L3-Switch configuratie

Algemene instellingen

Hostname instellen

Voeg het naam van het apparaat toe:

```
hostname <apparaat naam>
```

Privilige mode login

Maak een wachtwoord aan voor privilige mode autenticatie:

```
enable secret <wachtwoord>
```

Nu is het bewerken van het apparaat beveiligd met een wachtwoord.

Interne router instellingen (domains, etc)

Activeer de L3 routering:

```
ip routing
```

Geef het netwerk domein en DNS server door:

```
ip domain-name <domein-naam>
ip name-server <IPv6 dns-server>
```

IPv6 aanzetten

Om te kunnen starten met IPv6 moet het eerst 'enabled' worden:

```
ipv6 unicast-routing
```

Stel een DHCP server in om de DNS server door te geven:

```
ipv6 dhcp pool DNS-POOL
 dns-server <IPv6 dns-server>
```

SSH

SSH login

Maak een gebruiker aan voor SSH:

```
username <gebruikers naam> password 0 <wachtwoord>
```

Genereer een crypto key voor SSH

Om SSH te gebruiken hebben we een crypto key nodig. Maak daarvoor een sleutel met:

```
crypto key generate rsa
1024
```

De '1024' hier staat voor de sleutel lengte en het is aanbevolen om niet lager dan 1024 te kiezen.

Beveiligd inloggen

Om te zorgen dat alleen met SSH ingelogd kan worden i.p.v andere protocollen, moet dit in vty line ingesteld worden:

```
line vty 0 4
 exec-timeout 60 0
 logging synchronous
```

De lijn `exec-timeout 60 0` stelt in minuten hoe lang je niks mag doen voordat je uit de SSH sessie gegooid wordt.

L3-interface

Om een interface op L3 verbinding in te stellen moet er in de gewenste interface de commando `no switchport` gebruikt worden en moet er ook een IPv6 adres worden aangewezen:

```
interface <interface>
 no switchport
 ipv6 address <IPv6 adres>
```

OSPF

Configuratie

Om OSPF te gebruiken moeten we eerst de protocol instellen:

```
router ospfv3 <id>
 router-id <router-id>
 address-family ipv6 unicast
 exit-address-family
```

Om een netwerk in OSPF te zetten moet er bij de interface van dat netwerk OSPF op gezet worden met de area nummer van waar het netwerk zich bevind:

```
interface <interface>
 ipv6 ospf <id> area <area-nr>
```

Port-channels

Loadbalancing instellen

Voordat wij portchannels gaan instellen moeten we alvast tegen de switch zeggen dat er loadbalancing moet komen. Dit kan gedaan worden met:

```
port-channel load-balance src-dst-mac
```

Configuratie

Voor een etherchannel verbinding via Layer 2:

```
interface range GigabitEthernet <twee of meer interfaces verbonden met een L2 switch>
 switchport mode trunk
 channel-protocol pagp
 channel-group <group nummer> mode desirable

interface Port-channel <group nummer>
 switchport mode trunk
```

Hier worden de interfaces eerst in trunk mode gezet voor VLAN gebruik. Daarna wordt PagP ingesteld als etherchannel protocol. Als laatst moet er een channel groep nummer toegewezen worden. Let hier op dat groep nummers niet overlappen met andere etherchannel verbindingen.

Om hetzelfde te doen op een Layer 3 verbinding:

```
interface range GigabitEthernet <twee of meer interfaces verbonden met een L3 switch>
 no switchport
 channel-protocol pagp
 channel-group <group nummer> mode desirable

interface Port-channel <group nummer>
```

```
 no switchport
 no ip address
```

De enige verschill hier is dat de poort niet op switchport wordt gezet.

VLANs

Configuratie

Het creëren van een VLAN op een switch gaat als volgt:

```
vlan <nummer>
 name <vlan naam>
```

Het commando `name` hier is niet verplicht maar maakt het makkelijk overzichtbaar waar elk VLAN voor bedoelt is. Binnen het PoC wordt er alleen gebruik gemaakt van VLAN 40(Management), 60(IT) en 70(Servers).

