



Co-funded by
the European Union



Networking
Academy



WYŻSZA SZKOŁA
INFORMATYKI I ZARZĄDZANIA
z siedzibą w Rzeszowie

Soutěž profesionálních dovedností

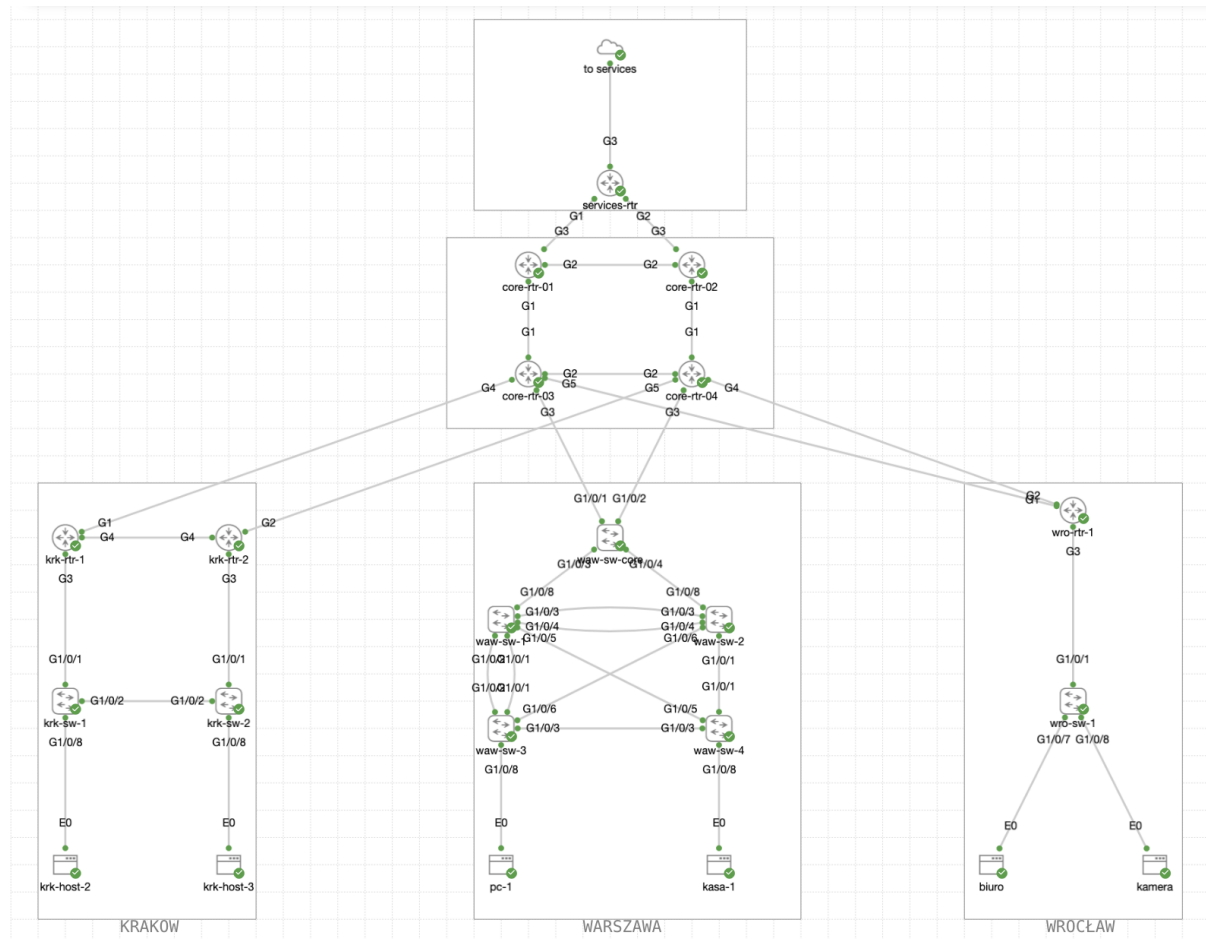
Správa síťových systémů

--- FINÁLE ---

1. DEN - 3. ČÁST
(14:45 – 16:15)

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

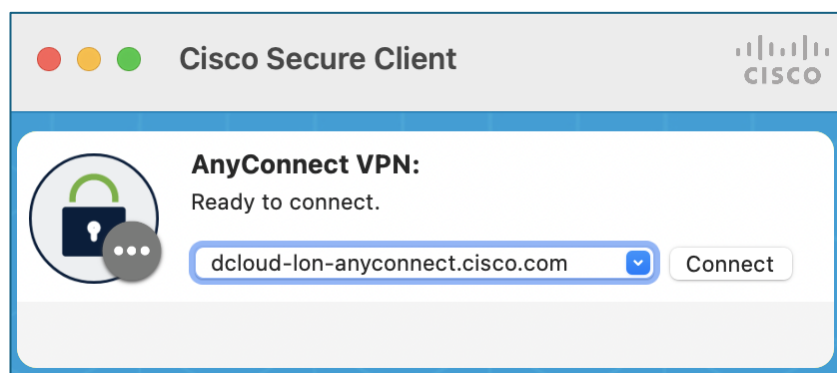
Celá soutěž byla simulována v prostředí Cisco dCloud s využitím následujících zařízení/verzí:

- 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

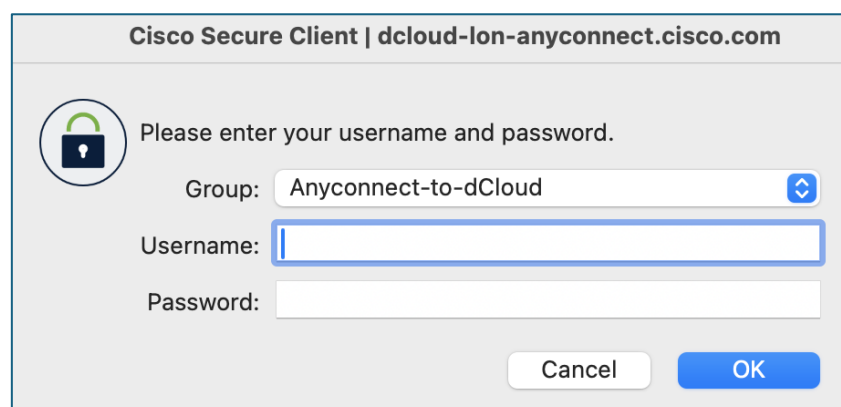
