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

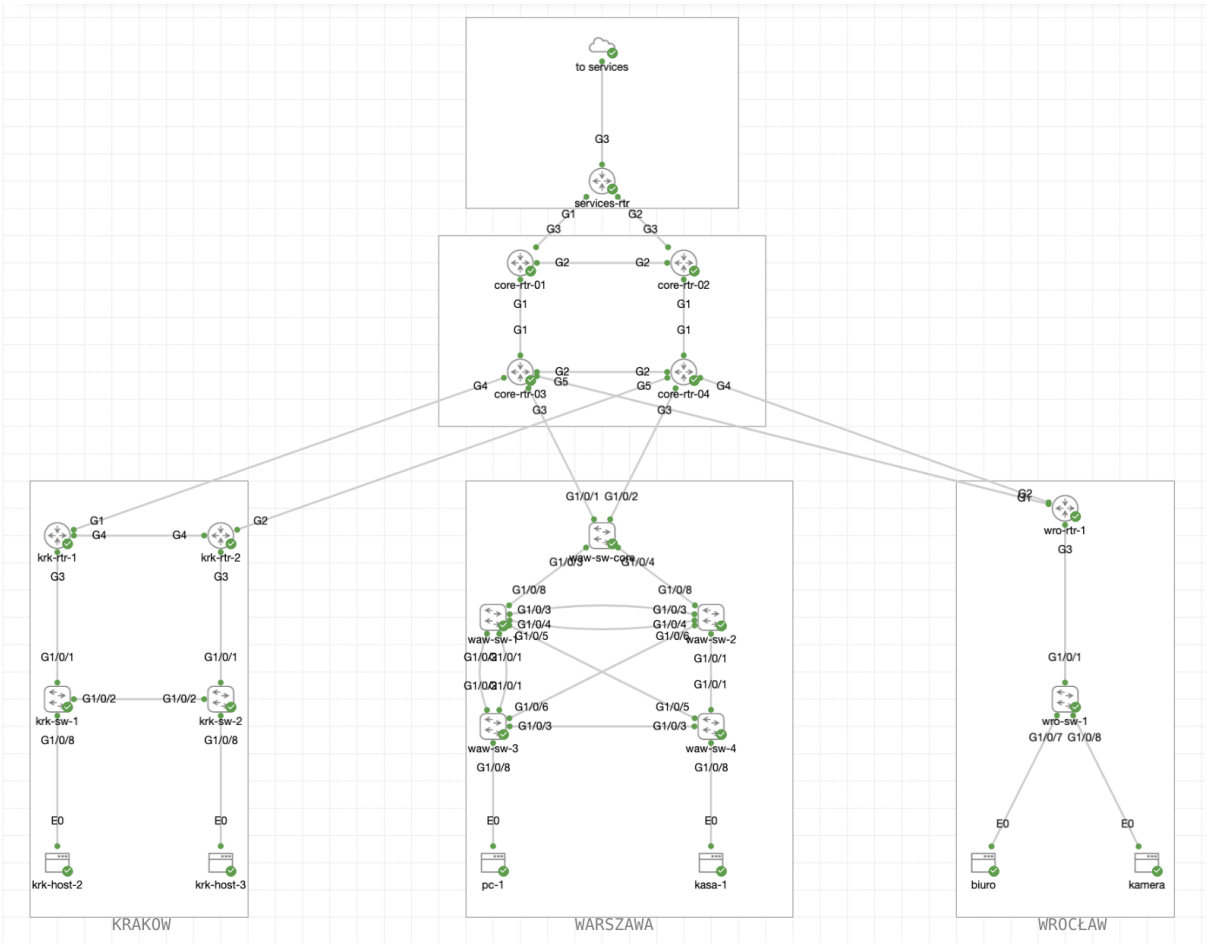
Managementul sistemelor de rețea

--- FINAL ---

ZIUA 1 - PARTEA 3
(14:45 – 16:15)

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

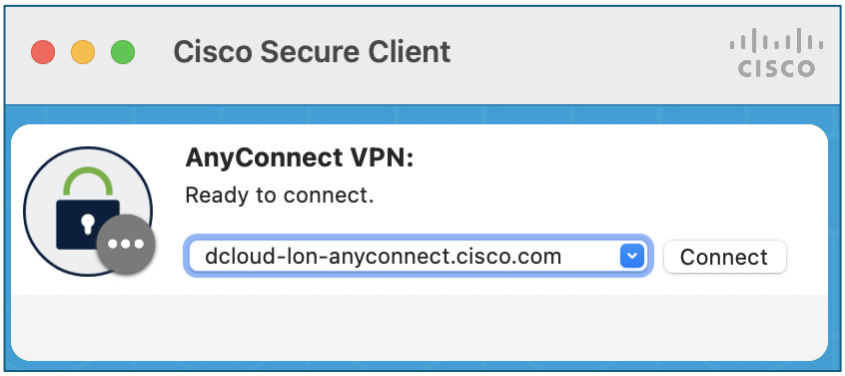
Întreaga competiție a fost simulată în mediul Cisco dCloud folosind următoarele dispozitive/versiuni:

