DAY 2 - PART 1
(10:30 – 12:00)

1. Topology

The diagram below shows the full network topology that will be used on day two of the competition (also available for full viewing in the CML environment):



2. Access to the test environment

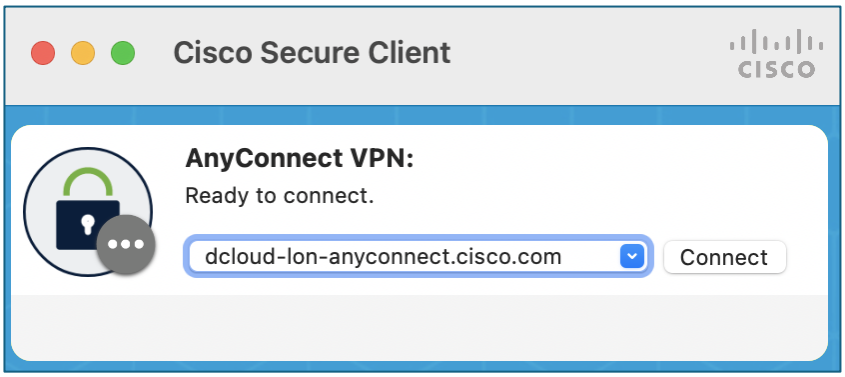
The entire competition was simulated in the Cisco dCloud environment using the following devices/versions:

1) Catalyst 8000v Series: Version : Cisco IOS-XE 17.09.01a
2) Catalyst 9000v Series: version : Cisco IOS-XE 17.10.1prd7
3) Alpine Linux, version: 3.16.2
4) Ubuntu Linux, version: 22.04.1 LTS

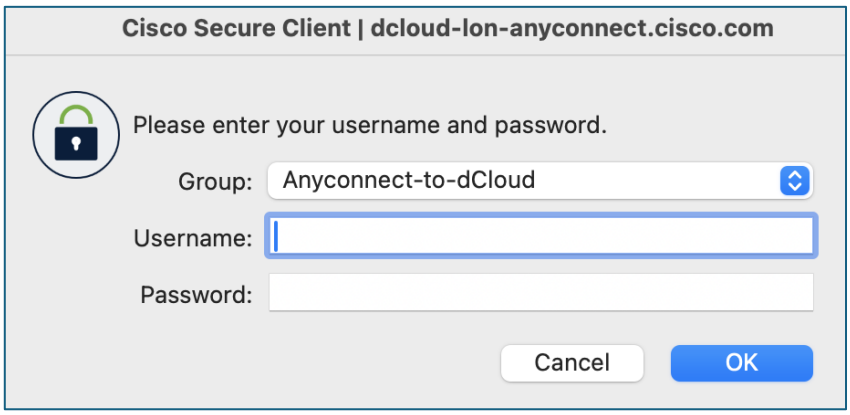
To gain full access to the test environment, follow these steps:

2.2. Cisco Secure Client VPN

1) Open the " **Cisco Secure Client** " application, enter the address: dcloud-lon-anyconnect.cisco.com



2) Click " **Connect** " and enter the username and password received from the competition organizer:



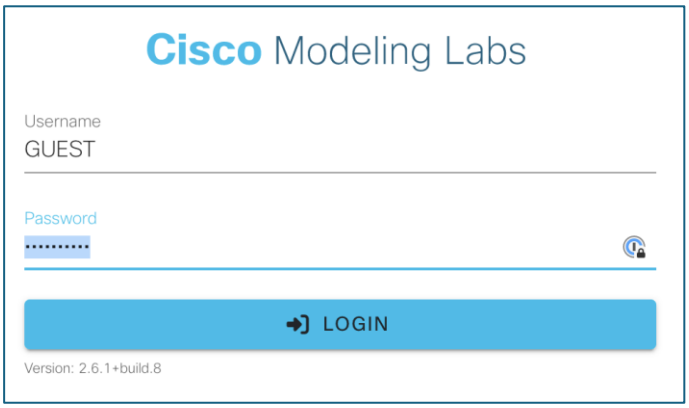
2.3. Cisco Modeling Labs (CML)

Cisco Modeling Labs (CML) provides access to a test environment that includes network topology, device access, and the ability to remotely power them on and off. To access CML, ensure you are connected via VPN (see section 2.2) and follow these steps:

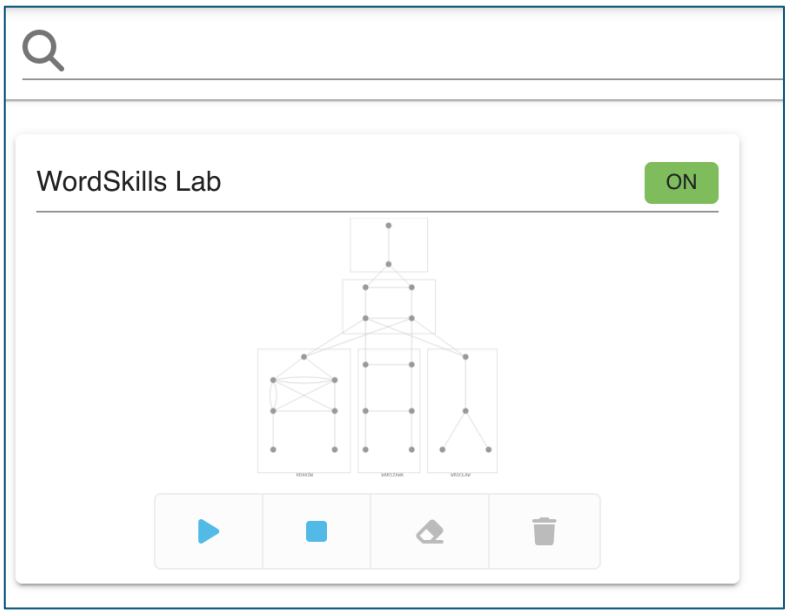
1) In your web browser, enter the address:
   https://198.18.133.111/

