SKILLScomp
Skills competitions for VET development

Co-funded by the European Union

Networking Academy
CISCO

WYŻSZA SZKOŁA INFORMATYKI i ZARZĄDZANIA
z siedzibą w Rzeszowie

Soutěž profesionálních dovedností

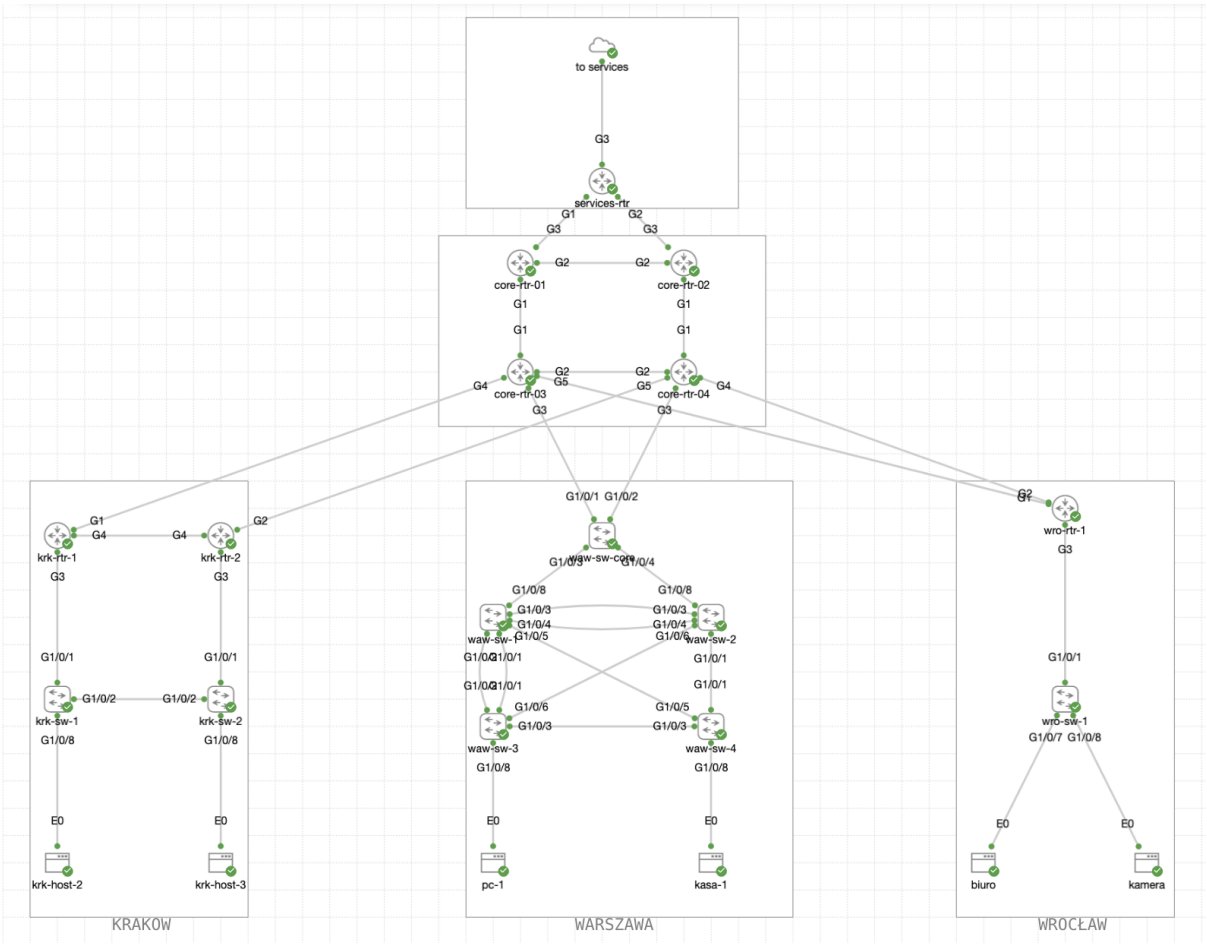
Správa síťových systémů

--- FINÁLE ---

1. DEN – 2. ČÁST
(1 3:00 – 14:30)

1. Topologie

Níže uvedený diagram ukazuje kompletní topologii sítě, která bude použita během prvního dne soutěže (k dispozici pro kompletní zobrazení v prostředí CML):



