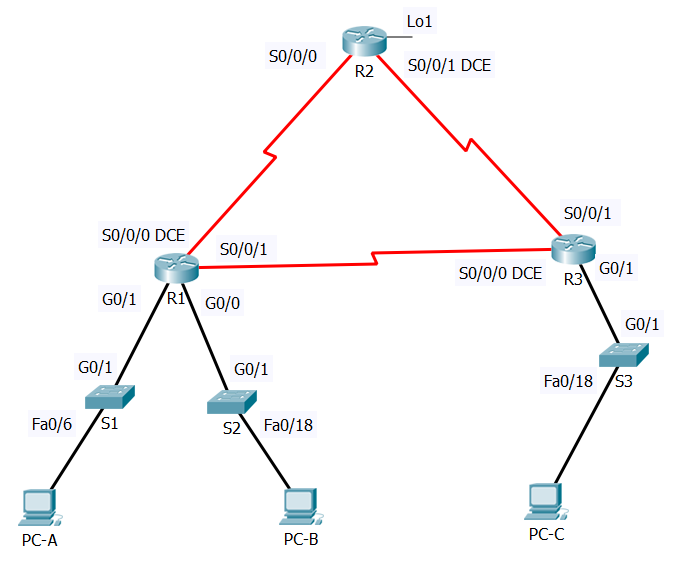
Opgave netwerk-labo projecten 3 Systeembeheer 2020-2021

**Gegeven:**

Volgende opstelling



Bijbehorende adressentabel:

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Default Gateway** |
| R1 (FE80::1) | S0/0/0(DCE) | 2001:DB8:AAAA:1::1/64 | N/A |
| S0/0/1 | 2001:DB8:AAAA:3::1/64 | N/A |
| G0/0 | 2001:DB8:ACAD:B::1/64 | N/A |
| G0/1 | 2001:DB8:ACAD:A::1/64 | N/A |
| R2 (FE80::2) | S0/0/0 | 2001:DB8:AAAA:1::2/64 | N/A |
| S0/0/1(DCE) | 2001:DB8:AAAA:2::2/64 | N/A |
| Lo1 | 2001:DB8:AAAA:4::1/64 | N/A |
| R3 (FE80::3) | S0/0/0(DCE) | 2001:DB8:AAAA:3::2/64 | N/A |
| S0/0/1 | 2001:DB8:AAAA:2::1/64 | N/A |
| G0/1 | 2001:DB8:ACAD:C::1/64 | N/A |
| S1 | VLAN1 | 2001:DB8:ACAD:A::A/64 | N/A |
| S2 | VLAN1 | 2001:DB8:ACAD:B::A/64 | N/A |
| S3 | VLAN1 | 2001:DB8:ACAD:C::A/64 | N/A |
| PC-A | NIC | 2001:DB8:ACAD:A::3/64 | FE80::1 |
| PC-B | NIC | 2001:DB8:ACAD:B::3/64 | FE80::1 |
| PC-C | NIC | 2001:DB8:ACAD:C::3/64 | FE80::3 |

**DEEL 1: maak de netwerkopstelling en initialiseer de toestellen**

*Stap 1:* bouw de netwerkopstelling uit overeenkomstig de gegeven topologie

*Stap 2:* initialiseer of reload eventueel de routers en switchen: zorg er dus voor dat er geen oude configuratie meer op de toestellen staat

**DEEL 2: configureer alle toestellen en controleer de verbindingen**

*Stap 1: configureer de IPv6 adressen op alle PC’s*

Configureer de IPv6 global unicast adressen overeenkomstig de gegeven adressentabel. Gebruik het link-local adres als default-gateway op alle Pc’s.

*Stap 2: configureer de switchen*

a. Maak DNS lookup ongedaan.

b. Configureer een hostname.

c. Wijs volgende domeinnaam toe: **ccna-lab.com**.

d. Encrypteer de plain-text paswoorden.

e. Maak een MOTD banner die de gebruikers waarschuwt : “Toegang voor onbevoegden is verboden”.

f. Maak een lokale user database met een gebruikersnaam **admin** en paswoord **classadm**.

g. Configureer **class** als het privileged EXEC geëncrypteerd paswoord.

h. Configureer **cisco** als het console paswoord en maak login mogelijk.

i. Maak login op de VTY lijnen mogelijk door gebruik te maken van de lokale database.

j. Genereer een crypto rsa key voor ssh, gebruik makend van een modulus grootte van 1024 bits.

k. Verander de transport input op alle VTY lijnen naar alleen SSH en Telnet.

l. Wijs een IPv6 adres toe aan VLAN 1 overeenkomstig de adrestabel.

