SKILLScomp
Skills competitions for VET development

Co-funded by the European Union

Networking Academy

WYŻSZA SZKOŁA INFORMATYKI i ZARZĄDZANIA
z siedzibą w Rzeszowie

Súťaž profesionálnych zručností

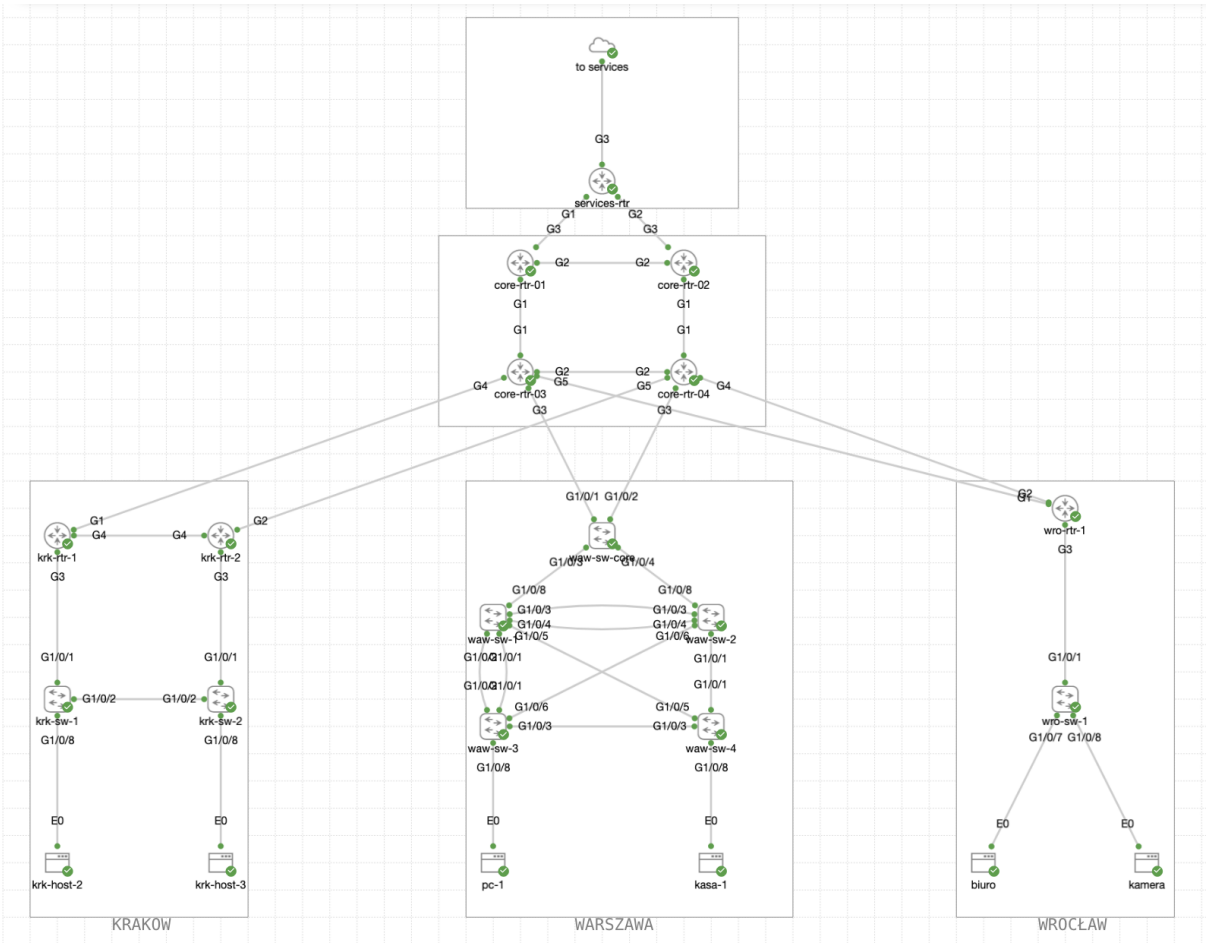
Správa sieťových systémov

--- FINÁLE ---

DEŇ 1 – ČASŤ 1
(10:00 – 12:00)

1. Topológia

Diagram nižšie zobrazuje kompletnú topológiu siete, ktorá bude použitá počas prvého dňa súťaže (k dispozícii na úplné zobrazenie aj v prostredí CML):