2. Přístup do testovacího prostředí

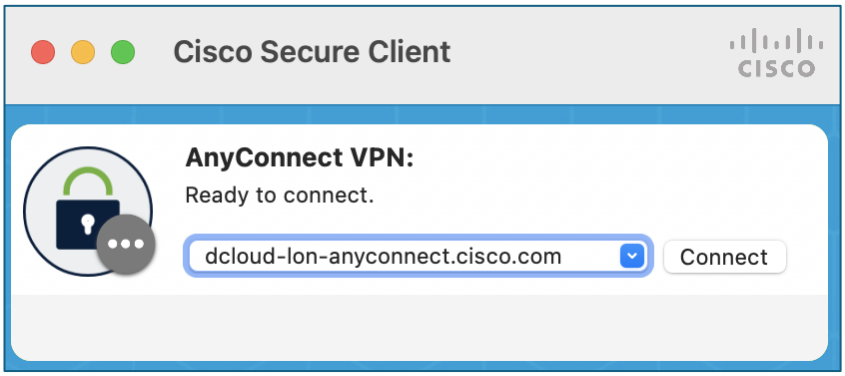
Celá soutěž byla simulována v prostředí Cisco dCloud s využitím následujících zařízení/verzí:

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

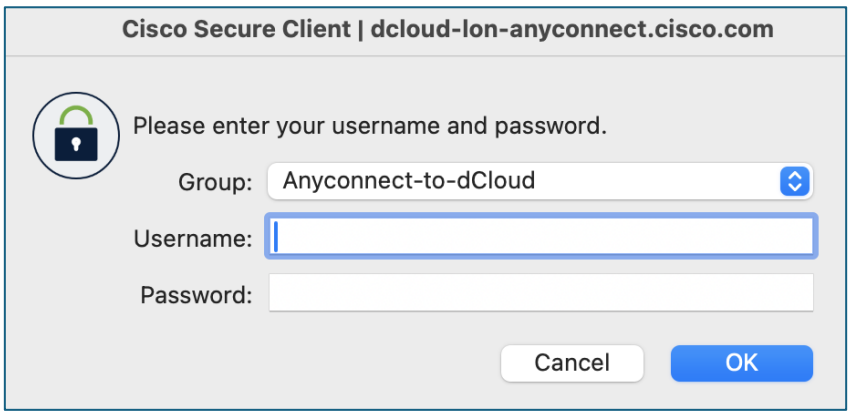
Chcete-li získat plný přístup k testovacímu prostředí, postupujte takto:

2.2. zabezpečeného klienta Cisco

1) Otevřete aplikaci „ **Cisco Secure Client** “ a zadejte adresu: dcloud-lon-anyconnect.cisco.com



2) Klikněte na tlačítko „ **Připojit** “ a zadejte uživatelské jméno a heslo , které jste obdrželi od organizátora soutěže:



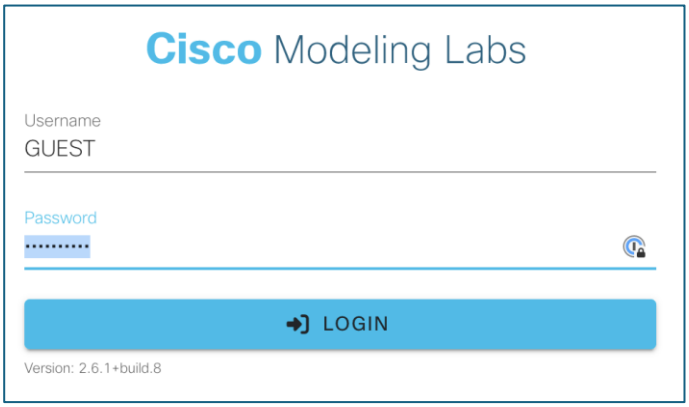
2.3. Cisco Modeling Labs (CML)