**Voeg hier tussen de runningconfiguration file van S1.**

*Stap 3: configureer de basisinstellingen op alle routers*

a. Maak DNS lookup ongedaan.

b. Configureer een hostname.

c. Wijs volgende domeinnaam toe: **ccna-lab.com**.

d. Encrypteer de plain-text paswoorden.

e. Maak een MOTD banner die de gebruikers waarschuwt : “Toegang voor onbevoegden is verboden”.

f. Maak een lokale user database met een gebruikersnaam **admin** en paswoord **classadm**.

g. Configureer **class** als het privileged EXEC geëncrypteerd paswoord.

h. Configureer **cisco** als het console paswoord en maak login mogelijk.

i. Maak login op de VTY lijnen mogelijk door gebruik te maken van de lokale database.

j. Genereer een crypto rsa key voor ssh, gebruik makend van een modulus grootte van 1024 bits.

k. Verander de transport input op alle VTY lijnen naar alleen SSH en Telnet.

*Stap 4: configureer IPv6 instellingen op R1*

a. Configureer de IPv6 unicast adressen op de volgende interfaces: G0/0, G0/1, S0/0/0 en S0/0/1.

b. Configureer de IPv6 link-local adressen op de volgende interfaces: G0/0, G0/1, S0/0/0 en S0/0/1. Gebruik **FE80::1** voor de link-local adressen op alle vier interfaces.

c. Zet de clock rate op S0/0/0 op 128000.

d. Zorg ervoor dat de interfaces IPv6-pakketten kunnen versturen.

e. Maak IPv6 unicast routing mogelijk.

f. Configureer OSPFv3 op R1 en zorg dat de LAN-interfaces passieve interfaces zijn.

**Voeg hier tussen de runningconfiguration file van R1.**

*Stap 5: configureer IPv6 instellingen op R2*

a. Configureer de IPv6 unicast adressen op de volgende interfaces: Lo1, S0/0/0 en S0/0/1.

b. Configureer de IPv6 link-local adressen op de volgende interfaces: S0/0/0 en S0/0/1. Gebruik **FE80::2** voor de link-local adressen op alle twee interfaces.

c. Zet de clock rate op S0/0/1 op 128000.

d. Zorg ervoor dat de interfaces IPv6-pakketten kunnen versturen.

e. Maak IPv6 unicast routing mogelijk.

f. Maak een default route die gebruik maakt van de loopback interface Lo1 (deze dient ter simulatie van een internetconnectie).

g. Configureer OSPFv3 op R2 en zorg dat de default route doorgegeven wordt op de andere routers van het domein.

**Voeg hier tussen de runningconfiguration file van R2.**

*Stap 6: configureer IPv6 instellingen op R3*

a. Configureer de IPv6 unicast adressen op de volgende interfaces: G0/1, S0/0/0 en S0/0/1.

b. Configureer de IPv6 link-local adressen op de volgende interfaces: G0/1, S0/0/0 en S0/0/1. Gebruik **FE80::3** voor de link-local adressen op alle drie interfaces.

c. Zet de clock rate op S0/0/0 op 128000.

d. Zorg ervoor dat de interfaces IPv6-pakketten kunnen versturen.

e. Maak IPv6 unicast routing mogelijk.

f. Configureer OSPFv3 op R3 en maak van de LAN-interface een passieve interface.

**Voeg hier tussen de runningconfiguration file van R3.**

*Stap 7: Controleer de connectiviteit*

a. Elke PC zou in staat moeten zijn om te kunnen pingen naar de andere PC’s in de topology.

b. Telnet naar R1 vanuit alle PC’s in de topology.

c. SSH naar R1 vanuit alle PC’s in de topology.

d. Telnet naar S1 vanuit alle PC’s in de topology.

e. SSH naar S1 vanuit alle PC’s in de topology.

f. Zorg ervoor dat nu alles werkt: troubleshoot indien nodig want de ACLs die je zal maken in DEEL3 gaan de toegang beperken tot bepaalde zones van het netwerk

**Opmerking**: Tera Term vereist dat het bestemmings IPv6 adres tussen vierkante haakjes staat. Voer het IPv6 adres in zoals in de figuur, klik op **OK** en vervolgens op **Continue** om de beveiligingswaarschuwing te accepteren en te connecteren met de router.



Voer de geconfigureerde gebruikerscredentials in (gebruikersnaam **admin** en paswoord **classadm**) en selecteer de **Use plain password to log in** in de SSH Authentication dialogue box. Klik op **OK** om verder te gaan.



