Meno a priezvisko: Dátum: 14.2.2020

**Net@FIIT 2020**

Predkonfigurované sú smerovače **Vengerberg**, **Cintra** a **Wall of Cintra** a prepínače Foltest a Dijkstra. Server **Yennefer** má IP adresu 123.123.123.123 a server **Calanthe** má IP adresu 111.111.111.111, ktoré by mali byť po dokončení úloh dostupné z počítačov. **Roach** a **Triss** majú prístup na server Yennefer a **Admin** na Calanthe.

Priamy **prístup** máte len k Admin počítaču a ku prepínaču Cirilla. Ku zariadeniam pristupujte cez **telnet**. Heslá na zariadenia postupne zistite z **banneru** zariadení (ak nie je určené v zadaní inak). V prípade, že nepoznáte IP adresu niektorého zariadenia alebo sieť, využite protokol CDP. V prípade, že CDP susedov nevidíte vo výpise, vyskúšajte spustiť CDP na rozhraní, aj napriek tomu, že už je na ňom spustené.

Zabezpečte telnet prístup na všetky **smerovače a prepínače**, zároveň na každom nastavte: hostname, nečitateľné heslo do privilegovaného režimu *cisco (použite najlepšiu možnú formu zabezpečenia hesla a pôvodné heslo odstráňte)*, enkrypciu **všetkých** hesiel. Vypnite všetky rozhrania, ktoré sa **nepoužívajú**.

1. Konfiguračná IP adresa prepínača **Jaskier** je 1.1.1.1 v predvolenej vlan. Heslo do konzoly a privilegovaného režimu je *0xAB v dvojkovej sústave*.
2. Nastavte prepínač tak, aby počítač Admin bol v rovnakej **vlan** (už predkonfigurovaná) ako smerovač Geralt a zároveň nestratil možnosť vzdialenej konfigurácie (dĺžka prefixu je /27, na prepínač nastavte **poslednú** **použiteľnú** IP adresu a na počítač **predposlednú** **použiteľnú** IP adresu).

Keď si budete istý, že konfigurácia v novej vlan už funguje odstráňte IP adresu 1.1.1.1 a vypnite rozhranie, na ktorom bola nakonfigurovaná.

1. Na smerovač **Geralt** nastavte banner „*Authorized users only*“ a na rozhranie GigabitEthernet 0/0 tretiu použiteľnú IP adresu s prefixom dĺžky siete pre 4 zariadenia podľa **VLSM**.
2. Po pripojení na prepínač **Vesemir** zistite IP adresy ostatných smerovačov v sieti.
3. Na smerovač **Rivia** nastavte **SSH** (modulo kľúča 1024, doména je fiit.sk, meno je *admin*, heslo *cisco* nech nie je čitateľné v konfigurácii*,* najvyšší priviledge level). Zabezpečte aby sa už nedalo pripojiť na smerovač Rivia pomocou telnetu.
4. Na prepínači **Cirilla** opravte **native vlan mismatch**. Medzi prepínačmi nezabudnite nastaviť trunk. Nakonfigurujte etherchannel s číslom skupiny 1(fa0/24, fa0/22), číslo skupiny 2(fa0/23, fa0/21), použite **voľný** (nie Cisco) protokol. Nech sa prepínače snažia aktívne vytvoriť etcherchannel.
5. Zistite čísla vlan pomocou **VTP** protokolu (doména: stuba.sk, heslo: cisco). Nakonfigurujte mód **spanning tree**, ktorý konverguje do 1 sekundy. Zabezpečte (pomocou jedného príkazu pre každú vlan) aby prepínač Cirilla bol **root bridge** s prioritou najnižšou možnou, ale väčšou ako 1.
6. Na smerovačoch **Vilgefortz** a **Tissaia** nastavte **router-on-a-stick** inter-vlan smerovanie. Čísla podrozhraní, nech zodpovedajú číslam vlan. K dispozícii máme sieť 192.168.0.0/21. Nech vlan s menším číslom má **512 hostov** a vlan s väčším číslom nech má **48 hostov**, natívnu vlan neadresujte. Použite **VLSM**. Na smerovačoch nastavte **prvú použiteľnú** adresu a na počítače **poslednú použiteľnú**. Počítač **Triss** nech je vo vlan s **menším číslom**. Nech je prepínač Cirilla konfigurovateľný cez **telnet** (heslo nastavte *cisco*) vo vlan s najmenším číslom na **tretej použiteľnej** IP adrese.
7. Na smerovačoch **Vilgefortz** a **Tissaia** nakonfigurujte redundanciu pomocou **HSRP**. Nech čísla skupín a posledných oktetov virtuálnych smerovačov reprezentujú čísla vlan (v prípade vlan X je číslo skupiny X a virtuálna ip adresa A.B.C.X). Zmena smerovačov nech je **preemptívna**. Smerovač Tissaia nech je **vždy** záložný (najnižšia priorita) a smerovač Vilgefortz nech je **vždy** hlavný (najvyššia priorita).
8. Nakonfigurujte smerovanie medzi smerovačmi pomocou **EIGRP**. Číslo **AS** nech je 11. Ohláste všetky siete, okrem sériového rozhrania na smerovači **Rivia** a siete za smerovačom **Geralt**. Na smerovači Rivia nastavte **statickú cestu** (použite exit interface) ku všetkému čo je za Riviou a **rozdistribuujte** túto cestu ostatným smerovačom pomocou **EIGRP**.
9. Medzi smerovačmi Rivia a Vengerberg nakonfigurujte spojenie protokolom **PPP**. Použite **obojsmernú CHAP** autentifikáciu. Smerovače sa autentifikujú svojim *hostname* a heslom *cisco.* Nezabudnite pridať informáciu o susednom smerovači do lokálnej databázy.
10. Smerovač **Vengerberg** má nastavený access list, ktorý **blokuje** všetky komunikácie z **lokálnych sietí**. Na smerovači Rivia nakonfigurujte **PAT**. Prekladajte len IP adresy zo sietí kde sú počítače **Roach a Triss**. Použite **ACL** s číslom 7. Nezabudnite nastaviť **vstupné a výstupné** (sériové rozhranie smerovača Rivia) rozhrania.

