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

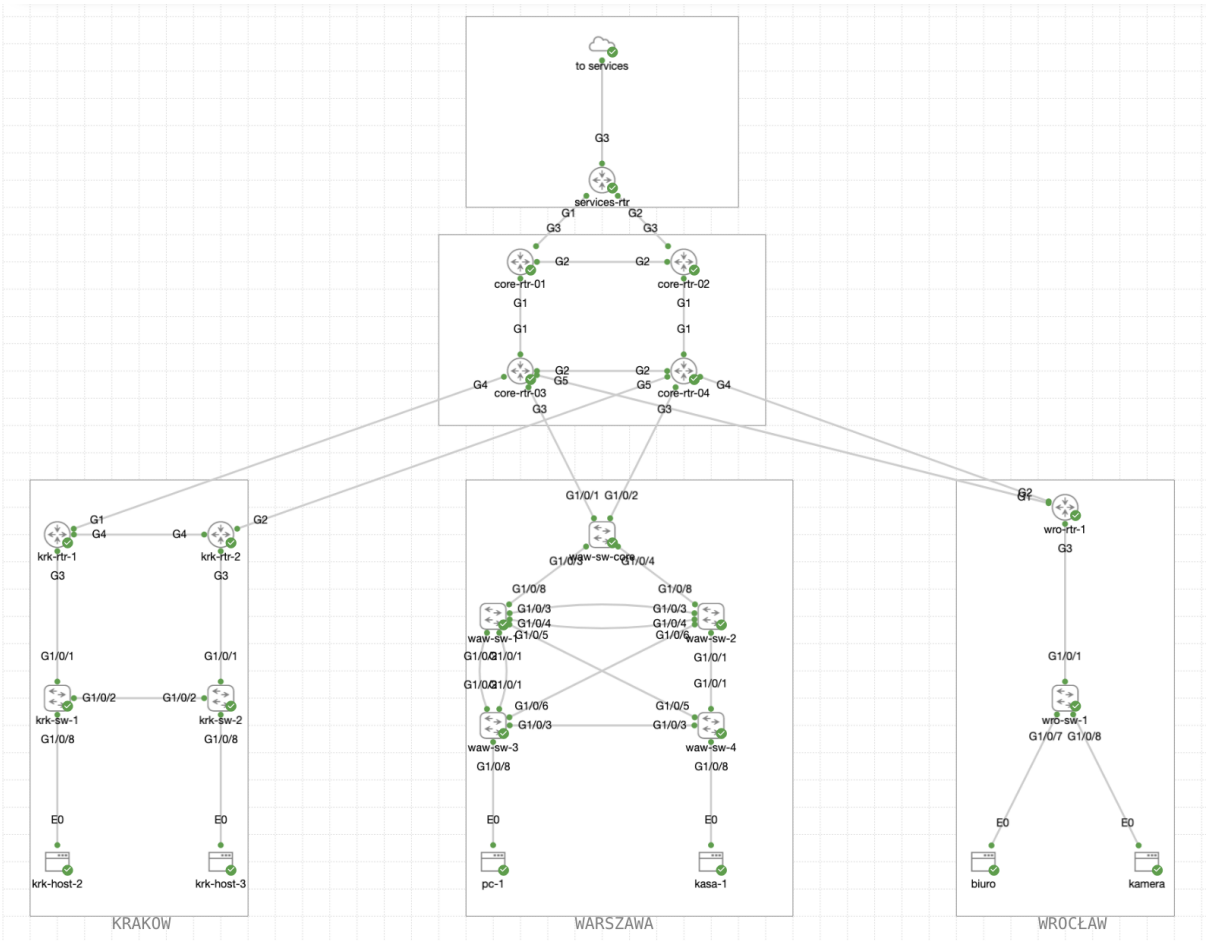
Network Systems Management

--- FINALE ---

DAY 1 - PART 3
(1 4:45 – 16:15)

