SKILLScomp
Skills competitions for VET development

Co-funded by the European Union

Networking Academy

WYŻSZA SZKOŁA INFORMATYKI i ZARZĄDZANIA
z siedzibą w Rzeszowie

Konkurs Umiejętności Zawodowych

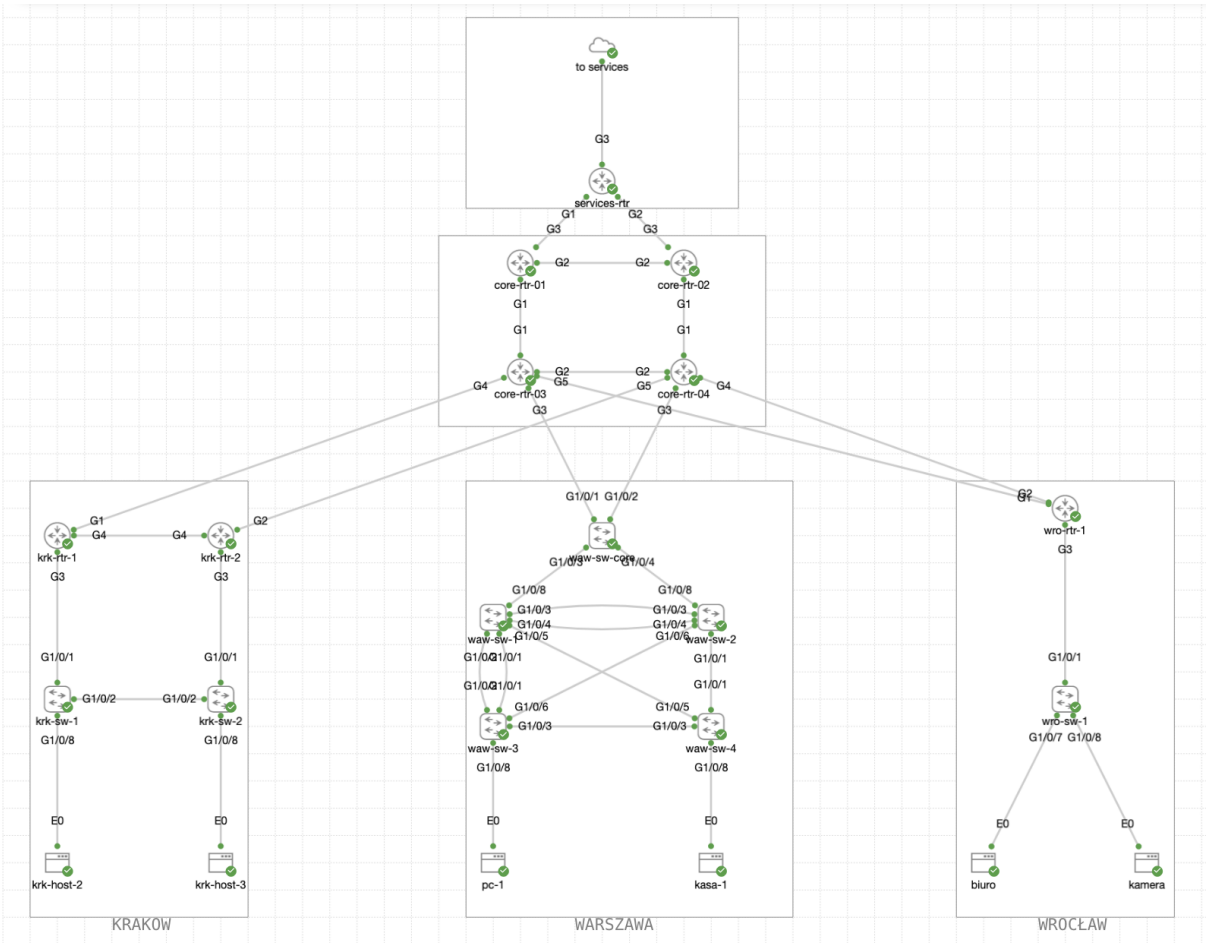
Zarządzanie Systemami Sieciowymi

--- FINAŁ ---

DZIEŃ 1 - CZĘŚĆ 1
(10:00 – 12:00)

1. Topologia

Poniższy schemat przedstawia pełną topologię sieci, która będzie używana w trakcie pierwszego dnia konkursu (dostępna także do pełnego wglądu w środowisku CML):



