# Arbeid 2

I dette dokumentet skal jeg gjøre rede for ulike begrunnelser knyttet til mitt konfigurerte nettverk.

## IPv4 adresseplan

Jeg har fått utdelt adresserommet 172.16.0.0/24 fra Olbejoer AS. Jeg har videre delt opp dette adresserommet inn flere mindre subnett i henhold til nettverkskravene til bedriften.

Ved å se på disse kravene kunne jeg lage en oversikt som ga et bedre bilde av hvilke subnett jeg måtte lage:

|  |  |  |
| --- | --- | --- |
| Subnett | Krav antall adresser | krav til prefix |
| UTVIKLING | 100 | 25 |
| AdmINISTRASJON | 4 | 28 |
| IT-DRIFT | 2 | 28 |
| SERVER |  | 28 |
| NETT-ADM |  | 28 |

Som man kan se så hadde Olbejoer gitt beskjed om at «Utviklingsavdelingen» skulle ha plass til opptil 100 enheter, derfor er /25 nettverk et passende subnett for denne avdelingen. Videre ville Olbejoer at de resterende subnettene skulle være /28 nettverk.

Dette resulterte i følgende subnett.

**172.16.0.0/24 🡪 /25**

|  |  |  |
| --- | --- | --- |
| NETTVERKSADRESSE | BROADCAST-ADRESSE | PREFIX |
| 172.16.0.0 | 172.16.0.127 | 25 |
| 172.16.0.128 | 172.16.0.255 | 25 |

Som man kan se, så oppfyller begge subnettene kravene om 100 adresser. Derfor blir adresserommet 172.16.0.0/25 tilegnet utviklingsavdelingen. Det resterende subnettet blir delt opp videre.

**172.16.0.128/25 🡪 /26**

|  |  |  |
| --- | --- | --- |
| NETTVERKSADRESSE | BROADCAST-ADRESSE | PREFIX |
| 172.16.0.128 | 172.16.0.191 | 26 |
| 172.16.0.192 | 172.16.0.255 | 26 |

De resterende subnettene skal alle ha /28 prefix. For å gjøre adresseblokken med ledige ip-adresser så stor som mulig, så valgte jeg å subnette 172.16.0.128/25 nettverket inn i to /26 nettverk. Alle de resterende /28 subnettene vil da få plass i adresserommet 172.16.0.128/26. Dette resulterer i at vi kan reservere adresserommet 172.16.0.192/26 til fremtidig bruk. Derfor blir adresserommet 172.16.0.128/26 delt opp videre.

**172.16.0.128/26 🡪 /28**

|  |  |  |
| --- | --- | --- |
| NETTVERKSADRESSE | BROADCAST-ADRESSE | PREFIX |
| 172.16.0.128 | 172.16.0.143 | 28 |
| 172.16.0.144 | 172.16.0.159 | 28 |
| 172.16.0.160 | 172.16.0.175 | 28 |
| 172.16.0.176 | 172.16.0.191 | 28 |

Her oppfyller alle adresserommene kravene til de resterende subnettene. Derfor blir disse subnettene tilegnet henholdsvis:

* Administrasjon
* IT-Drift
* Server
* Net-adm

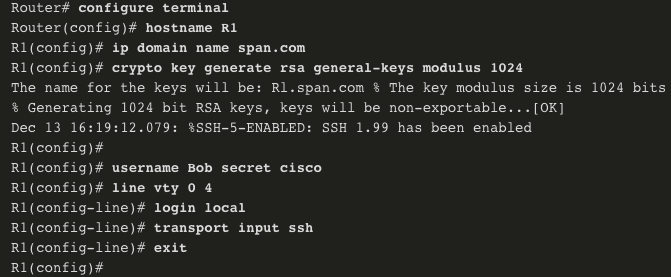
Jeg har også delt bedriftens nettverk inn i VLANs som korresponderer med subnettene. For at de forskjellige VLANene skal kunne få snakke sammen, så måtte jeg konfigurere router-on-a-stick på ruteren. Her måtte jeg konfigurere default gateway for hvert vlan(subnett).

Tabellen under viser derfor hvert subnett med korresponderende VLAN og default gateway.