Cisco Modeling Labs (CML) poskytuje přístup k testovacímu prostředí, které zahrnuje síťovou topologii, přístup k zařízením a možnost jejich vzdáleného zapínání a vypínání. Pro přístup k CML se ujistěte, že jste připojeni přes VPN (viz část 2.2), a postupujte takto:

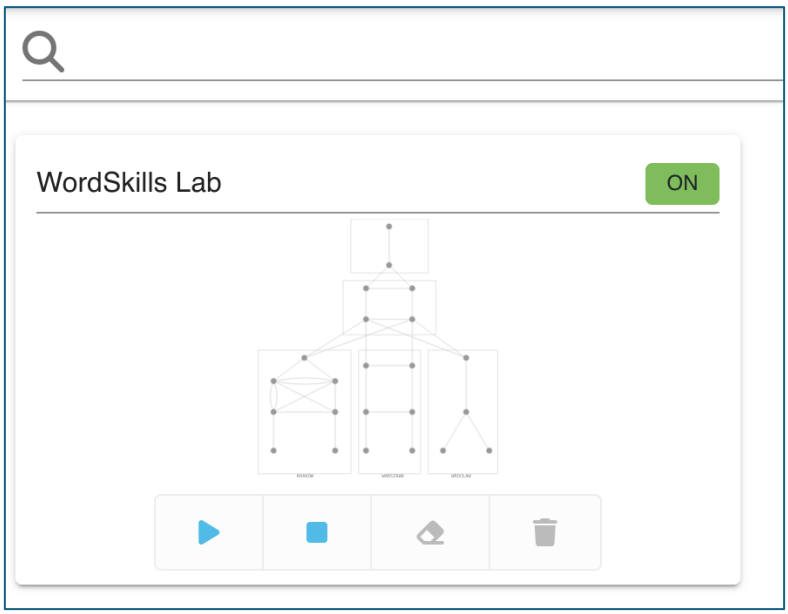
1) Do webového prohlížeče zadejte adresu:
   https://198.18.133.111/

2) Pro přihlášení do systému použijte následující údaje:

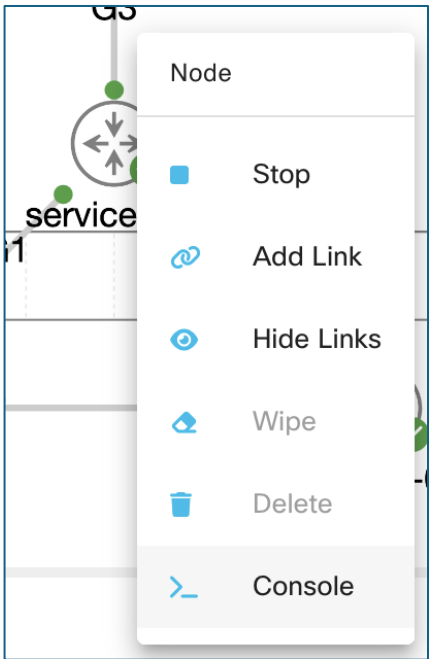
   Uživatelské jméno : HOST (velká písmena vyžadována)
   Heslo : C1sco12345



