SKILLScomp
Skills competitions for VET development

Co-funded by the European Union

Networking Academy

WYŻSZA SZKOŁA INFORMATYKI i ZARZĄDZANIA
z siedzibą w Rzeszowie

Concurs de competențe profesionale

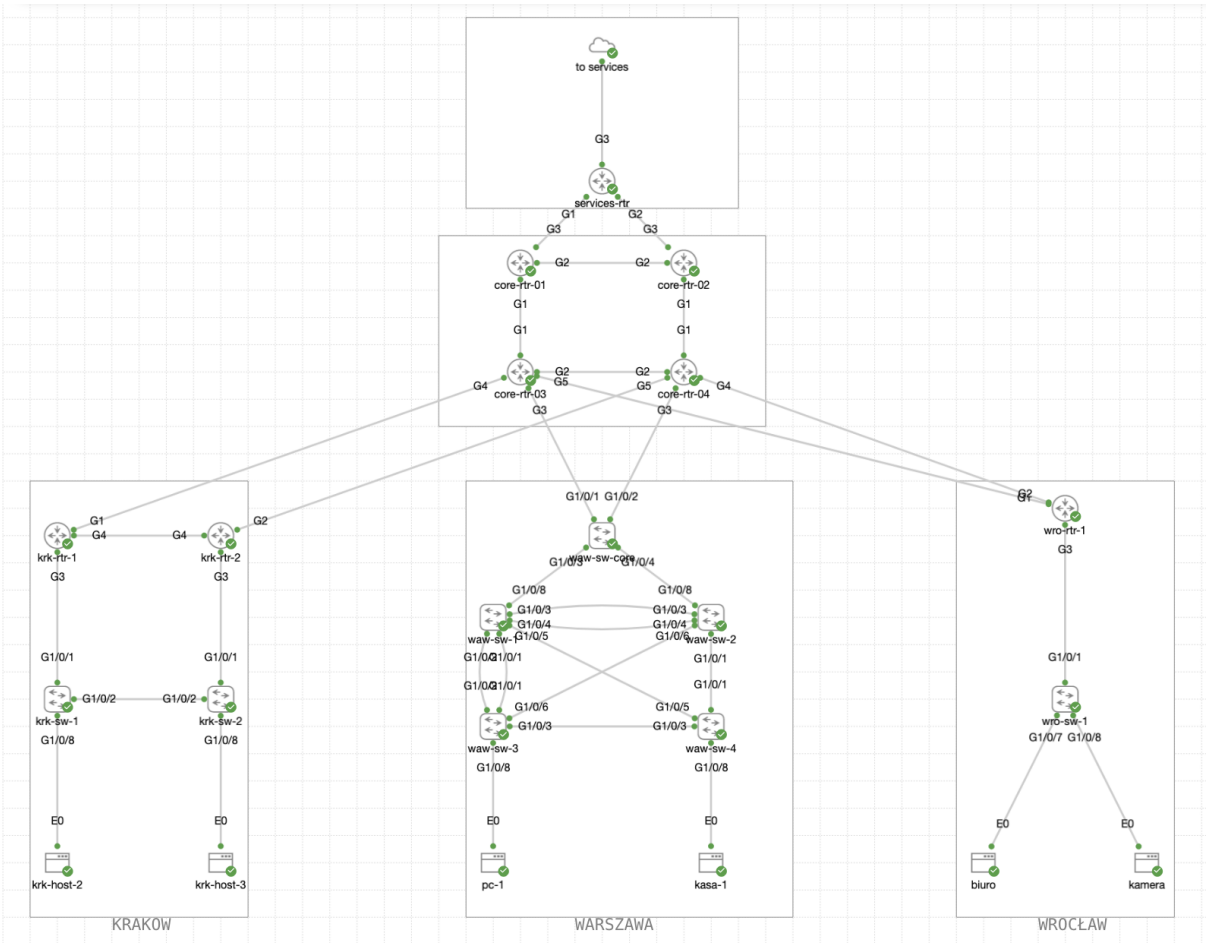
Managementul sistemelor de rețea

--- FINAL ---

ZIUA 1 - PARTEA 1
(10:00 – 12:00)