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

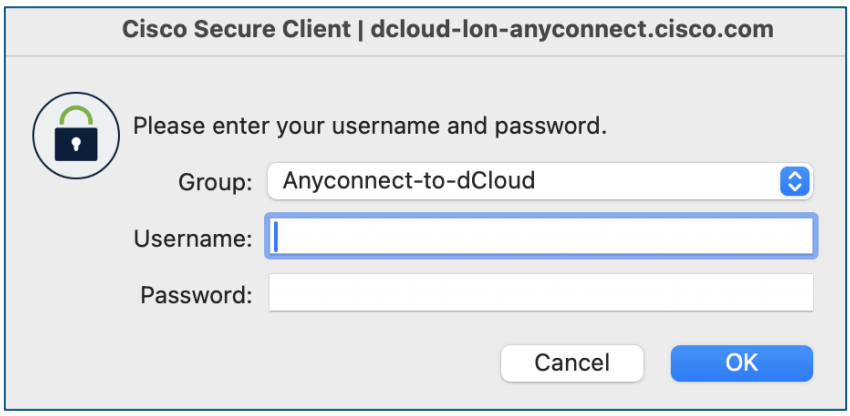
Pentru a obține acces complet la mediul de testare, urmați acești pași:

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:



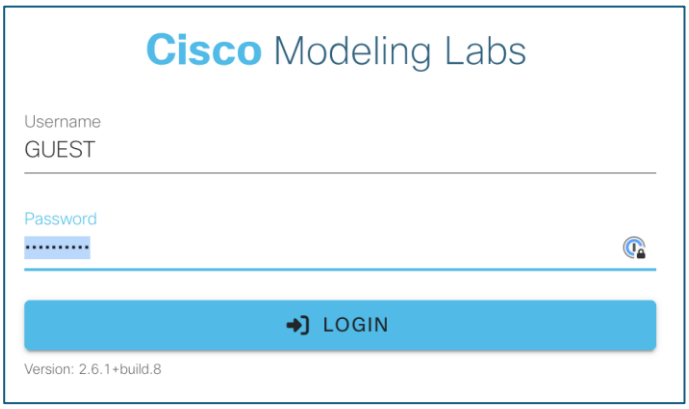
2.3. Laboratoarele de modelare Cisco (CML)

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:

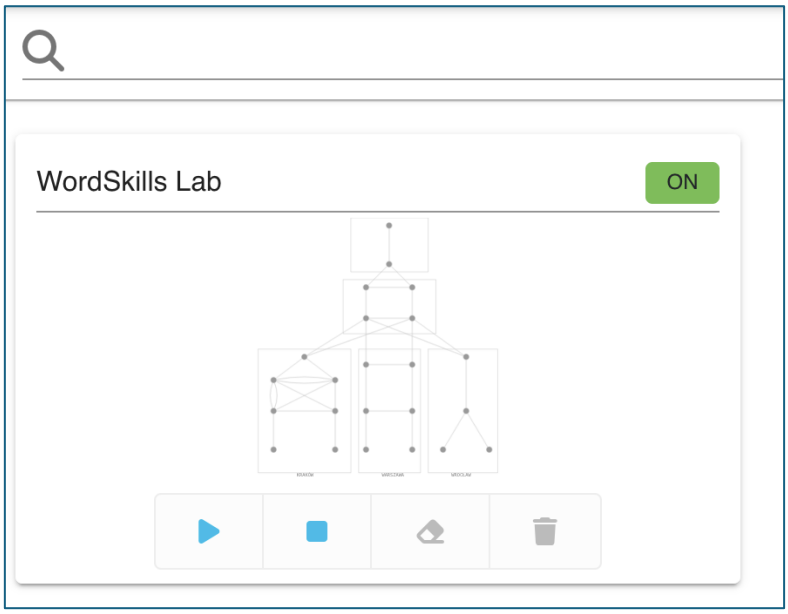
1) În browserul web, introduceți adresa:
   https://198.18.133.111/

