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

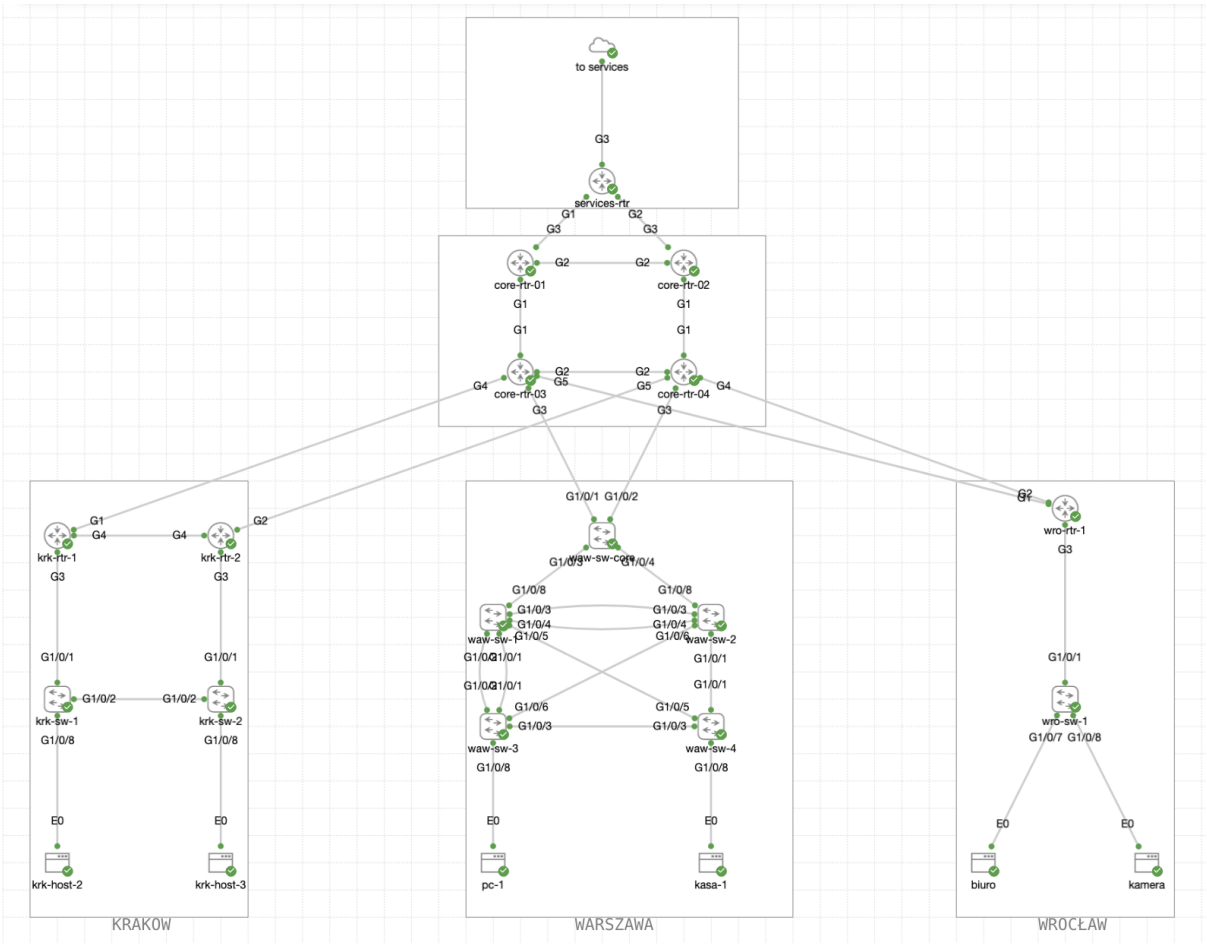
Zarządzanie Systemami Sieciowymi

--- FINAŁ ---

DZIEŃ 1 - CZĘŚĆ 3
(14:45 – 16:15)