2. Dostęp do środowiska testowego

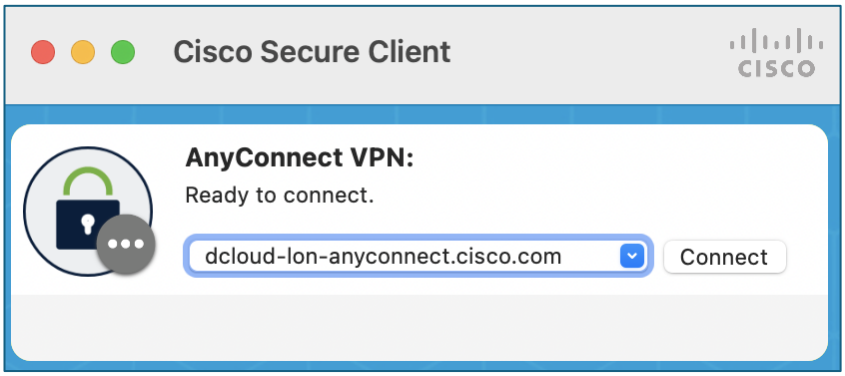
Całość konkursu została zasymulowana w środowisku Cisco dCloud przy wykorzystaniu następujących urządzeń/wersji:

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

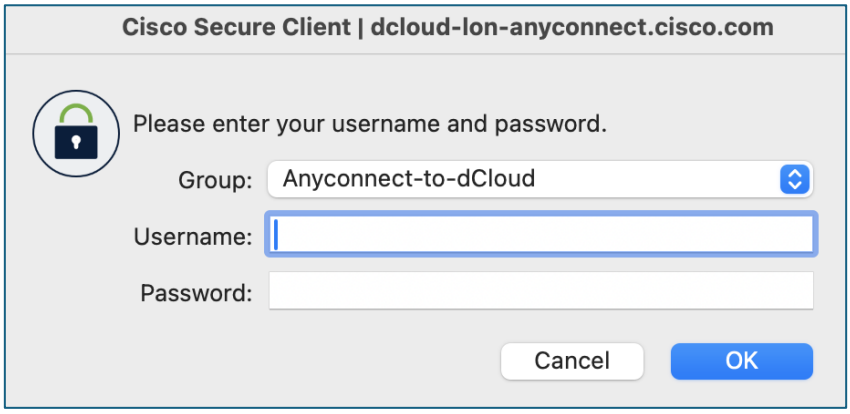
Aby uzyskać pełny dostęp do środowiska testowego, wykonaj następujące kroki:

2.2. VPN Cisco Secure Client

1) Otwórz aplikację „**Cisco Secure Client**”, podaj adres: dcloud-lon-anyconnect.cisco.com



2) Kliknij „**Connect**” i wpisz dane użytkownika (username) i hasło (password), otrzymane od organizatora konkursu:



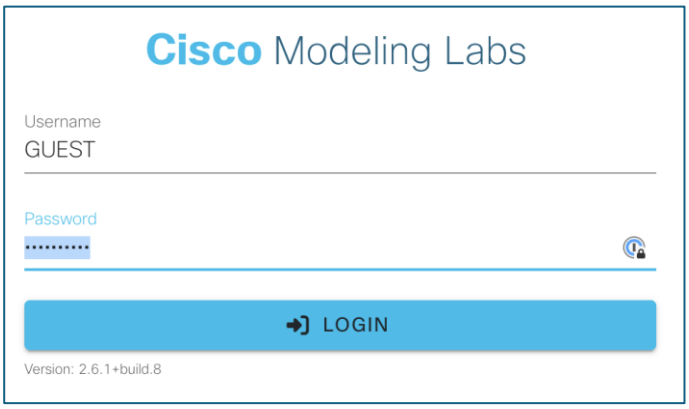
2.3. Cisco Modelling Labs (CML)

Cisco Modeling Labs (CML) umożliwia dostęp do środowiska testowego, obejmującego topologię sieci, dostęp do urządzeń oraz możliwość ich zdalnego włączania i wyłączania. Aby uzyskać dostęp do CML, upewnij się, że jesteś połączony przez VPN (zobacz punkt 2.2) i wykonaj następujące kroki:

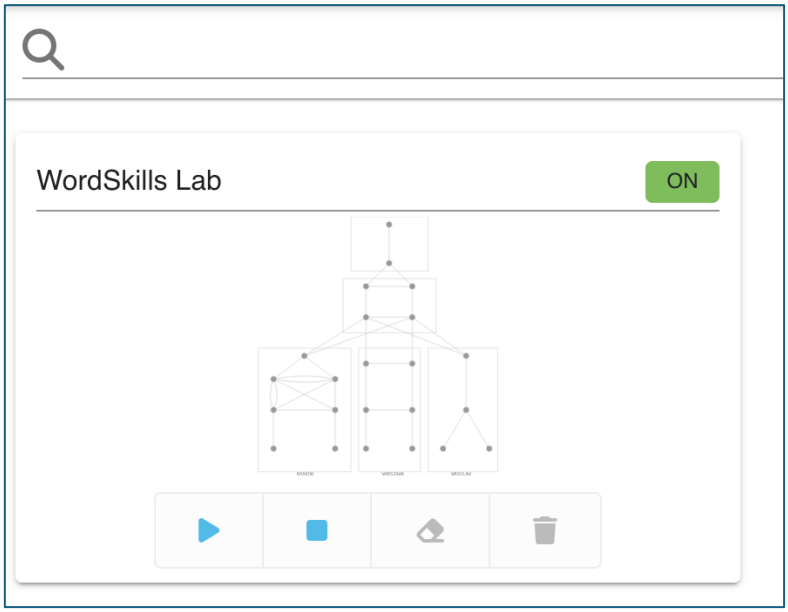
1) W przeglądarce internetowej wpisz adres:
   https://198.18.133.111/

2) Aby zalogować się do systemu użyj następujących danych:

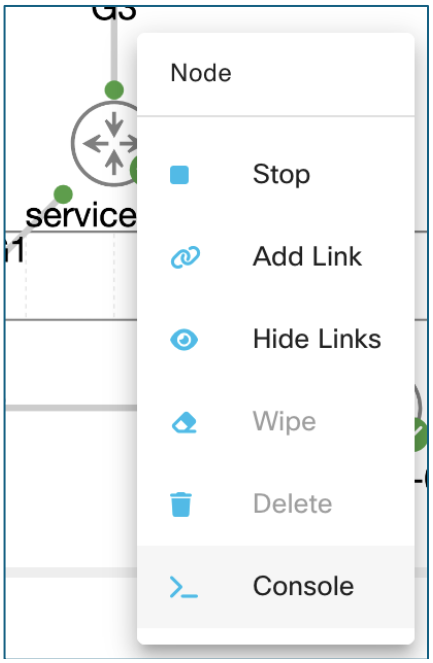
   Użytkownik: GUEST (wymagane duże litery)
   Hasło: C1sco12345



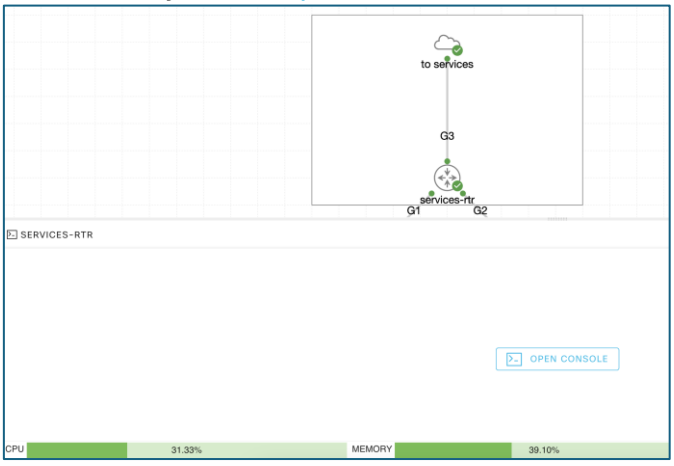
3) Środowisko labowe powinno być już zainicjowane - kliknij na topologię (unikaj klikania na przyciski start/stop/wipe/delete w dolnej części obszaru):



4) Aby uzyskać dostęp do konsoli, kliknij prawym przyciskiem myszy na konkretne urządzenie (switch, router, host) a następnie wybierz z menu opcję Console:



5) Z panelu na dole ekranu wybierz: „Open Console”:



Aby zalogować się do przełącznika/routera użyj następujących danych:

Użytkownik: cisco
Hasło: C1sco12345

2.4. Serwer Główny

Dodatkowo do topologii zasymulowanej w środowisku CML została podłączona (do routera oznaczonego jako **services-rtr**) maszyna wirtualna działająca w oparciu o system operacyjny Linux (Ubuntu).

