SKILLScomp
Skills competitions for VET development

Co-funded by
the European Union

CISCO Networking Academy

WYŻSZA SZKOŁA
INFORMATYKI i ZARZĄDZANIA
z siedzibą w Rzeszowie

Professional Skills Competition

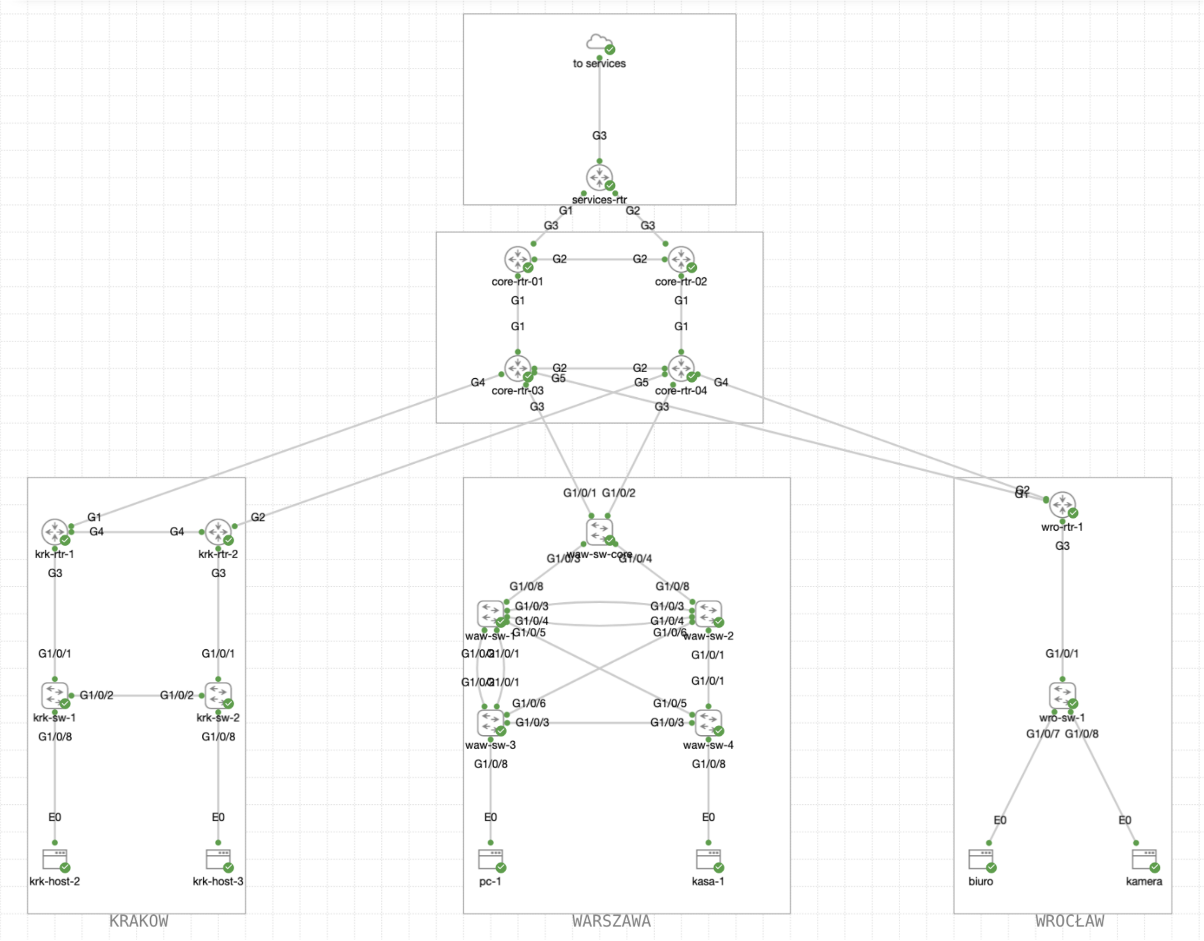
Network Systems Management

--- FINALE ---

DAY 1 - PART 2
(1 3:00 – 14:30)

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

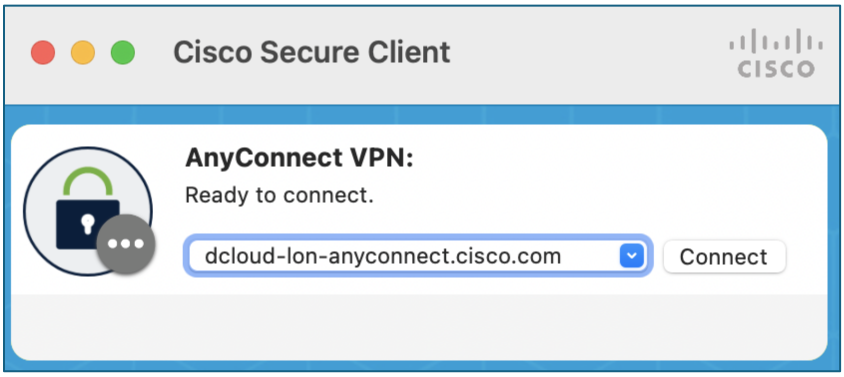
The entire competition was simulated in the Cisco dCloud environment using the following devices/versions:

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



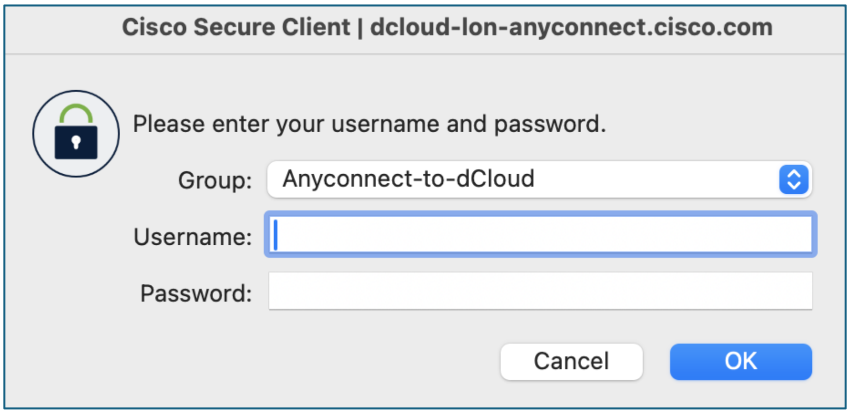
Cisco Secure Client

AnyConnect VPN:

Ready to connect.

dcloud-lon-anyconnect.cisco.com

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



Cisco Secure Client | dcloud-lon-anyconnect.cisco.com

Please enter your username and password.

Group: Anyconnect-to-dCloud

Username:

Password:

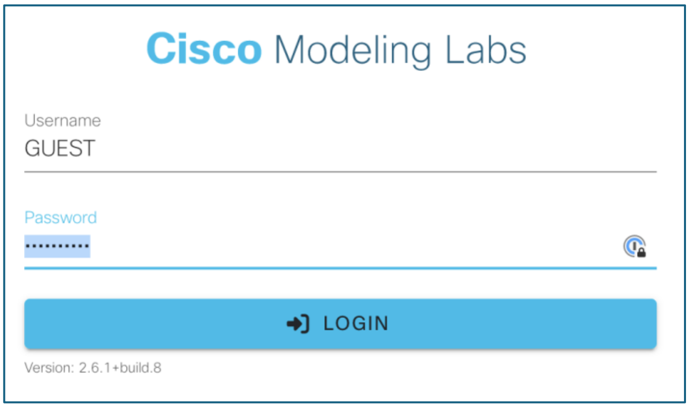
2.3. Cisco Modeling Labs (CML)

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



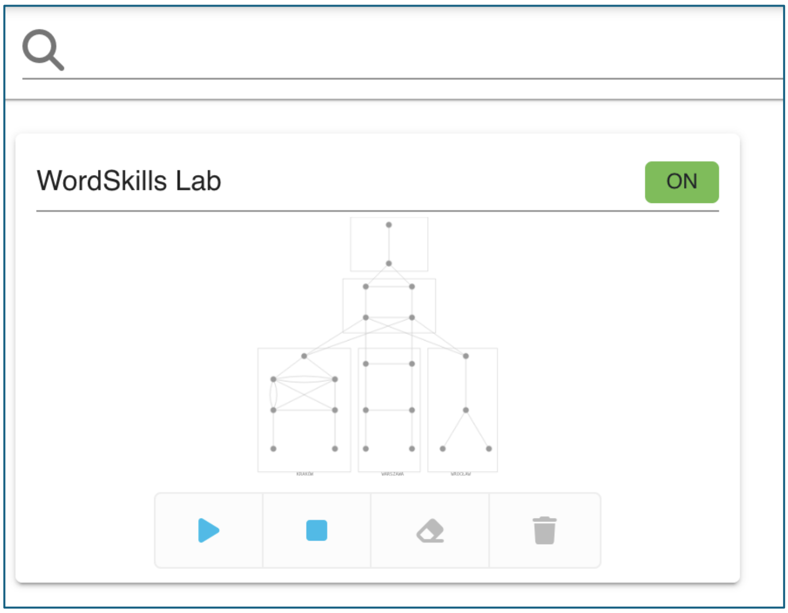
Cisco Modeling Labs

Username: GUEST

Password: ••••••••••

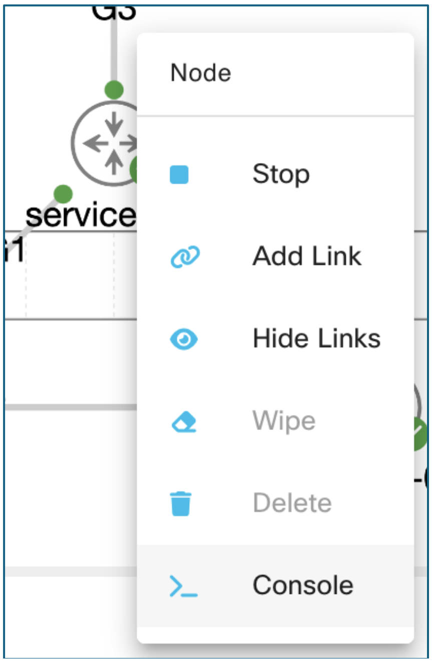
Version: 2.6.1+build.8

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):

