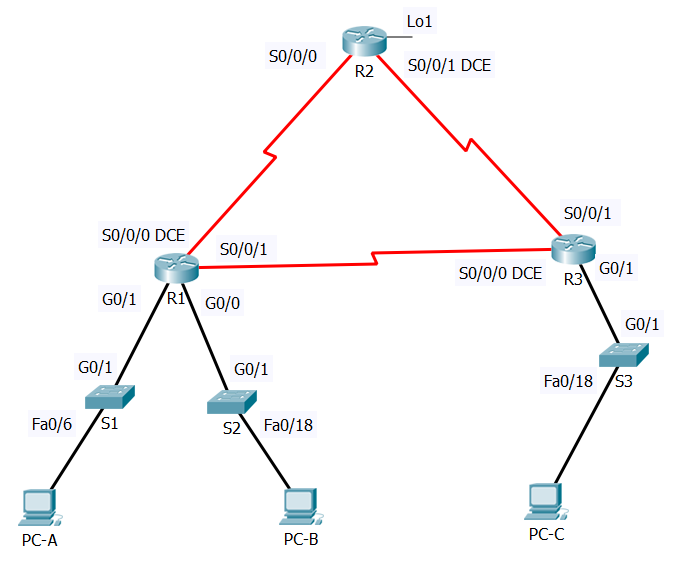
Opgave netwerk-labo projecten 3 Systeembeheer 2020-2021

**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:CAFE: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 |

**Om te beginnen zullen we de software van de switches aanpassen, dit om verdere problemen te vermijden.**

\* Dit geeft een probleem in packet tracer aangezien de switch een verouderd IOS gebruikt deze zullen we updaten

```

 1. Voeg een server toe

 2. geef deze een ip adress bv: 192.168.0.254

 3. geef de switch ook een ip adress bv:

    S1(config)#interface vlan 1

    S1(config-if)#ip address 192.168.0.1 255.255.255.0

    S1(config-if)#no shut

 4. S1#copy tftp flash

        hierna vraagt hij om het remote host adress, hier geef je het ip adres van de server in. Hierna zal hij de file naam vragen hier geef je hetvolgende in : c2960-lanbasek9-mz.150-2.SE4.bin, erna bevestig je gewoon met een enter.

 5. S1(config)#boot system flash:c2960-lanbasek9-mz.150-2.SE4.bin

    S1(config)#exit

 6. S1#copy running-config startup-config

 7. S1#reload

```

![IOSVersie](./IOSVersie.png)

```

  8. S1(config)#sdm prefer dual-ipv4-and-ipv6  default

  9. S1#reload

  10. S1>enable

      S1#config terminal

      S1(config)#interface vlan 1

      S1(config-if)#ipv6 enable

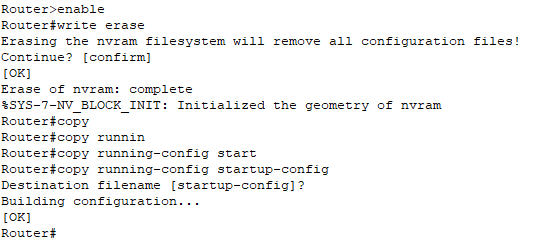
      S1(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64

```

**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

  
+ reload

**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.

```

  Switch>enable

  Switch#config terminal

  Switch(config)#no ip  domain-lookup

```

b. Configureer een hostname.

```

  Switch>enable

  Switch#config terminal

  Switch(config)#hostname S1

```

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

```

  Switch>enable

  Switch#config terminal

  Switch(config)#ip domain-name ccna-lab.com

```

d. Encrypteer de plain-text paswoorden.

\* Encrypteer de plain-text paswoorden

```

  Switch>enable

  Switch#config terminal

  Switch(config)#service password-encryption

```

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

```

  Switch>enable

  Switch#config terminal

  Switch(config)#banner motd #Toegang voor onbevoegden is verboden#

```

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

\* maak een lokale user database met een gebruikersnaam admin en paswoord classadm

```

  Switch>enable

  Switch#config terminal

  Switch(config)#username admin password classadm

```

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

```

  Switch>enable

  Switch#config terminal

  Switch(config)#enable secret class

```

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

```

  Switch>enable

  Switch#config terminal

  Switch(config)#line vty 0 15

  Switch(config-line)#password cisco

```

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

  Switch(config-line)#login local

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

```

  Switch>enable

  Switch#config terminal

  Switch(config)#crypto key generate rsa

  Geef 1024 in

```

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

```

  Switch>enable

  Switch#config terminal

  Switch(config)#line vty 0 15

  S1(config-line)#transport input all

