Konkurs Umiejętności Zawodowych

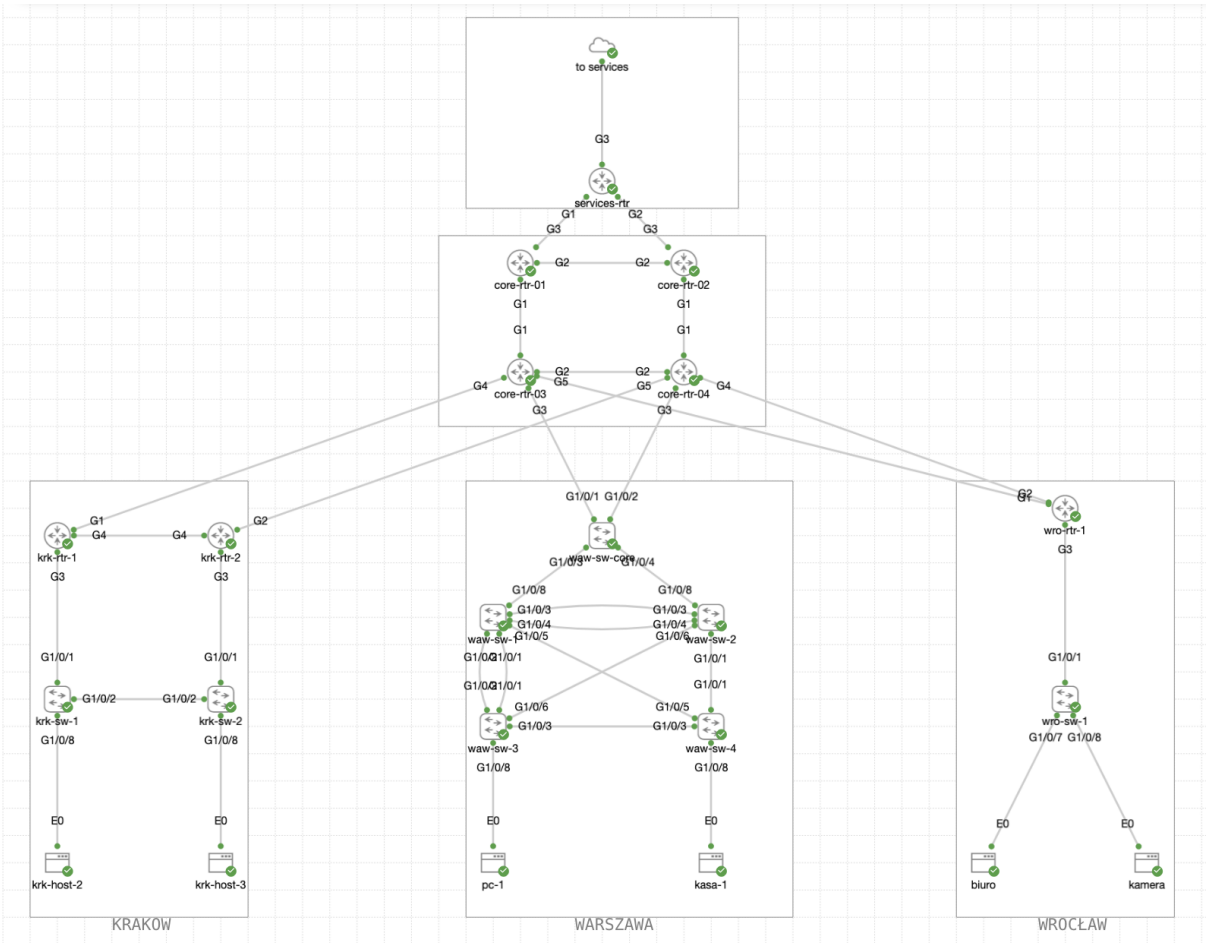
Zarządzanie Systemami Sieciowymi

--- FINAŁ ---

DZIEŃ 1 - CZĘŚĆ 2
(13:00 – 14:30)