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

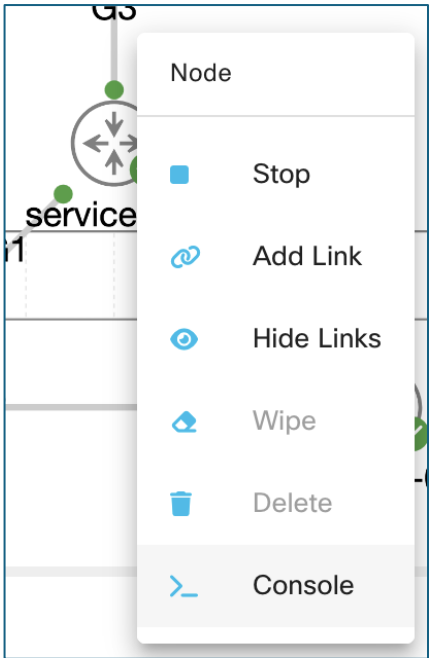
   Nume de utilizator : GUEST (majuscule obligatorii)
   Parolă : C1sco12345



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 internetului (cu excepția documentației oficiale furnizate 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 [20 de puncte]

4.1. Acces la dispozitiv/Aliasuri [1 punct]

Configurați dispozitivele wro-sw-01 și wro-rtr-01 în aşa fel că:

a. administrator prin executarea comenzii **routerului** s-ar putea conecta la dispozitivul wro-rtr-01 de pe dispozitivul: wro-sw-01 (0,5 puncte)
b. administrator prin executarea comenzii **switch** se putea conecta la dispozitivul wro-sw-01 de pe dispozitivul wro-rtr-01 (0,5 puncte)

4.2. Informații pentru administratori [2 puncte]

Configurați dispozitivul wro-rtr-01 şi wro-sw-01 în așa fel încât în momentul autentificării (dar înainte de introducerea datelor de autentificare corecte: nume de utilizator/parolă) să fie afișate următoarele informații (1 punct):

```
================================================
Accesul la sistem este limitat doar la
utilizatori autorizați.
================================================
```

În plus, configurați dispozitivele wro-rtr-01 și wro-sw-01 în așa fel încât informațiile suplimentare să apară numai după autentificarea cu succes (1 punct):

```
================================================
            Wrocław - <<nume gazdă>>

Bucla0: << adresă IP Lo0 >>
PID: <<model dispozitiv>>
S/N: <<număr de serie al dispozitivului>>
================================================
```

Unde variabilele: `< < nume gazdă> >, <<adresă IP Lo0>>, <<model dispozitiv>>, <<număr de serie dispozitiv>>` ar trebui înlocuite cu valorile corecte pentru dispozitivul specific.

4.3. Comutator temporizator sistem [2 puncte]

Configurați dispozitivul wro-sw-01 astfel încât:

a. în jurnale și depanări , iar marcajul temporal a fost afișat cu o precizie de milisecunde (0,5 puncte),
b. jurnalele au arătat informații despre fusul orar CET (unde CET este ora GMT decalată cu +1 oră) (0,5 puncte),
c. Când în Polonia este în vigoare ora de vară, dispozitivul ar trebui să informeze despre fusul orar CEST în loc de CET (schimbarea orei este pe 2 martie la ora 2:00 și pe 3 octombrie la ora 3:00) (1 punct).

4. 4. Autentificare [2 puncte]

În urma incidentelor recente care au implicat modificări neautorizate ale rețelei de către un fost angajat, echipa Departamentul de securitate a solicitat ajutor pentru implementarea auditării suplimentare a configurației și extinderea înregistrării evenimentelor de rețea.

dispozitivele wro-rtr-01 şi wro-sw-01 în așa fel încât:

a. jurnalele `critice și de nivel superior` ar trebui generate în consolă (0,5 puncte)
b. Ambele dispozitive au trimis jurnale către serverul principal (la adresa: 198.18.10.100), adresa sursă fiind adresa IP configurată pe interfața **Loopback0** și au fost marcate (facilitate) ca **local0** (0,5 puncte)
c. În plus, toate comenzile executate pe dispozitiv (în modul de configurare) ar trebui arhivate pe server (1 punct)

Notă *: În scopuri de verificare, accesul la serverul principal este posibil prin SSH.*

Adresă IP (administrare) numai) *: 198.18.128.100*
Utilizator *: cisco*
Parolă *: C1sco12345*

Serverul principal este complet configurat și nu necesită modificări. Toate informațiile trimise către serverul de la adresa IP 198.18.10.100 pe portul UDP 514 sunt salvate automat în fișiere. Numele fișierului corespunde adresei IP SRC a pachetului. Fișierele sunt stocate în directorul: ***/ var /log/network/***

