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

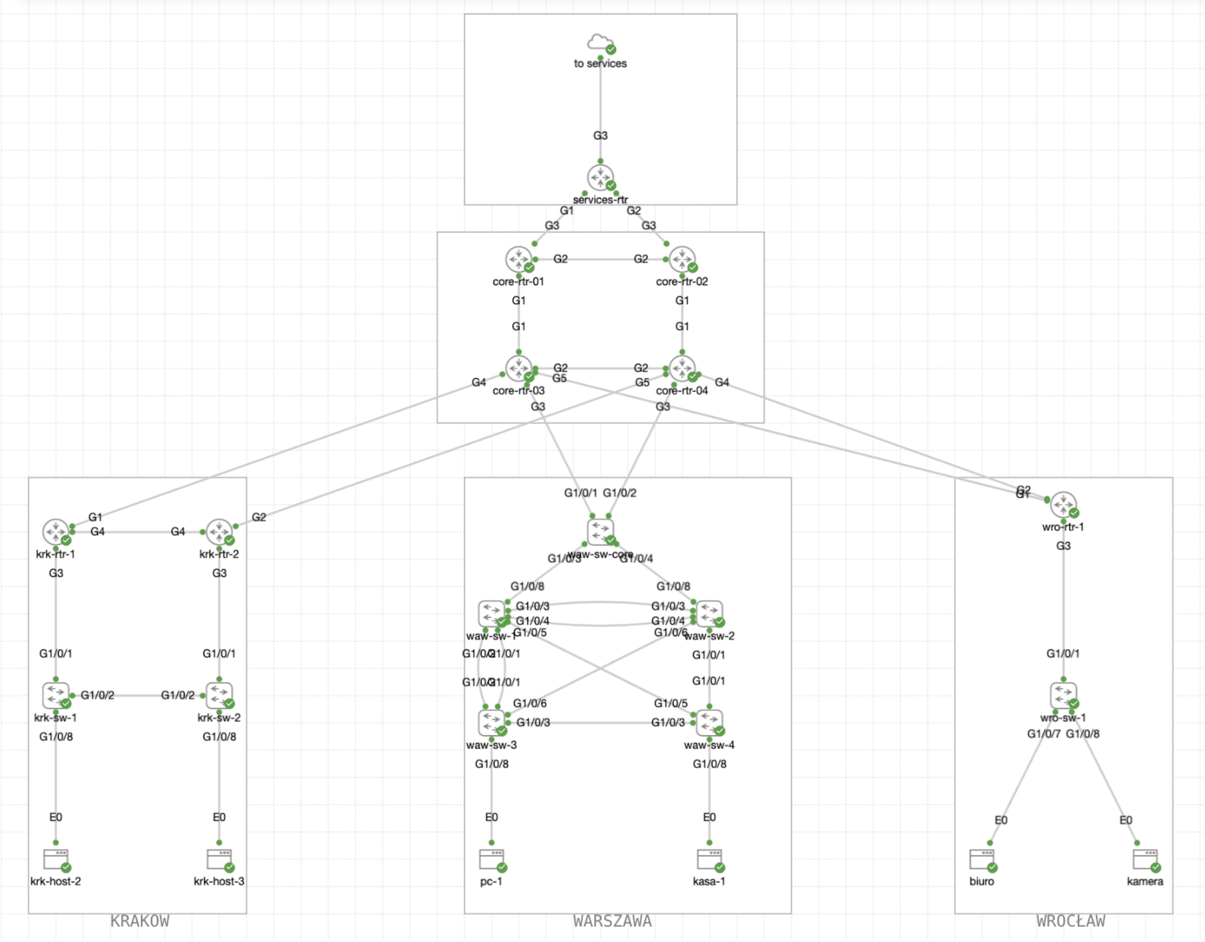
Network Systems Management

--- FINALE ---

DAY 1 - PART 1
(10:00 – 12:00)

