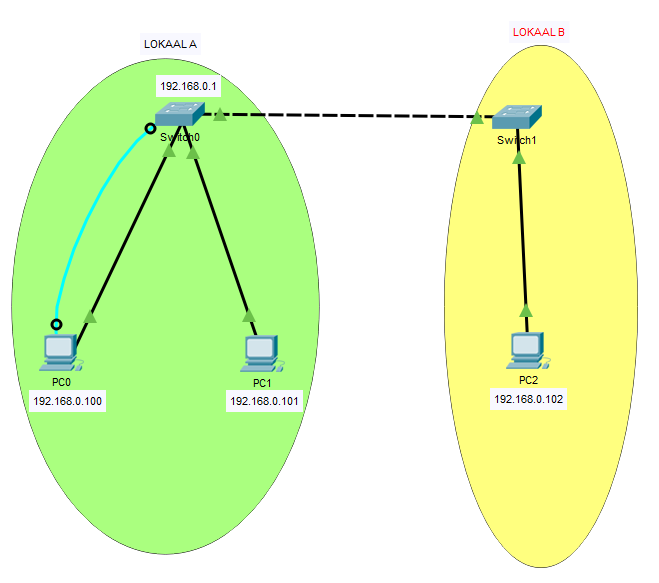
**LAB 03**

**UITGEBREIDE CONFIGURATIE VAN EEN SWITCH**

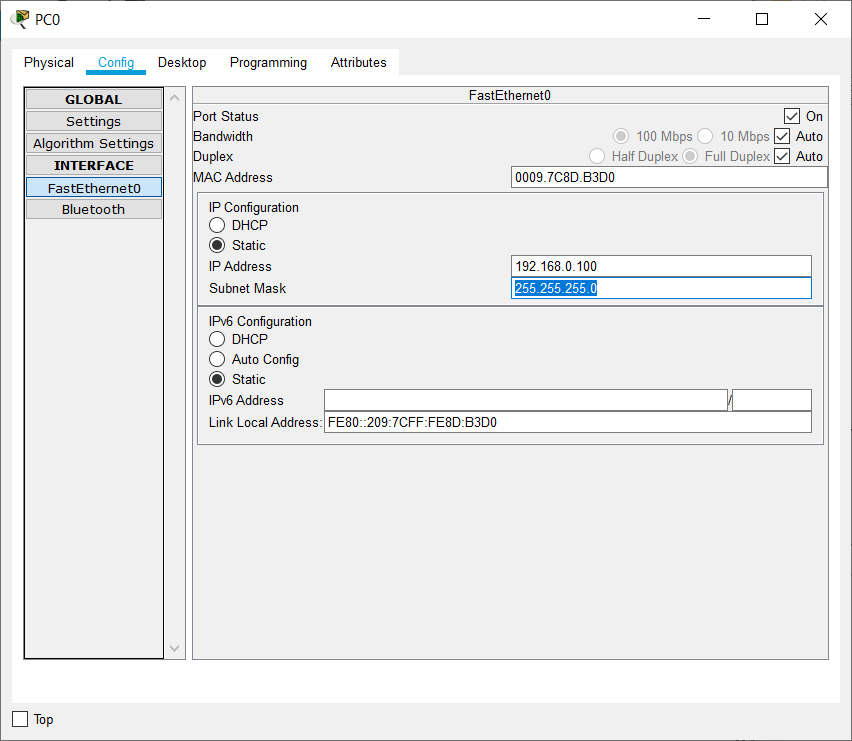
In dit labo leer je hoe je een Cisco-switch kan configureren, om deze vanop afstand te kunnen beheren.

1. Start PT op en open de Lab02.pkt file.
2. Voeg onderstaande elementen aan je netwerk toe.



1. Ken de aangeduide IP-adressen aan de (NIC’s van de) PC’s toe. Kies hierbij telkens voor het voorgestelde standaard subnetmasker 255.255.255.0. Laat de invulvakken voor de default gateway en de DNS Server ongemoeid (in dit netwerk niet belangrijk).

Opmerking: de IP-adressen kan je via de knop “Place Note” uit de onderste toolbar visueel aan de figuur toevoegen. Opgelet: hiermee worden de IP-adressen niet automatisch toegekend aan de NIC’s!