2. Prístup do testovacieho prostredia

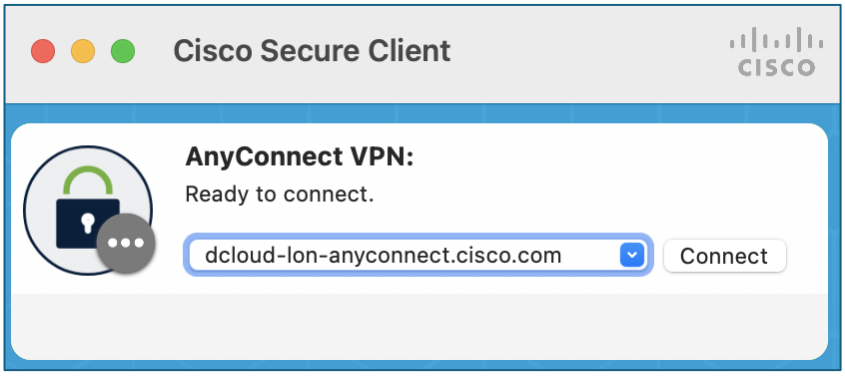
Celá súťaž bola simulovaná v prostredí Cisco dCloud s použitím nasledujúcich zariadení/verzií:

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

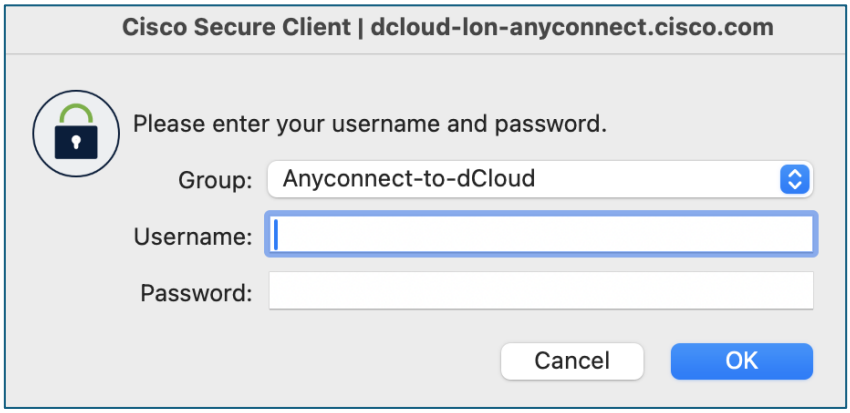
Ak chcete získať plný prístup k testovaciemu prostrediu, postupujte podľa týchto krokov:

2.2. zabezpečeného klienta Cisco

1) Otvorte aplikáciu „ **Cisco Secure Client** “ a zadajte adresu: dcloud-lon-anyconnect.cisco.com



2) Kliknite na tlačidlo „ **Pripojiť** “ a zadajte používateľské meno a heslo, ktoré ste dostali od organizátora súťaže:



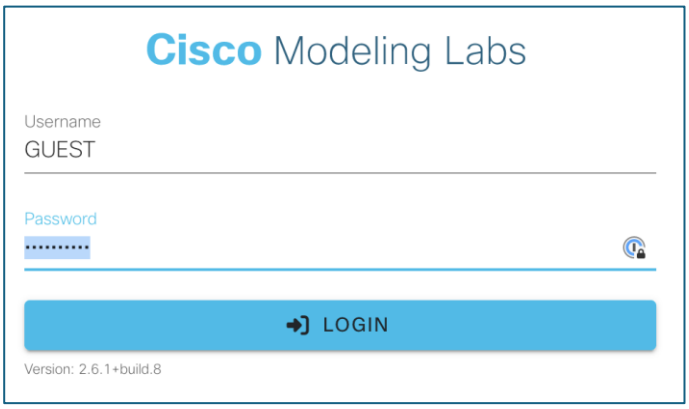
2.3. Cisco Modeling Labs (CML)

Cisco Modeling Labs (CML) poskytuje prístup k testovaciemu prostrediu, ktoré zahŕňa topológiu siete, prístup k zariadeniam a možnosť ich vzdialeného zapínania a vypínania. Ak chcete získať prístup k CML, uistite sa, že ste pripojení cez VPN (pozri časť 2.2) a postupujte podľa týchto krokov:

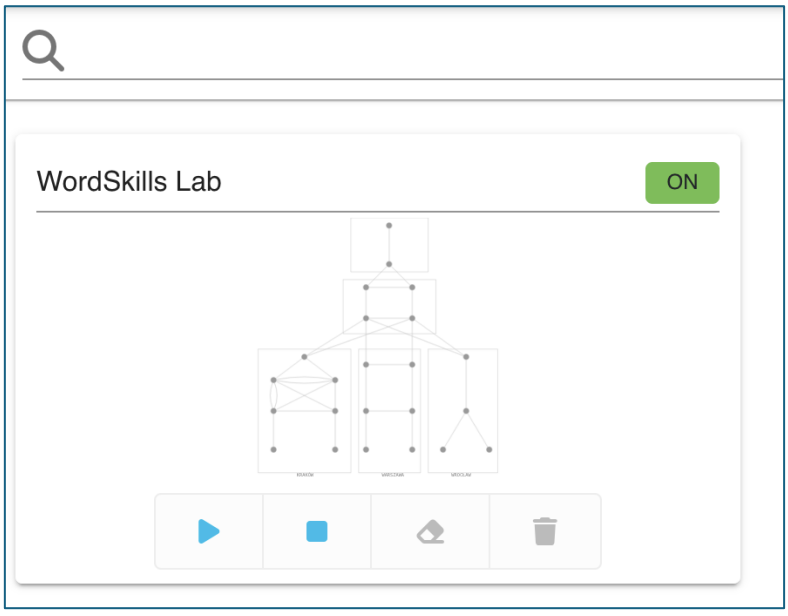
1) Do webového prehliadača zadajte adresu:
   https://198.18.133.111/

2) Na prihlásenie do systému použite nasledujúce údaje:

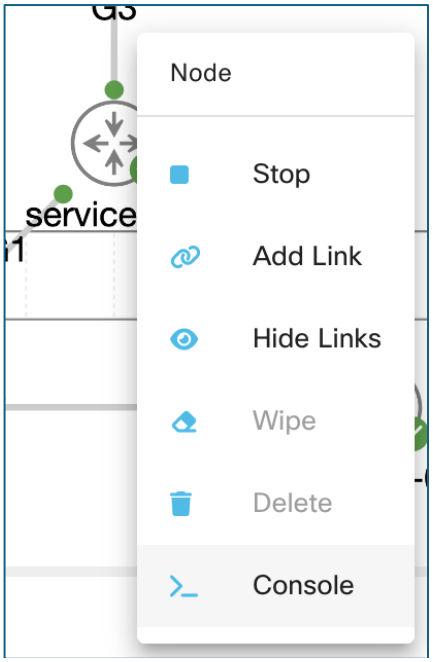
   Používateľské meno : HOST (veľké písmená sú povinné)
   Heslo : C1sco12345



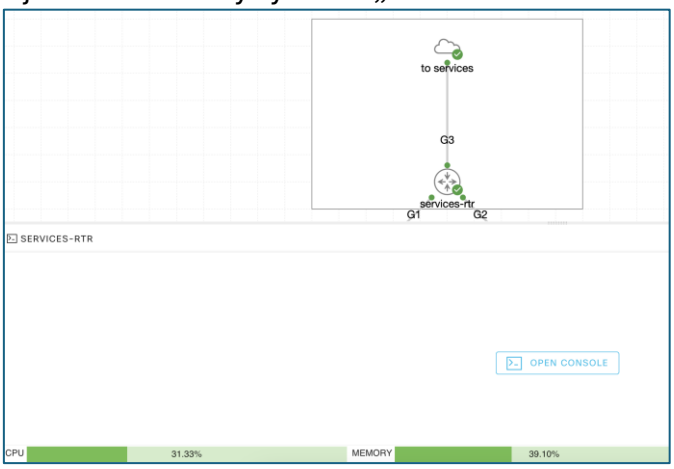
3) Laboratórne prostredie by teraz malo byť inicializované – kliknite na topológiu (vyhnite sa kliknutiu na tlačidlá štart/stop/ vymazanie / odstránenie v dolnej časti oblasti):



4) Pre prístup ku konzole kliknite pravým tlačidlom myši na konkrétne zariadenie (prepínač , smerovač, hostiteľ) a potom z ponuky vyberte možnosť Konzola :



5) V paneli v dolnej časti obrazovky vyberte: „ Otvoriť konzolu “:



Na prihlásenie do prepínača/smerovača použite nasledujúce údaje:

Používateľ : cisco

Heslo : C1sco12345

2.4. Hlavný server

virtuálny počítač s operačným systémom Linux (Ubuntu) (k routeru označenému ako **services -rtr)** .