1. Topology

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



2. Access to the test environment

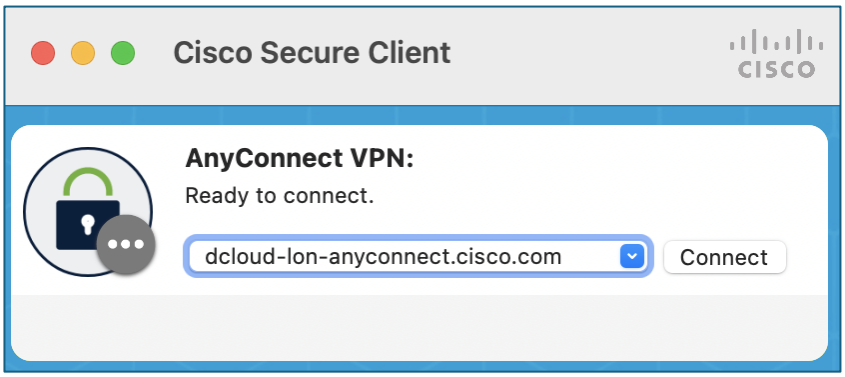
The entire competition was simulated in the Cisco dCloud environment using the following devices/versions:

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

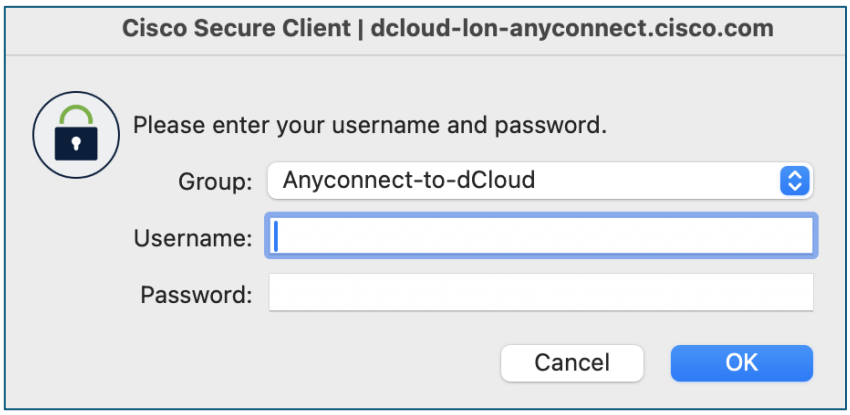
To gain full access to the test environment, follow these steps:

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:



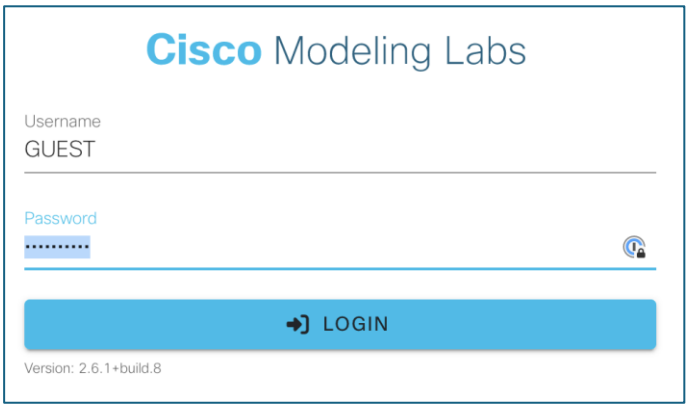
2.3. Cisco Modeling Labs (CML)

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:

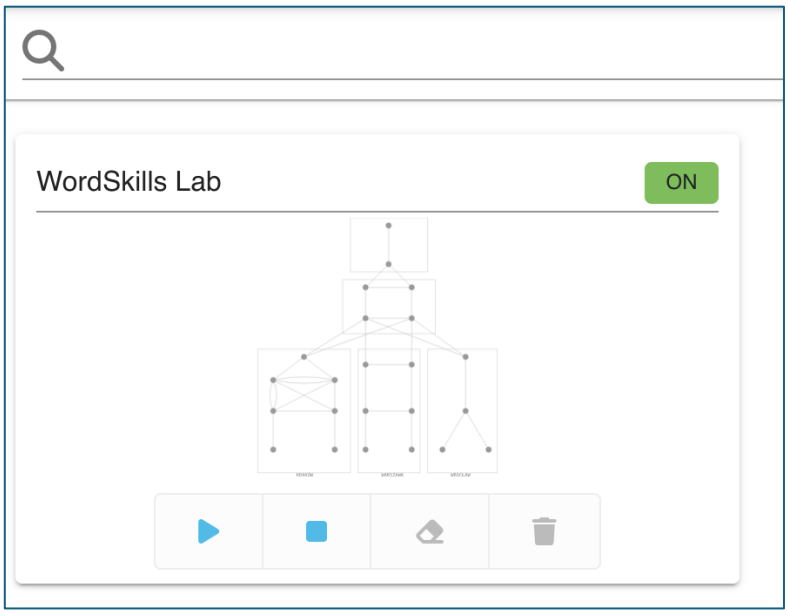
1) In your web browser, enter the address:
   https://198.18.133.111/

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

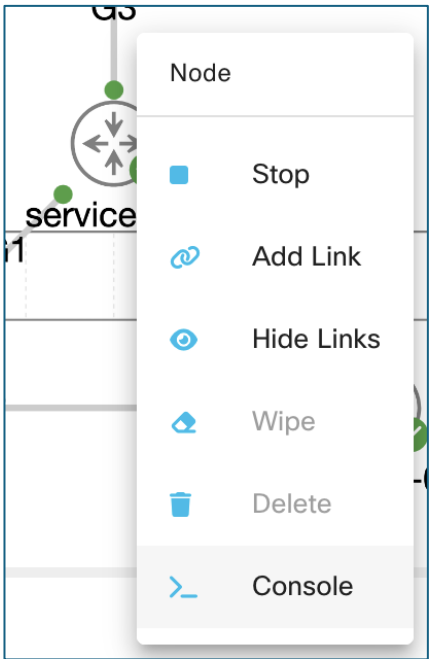
   Username : GUEST (uppercase required)
   Password : C1sco12345



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 [20 points]

4.1. Device Access/Aliases [1 point]

Configure the wro-sw-01 and wro-rtr-01 devices in such a way that:

a. administrator by executing the **router command** could log in to the wro-rtr-01 device from the device: wro-sw-01 (0.5 points)
b. administrator by executing the **switch command** could log in to the wro-sw-01 device from the wro-rtr-01 device (0.5 points)

4.2. Information for administrators [2 points]

Configure the wro-rtr-01 device and wro-sw-01 in such a way that at the moment of logging in (but before entering the correct login details: username/password) the following information will be displayed (1 point):

```
================================================
Access to the system is limited to only
authorized users.
================================================
```

Additionally, configure the wro-rtr-01 and wro-sw-01 devices in such a way that additional information appears only after successful login (1 point):

```
================================================
            Wroclaw - <<hostname>>

Loopback0: << IP address Lo0>>
PID: <<device model>>
S/N: <<device serial number>>
================================================
```

Where the variables: `< <hostname> >, <<Lo0 IP address>>, <<device model>>, <<device serial number>>` should be replaced with the correct values for the specific device.

4.3. System time switch [2 points]

Configure the wro-sw-01 device so that:

a. in logs and debugs , and the timestamp was displayed with an accuracy of milliseconds (0.5 points),
b. the logs showed information about the CET time zone (where CET is GMT time shifted by +1 hour) (0.5 points),
c. when summer time is in force in Poland, the device should inform about the time zone CEST instead of CET (the time change is on March 2 at 2 a.m. and on October 3 at 3 a.m.) (1 point).

4. 4. Login [2 points]

Following recent incidents involving unauthorized network changes by a former employee, the team security asked for help in implementing additional configuration auditing and expanding network event logging.