4.5. Monitorizare [2 puncte]

Echipă Echipa de monitorizare a rețelei a raportat o problemă legată de lipsa de vizibilitate a locației din Wrocław, ceea ce îi împiedică să detecteze corect orice probleme de rețea. Sarcina dumneavoastră este să îi ajutați și să rezolvați această problemă. Configurați dispozitivul **wro-rtr-01** :

a. astfel încât dispozitivul să poată fi „interogat” de la serverul principal din rețea folosind (1 punct):
   - comunitate : publică (doar citire)
   - comunitate : privată (citire/scriere)

b. comunitate serverului Linux la adresa 198.18.10.100. Cisco și cu adresa sursă a dispozitivului ca Trap (1pt)

Notă : În scopuri de verificare, accesul la serverul principal este posibil prin SSH.

Adresă IP : 198.18.128.100
Utilizator : cisco
Parolă : C1sco12345

Unde sunt disponibile comenzile: snmpget , snmpwalk etc.

Serverul principal este complet configurat și nu necesită modificări. Informațiile despre primirea unui pachet adresat serverului la adresa IP 198.18.10.100 pe portul UDP 162 sunt salvate automat în fișierul **traps.txt din directorul / var /log/ snmp** .

4.6. Adresarea dinamică a dispozitivelor terminale [7 puncte]

În filiala din Wrocław, a fost necesară adăugarea a două segmente de rețea suplimentare – unul pentru utilizatori (gazdă: office) și unul pentru dispozitive IoT (gazdă: kamea), fiecare suportând aproximativ 100 de dispozitive. Este disponibilă doar subrețeaua 172.18.100.0/24.

Configurați wro-rtr-01 și wro-sw-02 astfel încât:

Pentru subrețele utilizatori (3 puncte):
- prima adresă din subrețeaua atribuită a fost rezervată pentru gateway-ul implicit,
Adresele IP ar trebui atribuite dinamic, excluzând primele cinci adrese din subrețeaua atribuită,
- serverul DNS atribuit utilizatorilor a fost 8.8.8.8,
- domeniul pentru utilizatori era: users.wroclaw.org
Adresele IP pentru utilizatori trebuie alocate pentru maximum 4 ore.

Pentru subrețele Dispozitive IoT (3 puncte):
- ultima adresă din subrețeaua atribuită a fost rezervată pentru gateway-ul implicit,
- ultimele cinci adrese din subrețeaua atribuită ar trebui să fie rezervat,
- dispozitivul numit **cameră** ar trebui să aibă a cincea adresă din subrețea atribuită permanent.
- Serverele DNS atribuite dispozitivelor IoT au fost 8.8.8.8 și 1.1.1.1.
dispozitivele IoT era: iot.wroclaw.org

Notă : În scopuri de verificare, accesul este oferit la două gazde conectate la switch-ul **wro-sw-01.** numit: **birou** (care ar trebui să funcționeze în subrețeaua utilizatorilor) și **camera** (care ar trebui să funcționeze în subrețeaua dispozitivelor IoT). Ambele dispozitive ar trebui să obțină o adresă IP dinamic, în conformitate cu regulile menționate mai sus, și să poată comunica cu adresa 198.18.10.100 (1 punct).

Acces la gazde:
Utilizator : cisco
Parolă : Cisco

Pentru a reîmprospăta recuperarea adresei IP, executați comanda pe dispozitiv:
```
sudo /etc/init.d/networking restart
```

4.7.QoS [4 puncte]

IoT critic a fost instalat în filiala din Wrocław , al cărui trafic ar trebui să fie tratate astfel încât să nu fie respinse de ISP-ul din rețeaua centrală .

Conform acordului cu furnizorul de servicii de internet (ISP), traficul din rețeaua lor pentru clasa CS3 este tratat special, iar echipa dumneavoastră a întrebat el Trebuie să configurați ramura Wrocław astfel încât doar următorul trafic să utilizeze această clasă (2 puncte):
Sursă : Dispozitiv IoT numit **cameră** conectat la comutatorul wro-sw-01
Destinație : server principal: 198.18.10.10
Tipul de trafic : http

În plus, tot traficul provenit de la toate dispozitivele IoT trebuie marcat ca CS1. Tot traficul trebuie marcat ca BE atunci când intră în rețeaua principală (ISP) (2 puncte).

FELICITĂRI – AȚI FINALIZAT ETAPA: ZIUA 1 / PARTEA 3

SALVAȚI CONFIGURAȚIA PE TOATE DISPOZITIVELE
ȘI INFORMAȚI COMITETUL!