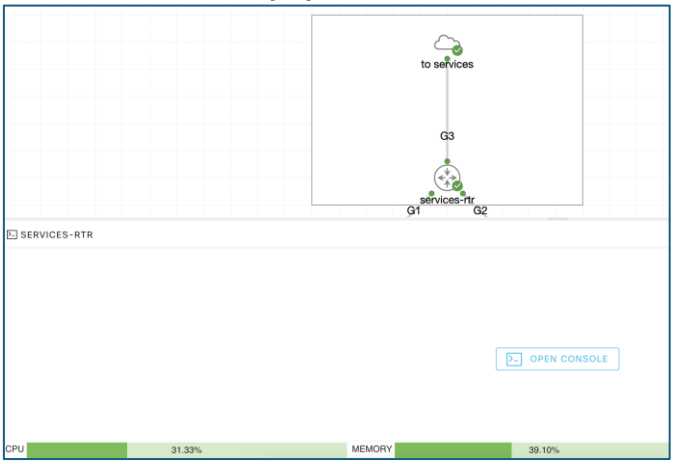
3) Laboratorní prostředí by nyní mělo být inicializováno – klikněte na topologii (vyhněte se klikání na tlačítka spustit/zastavit/ vymazat / odstranit ve spodní části oblasti):



4) Pro přístup do konzole klikněte pravým tlačítkem myši na konkrétní zařízení (přepínač , router, hostitel) a poté z nabídky vyberte Konzole :



5) V panelu ve spodní části obrazovky vyberte: „ Otevřít konzoli “:



Pro přihlášení k přepínači/routeru použijte následující údaje:

Uživatel : cisco

Heslo : C1sco12345

2.4. Hlavní server

virtuální stroj s operačním systémem Linux (Ubuntu) (k routeru označenému jako **services -rtr)** .

Přístup ke stroji je možný přímo z pracovní stanice pomocí protokolu SSH po připojení k testovacímu prostředí přes VPN.

IP adresa (vzdálený přístup / správa) : 198.18.128.100
Uživatel : cisco
Heslo : C1sco12345

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

2.6. Hosty

Dále jsou k síti připojeny další hostitelské počítače (např. krk-host-2, pc-1, kamera atd.), aby se ověřilo, že síť funguje správně. K těmto zařízením se přistupuje prostřednictvím CML stejným způsobem jako k síťovým zařízením (viz kapitola 2.3), přičemž se berou v úvahu následující data:

Uživatel : cisco
Heslo : cisco

3. Obecné poznámky

Je zakázáno:
- změny v topologii sítě (přidání nebo odebrání zařízení, připojení atd.),
- změny hesla / konfigurace konzole / VTY / ...,
- komunikace s dozorci, ostatními účastníky soutěže a třetími stranami,
- používání internetu (s výjimkou oficiální dokumentace uvedené na cisco.com).

Je nařízeno:
- uložení konfigurace na zařízení (copy run start) po každé části na všech zařízeních, která bude následně během přestávky zkopírována pro úplné ověření.

V případě jakýchkoli environmentálních problémů je účastník povinen nahlásit veškeré zjištěné problémy přímo komisi.

4. Soutěžní úkoly [30 bodů]

Síť varšavské pobočky zahrnuje čtyři přepínače a jeden router. Router je připraven na zamýšlené šíření paketů; konfigurační úlohy budou prováděny výhradně na síťových přepínačích a hostitelích. Přepínače v současné době nemají žádnou konfiguraci; jsou připravena pouze připojení. Úkol si klade za cíl připravit konfigurace pro tři oddělení, z nichž pouze dvě budou komunikovat s centrálou společnosti prostřednictvím síťového jádra. Těmito odděleními jsou účetnictví, pokladna a lidské zdroje.