Chcete-li získat plný přístup k testovacímu prostředí, postupujte takto:

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)

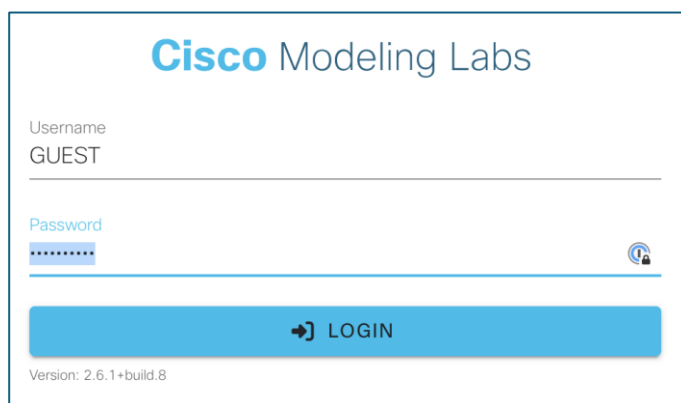
Cisco Modeling Labs (CML) poskytuje přístup k testovacímu prostředí, které zahrnuje síťovou topologii, přístup k zařízením a možnost jejich vzdáleného zapínání a vypínání. Pro přístup k CML se ujistěte, že jste připojeni přes VPN (viz část 2.2), a postupujte takto:

- 1) Do webového prohlížeče zadejte adresu:
<https://198.18.133.111/>
- 2) Pro přihlášení do systému použijte následující údaje:

Uživatelské jméno : HOST

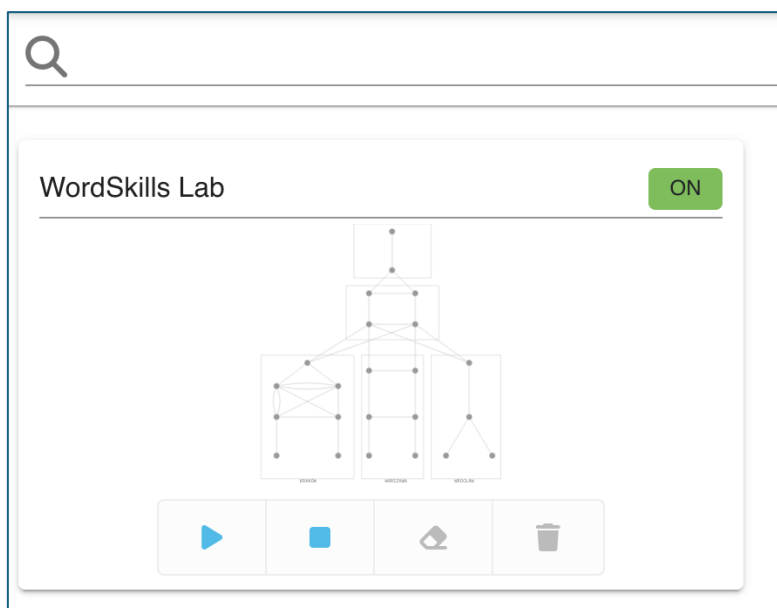
(velká písmena vyžadována)

Heslo : C1sco12345

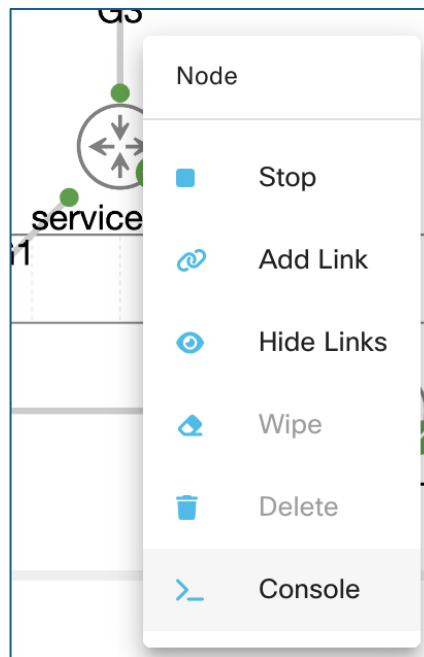


The image shows the Cisco Modeling Labs login interface. At the top, the text "Cisco Modeling Labs" is displayed in blue. Below it, there are two input fields: "Username" with the value "GUEST" and "Password" with a masked password "*****". To the right of the password field is a small icon of a person. Below the input fields is a large blue button with a right-pointing arrow and the text "LOGIN". At the bottom left, the version "Version: 2.6.1+build.8" is shown.

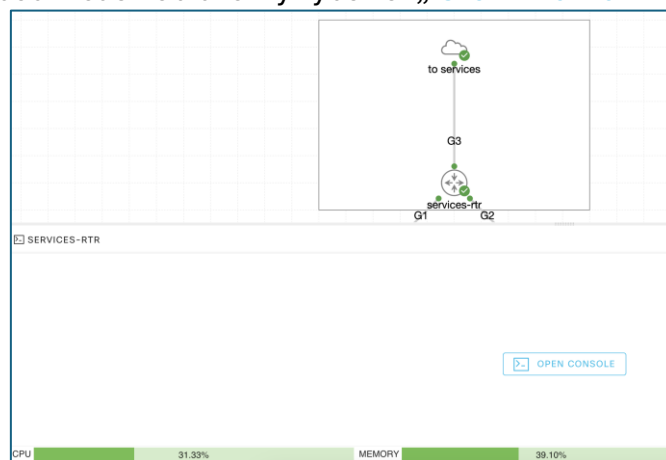
- 3) Laboratorní prostředí by nyní mělo být inicializováno – klikněte na topologii (vyhněte se klikání na tlačítka spustit/zastavit/ vymazat / odstranit ve spodní části oblasti):