**DEEL 3: Configureer en controleer IPv6 ACLs**

*Stap 1: Configureer en controleer VTY beperkingen op R1:*

a. Maak een (extended) ACL genaamd **RESTRICT-VTY** zodat alleen hosts van het 2001:db8:acad:a::/64 netwerk kunnen telnetten naar R1. Alle andere hosts kunnen alleen gebruik maken van SSH om te connecteren met R1.

Voeg hier de configuratie van de ACL in:

R1(config)# **ipv6 access-list RESTRICT-VTY**

R1(config-ipv6-acl)# **permit tcp 2001:DB8:ACAD:A::/64 any**

R1(config-ipv6-acl)# **permit tcp any any eq 22**

R1(config-ipv6-acl)# **deny tcp any any eq 23**

b. Pas de RESTRICT-VTY ACL toe op de VTY lijnen van R1.

Geef de gebruikte commando’s

R1(config-ipv6-acl)# **line vty 0 15**

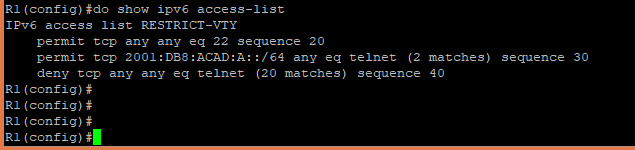
R1(config-line)# **ipv6 access-class RESTRICT-VTY in**

c. Toon de nieuwe ACL.

Geef het commando:

R1# **show access-lists**

Geef de uitvoer van bovenstaand commando :



d. Controleer dat de RESTRICT-VTY ACL alleen Telnet verkeer toelaat van het 2001:db8:acad:a::/64 netwerk.

*Stap 2: Beperk de Telnet-toegang tot het 2001:db8:acad:a::/64 netwerk:*

a. Maak een (extended) ACL genaamd **RESTRICTED-LAN**  dat alle Telnet-toegang tot het 2001:db8:acad:a::/64 netwerk blokkeert.

Voeg hier de configuratie van de ACL in:

R1(config)# **ipv6 access-list RESTRICTED-LAN**

R1(config-ipv6-acl)# **deny tcp any 2001:DB8:ACAD:A::/64 eq telnet**

R1(config-ipv6-acl)# **permit ipv6 any any**

b. Pas de RESTRICTED-LAN ACL toe op de G0/1 interface van R1 voor al het uitgaande verkeer.

Geef de gebruikte commando’s

R1(config)#  **int g0/0/1**

R1(config-if)# **ipv6 traffic-filter RESTRICTED-LAN out**

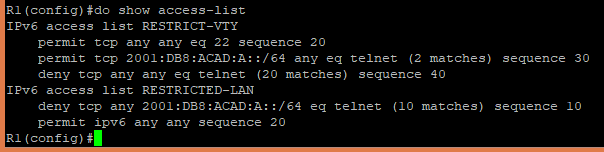
c. Telnet naar S1 van PC-B en PC-C om te controleren dat Telnet inderdaad geblokkeerd wordt. Gebruik vervolgens SSH van PC-C naar S1 om te controleren dat je via SSH wel nog S1 kan bereiken. Troubleshoot indien nodig.

d. Toon de nieuwe ACL.

Geef het commando:

R1# **show access-lists**

Geef de uitvoer van bovenstaand commando :



Merk op dat in elke lijn het aantal hits of matches staat die zijn opgetreden sinds de ACL was toegepast op de interface

e. Gebruik het **clear ipv6 access-list**-commandoomde match-tellers te resetten voor de RESRICTED-LAN ACL

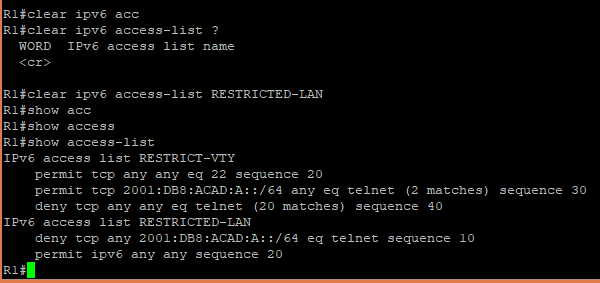
R1# **clear ipv6 access-list RESTRICTED-LAN**

f. Toon opnieuw de ACL om te controleren dat de tellers inderdaad terug op nul staan.

Geef het commando:

R1# **show access-list RESTRICTED-LAN**

Geef de uitvoer van bovenstaand commando :



**DEEL 4: Aanpassingen aan een IPv6 ACL**

Voordat je met de aanpassingen begint in de *RESTRICTED-LAN ACL*, verwijder je best eerst de ACL van de interface.