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

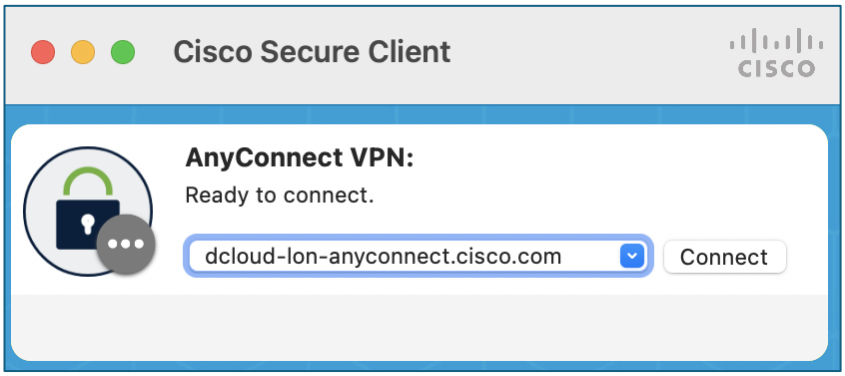
Całość konkursu została zasymulowana w środowisku Cisco dCloud przy wykorzystaniu następujących urządzeń/wersji:

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

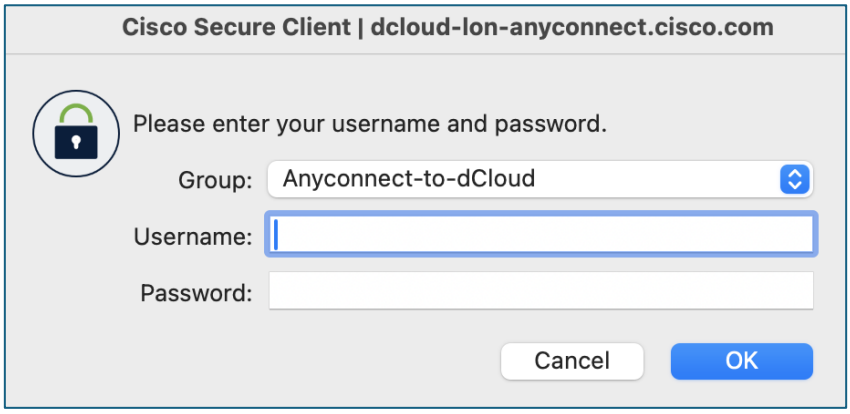
Aby uzyskać pełny dostęp do środowiska testowego, wykonaj następujące kroki:

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:



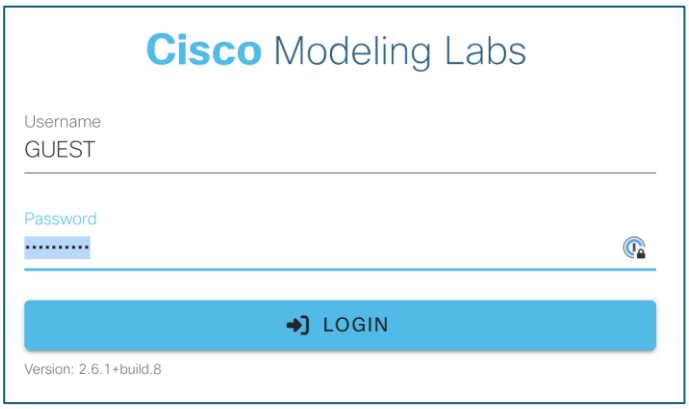
2.3. Cisco Modelling Labs (CML)

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:

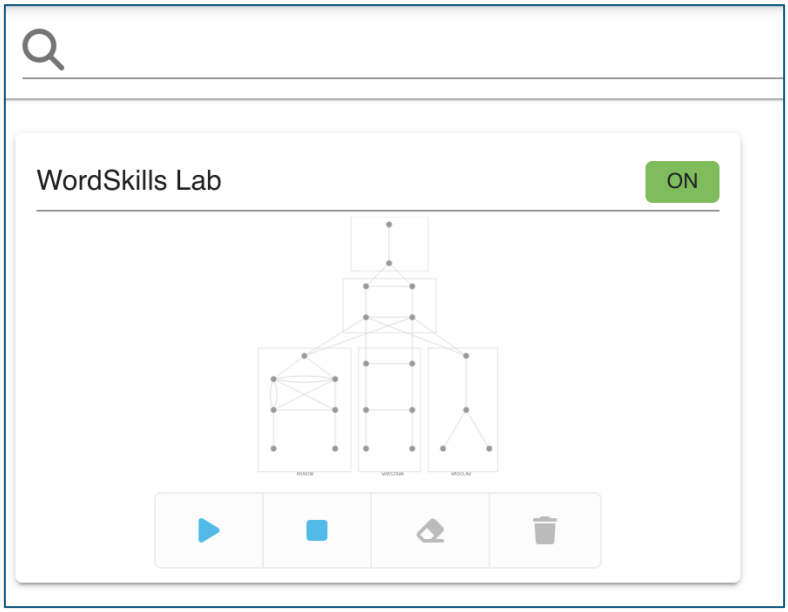
1) W przeglądarce internetowej wpisz adres:
   https://198.18.133.111/

2) Aby zalogować się do systemu użyj następujących danych:

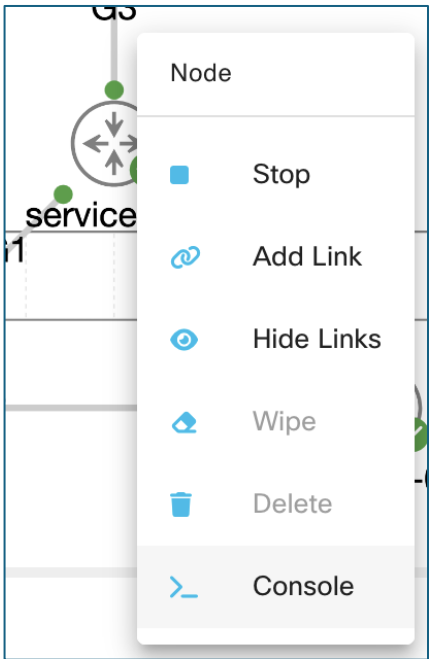
   Użytkownik: GUEST (wymagane duże litery)
   Hasło: C1sco12345



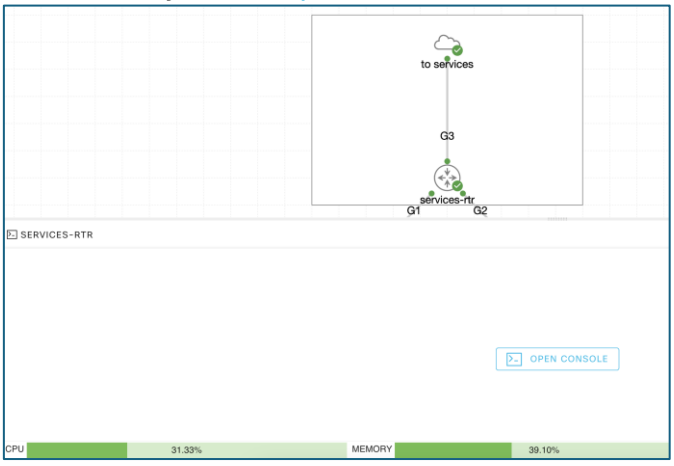
3) Środowisko labowe powinno być już zainicjowane - kliknij na topologię (unikaj klikania na przyciski start/stop/wipe/delete w dolnej części obszaru):



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 Internetu (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 [30pkt]

W sieci oddziału Warszawa znajdują się cztery przełączniki oraz jeden router. Router jest przygotowany do założonej propagacji pakietów, zadania konfiguracyjne będą wykonywane wyłącznie na przełącznikach sieciowych oraz hostach. Przełączniki nie posiadają obecnie żadnej konfiguracji przygotowane są jedynie połączenia. Celem zadania jest przygotowanie konfiguracji dla trzech departamentów z czego tylko dwa będą komunikować się z centralą firmy poprzez rdzeń sieci. Te oddziały to księgowość, kasy oraz kadry.

