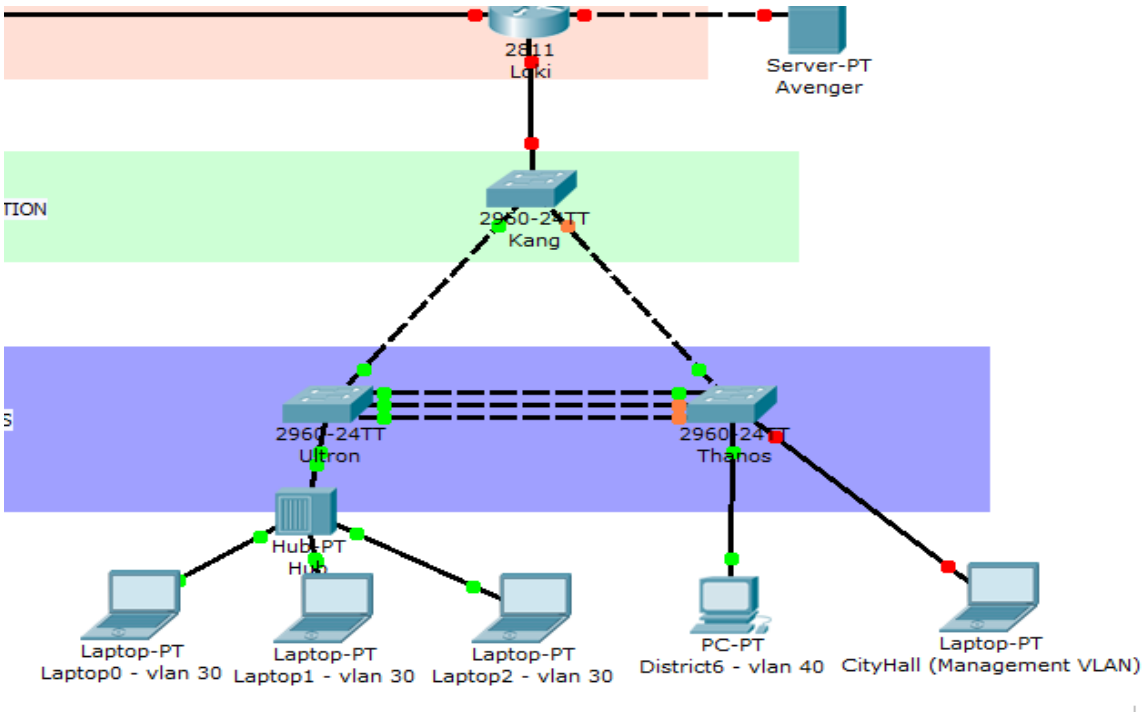
CCNA 3 – Laborator 2

1 Topologie

2 Cerințe



Pentru toate cerințele de mai jos, veți considera numai echipamentele din figura de mai sus și veți neglija configurările pe celelalte echipamente afișate de Packet Tracer.

1. Configurări de bază (CLI) pentru toate switchurile și routerul din figura de mai sus:

   - Configurați hostname-urile afișate în Packet Tracer.
   - Configurați parola încriptată „villain” de enable.
   - Configurați sincronizarea mesajelor de consolă cu comenzile.
   - Configurați un timeout executiv de 0 minute și 0 secunde.
   - Configurați parola „badguy” pe liniile de terminal.
   - Activați serviciul de încriptare a parolelor în running config.
   - Configurați bannerul message-of-the-day (motd) astfel încât să afișeze „No Avengers Allowed!”

- Ce face comanda write în modul privilegiat? Încercați secvența de comenzi „show runn”, „show startup”, „write” și apoi din nou „show startup”.

2. Terminal History :

   - Aflați ultimele 10 comenzi date pe Loki.
   - Măriți bufferul de istorie a comenzilor la 20 de comenzi pe Kang.
   - Dezactivați terminal history pe Loki.
   - Dați comenzi prin care să aflați versiunea de IOS și configurația running a routerului Loki. Vi s-au salvat aceste două comenzi în terminal history? Dar comenzile descoperite la primul subpunct ?

3. Management VLAN:

   - Activați vlanul 99 pe switch-ul Thanos și configurați-l ca vlan de management, oferindu-i adresa 192.168.99.2/24.
   - Configurați portul Fa0/2 al switchului Thanos astfel încât să facă parte din VLAN-ul de management.
   - Configurați adresa IP 192.168.99.3/24 pe laptopul din City Hall(Management VLAN) fără a configura un defaut gateway. Merge pingul de pe acest laptop către switch-ul Thanos? De ce?
   - Configurați default gateway 192.168.99.1 atât pe Thanos, cât si pe laptop-ul din CityHall.

4. Server SSH:

   - Configurați liniile de vty pe Loki astfel încât să fie posibilă conectarea încriptată la aceste linii prin protocolul SSH.
   - Domeniul de nume trebuie să fie avengers.com .
   - Cheia folosită pentru autentificare trebuie să fie de tip RSA.
   - Versiunea de SSH suportată va fi 2.
   - BONUS: Configurați timeout-ul SSH la 60 de secunde și numărul de reîncercări de autentificare la 5.

5. Tabela MAC – partea I:

   - Afișați tabela MAC a switchului Thanos.
   - Salvați ca intrare statică în tabela MAC a switchului Thanos pentru vlan-ul 99 IP-ul laptopului din City Hall.

     HINT: *mac-address-table static <mac-address> vlan <vlan-number> interface <interface-id>*

Salvați configurația lui Thanos în startup-config și resetați switchul. Ce s-a întâmplat cu tabela MAC a lui Thanos?

6. Tabela MAC și port security – partea II:

- Configurați Laptop0, Laptop1, Laptop2 cu adresele IP 192.168.99.11/24, 192.168.30.12/24 și 192.168.30.13/24.
- Includeți porturile Fa0/1 și Fa0/4 ale switchului Ultron, respectiv Fa0/4 a lui Thanos în vlanul de management 99.
- Activați port security pe portul Fa0/1 al lui Ultron.
- Ce fel de port security trebuie să configurăm astfel încât adresele MAC învățate de Ultron să fie salvate în running-configuration?
- Încercați să dați ping de la Laptop0 și de la Laptop 1 la Laptop-ul din CityHall.
- Afișați tabela MAC a switchului Ultron.
- Reactivați interfața Fa0/1 a lui Ultron. Dezactivați port security de tip sticky. Veti obține un port-security de tip dinamic. Ce s-a întâmplat cu mac-urile învățate anterior? Se mai găsesc în running configuration? Dar in tabela MAC?
- Limitați numărul de MAC-uri învățate pe portul Fa0/1 al lui Ultron la 2. Ce se întâmplă dacă dați ping de la Laptopul 2 la Laptopul din City Hall? Portul Fa0/1 al lui Ultron mai este activ? Verificați cu o comandă de show.
- BONUS: În mod default, la încălcarea limitării de port-security interfața unui switch se închide (shutdown). Configurați port security pe Ultron astfel încât la violarea limitării de port security să se aplice modul restrict.

  HINT: *switchport port-security violation ?*