*Stap 1: Verwijder de RESTRICTED-LAN ACL van de interface*

Geef de gebruikte commando’s

R1(config)# **int g0/0/1**

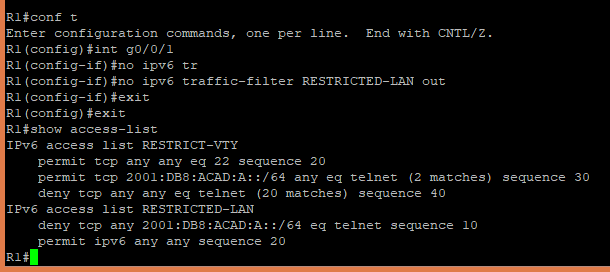
R1(config-if)# **no ipv6 traffic-filter RESTRICTED-LAN out**

*Stap 2: Toon alle ACL*

Geef het commando:

R1# **show access-lists**

Geef de uitvoer van bovenstaand commando :



*Stap 3: Voeg een nieuw ACL-statement toe door gebruik te maken van een volgnummer*

R1(config)# **ipv6 access-list RESTRICTED-LAN**

R1(config-ipv6-acl)# **permit tcp 2001:db8:acad:b::/64 host 2001:db8:acad:a::a eq 23 sequence 15**

Wat is het gevolg van deze nieuwe statement?

**Het zorgt er voor dat hosts van het 2001:DB8:ACAD:B::/64 kunnen telnetten naar Switch 1 (S1)**

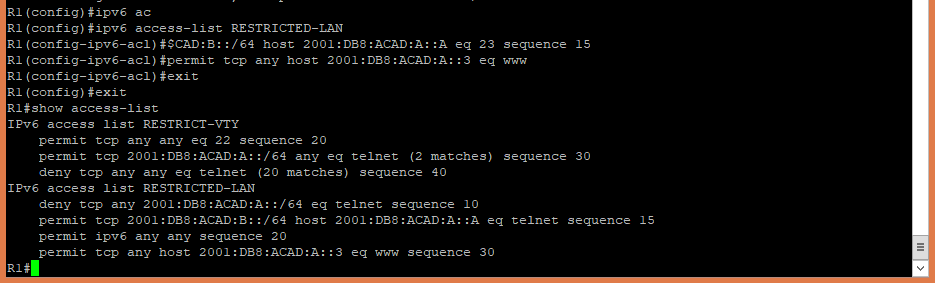
*Stap 4: Voeg een nieuw ACL-statement toe aan het einde van de RESTRICTED-LAN ACL*

R1(config-ipv6-acl)# **permit tcp any host 2001:db8:acad:a::3 eq www**

**Opmerking**: Eigenlijk is deze statement overbodig. Deze wordt enkel gebruikt om te tonen hoe een statement wordt toegevoegd aan het einde van een ACL.

*Stap 5: Toon opnieuw de ACLs om de veranderingen te controleren*

Geef de uitvoer van het commando:



*Stap 6: Verwijder de laatst toegevoegde lijn in de RESTRICTED-LAN ACL*

Geef het gebruikte commando:

R1(config)# **ipv6 access-list RESTRICTED-LAN**

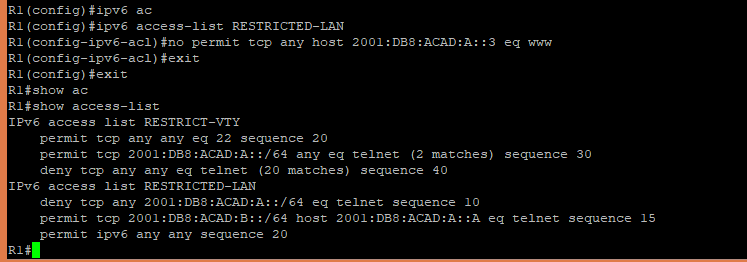
R1(config-ipv6-acl)# **no permit tcp any host 2001:db8:acad:a::3 eq www**

*Stap 7: Toon opnieuw de RESTRICTED-LAN ACL om de veranderingen te controleren*

Geef het gebruikte commando:

R1(config-ipv6-acl)# **do show access-list RESTRICTED-LAN**

Geef de uitvoer van het commando:



*Stap 8: Pas opnieuw de RESTRICTED-LAN ACL toe op de interface G0/1*

Geef de gebruikte commando’s:

R1(config)# **int g0/0/1**

R1(config-if)# **ipv6 traffic-filter RESTRICTED-LAN out**

*Stap 9: Test de veranderingen van de ACL.*

Telnet naar S1 vanuit PC-B. Troubleshoot indien nodig.