- 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 dozorcí, 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 [20 bodů]

4.1. Přístup k zařízením/aliasy [1 bod]

Nakonfigurujte zařízení **wro-sw-01** a **wro-rtr-01** takovým způsobem, že:

- správce spuštěním příkazu **routeru** mohl se přihlásit k zařízení **wro-rtr-01** ze zařízení: **wro-sw-01** (0,5 bodu)
- správce spuštěním příkazu **switch** mohl se přihlásit k zařízení **wro-sw-01** ze zařízení **wro-rtr-01** (0,5 bodu)

4.2. Informace pro administrátory [2 body]

Konfigurace zařízení **wro-rtr-01** a **wro-sw-01** tak, aby se v okamžiku přihlášení (ale před zadáním správných přihlašovacích údajů: uživatelského jména/hesla) zobrazily následující informace (1 bod):

```
=====
Přístup k systému je omezen pouze na
autorizovaní uživatelé.
=====
```

Dále nakonfigurujte zařízení **wro-rtr-01** a **wro-sw-01** takovým způsobem, že se další informace zobrazí až po úspěšném přihlášení (1 bod):

```
=====
Vratislav - <<název hostitele>>

Loopback0: << IP adresa Lo0>>
PID: <<model zařízení>>
S/N: <<sériové číslo zařízení>>
=====
```

Kde proměnné: < < název hostitele> >, <<IP adresa Lo0>>, <<model zařízení>>, <<sériové číslo zařízení>> by měly být nahrazeny správnými hodnotami pro konkrétní zařízení.

4.3. Systémový časový spínač [2 body]

Nakonfigurujte zařízení **wro-sw-01** tak, aby:

- v logech a ladění a časové razítko se zobrazovalo s přesností na milisekundy (0,5 bodu),
- Záznamy zobrazovaly informace o časovém pásmu SEČ (kde SEČ je čas GMT posunutý o +1 hodinu) (0,5 bodu),
- Pokud v Polsku platí letní čas, mělo by zařízení informovat o časovém pásmu CEST namísto CET (změna času je 2. března ve 2:00 a 3. října ve 3:00) (1 bod).

4. 4. Přihlášení [2 body]

Po nedávných incidentech zahrnujících neoprávněné změny v síti ze strany bývalého zaměstnance tým Bezpečnostní oddělení požádalo o pomoc s implementací dodatečného auditu konfigurace a rozšířením protokolování síťových událostí.

zařízení **wro-rtr-01** a **wro-sw-01** takovým způsobem, že:

- a. V konzoli by měly být generovány pouze **kritické** a **vyšší** úrovně protokolů (0,5 bodu)
- b. Obě zařízení odesílala logy na hlavní server (na adrese: 198.18.10.100), přičemž zdrojová adresa byla IP adresa nakonfigurovaná na rozhraní **Loopback0** a byla označena (facility) jako **local0** (0,5 bodu).
- c. Kromě toho by všechny příkazy provedené na zařízení (v konfiguračním režimu) měly být archivovány na serveru (1 bod).

Poznámka : Pro účely ověření je přístup k hlavnímu serveru možný přes SSH.

IP adresa (správa pouze) : 198.18.128.100

Uživatel : cisco

Heslo : C1sco12345

Hlavní server je plně nakonfigurován a nevyžaduje žádné změny. Veškeré informace odeslané na server na IP adrese 198.18.10.100 na UDP portu 514 se automaticky ukládají do souborů. Název souboru odpovídá SRC IP adrese paketu. Soubory jsou uloženy v adresáři: / var /log/network/

4.5. Monitorování [2 body]

Tým Tým pro monitorování sítě nahlásil problém s nedostatečnou viditelností lokality ve Vratislavi, což jim brání v řádné detekci jakýchkoli problémů se sítí. Vaším úkolem je jim pomoci a tento problém vyřešit. Nakonfigurujte zařízení **wro-rtr-01** :

- a. aby bylo možné zařízení „dotazovat“ z hlavního serveru v síti pomocí (1 bod):
 - komunita : veřejná (pouze pro čtení)
 - komunita : soukromá (čtení/zápis)
- b. Navíc v případě jakýchkoli změn konfigurace by měla být informace o takové události odeslána na Linuxový server na adresu 198.18.10.100 z komunity. Cisco a se zdrojovou adresou zařízení jako Trap (1 bod)

Poznámka : Pro účely ověření je přístup k hlavnímu serveru možný přes SSH.