1. Topologie

Diagrama de mai jos prezintă topologia completă a rețelei care va fi utilizată în prima zi a competiției (disponibilă și pentru vizualizare completă în mediul CML):



2. Accesul la mediul de testare

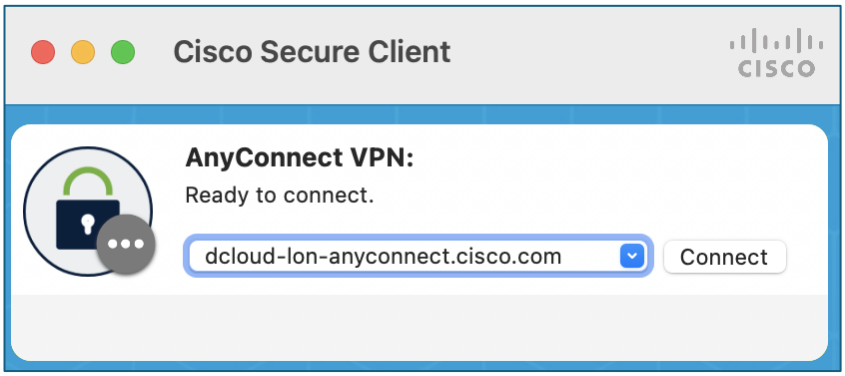
Întreaga competiție a fost simulată în mediul Cisco dCloud folosind următoarele dispozitive/versiuni:

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

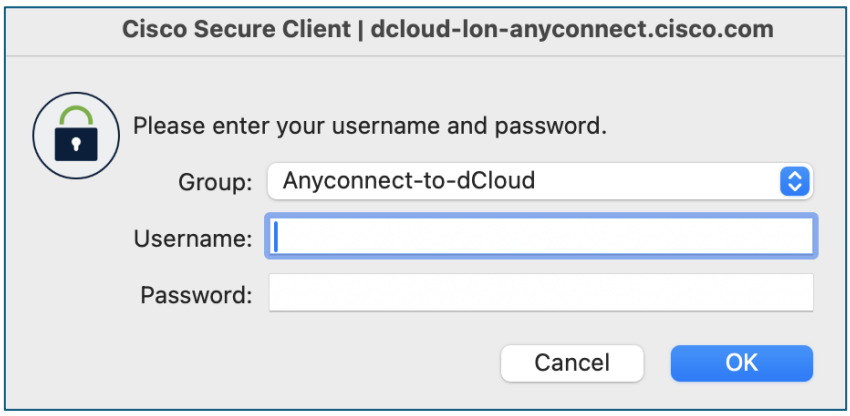
Pentru a obține acces complet la mediul de testare, urmați acești pași:

2.2. clientului securizat Cisco

1) Deschideți aplicația „ **Cisco Secure Client** ”, introduceți adresa: dcloud-lon-anyconnect.cisco.com



2) Faceți clic pe „ **Conectare** ” și introduceți numele de utilizator și parola primite de la organizatorul concursului:



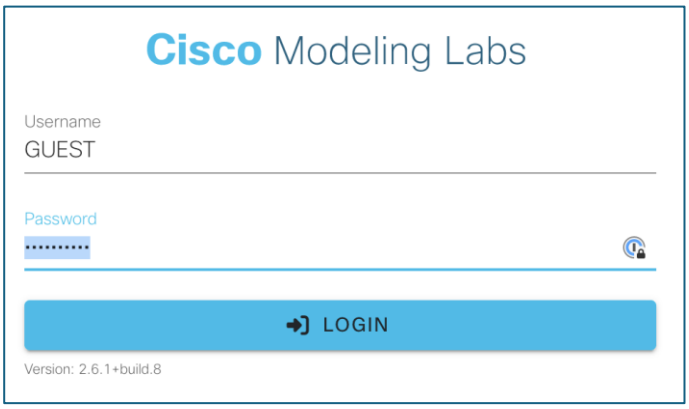
2.3. Laboratoarele de modelare Cisco (CML)