4.1. Základní konfigurace [5 bodů]

1. Nakonfigurujte názvy pro všechna zařízení. (1 bod)

2. Nakonfigurujte všechna redundantní připojení mezi následujícími dvojicemi zařízení (zařízení by měla používat LACP). (2 body)

Přepínač 1	**Přepínač 2**	**ID (kanál portu)**
waw-sw-1	waw-sw-2	10
waw-sw-1	waw-sw-3	20

3. Nakonfigurujte zařízení tak, aby umožňovala ověřování připojení z rozhraní příkazového řádku pomocí LLDP a CDP. (1 bod)

4. Nastavte popisy rozhraní propojujících přepínače tak, aby dokázaly identifikovat zařízení na druhé straně bez nutnosti použití protokolů CDP/LLDP. Poté nastavte propojení tak, aby umožňovalo odesílání rámců přes různé VLAN . (1 bod)

4.2. Virtuální sítě [15 bodů]

1. Nakonfigurujte zařízení waw-sw-1 a waw-sw-2 tak, aby automaticky šířila konfigurace virtuální sítě pomocí protokolu VTP podle níže uvedené tabulky (4 body):

Zařízení	Verze VTP	Režim	Doména
waw-sw-1	3	server	waw-01
waw-sw-2	3	Klient	waw-01
waw-sw-3	3	průhledný	waw-01
waw-sw-4	3	průhledný	waw-01

2. Nakonfigurujte VLAN 10 a pojmenujte ji jako: NATIVE (1 bod)

3. Vytvořte virtuální sítě s následujícím číslováním (2 body):

    a. 100 →zaměstnanců

    b. 110→ Účetnictví

    3. 120 →pokladních

Poznámka : Informace o umístění virtuální sítě naleznete v tabulce níže.

ID sítě VLAN	waw-sw-1	waw-sw-2	waw-sw-3	waw-sw-4
100	Ano	Ano	Ano	ŽÁDNÝ
110	Ano	Ano	Ano	ŽÁDNÝ
120	Ano	Ano	Ano	Ano

4. Nakonfigurujte připojení **kmenových sítí** podle níže uvedené tabulky (6 bodů):

Přepínač 1	Přepínač 2	Rozhraní	Nativní VLAN	VLAN povolena
waw-sw-1	waw-sw-2	Po 20.	10	100, 110, 120
waw-sw-1	waw-sw-3	Po 10.	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. Nakonfigurujte zařízení tak, aby všechna zařízení měla neblokovaná rozhraní směrem k přepínači waw-sw-core (platí pro všechny virtuální sítě nakonfigurované na daném přepínači) (2 body).

4.3. Konfigurace vrstvy přístup [10 bodů]

1. Nakonfigurujte hostitele kasa-1 a pc-1 takto (2 body)

Název hostitele	IP adresa	Maska
PC-1	172.16.0.10	/25
Pokladní-1	172.16.0.140	/25

Příkazy pro konfiguraci IP adresy na hostitelích kasa-1 a pc-1 :

```
sudo ifconfig eth0 <IP ADRESA> síťová maska <MASKA>
sudo route add default <BRÁNA> dev eth0
```

Příkazy pro ověření IP adresy na hostitelích pokladna-1 a ks-1 :

```
ifconfig eth0
ip adresa_routa -n
```

2. Nakonfigurujte rozhraní, ke kterým jsou připojeny hostitele kasa-1 a pc-1 takovým způsobem, že:
   a. Pro hostitele kasa-1 musí být připravena konfigurace, která splňuje následující požadavky: (5 bodů)

      - Přístup pouze k jedné VLAN s číslem 120 ,
      - Nakonfigurujte rozhraní tak, aby k němu měl přístup pouze hostitel kasa-1 ,
      - Pokud dojde k pokusu o připojení jiného hostitele k rozhraní, port by měl být automaticky zablokován,
      - Po připojení hostitele by rozhraní mělo okamžitě začít šířit pakety.

   b. Pro hostitelský počítač PC-1 musí být připravena konfigurace, která splňuje následující požadavky: (3 body)

      - Přístup pouze k jedné VLAN s číslem 100,
      - Po restartu připojení by mělo být rozhraní přepínače okamžitě pokračovat v šíření paketů .

GRATULUJEME – DOKONČILI JSTE FÁZI:
DEN 1 / ČÁST 2

ULOŽTE KONFIGURACE NA VŠECH ZAŘÍZENÍCH
A INFORMUJTE VÝBOR!