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

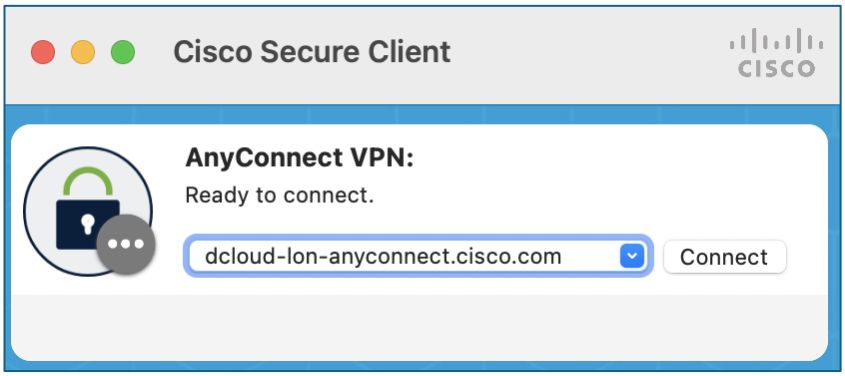
Całość konkursu została zasymulowana w środowisku Cisco dCloud przy wykorzystaniu następujących urządzeń/wersji:

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

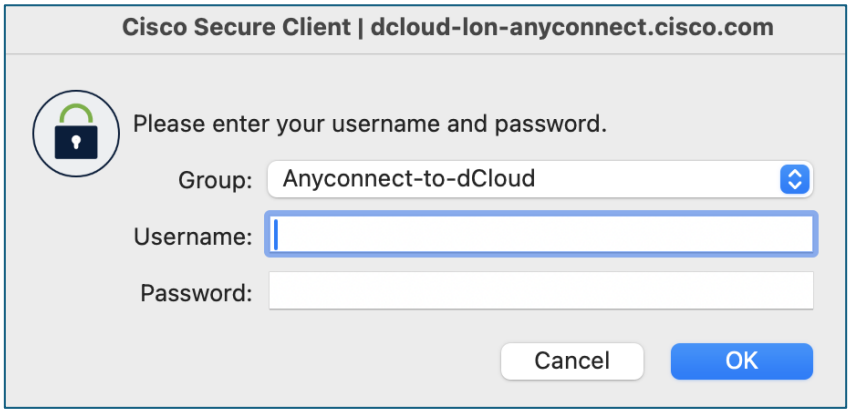
Aby uzyskać pełny dostęp do środowiska testowego, wykonaj następujące kroki:

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:



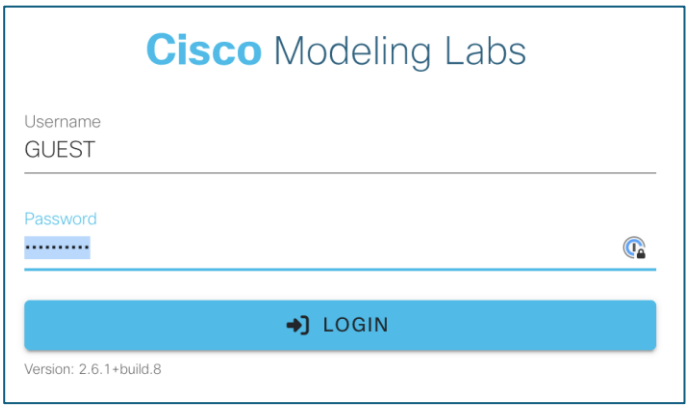
2.3. Cisco Modelling Labs (CML)

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:

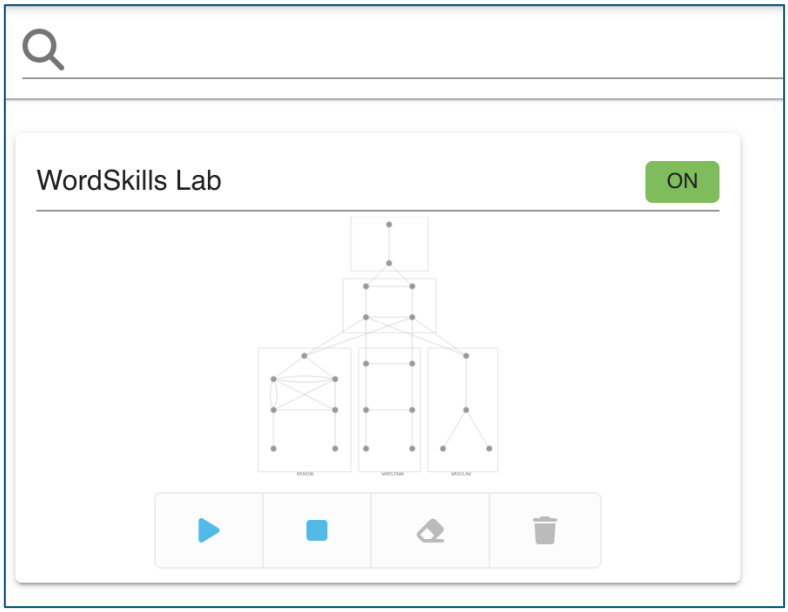
1) W przeglądarce internetowej wpisz adres:
   https://198.18.133.111/

2) Aby zalogować się do systemu użyj następujących danych:

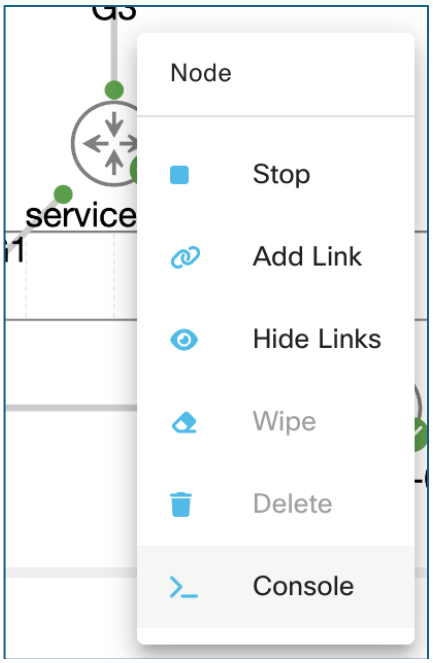
   Użytkownik: GUEST (wymagane duże litery)
   Hasło: C1sco12345



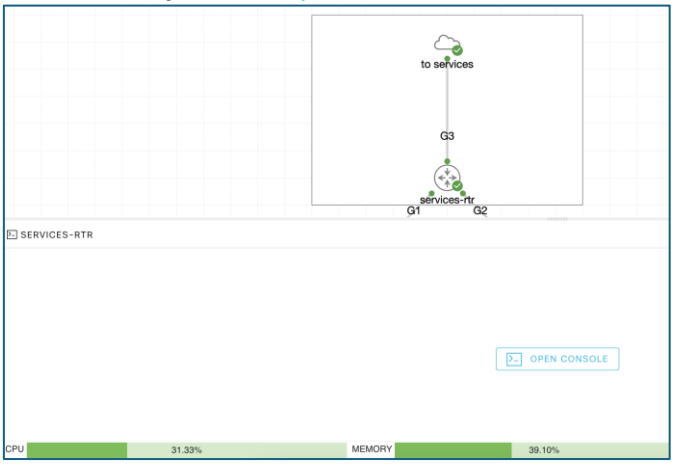
3) Środowisko labowe powinno być już zainicjowane - kliknij na topologię (unikaj klikania na przyciski start/stop/wipe/delete w dolnej części obszaru):



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 [20pkt]

4.1. Dostęp do urządzeń / aliasy [1 pkt]

Skonfiguruj urządzenia wro-sw-01 oraz wro-rtr-01 w taki sposób, aby:

a. administrator poprzez wykonanie komendy **router** mógł się zalogować na urządzenie wro-rtr-01 z urządzenia: wro-sw-01 (0.5pkt)
b. administrator poprzez wykonanie komendy **switch** mógł się zalogować na urządzenie wro-sw-01 z urządzenia wro-rtr-01 (0.5pkt)

