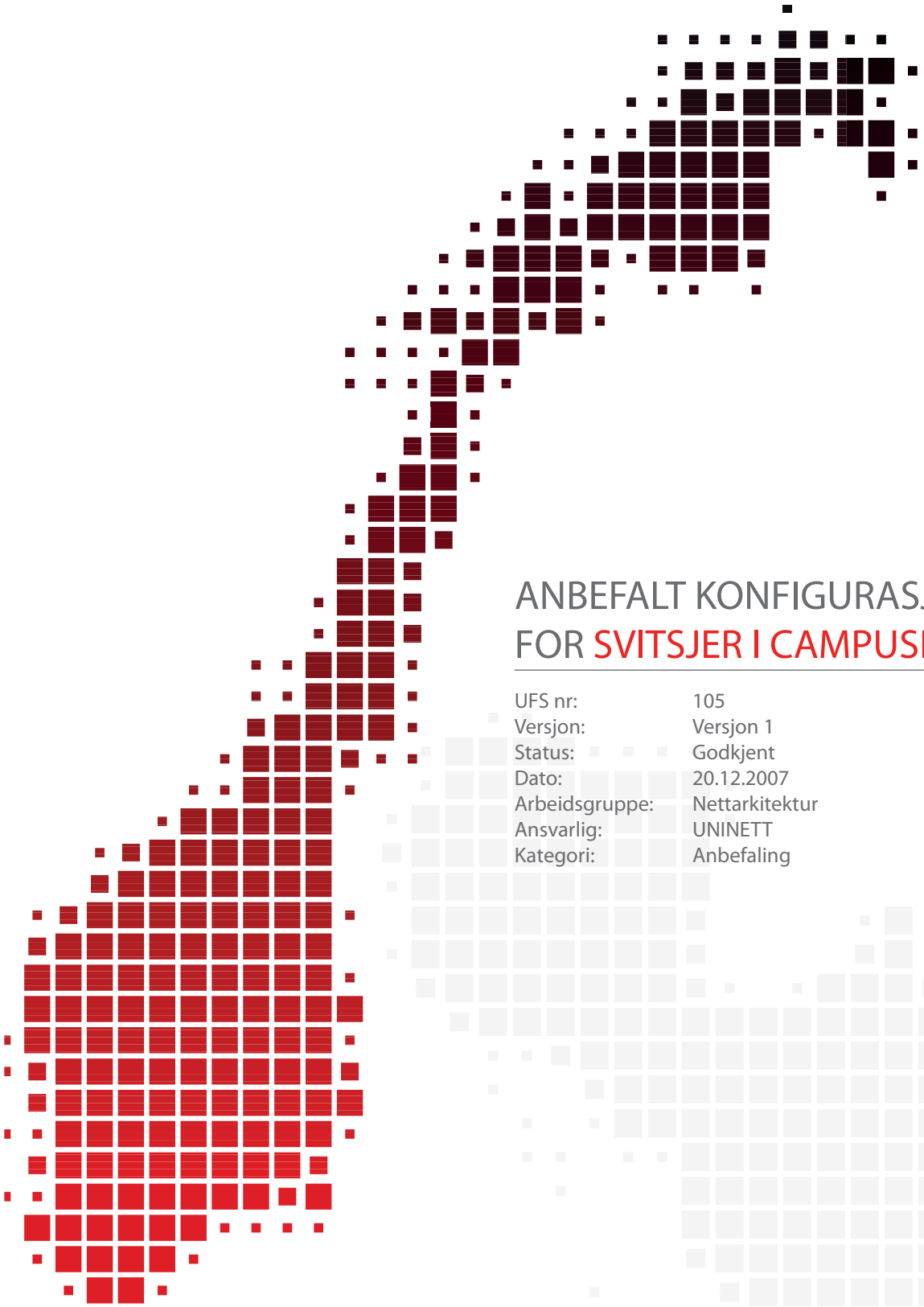
UNINETT Fagspesifikasjon



ANBEFALT KONFIGURASJON FOR SVITSJER I CAMPUSNETT

UFS nr:	105
Versjon:	Versjon 1
Status:	Godkjent
Dato:	20.12.2007
Arbeidsgruppe:	Nettarkitektur
Ansvarlig:	UNINETT
Kategori:	Anbefaling

Table of Contents

Sammendrag

Dette dokumentet gir en anbefaling relatert til konfigurasjon av svitsjer i campusnett. Lag2 og lag2+ funksjonalitet dekkes, ikke lag3 (ruting). Anbefalingen er generisk. En rekke oppskrifter myntet på leverandørspesifikke oppsett vil understøtte anbefalingen.