Prístup k stroju je možný priamo z pracovnej stanice pomocou protokolu SSH po pripojení k testovaciemu prostrediu cez VPN.

IP adresa (vzdialený prístup / správa) : 198.18.128.100
Používateľ : cisco
Heslo : C1sco12345

IP adresa (zo strany lab/services -rtr) : 198.18.10.100

2.6. Hosty

Okrem toho sa k sieti pripájajú ďalšie hostiteľské počítače (napr. krk-host-2, pc-1, kamera atď.), aby sa overilo, či sieť funguje správne. K týmto zariadeniam sa pristupuje prostredníctvom CML rovnakým spôsobom ako k sieťovým zariadeniam (pozri časť 2.3), pričom sa zohľadňujú nasledujúce údaje:

Používateľ : cisco
Heslo : cisco

3. Všeobecné poznámky

Je zakázané:
- zmeny v topológii siete (pridanie alebo odstránenie zariadení, pripojení atď.),
- zmeny hesla / konfigurácia konzoly / VTY / ...,
- komunikácia s opatrovníkmi, ostatnými účastníkmi súťaže a tretími stranami,
- použitie materiálov z internetu (s výnimkou oficiálnej dokumentácie dostupnej na stránke cisco.com).

Je nariadené:
- uloženie konfigurácie na zariadení (kopírovanie a spustenie) po každej časti na všetkých zariadeniach, ktorá sa potom počas prestávky skopíruje pre úplné overenie.

V prípade akýchkoľvek environmentálnych problémov je účastník povinný nahlásiť všetky zistené problémy priamo výboru.

4. Súťažné úlohy [50 bodov]

4.1. Protokoly redundancie prvého kroku [15 bodov]

1. Pripravte schému adresovania pre 2 podsiete, v ktorých budú umiestnené pripojené zariadenia – použitá adresa je 172.17.0.0/23:
   a. Podsieť HOSTS-2 , ku ktorej by mal byť pripojený hostiteľ krk-host-2, by mala pojať 60 koncových zariadení (1 bod)
   b. Podsieť HOSTS-3, ku ktorej by mal byť pripojený hostiteľ krk-host-3, by mala obsahovať 15 koncových zariadení (1 bod)
   c. Adresovanie by malo predpokladať čo najlepšie využitie vyššie uvedenej podsiete (1 bod).
   ID VLAN pre sieť HOSTS-2: VLAN 10
   ID siete VLAN pre sieť HOSTS-3: VLAN 20

2. Pomocou vybranej technológie spoľahlivosti pre konfiguráciu predvolenej brány nakonfigurujte zariadenia krk- rtr-1 a krk-rtr-2 na vykonávanie tejto funkcie:
   a. Adresa predvolenej brány je vždy prvá možná adresa podsiete (3 body)
   b. Ak je zariadenie krk-rtr-1 k dispozícii, uistite sa, že je aktívnou predvolenou bránou pre podsieť hostiteľa krk-host-2 . V prípade poruchy by zariadenie krk-rtr-2 malo zabezpečiť spoľahlivosť v modeli Active/ Standby (2 body).
   c. Pre hostiteľskú podsieť krk-host-2 by malo byť zariadenie krk-rtr-2 aktívne, zatiaľ čo zariadenie krk-rtr-1 by malo zabezpečovať spoľahlivosť v prípade poruchy prvého zariadenia (2 body).
   d. V prípade reštartu a obnovy by zariadenia mali automaticky prevziať funkciu predvolenej brány pre príslušné podsiete (3 body)

3. Konfigurácia IPv4 adresy pre hostiteľov: krk-host-2 a krk-host-3 s použitím vybraných podsietí, vyberte ľubovoľnú adresu z podsiete daného hostiteľa, mala by byť nakonfigurovaná aj predvolená brána (1 bod)

   Príkazy na konfiguráciu IP adresy na hostiteľoch krk-host-2 a krk-host-3 :

   ```
   sudo ifconfig eth0 <IP-ADRESA> sieťová maska <MASKA>
   ```

   ```
   sudo route add default <BRÁNA> dev eth0
   ```

   Príkazy na overenie IP adresy na hostiteľoch krk-host-2 a krk-host-3 :