4.2. Informacja dla administratorów [2 pkt]

Skonfiguruj urządzenie wro-rtr-01 oraz wro-sw-01 w taki sposób, iż w momencie logowania (ale jeszcze przed podaniem prawidłowych danych do logowania: użytkownika/hasła) będzie wyświetlona informacja (1pkt):

```
================================================
Dostęp do systemu jest ograniczony tylko do
autoryzowanych użytkowników.
================================================
```

Dodatkowo skonfiguruj urządzenia wro-rtr-01 oraz wro-sw-01 w taki sposób, aby tylko po udanym logowaniu pojawiła się dodatkowa informacja (1pkt):

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

Loopback0: <<adres IP Lo0>>
PID: <<model urządzenia>>
S/N: <<numer seryjny urządzenia>>
================================================
```

Gdzie zmienne: `<<hostname>>`, `<<adres IP Lo0>>`, `<<model urządzenia>>`, `<<numer seryjny urządzenia>>` powinny być podmienione poprawnymi wartościami dla konkretnego urządzenia.

4.3. Czas systemowy - przełącznik [2 pkt]

Skonfiguruj urządzenie wro-sw-01 w taki sposób, aby:

a. w logach i debugach pokazywała się dokładna data i godzina, a znacznik czasu był wyświetlany z dokładnością do milisekund (0.5pkt),
b. w logach pokazywała się informacja o strefie czasowej CET (gdzie CET jest czasem GMT przesuniętym o +1 godzinę) (0.5pkt),
c. na momencie, kiedy w Polsce obowiązuje czas letni, urządzenie powinno informować o strefie czasowej CEST zamiast CET (zmiana czasu jest 2 marca o godzinie 2 w nocy oraz 3 października o godzinie 3 w nocy) (1pkt).

4.4. Logowanie [2 pkt]

Po niedawnych incydentach związanych z nieuprawnionymi zmianami w sieci przez byłego pracownika, zespół security poprosił o pomoc w implementacji dodatkowego audytu konfiguracji i rozszerzenie logowania zdarzeń w sieci.

Skonfiguruj urządzenia wro-rtr-01 oraz wro-sw-01 w taki sposób, aby:

a. tylko logi na poziomie `critical` i wyższym powinny być generowane na konsoli (0.5pkt)
b. oba urządzenia wysyłały logi do serwera głównego (pod adresem: 198.18.10.100) z adresem źródłowym będącym adresem IP skonfigurowanym na interfejsie **Loopback0** i były oznaczone (facility) jako **local0** (0.5pkt)
c. dodatkowo wszystkie komendy wykonywane na urządzeniu (w trybie konfiguracyjnym) powinny być archiwizowane na serwerze (1pkt)

***Uwaga**: celem weryfikacji, dostęp do serwera głównego jest możliwy przez SSH.*

***Adres IP (mgmt only)**: 198.18.128.100*
***Użytkownik**: cisco*
***Hasło**: C1sco12345*

*Serwer główny jest w pełni skonfigurowany i nie wymaga żadnych zmian. Wszystkie informacje wysłane do serwera na adres IP: 198.18.10.100 na porcie UDP/514 są automatycznie zapisywane do plików. Nazwa pliku odpowiada adresowi SRC IP pakietu. Pliki są przetrzymywane w katalogu: **/var/log/network/***

4.5. Monitorowanie [2 pkt]

Zespół odpowiadający za monitorowanie sieci zgłosił problem z brakiem widoczności lokalizacji wrocławskiej, co uniemożliwia im prawidłowe wykrywanie jakichkolwiek problemów związanych z siecią. Twoim zadaniem jest im pomóc i zaadresować ten problem. Skonfiguruj urządzenie **wro-rtr-01**:

a. aby urządzenie mogło być „odpytywane" z serwera głównego w sieci za pomocą (1pkt):
   - community: public (tylko do odczytu)
   - community: private (odczyt/zapis)