```

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

  10. S1>enable

      S1#config terminal

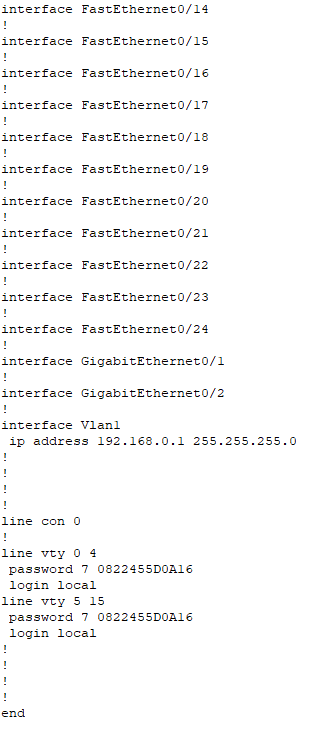
      S1(config)#interface vlan 1

      S1(config-if)#ipv6 enable

      S1(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64

```

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



*Stap 3: configureer de basisinstellingen op alle routers*

a. Maak DNS lookup ongedaan.

\* maak DNS lookup ongedaan, configureer hostname en wijs volgende domeinnaam toe: ccna-lab.com

```

  Router>enable

  Router#configure terminal

  Router(config)#no ip domain-lookup

```

b. Configureer een hostname.

  Router(config)#hostname R1

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

  R1(config)#ip domain-name ccna-lab.com

d. Encrypteer de plain-text paswoorden.

```

  R1>enable

  R1#configure terminal

  R1(config)#service password-encryption

```

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

```

  R1>enable

  R1#configure terminal

  R1(config)#banner motd #Toegang voor onbevoegden is verboden"

```

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

```

  R1>enable

  R1#configure terminal

  R1(config)#username admin password classadm

```

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

  R1(config)#enable secret class

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

```

  R1>enable

  R1#config terminal

  R1(config)#line vty 0 15

  R1(config-line)#password cisco

```

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

  R1(config-line)#login local

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

```

  R1>enable

  R1#config terminal

  R1(config)#crypto key generate rsa

  Geef 1024 in

```

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

```

  R1>enable

  R1#config terminal

  R1(config)#line vty 0 15

  R1(config)#transport input all

```

*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.

```

  R1>enable

  R1#config terminal

  R1(config)#interface gigabitEthernet 0/0/0

  R1(config-if)#ipv6 address 2001:DB8:ACAD:B::1/64

  R1(config)#interface gigabitEthernet 0/0/1

  R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64

  R1(config)#interface serial 0/0/0

  R1(config-if)#ipv6 address 2001:DB8:AAAA:1::1/64

  R1(config)#interface serial 0/0/1

  R1(config-if)#ipv6 address 2001:DB8:AAAA:3::1/64

```

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.

```

  R1>enable

  R1#config terminal

  R1(config)#interface gigabitEthernet 0/0/0

  R1(config-if)#ipv6 address FE80::1 link-local

  R1(config)#interface gigabitEthernet 0/0/1

  R1(config-if)#ipv6 address FE80::1 link-local

  R1(config)#interface serial 0/0/1

  R1(config-if)#ipv6 address FE80::1 link-local

  R1(config)#interface serial 0/0/0

  R1(config-if)#ipv6 address FE80::1 link-local

```

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

  R1(config)#interface serial 0/0/0

  R1(config-if)#clock rate 128000

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

```

  R1>enable

  R1#config terminal

  R1(config)#interface gigabitEthernet 0/0/0

  R1(config-if)#ipv6 enable

```

e. Maak IPv6 unicast routing mogelijk.

```

  R1>enable

  R1#config terminal

  R1(config)#ipv6 unicast-routing

```

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