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

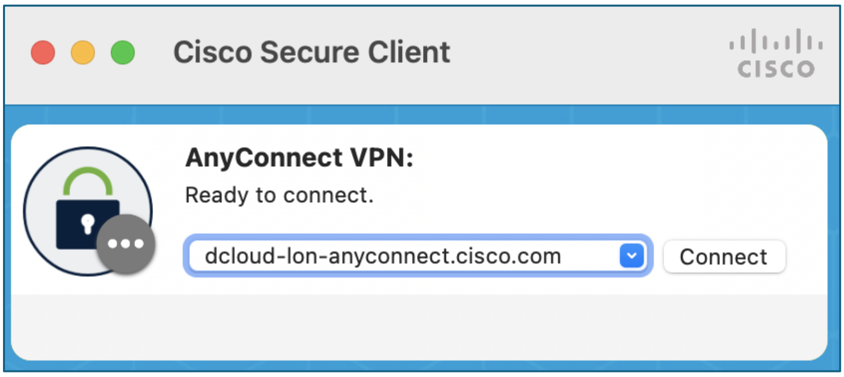
The entire competition was simulated in the Cisco dCloud environment using the following devices/versions:

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



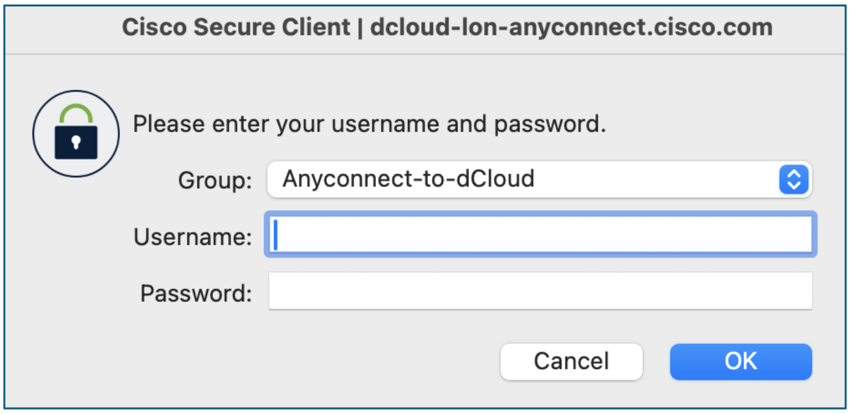
Cisco Secure Client

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:

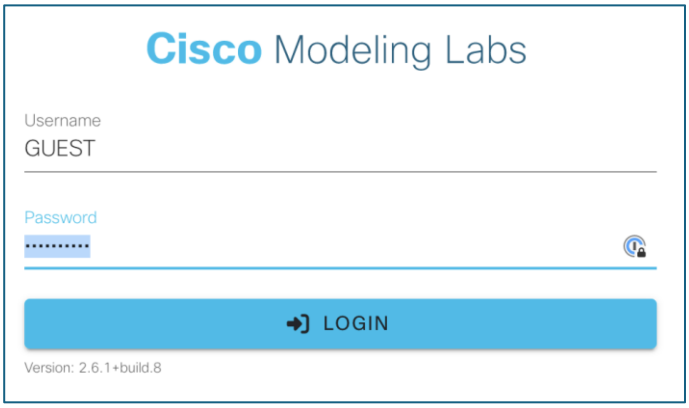
2.3. Cisco Modeling Labs (CML)