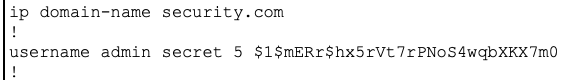
|  |  |  |  |
| --- | --- | --- | --- |
| Avdeling | subnett | vlan | default gateway |
| Utvikling | 172.16.0.0/25 | 30 | 172.16.0.1 |
| admin | 172.16.0.128/28 | 10 | 172.16.0.129 |
| it-drift | 172.16.0.144/28 | 20 | 172.17.0.145 |
| server | 172.16.0.160/28 | 40 | 172.16.0.161 |
| net-adm | 172.16.0.176/28 | 99 | 172.16.0.177 |

## Fjernadministrering

For å konfigurere oppkobling av fjernadministrering som skal ha en kryptert forbindelse, må man benytte SSH. SSH krypterer trafikk mellom avsender og mottaker i motsetning til Telnet. For å konfigurere SSH så er det noen viktige steg som må til. Man må først

opprette navnet på nettverksenheten. Deretter må man konfigurere et ip-domene navn. Deretter genererer man selve nøkkelen som krypterer SSH trafikk. Nøkkelen kan være mellom 360 bits – 2048 bits. Desto flere bits, desto sikrere nøkkel, men større nøkler bruker også lenger tid på å kryptere og dekryptere trafikk. Etter at nøkkelen er generert, så lager man seg en bruker med brukernavn og passord som blir lagret i en lokal database enheten. Deretter brukere man «login local» kommandoen i vty grensesnittet for å fortelle grensesnittet at den skal autentisere login mot den lokale databasen. Det siste man gjør er å benytte seg av kommandoen «transport input ssh» som forteller vty grensesnittet at bare fjernadministrering gjennom SSH er tillatt. (NB: Bildet over er hentet fra NetAcad, men representerer den samme fremgangsmåten for konfigurering.)

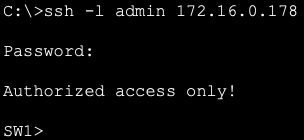
Utklipp fra startup-config:



Som man kan se så benyttet jeg ip domenet: security.com

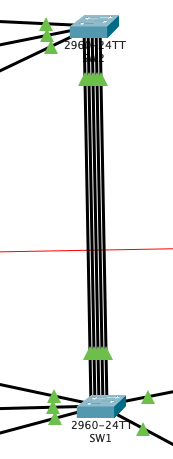
Jeg laget også en bruker med brukernavn «admin». Passordet er «cisco» i henholdsvis til oppgaven, men er her kryptert. Jeg benyttet meg av en 2048 bits nøkkel.

Siden vlan 99, Net-adm, skal benyttes til fjernadministrering, så er management grensesnittet på nettverksenhetene konfigurert til vlan 99.

Dette gjør at jeg nå kan fjernadministrere switchene og ruteren gjennom vlan 99 som er koblet til adresserommet 172.16.0.176/28. På bildet kan man se at jeg kobler meg til switchen i første etasje ved hjelp av SSH.

## EtherChannel og STP

Ved å analysere kravene til bedriften, så ser man at kapasiteten mellom de to switchene skal være på 500 Mbps. Hver FastEthernet port gir maksimalt 100 Mbps. Derfor måtte jeg benytte meg av EtherChannel for å oppnå den ønskelige hastigheten. Ved å bruke EtherChannel vil vi få høyere båndbredde, samtidig som at feiltoleransen blir bedre.



EtherChannel vil også fordele nettverksbelastningen mellom linkene i «kanalen». Grunnen til at man benytter seg av EtherChannel og ikke flere uavhengige linker mellom switchene, er på grunn av Spanning Tree Protokollen (STP). STP er en protokoll som forhindrer looping på nettverket, som potensielt kan oppstå ved broadcast, multicast eller ukjent unicast rammer. Derfor vil uavhengige linker fra switch til switch bli påvirket av STP. STP vil da blokkere alle linkene bortsett fra én for å forhindre at datarammene går i loop på nettverket.

Derfor benytter EtherChannel seg i stedet av en grupperingsmekanisme som grupperer flere linker sammen til en logisk link. Dette vil da skape en «kanal» med flere linker som kan dele på belastningen.