```

  R1>enable

  R1#config terminal

  R1(config)#ipv6 router ospf 20

  R1(config-rtr)#router-id 1.1.1.1

  R1(config-rtr)#passive-interface gigabitEthernet g0/0/0

```

Dit laatste lijntje voor alle LAN interfaces.

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

**Building configuration...**

**Current configuration : 1865 bytes**

**!**

**version 15.4**

**no service timestamps log datetime msec**

**no service timestamps debug datetime msec**

**service password-encryption**

**!**

**hostname R1**

**!**

**!**

**!**

**enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1**

**!**

**!**

**!**

**!**

**!**

**!**

**no ip cef**

**ipv6 unicast-routing**

**!**

**no ipv6 cef**

**!**

**!**

**!**

**!**

**!**

**!**

**!**

**!**

**!**

**!**

**no ip domain-lookup**

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

**!**

**!**

**spanning-tree mode pvst**

**!**

**!**

**!**

**!**

**!**

**!**

**interface Loopback1**

**no ip address**

**!**

**interface GigabitEthernet0/0/0**

**no ip address**

**duplex auto**

**speed auto**

**ipv6 address FE80::1 link-local**

**ipv6 address 2001:DB8:ACAD:B::1/64**

**ipv6 enable**

**!**

**interface GigabitEthernet0/0/1**

**no ip address**

**ipv6 traffic-filter RESTRICTED-LAN out**

**duplex auto**

**speed auto**

**ipv6 address FE80::1 link-local**

**ipv6 address 2001:DB8:ACAD:A::1/64**

**!**

**interface Serial0/1/0**

**no ip address**

**ipv6 address FE80::1 link-local**

**ipv6 address 2001:DB8:AAAA:1::1/64**

**ipv6 ospf 20 area 2**

**clock rate 128000**

**!**

**interface Serial0/1/1**

**no ip address**

**ipv6 address FE80::1 link-local**

**ipv6 address 2001:DB8:AAAA:3::1/64**

**ipv6 ospf 20 area 2**

**clock rate 2000000**

**!**

**interface Vlan1**

**no ip address**

**shutdown**

**!**

**router ospf 1**

**log-adjacency-changes**

**!**

**router ospf 2**

**log-adjacency-changes**

**passive-interface GigabitEthernet0/0/0**

**passive-interface GigabitEthernet0/0/1**

**!**

**router ospf 200**

**log-adjacency-changes**

**!**

**ipv6 router ospf 20**

**router-id 1.1.1.1**

**log-adjacency-changes**

**!**

**ipv6 router ospf 1**

**log-adjacency-changes**

**!**

**ip classless**

**!**

**ip flow-export version 9**

**!**

**!**

**ipv6 access-list RESTRICT-VTY**

**permit tcp 2001:DB8:ACAD:A::/64 eq telnet any**

**permit tcp any eq 22 any**

**ipv6 access-list RESTRICTED-LAN**

**deny tcp any 2001:DB8:ACAD:A::/64 eq telnet**

**permit tcp any any**

**permit udp any any**

**!**

**banner motd ^CToegang voor onbevoegden is verboden^C**

**!**

**!**

**!**

**!**

**!**

**line con 0**

**!**

**line aux 0**

**!**

**line vty 0 4**

**ipv6 access-class RESTRICT-VTY in**

**login local**

**line vty 5 15**

**ipv6 access-class RESTRICT-VTY in**

**login local**

**!**

**!**

**!**

**end**

*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.

```

  R2>enable

  R2#config terminal

  R2(config)#interface loopback 1

  R2(config-if)#ipv6 address 2001:DB8:AAAA:4::1/64

  R2(config)#interface s0/1/0

  R2(config-if)#ipv6 address 2001:DB8:AAAA:1::2/64

  R2(config-if)#interface s0/1/1

  R2(config-if)#ipv6 address 2001:DB8:AAAA:2::2/64

```

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.

````

  R2>enable

  R2#config terminal

  R2(config)#interface serial 0/0/0

  R2(config-if)#ipv6 address FE80::2 link-local

  R2(config)#interface serial 0/0/1

  R2(config-if)#ipv6 address FE80::2 link-local

```

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

  R2(config)#interface serial 0/0/1

  R2(config-if)#clock rate 128000

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

```

  R2>enable

  R2#config terminal

  R2(config)#interface serial 0/0/0

  R2(config-if)#ipv6 enable

```

e. Maak IPv6 unicast routing mogelijk.

```

  R2>enable

  R2#config terminal

  R2(config)#ipv6 unicast-routing

```

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

```

ipv6 route ::/0 loopback1

```

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

```

  ipv6 router ospf 10

  router-id 2.2.2.2

  default-info originate

  intf s0/0/0

  ipv6 ospf 10 area 0

  intf s0/0/1

  ipv6 ospf 10 area 0

  ipv6 router ospf 10

  passive-intf loopback 1

  clear ipv6 ospf process

```

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

R2#show running-config

Building configuration...

Current configuration : 1050 bytes

!

version 15.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname R2

!

!

!

enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1

!

!

!

!

!

!

no ip cef

ipv6 unicast-routing

!

no ipv6 cef

!

!

!

!

!

!

!

!

!

!

no ip domain-lookup

ip domain-name ccna-lab.com

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface Loopback1

no ip address

ipv6 address 2001:DB8:AAAA:4::1/64

!

interface GigabitEthernet0/0/0

no ip address

duplex auto

speed auto

shutdown

!

interface GigabitEthernet0/0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/1/0

no ip address

ipv6 address 2001:DB8:AAAA:1::2/64

!

interface Serial0/1/1

no ip address

ipv6 address 2001:DB8:AAAA:2::2/64

!

interface Vlan1

no ip address

shutdown

!

ipv6 router ospf 20

router-id 2.2.2.2

log-adjacency-changes

!

ip classless

!

ip flow-export version 9

!

!

!

banner motd ^CToegang voor onbevoegden is verboden^C

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login local

line vty 5 15

login local

!

!

!

End

*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.