Dokumentet dekker ikke design av campusnett, men fokuserer på enkeltkomponentene og konfigurasjon av disse.

1. Introduksjon

Det er en rekke ting man må tenke på ved oppsett av en svitsj i et campusnett. En svitsj avhengig av plassering vil ha ulike roller. Vi klassifiserer her svitsjer i tre klasser; kjerne, gren og kant, nærmere definert under. Innen hver klasse kan ulike svitsjer med ulik porttetthet og portsammensetning (ulike hastigheter) benyttes. Vi diskuterer ikke hva slags enheter som bør brukes men gir en generisk kravliste for oppsett og konfigurasjon.

2. Definisjoner

- **Lag 2** : Lag 2 i OSI-stakken. På lag2 forstår ikke svitsjen IP-adresser, men forholder seg til mac-adresser.
- **Lag 2+** : Noen svitsjer har evnen til å forstå ulike egenskaper ved IP-header og høyere lag. Et eksempel er dhcp snooping. Slik funksjonalitet benevnes lag 2+.
- **Lag 3**: Vi er da på nettverkslaget med forståelse av IP-adresser. Noen svitsjer kan gjøre ruting. Dette dokumentet dekker ikke slik funksjonalitet.
- **Kantsvitsj**: En svitsj som står i periferien av nettverket, nærmest brukerne.
- **Grensvitsj**: En svitsj som håndterer aggregert trafikk fra en rekke kantsvitsjer og forbinder dette med kjernesvitsjer.
- **Kjernesvitsjer**: Svitsjer som står i kjernen av nettet og i hovedsak ikke har brukere direkte tilkoblet, primært høykapasitetes forbindelse til andre svitsjer og servere.
- **Klientporter**: Porter på svitsjen som er rettet mot klientmaskiner i nettverket. Dette inkluderer også servere, skrivere og annet endeutstyr. Slike porter har en del andre egenskaper enn nettverksporter, altså porter som har forbindelse til andre nettverkskomponenter (rutere, svitsjer, basestasjoner).

3. Fysiske krav

3.1 Montering

Svitsjen skal rackmonteres og merkes med lett synlig navn. Kabelføring (patching) skal gjøres ryddig, der det vektlegges at det er overkommerlig å bytte svitsjen dersom den ryker. Lysdioder skal være lett synlig.

3.2 Strøm

Det settes ikke krav til UPS eller dobbel strømforsyning for kantsvitsjer og grensvitsjer. For kjernesvitsjer anbefales begge deler. Typisk bør primær strømforsyning gå mot UPS, sekundær mot bystrøm.

3.3 Flash

For kjernesvitsjer bør det være flash dimensjonert til å kunne lagre minst 2 versjoner av programvare. Det er da mulig å konfigurere svitsjen til å gå tilbake til forrige versjon, dersom ny programvare feiler ved oppstart.

4. Programvare

Programvare skal til enhver tid være oppdatert til anbefalt versjon. UNINETT vedlikeholder en oppdatert liste, denne bør følges.

Programvare bør lastes opp fra lokal tftp/ftp/scp-tjener.

5. Navning

Enhver svitsj gis et unikt navn. En gjennomtenkt konvensjon for navnsetting skal anvendes. Navnet kan med fordel gi informasjon om svitsjens beliggenhet og bruksområde. Navnet bør konfigureres på svitsjen som dets sysname. Det bør også registreres i dns. Videre bør svitsjen fysisk merkes med samme navn.

Tilsvarende bør svitsjeporter navnes. Også her anvendes gjennomtenkt konvensjon. Det kan være naturlig å navngi med punkt/romnr porten er patchet mot, evt servernavn eller navn på annen svitsj/ruter, dersom dette er anvendelsen for porten.