1. Ga na of je vanaf PC0 kan pingen naar PC1 en naar PC2.

Je kan pingen tussen deze 3 PC’s omdat de computers tot het zelfde netwerk behoren en dmv switches verbonden zijn.

Om na te gaan of IP-adressen tot het zelfde netwerk behoren, wordt er gebruikgemaakt van het subnetmasker.

Het gebruik van subnetmaskers komt later in de cursus uitvoerig aan bod, maar onthou voorlopig:

**Alle IP-adressen waarvan de eerste 3 getallen gelijk zijn (in de dotted decimal notation) en die als subnetmasker 255.255.255.0 hebben, behoren tot het zelfde netwerk.**

1. Test de vorige regel uit door het IP-adres van PC2 te wijzigen in 192.168.**1**.102. Probeer daarna te pingen vanaf PC0 naar PC2. Je zal merken dat dit niet lukt…

Wijzig daarna terug het IP-adres van PC2 in 192.168.**0**.102.

1. Normaliter werken we in PT altijd in de standaard **Realtime Mode**, maar soms kan het ook eens interessant zijn om in de **Simulation Mode** te werken. Dit kan bv gebruikt worden om na te gaan hoe een PING-commando werkt.

Schakel daarom over naar de Simulation Mode door rechts onderaan in je werkblad op de gelijknamige knop te drukken.

Klik rechts onderaan op je scherm op de “Edit Filters” knop en selecteer enkel het **ICMP-protocol** (dit is immers het protocol dat door het PING-commando gebruikt wordt).

Tik opnieuw het ping-commando in om vanaf PC0 naar PC2 te pingen. Normaliter moet je aan de hand van een animatie kunnen meevolgen wat er “achter de schermen” van het PING-commando gebeurt…

Klik daarna onder “Play Controls” (rechtsonderaan in het werkblad) op de Play-knop om de simulatie te starten.

Als je goed opgelet hebt, dan zal je gemerkt hebben dat Switch0 het eerste ICMP-pakketje ook naar PC1 stuurde. Dit komt omdat switch0 op dat moment nog niet wist via welke poort hij PC2 kon bereiken. Daarom stuurde Switch0 het ICMP-pakketje naar alle devices waarmee het rechtsreeks verbonden is (met uitzondering van de afzender zelf, uiteraard). Bij het tweede pakketje weet Switch0 wel al hoe hij PC2 kan bereiken en stuurt het daarom niet langer naar PC1 door.

Keer daarna terug naar de Realtime Mode.

1. Als PC2 in een ander lokaal staat dan Switch0, kunnen we PC2 niet dmv een consoleverbinding met de deze switch verbinden. De initiële basisconfiguratie kan dus niet vanaf PC2 gebeuren. Toch kunnen we vanaf PC2 vanop afstand Switch0 nog verder configureren. Een eerste belangrijke voorwaarde hiervoor is dat we aan Switch0 een IP-adres toekennen.

Daarom zullen we een IP-adres toekennen aan een virtuele interface van Switch0 (aangeduid als **SVI = Switch Virtual Interface**). Omdat de standaard SVI van een Cisco-switch als naam *vlan1* heeft, dien je dit met onderstaande commando’s te configureren. Tik deze commando’s in vanaf de consoleverbinding op PC0.

***interface vlan1***

***ip address 192.168.0.1 255.255.255.0***

***no shutdown***

Opgelet: zoals je kan zien, vereist het gebruikte *ip address* commando dat je 2 parameters intikt: als eerste een IP-adres (hier: 192.168.0.1), en als tweede een bijhorend **subnetmasker** (hier: 255.255.255.0). Beide parameters dienen door een spatie gescheiden te worden.

Het commando *no shutdown* is verplicht en zorgt ervoor dat de virtuele interface ingeschakeld wordt (want deze staat standaard uit).

1. Ga na of je vanaf PC2 naar Switch0 kan pingen.

Ja, dat kan

Uiteraard moet je ook omgekeerd kunnen pingen vanaf Switch0 naar een PC. Test ook dit even uit!

Kijk goed naar de output van je IOS ping-commando. Wat is het grote verschil met het Windows ping-commando (dat op de PC’s geëmuleerd wordt)?