   ```
   ifconfig eth0
   ```

```
ip adresa
trasa -n
```

4. Uistite sa, že krk-host-2 a krk-host-3 môžu komunikovať (1 bod)

4.2. OSPF [20 bodov]

Zariadenia krk-rtr-1 a krk-rtr-2 boli pripojené k core-rtr-3 a core-rtr-4, ako je znázornené na diagrame (pozri bod 1). Základné zariadenia už boli nakonfigurované – nie je potrebné ich upravovať (prístup k týmto zariadeniam bol tiež dodatočne obmedzený, aby sa zabránilo zmenám konfigurácie). Základné zariadenia inzerujú predvolenú trasu k zariadeniam krk-rtr-1 a krk-rtr-2 .

Nakonfigurujte si sieť tak, aby:

1. Zariadenia krk-rtr-1 a krk-rtr-1 by mali komunikovať s pripojenými podsieťami HOSTS-2 a HOSTS-3 pomocou protokolu OSPF. Adresovanie pripojení medzi hlavnými zariadeniami a krk-rtr-1 a krk-rtr-1 už bolo dokončené (3 body).

2. Konfigurácia OSPF na zariadeniach krk-rtr-1 a krk-rtr-2 (5 bodov)
    a. ID smerovača pre krk-rtr-1 -> 1.1.1.1
    b. ID smerovača pre krk-rtr-2 -> 1.1.1.2
    c. Oblasť – chrbtica

3. Zariadenia krk-rtr-1 a krk-rtr-2 by mali byť nakonfigurované tak, aby v prípade výpadku všetkých pripojení daného zariadenia k jadrovej sieti bola komunikácia stále možná (2 body).

4. Protokol OSPF by mal byť nakonfigurovaný tak, aby susedné siete bolo možné nadviazať iba na určených rozhraniach a boli štandardne zamietnuté (2 body).

5. OSPF by mal byť nakonfigurovaný tak, aby v blízkosti medzi krk-rtr-1 a krk-rtr-1 (na rozhraniach Gig 4) nebol zvolený žiadny DR/BDR . (2 body)

6. Nakonfigurujte OSPF tak, aby za normálnych okolností bola všetka prevádzka smerovaná cez odkaz na core-rtr-3 . V prípade zlyhania odkazu alebo zariadenia by sa mal automaticky prepnúť na core-rtr-4 . Na riadenie prevádzky použite atribúty OSPF. (3 body)

7. V prípade, že proces OSPF zlyhá na hlavných zariadeniach , nakonfigurujte predvolenú statickú trasu na routeri krk-rtr-1 , ktorá sa použije iba v prípade, že nie je k dispozícii žiadna predvolená trasa odvodená z OSPF. (3 body)

4.3. Bezpečnosť a NAT [15 bodov]

1. Pomocou zoznamu riadenia prístupu zabezpečte podsiete HOSTS-2 a HOSTS-3 tak, aby:

a. Hostitelia z podsietí HOSTS-2 a HOSTS-3 mohli medzi sebou komunikovať iba pomocou protokolov SSH a ICMP (3 body)

b. Hostitelia z podsietí HOSTS-2 a HOSTS-3 sa mohli pripojiť iba k službám DNS, NTP a HTTP/HTTPS bez ohľadu na IP adresy týchto služieb a ich umiestnenie. (3 body)

c. Hostitelia z podsietí HOSTS-2 a HOSTS-3 mohli vykonávať testovanie siete bez ohľadu na umiestnenie pomocou nástroja traceroute (3 body)

2. Nakonfigurujte zariadenia krk-rtr-1 a krk-rtr-2 tak , aby pri komunikácii zariadení z podsietí HOSTS-2 a HOSTS-3 neboli ich adresy viditeľné v jadre siete , ale boli skryté za adresami rozhraní Gig4 týchto zariadení. (3 body)

   Konfigurácia by mala umožniť použitie rovnakej adresy viacerými hostiteľmi v danej podsieti a na viacerých portoch. V prípade zlyhania zariadenia by mal mať krk-rtr-1 rovnakú funkcionalitu dostupnú na krk-rtr-2 (3 body).

GRATULUJEME – DOKONČILI STE FÁZU:
DEŇ 1 / ČASŤ 1

ULOŽTE SI KONFIGURÁCIU NA VŠETKÝCH ZARIADENIACH
A INFORMUJTE VÝBOR!