SVI configuratie

Bij een L3-switch wordt SVI ingesteld om te kunnen routeren met de VLAN's. Het configureren hiervan ziet er als volgt uit:

```
interface vlan <vlan-nummer>
 ipv6 address <IPv6 adres>
 ipv6 nd other-config-flag
 ipv6 dhcp server DNS-POOL
 ipv6 ospf 1 area 0
```

Hier net als bij een L3 portchannel stellen we gelijk ook OPSF en DHCP in.

Spanning-tree

Configuratie

Om RPVST in te stellen voeren wij het volgende uit:

```
spanning-tree mode rapid-pvst
```

Om te bepalen wie de root switch of secondairy is van een gegeven VLAN:

```
spanning-tree vlan <nummer> root <primary/secondairy>
```

HSRP

Configuratie

Om HSRP te gebruiken moet er eerst in de interface nog wat gedaan worden zoals het instellen van een virtuele IP. Hier onder een basis configuratie van HSRP:

```
interface <interface>
 standby version 2
 standby <nr> ipv6 <virtuele IPv6 adress>
 standby <nr> priority <priority-nr>
 standby <nr> preempt
 standby <nr> track <track-nr> decrement 50
```

Eerst wordt HRSP versie 2 gespecificeerd. Daarna wordt er een virtuele IP ingesteld. Deze moet hetzelfde zijn als op de andere L3-switch. Dan wordt de priority nummer toegewezen om te bepalen welke L3-switch active wordt en welke op standby. Als laatst wordt er een track aangemaakt die aan een interface gekoppeld kan worden. Zo wordt er gekeken of een van de L3-switches is uitgevallen.

Om de track op een interface te zetten gebruik je de `track` commando:

```
track <track-nr> interface <interface> line-protocol
```

QoS

Configuratie

Om QoS toe te passen wordt er gebruik gemaakt met policy maps. Om bijvoorbeeld een policy map te creëren die VOIP voorrang geeft, maken we een class binnen de gecreërde policy map:

```
policy-map <policy-name>
 class VOICE_VIDEO_EF
  set dscp ef
```

Hier wordt er voorrang op voice video calls in het netwerk.

Om de policy map te gebruiken, kan de policy map ingesteld worden op een interface:

```
interface <interface>
 service-policy output <policy-name>
```

SNMP

Voordat wij SNMP kunnen gebuiken moet er een ACL komen om te defineren wie toegang heeft:

```
ipv6 access-list SNMP-ACCESS
 permit ipv6 <IPv6 netwerk> any
```

Om SNMP te gebruiken moet er een snmp server gestart worden met:

```
snmp-server community public RW ipv6 access-list
```

Nu is het mogelijk om via een host binnen het toegelaten netwerk, om het apparaat te monitoren.

ACL

Creëren

Om een ACL te kunnen creëren in IPv6 moeten we het eerst een naam geven:

```
ipv6 access-list <naam>
```

Na het uitvoeren van de prompt hierboven is het mogelijk om de gemaakte list te defineren:

```
 permit icmp any any echo-reply
 permit udp any any eq 1812
 deny ipv6 any 2000:0:0:60::/64
 permit ipv6 any any
```

In dit voorbeeld wordt alle verkeer dat naar 2000:0:0:60:: wil, geblokkeerd met uitzonderingen zoals een icmp antwoord en alles dat door poort 1812 gaat.

Invoeren

Om de zojuist net gemaakte ACL te kunnen gebruiken moet dit op de gewenste interface gedaan worden:

```
interface <interface>
 ipv6 traffic-filter <naam> <in/out>
```

De ACL kan zowel inkomend of uitgaand ingevoerd worden. Dit hangt af van wat het doel is van de ACL.