2) To log in to the system, use the following details:

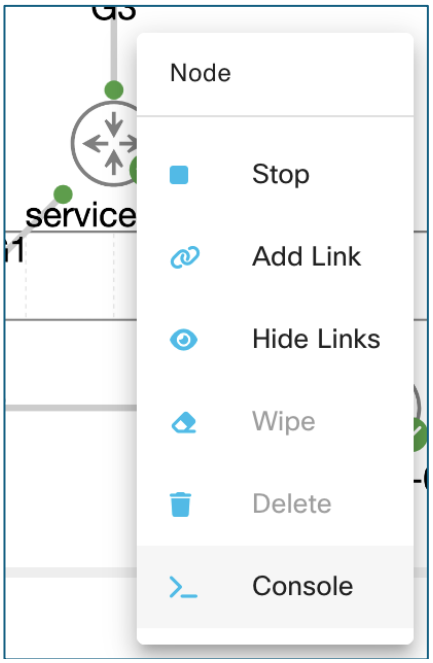
   Username : GUEST (uppercase required)
   Password : C1sco12345



3) lab environment should now be initialized - click on the topology (avoid clicking on the start/stop/ wipe / delete buttons at the bottom of the area):



4) To access the console, right-click on a specific device (switch , router, host) and then select Console from the menu :



5) From the panel at the bottom of the screen, select: " Open Console ":

To log in to the switch/router, use the following details:

User : cisco

Password : C1sco12345

2.4. Main Server

, a virtual machine running the Linux operating system (Ubuntu) was connected to the topology simulated in the CML environment (to the router marked as **services -rtr).**

Access to the machine is possible directly from the workstation using the SSH protocol after connecting to the test environment via VPN.

IP address (remote access / mgmt) : 198.18.128.100
User : cisco
Password : C1sco12345

IP address (from lab/services -rtr side) : 198.18.10.100

2.6. Hostas

Additionally, additional hosts (e.g., krk-host-2, pc-1, camera, etc.) are connected to the network to verify that the network is functioning properly. These devices are accessed via CML in the same manner as network devices (see section 2.3), taking into account the following data:

User : cisco
Password : cisco

3. General notes

It is prohibited to:
- changes to the network topology (adding or removing devices, connections, etc.),
- password changes / console configuration / VTY / ...,
- communicating with guardians, other competition participants and third parties,
- using the Internet (except for the official documentation provided on cisco.com).

It is ordered:
- saving the configuration on the device (copy run start) after each part on all devices, which will then be copied during the break for full verification.

In the event of any environmental problems, the participant is obliged to report any observed problems directly to the committee.

4. Competition tasks [50 points]

4.1. Krakow Branch

In the Kraków branch, krk-host-2 and krk-host-3 devices are unable to communicate with each other and with the outside world (external IP address for testing – 172.31.255.3 and 172.31.255.4)

Check the network configuration to restore communication. The krk-rtr-1 and krk-rtr-2 devices are connected to the core network using OSPF in the backbone area .

Note : Make sure that changes made to the configuration will not reduce the security of the network (only necessary changes to the Access Control List, and as detailed as possible). It is not allowed to delete the Access Control List or add entries such as (ip any any).

As part of the task:

1) Verify the existing network configuration,
2) Identify any issues that prevent communication between hosts,
3) Propose the optimal solution, implement it on the network and fully test it.

Use the area below (next page) to describe precisely:

- identified problems in the network (problem description),
- selected solution method (solution description).

PROBLEM DESCRIPTION

SOLUTION DESCRIPTION

4.3. Warsaw Branch

At the Warsaw branch, there's a communication problem between hosts PC-1 and Cashier-1 . Analyze the network issues to implement an optimal solution that will enable communication between hosts and default gateways. Any changes made must not negatively impact the security level across the entire branch.

As part of the task:

1) Verify the existing network configuration,
2) Identify any issues that prevent communication between hosts,
3) Propose the optimal solution, implement it on the network and fully test it.

Use the area below (next page) to describe precisely:

- identified problems in the network (problem description),
- selected solution method (solution description).

PROBLEM DESCRIPTION

SOLUTION DESCRIPTION

CONGRATULATIONS – YOU HAVE COMPLETED STAGE:
DAY 2 / PART 1

SAVE THE CONFIGURATION ON ALL DEVICES, SUBMIT YOUR ANSWERS IN WRITING AND INFORM THE COMMITTEE!