 ```

  R3>enable

  R3#config terminal

  R3(config)#interface s0/1/0

  R3(config-if)#ipv6 address 2001:DB8:AAAA:3::2/64

  R3(config-if)#interface s0/1/1

  R3(config-if)#ipv6 address 2001:DB8:AAAA:2::2/64

  R3(config)#interface g0/1

  R3(config-if)#ipv6 address 2001:DB8:CAFE:C::2/64

```

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.

```

  R3>enable

  R3#config terminal

  R3(config)#interface g0/1

  R3(config-if)#ipv6 address FE80::3 link-local

  R3(config)#interface serial 0/0/0

  R3(config-if)#ipv6 address FE80::3 link-local

  R3(config)#interface serial s0/0/1

  R3(config-if)#ipv6 address FE80::3 link-local

```

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

  R3(config)#interface serial 0/0/0

  R3(config-if)#clock rate 128000

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

```

  R3>enable

  R3#config terminal

  R3(config)#interface serial 0/0/0

  R3(config-if)#ipv6 enable

```

e. Maak IPv6 unicast routing mogelijk.

```

  R3>enable

  R3#config terminal

  R3(config)#ipv6 unicast-routing

```

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

```

  R1>enable

  R1#config terminal

  R1(config)#ipv6 router ospf 20

  R1(config-rtr)#router-id 1.1.1.1

  R1(config-rtr)#passive-interface gigabitEthernet g0/0/1

```

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

Building configuration...

Current configuration : 1245 bytes

!

version 15.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname R3

!

!

!

enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1

!

!

!

!

!

!

no ip cef

ipv6 unicast-routing

!

no ipv6 cef

!

!

!

!

!

!

!

!

!

!

no ip domain-lookup

ip domain-name ccna-lab.com

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface GigabitEthernet0/0/0

no ip address

duplex auto

speed auto

shutdown

!

interface GigabitEthernet0/0/1

no ip address

duplex auto

speed auto

ipv6 address FE80::3 link-local

ipv6 address 2001:DB8:CAFE:C::1/64

!

interface Serial0/1/0

no ip address

ipv6 address FE80::3 link-local

ipv6 address 2001:DB8:AAAA:2::1/64

ipv6 ospf 10 area 2

clock rate 2000000

!

interface Serial0/1/1

no ip address

ipv6 address FE80::3 link-local

ipv6 address 2001:DB8:AAAA:3::2/64

ipv6 ospf 20 area 2

!

interface Vlan1

no ip address

shutdown

!

ipv6 router ospf 10

log-adjacency-changes

!

ipv6 router ospf 20

router-id 4.4.4.4

log-adjacency-changes

auto-cost reference-bandwidth 1000

!

ip classless

!

ip flow-export version 9

!

!

!

banner motd ^CToegang voor onbevoegden is verboden^C

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login local

line vty 5 15

login local

!

!

!

End

*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 eq telnet any

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

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 ipv6 access-list

Geef de uitvoer van bovenstaand commando :

R1#show ipv6 access-list

IPv6 access list RESTRICT-VTY

permit tcp 2001:DB8:ACAD:A::/64 eq telnet any

permit tcp any eq 22 any

IPv6 access list RESTRICTED-LAN

deny tcp any 2001:DB8:ACAD:A::/64 eq telnet

permit tcp any any

permit udp any any

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

R1(config-ipv6-acl)# exit

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 g0/1

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 RESTRICTED-LAN

```

Geef de uitvoer van bovenstaand commando :

IPv6 access list RESTRICTED-LAN

deny tcp any 2001:DB8:ACAD:A::/64 eq telnet

permit ipv6 any any

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 ipv6 access-lists 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 g0/1

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

```

*Stap 2: Toon alle ACL*

Geef het commando:

```

R1# show ipv6 access-lists

```

Geef de uitvoer van bovenstaand commando :

R1#show ipv6 access-list

IPv6 access list RESTRICT-VTY

permit tcp 2001:DB8:ACAD:A::/64 eq telnet any

permit tcp any eq 22 any

IPv6 access list RESTRICTED-LAN

deny tcp any 2001:DB8:ACAD:A::/64 eq telnet

permit tcp any any

permit udp any any

*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?

Toelating dat hosts van het **2001:db8:acad:b::/64**  netwerk kunnen telnetten naar 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-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)#. show ipv6 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 g0/1

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.