Dostęp do maszyny możliwy jest bezpośrednio ze stacji roboczej z wykorzystaniem protokołu SSH po uprzednim połączeniu się do środowiska testowego przez VPN.

Adres IP (dostęp zdalny / mgmt): 198.18.128.100
Użytkownik: cisco
Hasło: C1sco12345

Adres IP (od strony lab / services-rtr): 198.18.10.100

2.6. Hosty

Dodatkowo w sieci podłączono dodatkowe hosty (np. krk-host-2, pc-1, kamera, ...), które pozwalają sprawdzić, czy sieć działa prawidłowo. Dostęp do tych urządzeń odbywa się przez CML w taki sam sposób jak dostęp do urządzeń sieciowych (patrz punkt 2.3) przy uwzględnieniu podanych poniżej danych:

Użytkownik: cisco
Hasło: cisco

3. Uwagi ogólne

Zabrania się:
- zmiany topologii sieci (dodawanie usuwanie urządzeń, połączeń, itp.),
- zmiany haseł / konfiguracji konsoli / VTY / ...,
- komunikowania z opiekunami, innymi uczestnikami konkursu i osobami trzecimi,
- korzystania z materiałów zInternetu (poza udostępnioną oficjalną dokumentacją na stronie cisco.com).

Nakazuje się:
- zapisanie konfiguracji na urządzeniu (copy run start) po każdej części na wszystkich urządzeniach, które następnie będą skopiowane w trakcie przerwy celem pełnej weryfikacji.

W razie jakichkolwiek problemów ze środowiskiem uczestnik jest zobowiązany zgłosić wszelkie zaobserwowane problemy bezpośrednio do komisji.

4. Zadania konkursowe [50pkt]

4.1. Protokoły First Hop Redundacy Protocol [15 pkt]

1. Przygotuj schemat adresacji dla 2 podsieci w których znajdować się będą podłączone urządzenia – adresacja do wykorzystania 172.17.0.0/23:
   a. Podsieć HOSTS-2, do której powinien być podłączony host krk-host-2 powinna pomieścić 60 urządzeń końcowych (1pkt)
   b. Podsieć HOSTS-3, do której powinien być podłączony host krk-host-3 powinna pomieścić 15 urządzeń końcowych (1pkt)
   c. Adresacja powinna zakładać jak najlepsze wykorzystanie podsieci podanej powyżej (1pkt)
   Vlan ID dla sieci HOSTS-2: VLAN 10
   Vlan ID dla sieci HOSTS-3: VLAN 20

2. Używając wybranej technologii niezawodności dla konfiguracji bramy domyślnej, skonfiguruj urządzenia krk-rtr-1 i krk-rtr-2 aby pełniły taką funkcję:
   a. Adres bramy domyślnej to zawsze pierwszy możliwy adres podsieci (3pkt)
   b. W sytuacji, gdy urządzenie krk-rtr-1 jest dostępne, upewnij się, iż jest ono aktywną bramą domyślną dla podsieci hosta krk-host-2, w przypadku awarii urządzenie krk-rtr-2 powinno zapewniać niezawodność w modelu Active/Standby (2pkt)
   c. Dla podsieci hosta krk-host-2, urządzenie krk-rtr-2 powinno być aktywne, podczas gdy urządzenie krk-rtr-1 powinno zapewniać niezawodność w przypadku awarii pierwszego urządzenia (2pkt)
   d. W przypadku restartu i powrotu urządzenia powinny przejąć swoją funkcję bramy domyślnej dla odpowiednich podsieci automatycznie (3pkt)

3. Skonfiguruj adres Ipv4 dla hostach: krk-host-2 oraz krk-host-3 przy pomocy wybranych podsieci, wybierz dowolny adres z podsieci danego hosta, brama domyślna powinna również zostać skonfigurowana (1pkt)

   Komendy do konfiguracji IP na hostach krk-host-2 oraz krk-host-3:

   ```
   sudo ifconfig eth0 <IP-ADDR> netmask <MASK>
   sudo route add default <GATEWAY> dev eth0
   ```

   Komendy do weryfikacji IP na hostach krk-host-2 oraz krk-host-3:

   ```
   ifconfig eth0
   ```

```
ip addr
route -n
```

4. Upewnij się iż krk-host-2 oraz krk-host-3 mogą się komunikować (1pkt)

4.2. OSPF [20 pkt]

Urządzenia krk-rtr-1 and krk-rtr-2 zostały podłączone do core-rtr-3 oraz core-rtr-4 jak przedstawione na schemacie (patrz punkt 1). Urządzenia core zostały już skonfigurowane – nie jest konieczna ich modyfikacja (dostęp do tych urządzeń został także dodatkowo ograniczony, tak aby nie była możliwa zmiana konfiguracji). Urządzenia core rozgłaszają trasę domyślną do urządzeń krk-rtr-1 oraz krk-rtr-2.