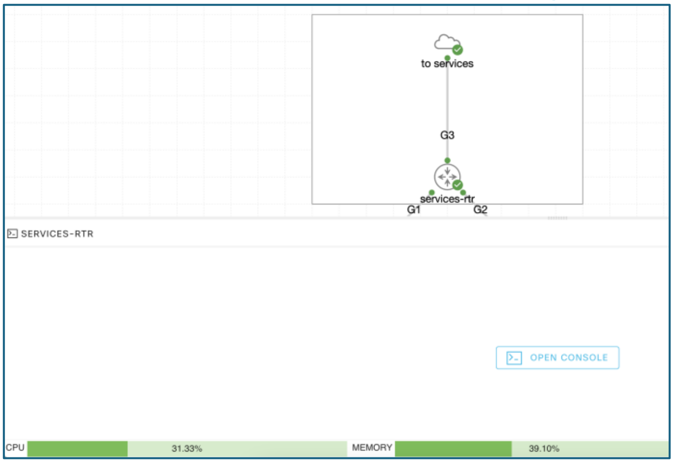


WordSkills Lab

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 [30 points]

The Warsaw branch network includes four switches and one router. The router is prepared for the intended packet propagation; configuration tasks will be performed solely on network switches and hosts. The switches currently have no configuration; only connections are prepared. The task aims to prepare configurations for three departments, only two of which will communicate with the company headquarters via the network core. These departments are accounting, cashiers, and human resources.

4.1. Basic configuration [5 points]

1. Configure names for all devices. (1 point)

2. Configure all redundant connections between the following pairs of devices (Devices should use LACP). (2 points)

Switch 1	Switch 2	ID (port channel)
waw-sw-1	waw-sw-2	10
waw-sw-1	waw-sw-3	20

3. Configure devices to enable connection verification from the CLI using LLDP and CDP. (1 point)

4. Set up the interface descriptions connecting the switches so that they can identify the device on the other side without having to use CDP/LLDP protocols. Then, set the links to allow frames to be sent across different VLANs . (1 point)

4.2. Virtual networks [15 points]

1. Configure the waw-sw-1 and waw-sw-2 devices to automatically propagate virtual network configurations using the VTP protocol according to the table below (4 points):

Device	VTP version	Mode	Domain
waw-sw-1	3	server	waw-01
waw-sw-2	3	Client	waw-01
waw-sw-3	3	transparent	waw-01
waw-sw-4	3	transparent	waw-01

2. Configure VLAN 10 and name it as: NATIVE (1 point)

3. Create virtual networks with the following numbering (2 points):

   a. 100 →Staff

   b. 110→ Bookkeeping

   3. 120 →Cashiers

Note : For information on virtual network placement, see the table below.

VLAN ID	waw-sw-1	waw-sw-2	waw-sw-3	waw-sw-4
100	Yes	Yes	Yes	NO
110	Yes	Yes	Yes	NO
120	Yes	Yes	Yes	Yes

4. **trunk** connections according to the table below (6 points):

Switch 1	Switch 2	Interface	Native VLAN	VLAN allowed
waw-sw-1	waw-sw-2	After 20	10	100,110,120
waw-sw-1	waw-sw-3	After 10	10	100,110,120
waw-sw-1	waw-sw-4	G1/0/5	10	120
waw-sw-2	waw-sw-4	G1/0/1	10	120
waw-sw-2	waw-sw-3	G1/0/6	10	100,110,120
waw-sw-3	waw-sw-4	G1/0/3	10	120

5. Configure devices so that all devices have unblocked interfaces towards the waw-sw-core switch (applies to all virtual networks configured on a given switch) (2 points).

4.3. Configuration layers access [10 points]

1. Configure the kasa-1 and pc-1 hosts as follows (2 points)

Host Name	**IP address**	**Mask**
Pc-1	172.16.0.10	/25
Cashier-1	172.16.0.140	/25

Commands for IP configuration on hosts kasa-1 and pc-1 :

```
sudo ifconfig eth0 <IP-ADDR> netmask <MASK>

sudo route add default <GATEWAY> dev eth0
```

Commands for IP verification on hosts cash register-1 and pc-1 :

```
ifconfig eth0
ip addrroute -n
```

2. Configure the interfaces to which the kasa-1 hosts are connected and pc-1 in such a way that:
   a. For the kasa-1 host , a configuration must be prepared that meets the following requirements: (5 points)

      - Access only to a single VLAN with the number 120 ,
      - Configure the interface so that only the kasa-1 host has access to it ,
      - If an attempt is made to connect another host to the interface, the port should be automatically blocked,
      - After connecting the host, the interface should immediately start propagating packets.

   b. For host pc-1, a configuration must be prepared that meets the following requirements: (3 points)

      - Access only to a single VLAN with the number 100,
      - After restarting the connection, the switch interface should be immediately proceed to packet propagation .

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

SAVE THE CONFIGURATION ON ALL DEVICES
AND INFORM THE COMMITTEE!