Cisco Modeling Labs (CML) oferă acces la un mediu de testare care include topologia rețelei, accesul la dispozitive și posibilitatea de a le porni și opri de la distanță. Pentru a accesa CML, asigurați-vă că sunteți conectat prin VPN (consultați secțiunea 2.2) și urmați acești pași:

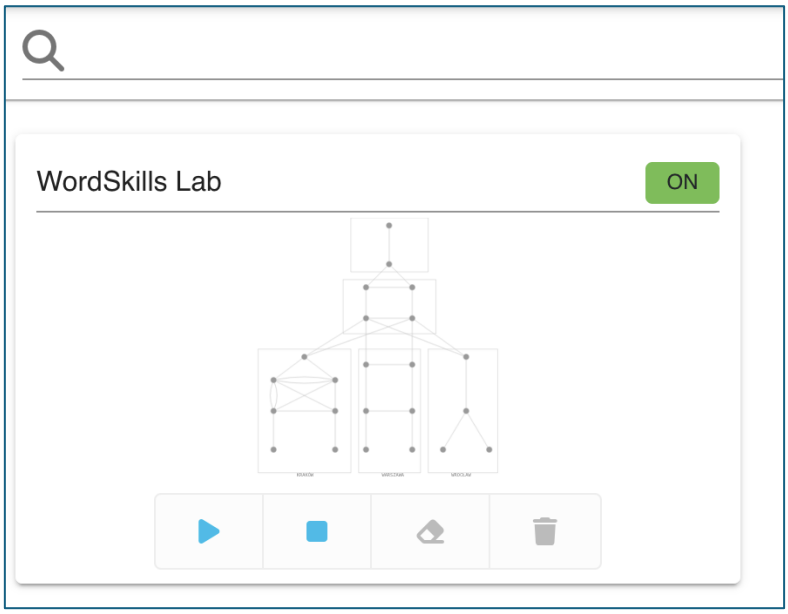
1) În browserul web, introduceți adresa:
   https://198.18.133.111/

2) Pentru a vă conecta la sistem, utilizați următoarele detalii:

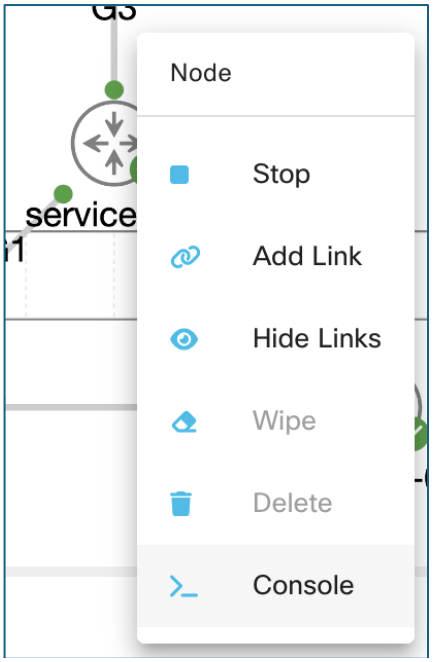
   Nume de utilizator : GUEST (majuscule obligatorii)
   Parolă : C1sco12345



3) Mediul de laborator ar trebui acum inițializat - faceți clic pe topologie (evitați să faceți clic pe butoanele de pornire/oprire/ ștergere / ștergere din partea de jos a zonei):



4) Pentru a accesa consola, faceți clic dreapta pe un anumit dispozitiv (switch , router, host) și apoi selectați Console din meniu :



5) Din panoul din partea de jos a ecranului, selectați: „ Deschideți consola ”:

Pentru a vă conecta la switch/router, utilizați următoarele detalii:

Utilizator : cisco

Parolă : C1sco12345

2.4. Serverul principal

o mașină virtuală care rulează sistemul de operare Linux (Ubuntu) a fost conectată la topologia simulată în mediul CML (la routerul marcat ca **services -rtr)** .

Accesul la mașină este posibil direct de pe stația de lucru folosind protocolul SSH după conectarea la mediul de testare prin VPN.