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



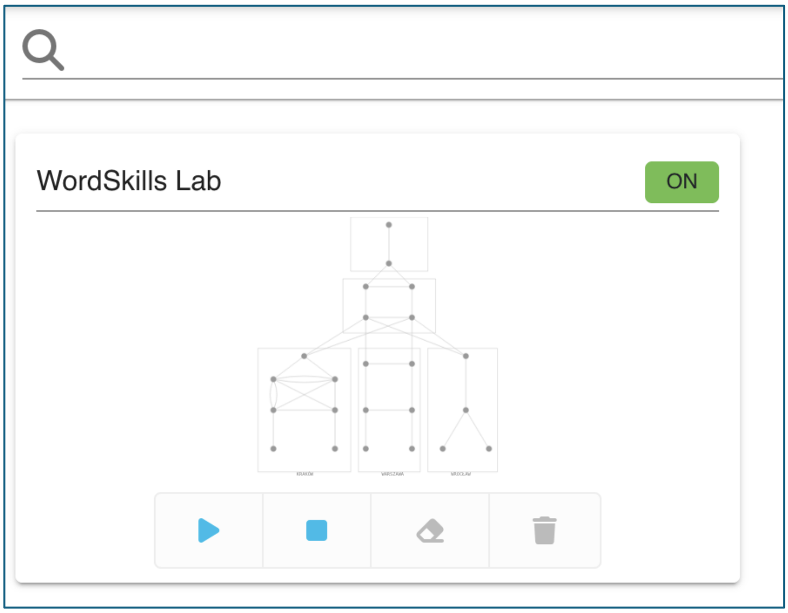
Cisco Modeling Labs

Username
GUEST

Password
••••••••••

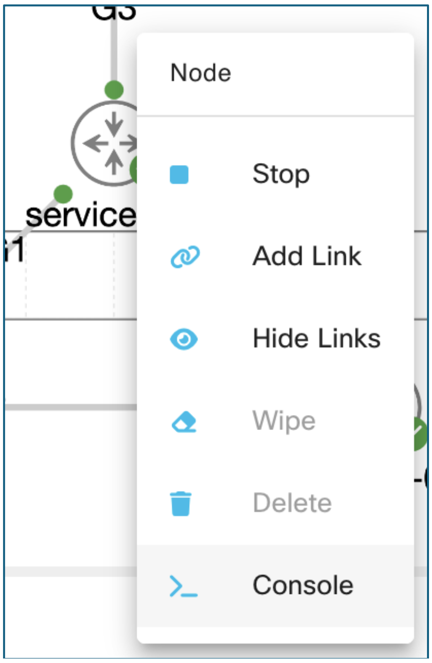
Version: 2.6.1+build.8

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):

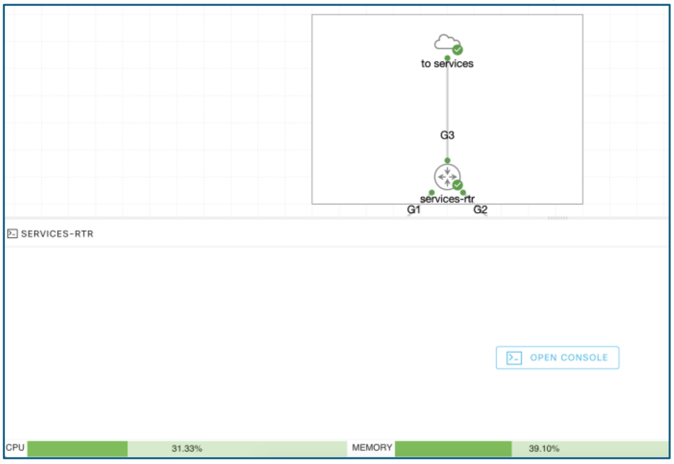


WordSkills Lab

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,
- use of materials from the Internet (except for the official documentation available 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. First Hop Redundancy Protocols [15 points]

1. Prepare an addressing scheme for 2 subnets in which the connected devices will be located – the address to be used is 172.17.0.0/23:
   a. The HOSTS-2 subnet to which the krk-host-2 host should be connected should accommodate 60 end devices (1 point)
   b. The HOSTS-3 subnet to which the krk-host-3 host should be connected should accommodate 15 end devices (1 point)
   c. Addressing should assume the best possible use of the subnet given above (1 point)
   Vlan ID for the HOSTS-2 network: VLAN 10
   Vlan ID for HOSTS-3 network: VLAN 20