Jeg benyttet meg av LACP for å konfigurere EtherChannel linken. LACP hjelper begge switchene med forhandlinger angående den logiske linken. Dette skjer ved at switchene sender LACP pakker til hverandre. Jeg benyttet med av «LACP active» modusen. Dette gjør at switchen begynner å sende LACP pakkene.



NB: Bildet er hentet fra NetAcad, men representerer den samme fremgangsmåten for konfigurering.

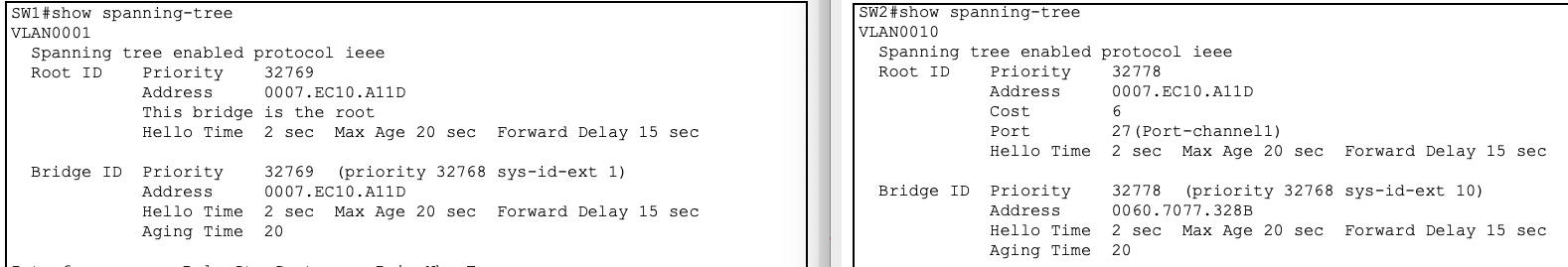
Etter at port-channel 1 er konfigurert, så konfigurerte jeg port-channel 1 som en trunk grensesnitt, før jeg konfigurerte hvilke VLANS som var tillatt å sende gjennom trunk grensesnittet.



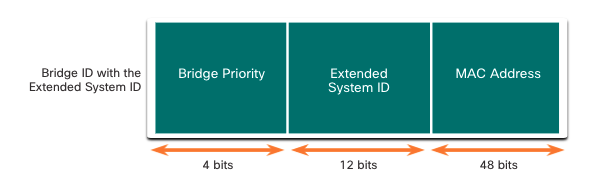
NB: Bildet er hentet fra NetAcad, men representerer den samme fremgangsmåten for konfigurering.

Jeg benyttet kommandoen: switchport trunk allowed vlan 10,20,30,40,99. 🡪 Disse representerer mine VLANs.

Ved å benytte seg av kommandoen: «show spanning-tree» på både begge switchene, så vil jeg kunne se hvilken switch som er roten i spennetreet.



Her kan vi se at SW1 (Switchen i første etasje, og bildet til venstre) er satt opp som roten i spennetreet, siden det står «This bridge is the root». Roten bestemmes av BID (bridge ID) til hver switch.



Denne IDen blir sendt ved hjelp av Bridge Protocol Data Units mellom switchene. Den switchen som har den laveste BID verdien blir roten i spennetreet. I bildet som viste konfigurasjonen av spennetreet kan vi se at SW1 har BID verdi: 32769 og SW2 har: 32778. Derfor har SW1 lavest BID og blir roten i spennetreet.

## Nettverkskort server

Jeg oppgraderte nettverkskortet på serveren slik at den nå benytter seg av PT-HOST-NM-1CGE. Dette nettverkskortet har én Gigabit Ethernet port, slik at hastigheten mellom serveren og switchen kan være på 1Gbps.

## Konklusjon

Jeg er stort sett fornøyd med hvordan nettverket mitt ble konfigurert selv om jeg kunne benyttet meg av et eget VLAN for native VLAN. Etter at oppgaveteksten ble publisert, benyttet jeg tiden til å planlegge hvordan jeg skulle konfigurere nettverket. I denne planleggingsfasen diskuterte jeg ulike design med medstudent Kristoffer Lie.