Adresă IP (acces la distanță / administrare) : 198.18.128.100
Utilizator : cisco
Parolă : C1sco12345

Adresă IP (din partea laboratorului/serviciilor - rtr) : 198.18.10.100

2.6. Hostas

În plus, la rețea sunt conectate gazde suplimentare (de exemplu, krk-host-2, pc-1, cameră etc.) pentru a verifica dacă rețeaua funcționează corect. Aceste dispozitive sunt accesate prin CML în același mod ca și dispozitivele de rețea (vezi secțiunea 2.3), ținând cont de următoarele date:

Utilizator : cisco
Parolă : Cisco

3. Note generale

Este interzis să:
- modificări ale topologiei rețelei (adăugarea sau eliminarea de dispozitive, conexiuni etc.),
- modificări parolă / configurare consolă / VTY / ...,
- comunicarea cu tutorii, alți participanți la concurs și terți,
- utilizarea materialelor de pe internet (cu excepția documentației oficiale disponibile pe cisco.com).

Se ordonează:
- salvarea configurației pe dispozitiv (copy run start) după fiecare parte pe toate dispozitivele, care va fi apoi copiată în timpul pauzei pentru verificare completă.

În cazul apariției oricăror probleme de mediu, participantul este obligat să raporteze orice problemă observată direct comitetului.

4. Sarcini de concurs [50 de puncte]

4.1. Protocoale de redundanță de prim salt [15 puncte]

1. Pregătiți o schemă de adresare pentru 2 subrețele în care vor fi amplasate dispozitivele conectate – adresa care va fi utilizată este 172.17.0.0/23:
   a. Subrețeaua HOSTS-2 la care ar trebui conectată gazda krk-host-2 ar trebui să găzduiască 60 de dispozitive terminale (1 punct)
   b. Subrețeaua HOSTS-3 la care ar trebui conectată gazda krk-host-3 ar trebui să găzduiască 15 dispozitive terminale (1 punct)
   c. Adresarea ar trebui să presupună cea mai bună utilizare posibilă a subrețelei date mai sus (1 punct)
   ID Vlan pentru rețeaua HOSTS-2: VLAN 10
   ID VLAN pentru rețeaua HOSTS-3: VLAN 20

2. Folosind tehnologia de fiabilitate selectată pentru configurația gateway-ului implicit, configurați dispozitivele krk -rtr-1 și krk-rtr-2 pentru a îndeplini această funcție:
   a. Adresa implicită a gateway-ului este întotdeauna prima adresă de subrețea posibilă (3 puncte)
   b. Dacă dispozitivul krk-rtr-1 este disponibil, asigurați-vă că este gateway-ul implicit activ pentru subrețeaua gazdă krk-host-2 ; în caz de defecțiune, dispozitivul krk-rtr-2 ar trebui să ofere fiabilitate în modelul Activ/ Standby (2 puncte).
   c. Pentru subrețeaua gazdă krk-host-2 , dispozitivul krk-rtr-2 ar trebui să fie activ, în timp ce dispozitivul krk-rtr-1 ar trebui să ofere fiabilitate în cazul defectării primului dispozitiv (2 puncte)
   d. În caz de repornire și recuperare, dispozitivele ar trebui să preia automat funcția de gateway implicit pentru subrețelele corespunzătoare (3 puncte)

3. Configurați adresa IPv4 pentru gazde: krk-host-2 și krk-host-3 folosind subrețelele selectate, selectați orice adresă din subrețeaua gazdei date, gateway-ul implicit ar trebui, de asemenea, configurat (1 punct)

   Comenzi pentru configurarea IP-ului pe gazdele krk-host-2 și krk-host-3 :

```
sudo ifconfig eth0 <ADRESĂ IP> mască de rețea <MASCĂ>
```

```
sudo adaugă implicit <GATEWAY> dev eth0
```

Comenzi pentru verificarea IP-ului pe gazde krk-host-2 și krk-host-3 :

```
ifconfig eth0
adresa IP
ruta -n
```

4. Asigurați-vă că krk-host-2 și krk-host-3 pot comunica (1 punct)

4.2. OSPF [20 puncte]

Dispozitivele krk-rtr-1 și krk-rtr-2 au fost conectate la core-rtr-3 și core-rtr-4 așa cum se arată în diagramă (vezi punctul 1). Dispozitivele principale au fost deja configurate - nu este nevoie să fie modificate (accesul la aceste dispozitive a fost, de asemenea, restricționat suplimentar pentru a preveni modificările de configurație). Dispozitivele principale promovează o rută implicită către dispozitivele krk-rtr-1 și krk-rtr-2 .