Wie dit niet meteen ziet, kan deze opdracht best nog eens opnieuw doen in de Simulation Mode…

Bij IOS worden er 5 testpakketten gestuurd.

1. Nu Switch0 een IP-adres heeft, kunnen we proberen deze vanop afstand te beheren. Een eenvoudige manier hiervoor is het gebruik van het programma **Telnet** dat in PT standaard op elke PC kan gebruikt worden (op een Windows 10 PC is dit standaard niet geactiveerd).

Maak vanaf PC2 een Telnet-connectie met Switch0, op basis van zijn IP-adres. Gebruik hiervoor onderstaand commando:

***telnet 192.168.0.1***

Je zal merken dat je Telnet-connectie automatisch afgebroken wordt door de switch.

De reden hiervoor is dat een Cisco-switch om veiligheidsredenen standaard geen Telnet-connecties toelaat.

1. Meld je vanaf PC0 aan op Switch0 en zorg ervoor dat er 3 simultane Telnet-connecties met de switch toegelaten worden en beveilig deze connecties met een wachtwoord. Maak hiervoor gebruik van onderstaande commando’s:

***line vty 0 2***

***password class***

***login***

***transport input telnet***

De eerste regel duid aan dat je de “virtual lines” vty0, vty1 en vty2 met één enkel commando kan selecteren. De spatie in het commando tussen de 0 en de betekent dus vanaf 0 tot en met 2.

De laatste regel zorgt ervoor dat Telnet toegelaten wordt op die “virtual lines”.

1. Ga na of je simultaan kan Telnetten vanaf PC0, PC1 en PC2 naar de switch.

Ja, na invoer van het wachtwoord

1. Merk op dat eens je een Telnet-connectie gemaakt hebt met de switch gemaakt hebt, je van alle IOS-commando’s gebruik kan maken.

Test dit op 1 PC uit door in de Telnet-connectie de inhoud van de huidige configuratie van de switch op te vragen.

show running-config (of korter: sh ru)

1. Eén van de grootste nadelen van Telnet is dat het een oud en onveilig protocol is (wachtwoorden worden niet geëncrypteerd doorgestuurd). Daarom gaan we gebruikmaken van een veiliger manier om vanop afstand een connectie te maken met een switch, nl SSH.

Vooraleer we dit gaan toepassen op Switch0, gaan we eerste het onveilig Telnet-protocol dat we in opdracht 10 op de vty lines toegelaten hebben, terug verwijderen. Hiervoor moet je de 3 bijhorende commando’s die op die lines toegepast werden, terug verwijderen. Dit doe je door elk van die commando’s opnieuw in te voeren, maar telkens voorafgegaan door het commando ***no***.

Pas dus onderstaande commando’s op die lines toe:

***no password class***

***no login***

***no transport input telnet***

1. Vooraleer ssh op de switch kan geactiveerd worden, dien je nog 4 dingen te doen:
   1. Een domeinnaam kiezen 🡪 we kiezen voor ccna.com
   2. RSA-sleutels genereren 🡪 kies voor een sleutellengte van 1024 bits
   3. Een lokale gebruikersaccount op de switch aanmaken om je ermee lokaal aan te melden 🡪 kies je voornaam als naam
   4. Enkel het gebruik van versie 2 van ssh toelaten

Maak hiervoor gebruik van onderstaande commando’s:

***ip domain-name ccna.com***

***crypto key generate rsa***

***username chris secret 0123456789***

***ip ssh version 2***

1. Tenslotte dien je op de 3 vty-lines ssh te activeren met onderstaande commando’s:

***line vty 0 2***

***password class***

***login***

***transport input ssh***

1. Ga na of je vanaf elke PC simultaan een ssh-connectie met de switch kan maken.

Tip: maak gebruik van ssh /? Om de syntax van het commando te bekijken.

ssh -l chris 192.168.0.1

1. Merk op dat eens je een SSH-connectie met de switch gemaakt hebt, je van alle IOS-commando’s gebruik kan maken.

Test dit op 1 PC uit door in de SSH-connectie de inhoud van de huidige configuratie van de switch op te slaan in NVRAM.

copy running-config startup-config (of korter: copy ru st)

1. Bewaar de PT-oefening in een file met als naam **familienaam-voornaam-lab03.pkt** en upload deze via Leho.