2. Using the selected reliability technology for the default gateway configuration, configure the krk- rtr-1 and krk-rtr-2 devices to perform this function:
   a. The default gateway address is always the first possible subnet address (3 points)
   b. If the krk-rtr-1 device is available, make sure that it is the active default gateway for the krk-host-2 host subnet , in case of failure the krk-rtr-2 device should provide reliability in the Active/ Standby model (2 points)
   c. For host subnet krk-host-2 , device krk-rtr-2 should be active, while device krk-rtr-1 should provide reliability in case of failure of the first device (2 points)
   d. In case of restart and recovery, devices should take over their default gateway function for the appropriate subnets automatically (3 points)

3. Configure IPv4 address for hosts: krk-host-2 and krk-host-3 using selected subnets, select any address from the subnet of the given host, the default gateway should also be configured (1 point)

Commands for configuring IP on hosts krk-host-2 and krk-host-3 :

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

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

Commands for IP verification on hosts krk-host-2 and krk-host-3 :

```
ifconfig eth0
```

```
ip addr
route -n
```

4. Make sure krk-host-2 and krk-host-3 can communicate (1 point)

4.2. OSPF [20 points]

The krk-rtr-1 and krk-rtr-2 devices have been connected to core-rtr-3 and core-rtr-4 as shown in the diagram (see point 1). The core devices have already been configured – there is no need to modify them (access to these devices has also been additionally restricted to prevent configuration changes). The core devices advertise a default route to the krk-rtr-1 and krk-rtr-2 devices .

Configure your network so that:

1. The krk-rtr-1 and krk-rtr-1 devices should communicate with the connected HOSTS-2 and HOSTS-3 subnets using the OSPF protocol. Addressing the connections between the core devices and the krk-rtr-1 and krk-rtr-1 has already been completed (3 points)

2. Configure OSPF on krk-rtr-1 and krk-rtr-2 devices (5 points)
    a. Router ID for krk-rtr-1 -> 1.1.1.1
    b. Router ID for krk-rtr-2 -> 1.1.1.2
    c. Area – backbone

3. The krk-rtr-1 and krk-rtr-2 devices should be configured so that in the event of a failure of all connections of a given device to the core network , communication is still possible (2 points)

4. The OSPF protocol should be configured in such a way that adjacencies can only be established on specified interfaces, and are denied by default (2 points)

5. OSPF should be configured so that no DR/BDR is elected in the vicinity between krk-rtr-1 and krk-rtr-1 (on Gig 4 interfaces). (2 points)

6. Configure OSPF so that under normal circumstances all traffic is routed through the link to core-rtr-3 . In the event of a link or device failure, it should automatically fail over to core-rtr-4 . Use OSPF attributes to control traffic. (3 points)

7. In case the OSPF process fails on the core devices , configure a default static route on the krk-rtr-1 router that will only be used if no OSPF-derived default route is available. (3 points)

4.3. Security and NAT [15 points]

1. Using the Access Control List, secure the HOSTS-2 and HOSTS-3 subnets so that:

a. Hosts from the HOSTS-2 and HOSTS-3 subnets could communicate with each other only using the SSH and ICMP protocols (3 points)

b. Hosts from the HOSTS-2 and HOSTS-3 subnets could only connect to DNS, NTP, and HTTP/HTTPS services, regardless of the IP addresses of these services and their locations. (3 points)

c. Hosts from the HOSTS-2 and HOSTS-3 subnets could perform network testing, regardless of location, using the traceroute tool (3 points)

2. Configure the krk-rtr-1 and krk-rtr-2 devices so that when devices from the HOSTS-2 and HOSTS-3 subnets communicate , their addresses are not visible in the core network , but are hidden behind the addresses of the Gig4 interfaces of these devices. (3 points)

   The configuration should allow the same address to be used by multiple hosts on a given subnet and on multiple ports. In the event of a device failure, krk-rtr-1 should have the same functionality available on krk-rtr-2 (3 points).

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

SAVE THE CONFIGURATION ON ALL DEVICES
AND INFORM THE COMMITTEE!