Configurați-vă rețeaua astfel încât:

1. Dispozitivele krk-rtr-1 și krk-rtr-1 ar trebui să comunice cu subrețelele HOSTS-2 și HOSTS-3 conectate utilizând protocolul OSPF. Adresarea conexiunilor dintre dispozitivele principale și krk-rtr-1 și krk-rtr-1 a fost deja finalizată (3 puncte)

2. Configurați OSPF pe dispozitivele krk-rtr-1 și krk-rtr-2 (5 puncte)
    a. ID router pentru krk-rtr-1 -> 1.1.1.1
    b. ID router pentru krk-rtr-2 -> 1.1.1.2
    c. Zona – coloana vertebrală

3. Dispozitivele krk-rtr-1 și krk-rtr-2 ar trebui configurate astfel încât, în cazul unei defecțiuni a tuturor conexiunilor unui anumit dispozitiv la rețeaua centrală , comunicarea să fie în continuare posibilă (2 puncte)

4. Protocolul OSPF ar trebui configurat astfel încât adiacențele să poată fi stabilite doar pe interfețe specificate și să fie refuzate în mod implicit (2 puncte)

5. OSPF ar trebui configurat astfel încât să nu fie ales niciun DR/BDR în vecinătatea dintre krk-rtr-1 și krk-rtr-1 (pe interfețele Gig 4). (2 puncte)

6. Configurați OSPF astfel încât, în circumstanțe normale, tot traficul să fie rutat prin link către core-rtr-3 . În cazul unei erori de link sau de dispozitiv, acesta ar trebui să se reia automat la core-rtr-4 . Folosiți atributele OSPF pentru a controla traficul. (3 puncte)

7. În cazul în care procesul OSPF eșuează pe dispozitivele principale , configurați o rută statică implicită pe routerul krk-rtr-1 , care va fi utilizată numai dacă nu este disponibilă nicio rută implicită derivată din OSPF. (3 puncte)

4.3. Securitate și NAT [15 puncte]

1. Folosind Lista de control al accesului, securizați subrețelele HOSTS-2 și HOSTS-3 astfel încât:

a. Gazdele din subrețelele HOSTS-2 și HOSTS-3 ar putea comunica între ele doar folosind protocoalele SSH și ICMP (3 puncte)

b. Gazdele din subrețelele HOSTS-2 și HOSTS-3 se puteau conecta doar la servicii DNS, NTP și HTTP/HTTPS, indiferent de adresele IP ale acestor servicii și de locațiile lor. (3 puncte)

c. Gazdele din subrețelele HOSTS-2 și HOSTS-3 ar putea efectua teste de rețea, indiferent de locație, folosind instrumentul traceroute (3 puncte)

2. Configurați dispozitivele krk-rtr-1 și krk-rtr-2 astfel încât, atunci când dispozitivele din subrețelele HOSTS-2 și HOSTS-3 comunică, adresele lor să nu fie vizibile în rețeaua principală , ci să fie ascunse în spatele adreselor interfețelor Gig4 ale acestor dispozitive. (3 puncte)

   Configurația ar trebui să permită utilizarea aceleiași adrese de către mai multe gazde pe o anumită subrețea și pe mai multe porturi. În cazul unei defecțiuni a dispozitivului, krk-rtr-1 ar trebui să aibă aceeași funcționalitate disponibilă pe krk-rtr-2 (3 puncte).

FELICITĂRI – AȚI FINALIZAT ETAPA: ZIUA 1 / PARTEA 1

SALVAȚI CONFIGURAȚIA PE TOATE DISPOZITIVELE
ȘI INFORMAȚI COMITETUL!