Skonfiguruj sieć, w taki sposób, aby:

1. Urządzenia krk-rtr-1 oraz krk-rtr-1 powinny komunikować podłączone podsieci HOSTS-2 oraz HOSTS-3 przy pomocy protokołu OSPF. Adresacja połączeń pomiędzy urządzeniami core oraz krk-rtr-1 oraz krk-rtr-1 została już wykonana (3pkt)

2. Skonfiguruj protokół OSPF na urządzeniach krk-rtr-1 oraz krk-rtr-2 (5pkt)
    a. Router ID dla krk-rtr-1 -> 1.1.1.1
    b. Router ID dla krk-rtr-2 -> 1.1.1.2
    c. Obszar – backbone

3. Urządzenia krk-rtr-1 oraz krk-rtr-2 powinny zostać skonfigurowane tak, aby na wypadek awarii wszystkich połączeń danego urządzenia do sieci core komunikacja nadal była możliwa (2pkt)

4. Protokół OSPF powinien być skonfigurowany w taki sposób, aby sąsiedztwa mogły być nawiązywane wyłącznie na wskazanych interfejsach, a domyślnie zabronione (2pkt)

5. Protokół OSPF powinien zostać skonfigurowany w taki sposób, aby w sąsiedztwie pomiędzy urządzeniami krk-rtr-1 oraz krk-rtr-1 (na interfejsach Gig 4) nie był wybierany DR/BDR. (2pkt)

6. Skonfiguruj protokół OSPF tak, aby w normalnej sytuacji cały ruch był prowadzony przez link do urządzenia core-rtr-3, na wypadek awarii linku lub urządzenia automatycznie powinien zostać przełączony na core-rtr-4. Wykorzystaj atrybuty protokołu OSPF w celu sterowania ruchem. (3pkt)

7. Na wypadek awarii procesu OSPF na urządzeniach core, skonfiguruj domyślną trasę statyczna na routerze krk-rtr-1, która będzie używana wyłącznie w przypadku braku trasy domyślnej pochodzącej z protokołu OSPF. (3pkt)

4.3. Bezpieczeństwo i NAT [15 pkt]

1. Przy pomocy Access Control List zabezpiecz podsieci HOSTS-2 oraz HOSTS-3 tak aby:
    a. Hosty z podsieci HOSTS-2 i HOSTS-3 mogły komunikować się między sobą wyłącznie przy pomocy protokołu SSH i ICMP (3 pkt)

    b. Hosty z podsieci HOSTS-2 oraz HOSTS-3 mogły łączyć się wyłącznie z usługami DNS, NTP, HTTP/HTTPS niezależnie od adresów IP tych serwisów i ich lokalizacji. (3pkt)

    c. Hosty z podsieci HOSTS-2 oraz HOSTS-3 mogły wykonywać testowanie sieci, niezależnie od lokalizacji, przy pomocy narzędzia traceroute (3pkt)

2. Skonfiguruj urządzenia krk-rtr-1 oraz krk-rtr-2, aby podczas komunikacji urządzeń z podsieci HOSTS-2 oraz HOSTS-3 ich adresy nie były widoczne w sieci core, ale były ukryte za adresami interfejsów Gig4 tych urządzeń. (3pkt)

   Konfiguracja powinna pozwalać na wykorzystanie tego samego adresu przez wiele hostów danej podsieci i na wielu portach. W przypadku awarii urządzenia, krk-rtr-1 ta sama funkcja powinna być dostępna na krk-rtr-2 (3pkt)

GRATULACJE – ZAKOŃCZYŁEŚ ETAP:
DZIEŃ 1 / CZĘŚĆ 1

ZAPISZ KONFIGURACJĘ NA WSZYSTKICH URZĄDZENIACH
I POINFORMUJ KOMISJĘ!