1. Smerovač **Cintra** blokuje všetky IP adresy z WAN siete. Nastavte **GRE** point-to-point tunel medzi smerovačom **Rivia** a smerovačom **Cintra**. Použite rozhranie *tunnel7*. Použite sieť 7.7.7.4/30. Smerovač Rivia nech má vyššiu IP adresu z adresného priestoru. Cieľová IP adresa tunelu nech je 10.10.10.13 (rozhranie S0/0/1 na smerovači Cintra).
2. Zabezpečte nadviazanie **OSPF** susedstva medzi smerovačmi **Rivia** a **Cintra** cez vytvorený GRE tunel (proces 7, oblasť 0). Nahláste iba sieť na rozhraní GigabitEthernet 0/0 smerovača **Rivia**. Sieť pridajte do smerovacieho procesu v najšpecifickejšej forme.
3. Na smerovači Geralt vytvorte rozšírený číslovaný ACL, v ktorom povolíte prechod **HTTP trafiky** cez tunel len pre IP adresy z Geralt (Admin) siete. Číslo ACL nech je administratívna vzdialenosť protokolu OSPF (dá sa zistiť zo smerovacej tabuľky). Pomocou web prehliadača na Admin PC sa pripojte na web server **Calanthe** s IP adresou 111.111.111.111.

**Informácie:**

1. Prihláste sa na virtuálny desktop (príp. aj do OS Windows) pomocou prihlasovacieho mena „priezvisko“ a hesla „Meno.Priezvisko“ (použite vaše prvé meno a priezvisko bez diakritiky a úvodzoviek). *Niektoré prihlasovacie mená boli už obsadené, tak ak nebude fungovať „priezvisko“, tak použite prihlasovacie meno „priezviskom“, kde m je prvé písmeno vášho mena*.

2. Prihláste sa do triedy Net@FIIT2020 v systéme netacad.com pomocou odkazu

[link]

3. Aktivitu stiahnite z Assignments -> Net@FIIT.

4. Súbor presuňte na plochu a premenujte podľa svojho priezviska (napr. macko.pka).

5. Po spustení aktivity sa prihláste do simulátora svojimi prihlasovacími údajmi pre systém netacad.com (bez prihlásenia môžete aktivitu uložiť len niekoľkokrát).

6. Aktivitu priebežne ukladajte počas riešenia.

7. Ak chcete skončiť pred vypršaním času, aktivitu uložte a vypnite simulátor.

8. Ak vypršal čas, aktivitu uložte, následne reštartujte a simulátor vypnite (**POZOR: reštartovanú aktivitu neukladať, lebo by sa vám riešenie vymazalo a získate 0 %**).

9. Súbor s vyriešenou aktivitou odovzdajte v systéme netacad.com (Assignments -> Net@FIIT -> Submit Assignment).

**Úspešným riešiteľom sa študent stáva pri zisku aspoň 56 % bodového hodnotenia samohodnotiacej aktivity v simulátore Cisco Packet Tracer.**