b. dodatkowo, w przypadku jakiekolwiek zmiany konfiguracji, informacja i takim zdarzeniu powinna być wysyłana do serwera Linux na adres 198.18.10.100 z community cisco i z adresem źródłowym urządzenia jako Trap (1pkt)

Uwaga: celem weryfikacji, dostęp do serwera głównego jest możliwy przez SSH.

Adres IP: 198.18.128.100
Użytkownik: cisco
Hasło: C1sco12345

Gdzie dostępne są komendy: snmpget, snmpwalk, itp.

Serwer główny jest w pełni skonfigurowany i nie wymaga żadnych zmian. Informacja o otrzymaniu pakietu skierowanego do serwera na adres IP: 198.18.10.100 na porcie UDP/162 jest automatycznie zapisywana do pliku: **traps.txt** w katalogu: **/var/log/snmp**

4.6. Dynamiczne adresowanie urządzeń końcowych [7 pkt]

W oddziale wrocławskim zaistniała konieczność dodania dwóch dodatkowych segmentów sieci – dla użytkowników (host: biuro) i urządzeń IoT (host: kamea) - każda wpierająca około 100 urządzeń. Do dyspozycji jest jedynie podsieć 172.18.100.0/24.

Skonfiguruj wro-rtr-01 oraz wro-sw-02 w taki sposób, aby:

Dla podsieci użytkowników (3pkt):
- pierwszy adres z przydzielonej podsieci był zarezerwowany dla bramy domyślnej,
- adresy IP powinny być przydzielane dynamicznie z pominięciem pierwszych pięciu adresów w przydzielonej podsieci,
- serwer DNS przydzielany użytkownikom był równy 8.8.8.8,
- domena dla użytkowników była równa: users.wroclaw.org
- adres IP dla użytkowników powinien być przydzielany na maksymalnie 4 godziny.

Dla podsieci urządzeń IoT (3pkt):
- ostatni adres z przydzielonej podsieci był zarezerwowany dla bramy domyślnej,
- ostatnie pięć adresów w przydzielonej podsieci powinny być zarezerwowane,
- urządzenie o nazwie **kamera** powinno mieć na stałe przypisany piąty w kolejności adres z podsieci.
- serwery DNS przydzielana urządzeniom IoT były równe 8.8.8.8 i 1.1.1.1.
- domena dla urządzeń IoT była równa: iot.wroclaw.org

Uwaga: celem weryfikacji, zapewniony jest dostęp do dwóch hostów, które są podłączone do przełącznika **wro-sw-01** o nazwach: **biuro** (który powinien funkcjonować w podsieci użytkowników) oraz **kamera** (który powinien funkcjonować w podsieci urządzeń IoT). Oba urządzenia powinny pobrać adres IP w sposób dynamiczny, zgodnie z w/w regułami i móc komunikować się z adresem 198.18.10.100 (1pkt).

Dostęp do hostów:
Użytkownik: cisco
Hasło: cisco

Aby odświeżyć pobranie adresu IP, należy wykonać komendę na urządzeniu:
```
sudo /etc/init.d/networking restart
```

4.7. QoS [4 pkt]

W oddziale wrocławskim została zainstalowana krytyczny system IoT, którego ruch powinien być traktowany w taki sposób, aby nie był on odrzucany przez dostawcę ISP w core sieci.

Zgodnie z umową z ISP, ruch w ich sieci dla klasy CS3 jest traktowany w sposób specjalny i Twój zespół poprosił Ciebie o takie skonfigurowanie oddziału wrocławskiego, aby tylko poniższy ruch wykorzystywał tę klasę (2pkt):
Source: urządzenie IoT o nazwie **kamera** podłączone do przełącznika wro-sw-01
Destination: serwer główny: 198.18.10.10
Typ ruchu: http

Dodatkowo, cały pozostały ruch ze wszystkich urządzeń IoT powinien być oznaczany jako CS1. Cały pozostały ruch powinien być oznaczony jako BE w momencie, kiedy trafia on do sieci core (ISP) (2pkt).

GRATULACJE – ZAKOŃCZYŁEŚ ETAP:
DZIEŃ 1 / CZĘŚĆ 3

ZAPISZ KONFIGURACJĘ NA WSZYSTKICH URZĄDZENIACH
I POINFORMUJ KOMISJĘ!