4.1. Konfiguracja podstawowa [5 pkt]

1. Skonfiguruj nazwy wszystkich urządzeń. (1 pkt)

2. Skonfiguruj wszystkie redundantne połączenia pomiędzy następującymi parami urządzeń (Urządzenia powinny korzystać z protokołu LACP). (2 pkt)

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

3. Skonfiguruj urządzenia tak, aby była możliwa weryfikacja połączeń z poziomu CLI za pomocą LLDP oraz CDP. (1 pkt)

4. Ustaw opisy interfejsów łączących przełączniki w taki sposób, aby móc na ich podstawie identyfikować urządzenie po drugiej stronie bez konieczności korzystania z protokołów CDP/LLDP. Następnie ustaw linki w trybie umożliwiającym przesłanie ramek w różnych VLAN'ach. (1 pkt)

4.2. Sieci wirtualne [15 pkt]

1. Skonfiguruj urządzenia waw-sw-1 oraz waw-sw-2 do automatycznej propagacji konfiguracji sieci wirtualnych za pomocą protokołu VTP zgodnie z poniższą tabelą (4 pkt):

Urządzenie	Wersja VTP	Tryb	Domena
waw-sw-1	3	serwer	waw-01
waw-sw-2	3	klient	waw-01
waw-sw-3	3	transparentny	waw-01
waw-sw-4	3	transparentny	waw-01

2. Skonfiguruj VLAN 10 oraz nazwij go jako: NATIVE (1 pkt)

3. Utwórz sieci wirtualne o następującej numeracji (2 pkt):

    a. 100 → Kadry

    b. 110 → Ksiegowosc

    3. 120 → Kasy

    Uwaga: informacje na temat rozmieszczenia sieci wirtualnych można znaleźć w tabeli poniżej.

VLAN ID	waw-sw-1	waw-sw-2	waw-sw-3	waw-sw-4
100	tak	tak	tak	nie
110	tak	tak	tak	nie
120	tak	tak	tak	tak

4. Skonfiguruj połączenia typu **trunk** zgodnie z poniższą tabelą (6 pkt):

Przełącznik 1	Przełącznik 2	Interface	Native VLAN	VLAN allowed
waw-sw-1	waw-sw-2	Po20	10	100,110,120
waw-sw-1	waw-sw-3	Po10	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. Skonfiguruj urządzenia w taki sposób, aby wszystkie urządzenia miały odblokowane interfejsy w kierunku przełącznika waw-sw-core (dotyczy wszystkich sieci wirtualnych skonfigurowanych na danym przełączniku) (2 pkt).

4.3. Konfiguracja warstwy dostępowej [10pkt]

1. Skonfiguruj hosty kasa-1 oraz pc-1 w następujący sposób (2 pkt)

Nazwa Hosta	Adres IP	Maska
Pc-1	172.16.0.10	/25
Kasa-1	172.16.0.140	/25

Komendy do konfiguracji IP na hostach kasa-1 oraz pc-1:

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

Komendy do weryfikacji IP na hostach kasa-1 oraz pc-1:

```
ifconfig eth0
ip addr
route -n
```

2. Skonfiguruj interfejsy, do których podłączone zostały hosty kasa-1 oraz pc-1 w taki sposób, aby:
   a. Dla hosta kasa-1 należy przygotować konfigurację spełniającą następujące wymagania: (5 pkt)

      - Dostęp tylko do pojedynczego VLAN'u o numerze 120,
      - Konfiguracja interfejsu w taki sposób, aby tylko host kasa-1 miał do niego dostęp,
      - W razie próby podłączenia do interfejsu innego hosta port powinien został automatycznie zablokowany,
      - Po podłączeniu hosta interfejs powinien w sposób natychmiastowy przechodzić do propagacji pakietów.

   b. Dla hosta pc-1 należy przygotować konfigurację spełniającą następujące wymagania: (3 pkt)

      - Dostęp tylko do pojedynczego VLAN'u o numerze 100,
      - Po restarcie połączenia interfejs przełącznika powinien od razu przechodzić do propagacji pakietów.

GRATULACJE – ZAKOŃCZYŁEŚ ETAP:
DZIEŃ 1 / CZĘŚĆ 2

ZAPISZ KONFIGURACJĘ NA WSZYSTKICH URZĄDZENIACH
I POINFORMUJ KOMISJĘ!