Configure wro-rtr-01 devices and wro-sw-01 in such a way that:

a. `critical and higher` level logs should be generated on the console (0.5 points)
b. both devices sent logs to the main server (at the address: 198.18.10.100) with the source address being the IP address configured on the **Loopback0 interface** and were marked (facility) as **local0** (0.5 points)
c. Additionally, all commands executed on the device (in configuration mode) should be archived on the server (1 point)

Note *: For verification purposes, access to the main server is possible via SSH.*

IP address (mgmt only) *: 198.18.128.100*
User *: cisco*
Password *: C1sco12345*

The master server is fully configured and requires no changes. All information sent to the server at IP address 198.18.10.100 on UDP port 514 is automatically saved to files. The file name corresponds to the packet's SRC IP address. The files are stored in the directory: ***/ var /log/network/***

4.5. Monitoring [2 points]

Team The network monitoring team reported a problem with the lack of visibility of the Wrocław location, which prevents them from properly detecting any network issues. Your task is to help them and address this issue. Configure the **wro-rtr-01 device** :

a. so that the device can be "queried" from the main server on the network using (1 point):
   - community : public (read only)
   - community : private (read/write)

b. Additionally, in case of any configuration changes, information about such an event should be sent to the Linux server at the address 198.18.10.100 from the community cisco and with device source address as Trap (1pt)

Note : For verification purposes, access to the main server is possible via SSH.

IP address : 198.18.128.100
User : cisco
Password : C1sco12345

Where commands are available: snmpget , snmpwalk , etc.

The master server is fully configured and requires no changes. Information about receiving a packet addressed to the server at IP address 198.18.10.100 on UDP port 162 is automatically saved to the **traps.txt file in the / var /log/ snmp** directory.

4.6. Dynamic addressing of end devices [7 points]

In the Wrocław branch, it was necessary to add two additional network segments – one for users (host: office) and one for IoT devices (host: kamea), each supporting approximately 100 devices. Only the 172.18.100.0/24 subnet is available.

Configure wro-rtr-01 and wro-sw-02 so that:

For subnets users (3 points):
- the first address from the assigned subnet was reserved for the default gateway,
- IP addresses should be assigned dynamically, excluding the first five addresses in the assigned subnet,
- the DNS server assigned to users was 8.8.8.8,
- the domain for users was: users.wroclaw.org
- IP addresses for users should be assigned for a maximum of 4 hours.

For subnets IoT devices (3 points):
- the last address from the assigned subnet was reserved for the default gateway,
- the last five addresses in the assigned subnet should be reserved,
- the device named **camera** should have the fifth address from the subnet permanently assigned.
- DNS servers assigned to IoT devices were 8.8.8.8 and 1.1.1.1.
IoT devices was: iot.wroclaw.org

Note : For verification purposes, access is provided to two hosts that are connected to the **wro-sw-01 switch** named: **office** (which should function in the users' subnet) and **the camera** (which should operate in the IoT devices subnet). Both devices should obtain an IP address dynamically, in accordance with the above-mentioned rules, and be able to communicate with the address 198.18.10.100 (1 point).

Access to hosts:
User : cisco
Password : cisco

To refresh the IP address retrieval, execute the command on the device:
```
sudo /etc/init.d/networking restart
```

4.7.QoS [4 points]

IoT system has been installed in the Wrocław branch , the traffic of which should be treated in such a way that it is not rejected by the ISP in the core network.

According to the agreement with the ISP, traffic on their network for the CS3 class is treated specially and your team he asked You to configure the Wrocław branch so that only the following traffic uses this class (2 points):
Source : IoT device called **camera** connected to the wro-sw-01 switch
Destination : main server: 198.18.10.10
Traffic type : http

Additionally, all other traffic from all IoT devices should be marked as CS1. All other traffic should be marked as BE when it enters the core (ISP) network (2 points).

CONGRATULATIONS – YOU HAVE COMPLETED STAGE: DAY 1 / PART 3

SAVE THE CONFIGURATION ON ALL DEVICES
AND INFORM THE COMMITTEE!