IP adresa : 198.18.128.100

Uživatel : cisco

Heslo : C1sco12345

Kde jsou k dispozici příkazy: snmpget , snmpwalk atd.

Hlavní server je plně nakonfigurován a nevyžaduje žádné změny. Informace o přijetí paketu adresovaného serveru na IP adrese 198.18.10.100 na UDP portu 162 se automaticky ukládá do souboru **traps.txt v adresáři /var /log/ snmp** .

4.6. Dynamické adresování koncových zařízení [7 bodů]

Ve vratslavské pobočce bylo nutné přidat dva další síťové segmenty – jeden pro uživatele (host: office) a jeden pro IoT zařízení (host: kamea), přičemž každý z nich bude podporovat přibližně 100 zařízení. K dispozici je pouze podsít 172.18.100.0/24.

Nakonfigurujte **wro-rtr-01** a **wro-sw-02** tak, aby:

Pro podsítě uživatelé (3 body):

- první adresa z přiřazené podsítě byla rezervována pro výchozí bránu,
- IP adresy by měly být přidělovány dynamicky, s výjimkou prvních pěti adres v přidělené podsíti,
- DNS server přiřazený uživatelům byl 8.8.8.8,
- doména pro uživatele byla: users.wroclaw.org
- IP adresy uživatelů by měly být přidělovány maximálně na 4 hodiny.

Pro podsítě Zařízení IoT (3 body):

- poslední adresa z přiřazené podsítě byla rezervována pro výchozí bránu,
 - posledních pět adres v přiřazené podsíti by mělo být Rezervováno,
 - zařízení s názvem **kamera** by mělo mít trvale přiřazenou pátou adresu z podsítě.
 - DNS servery přiřazené zařízením IoT byly 8.8.8.8 a 1.1.1.1.
- zařízení IoT byla: iot.wroclaw.org

Poznámka : Pro účely ověření je přístup poskytnut dvěma hostitelům, které jsou připojeny k přepínači **wro-sw-01**. pojmenovaný: **kancelář** (který by měl fungovat v podsíti uživatelů) a **kamera** (která by měla fungovat v podsíti IoT zařízení). Obě zařízení by měla dynamicky získávat IP adresu v souladu s výše uvedenými pravidly a měla by být schopna komunikovat s adresou 198.18.10.100 (1 bod).

Přístup k hostitelům:

Uživatel : cisco

Heslo : cisco

Chcete-li obnovit načtení IP adresy, spusťte na zařízení příkaz:

```
sudo /etc/init.d/networking restart
```

4.7.QoS (QoS) [4 body]

V pobočce ve Vratslavi byl instalován kritický systém IoT , jehož provoz by měl být zacházeno tak, aby nebylo odmítnuto poskytovatelem internetových služeb v jádrové síti.

Podle dohody s poskytovatelem internetových služeb je provoz v jejich síti pro třídu CS3 zacházen speciálně a váš tým... zeptal se Nakonfigurujte pobočku Wrocław tak, aby ji využíval pouze následující provoz tato třída (2 body):

Zdroj: Zařízení IoT s názvem **kamera** připojeno k přepínači wro-sw-01

Cíl: hlavní server: 198.18.10.10

Typ provozu: http

Kromě toho by veškerý ostatní provoz ze všech zařízení IoT měl být označen jako CS1. Veškerý ostatní provoz by měl být označen jako BE, když vstupuje do jádrové sítě (ISP) (2 body).

GRATULUJEME – DOKONČILI JSTE FÁZI:
DEN 1 / ČÁST 3

ULOŽTE KONFIGURACE NA VŠECH
ZAŘÍZENÍCH
A INFORMUJTE VÝBOR!