Man kan vurdere å utelate portnavnsetting mot sluttbrukere dersom dokumentasjon her er vedlikeholdt på annet vis, eksempelvis i managementapplikasjon.

6. Administrasjon av svitsjen

Svitsjen må kunne konfigureres ved fjernpålogning, den må også kunne overvåkes med SNMP. Man bør vurdere SNMP også for konfigurasjon, i hvertfall for enkelte egenskaper. Webgrensesnitt mot svitsjen kan vurderes, erfaring tilsier imidlertid at dette grensesnittet i de fleste tilfeller er uegnet.

Kun den tilgang som er påkrevd for drift bør være åpen. Alt annet bør skrus av, se 6.6.

6.1 Managementadresse

Management IP-adressen til svitsjen bør være på et dedikert nett for svitsjer/nettelektronikk. Dette nettet bør være godt beskyttet med aksessliste som kun gir driftspersonell adgang.

6.2 Fjernpålogning (med banner)

Fjernpålogning bør gjøres med ssh. Dersom telnet brukes skal dette være over en sikker transportvei, jfr 6.1.

Et banner bør settes, dette kan gjerne angi at uautorisert personell ikke har adgang.

6.3 Autentisering ved fjernpålogning

Det bør være brukerbasert pålogging på svitsjen. Dette har flere fordeler, bl.a. at det er lett å nekte adgang til personale som har sluttet. Videre at personlige passord fremfor felles passord er å foretrekke. Sist, men ikke minst, at det er mulig å se i konfigurasjonsarkivet hvem som har gjort hvilken endring. Brukerbasert pålogging bør basere seg på radius, tacacs+ eller tilsvarende. Dette åpner for mulighet til å gi ulike brukere ulike autorisasjon.

Konfigurasjonsmodus krever ofte en ekstra pålogging etter brukerbasert pålogging. Passord her er en felles hemmelighet, men man må være en godkjent bruker for å kunne anvende dette. Det må uansett være rutiner for å endre dette passordet ved en definert hyppighet.

Det er svært viktig at standardpassord fra leverandør ikke brukes etter at svitsjen er nåbar over nett. Dette må endres ved første gangs konfigurasjon.

6.4 Lagring av konfigurasjon

Siste versjon av konfigurasjon skal til enhvert tid lagres i nvram på svitsjen. I tillegg skal den til enhver tid være lagret på tftp-tjener. tftp-tjener bør støtte revisjonskontroll (RCS eller lignende), slik at man har et historisk arkiv over foretatte endringer.

6.5 SNMP tilgang

SNMP v2c er mest utbredt og må støttes. Denne har en lav grad av sikkerhet, derfor må sikkerhet være basert på filter som regulerer hvem som kan få SNMP-adgang til enheten.

Dette kan ofte konfigures direkte på svitsjen, hvilket er best. Alternativt reguleres det på lag3-filter på management-nettet (se 6.1).

SNMP read skal støttes. SNMP write kan vurderes. Det kan bl.a. være hensiktsmessig for å tillate portstenging fra managementapplikasjon, automatisert oppgradering eller automatisert øvrig konfigurasjon. Man må være klar over faremomentene ved å tillate SNMP write. God beskyttelse av SNMP-aksessen er her svært viktig.

6.6. Naboppdagelsesprotokoll - LLDP / CDP e.l.

Cisco har lenge hatt en proprietær løsning for nabooppdagelse; CDP, Cisco Discovery Protocol. Det foreligger nå en standard for dette, IEEE 802.1AB eller LLDP (Link Layer Discovery Protocol). Av hensyn til administrasjon bør denne funksjonaliteten være påskrudd. Det gir store fordeler ved daglig drift og kan også være nyttig informasjon for administrasjonssystemets evne til å oppdage topologi. Man kan argumentere at sluttbrukere da kan få unødvenig informasjon. Dersom svitsj forøvrig er godt sikret anses dette for å være levelig.

Dersom svitsjen støtter LLDP bør dette brukes, alternativt benyttes proprietær løsning, herunder CDP.

6.7 Syslogging

Svitsjen bør logge feilmeldinger til buffer på svitsjen og i tillegg til ekstern sysloggserver.

Syslogging må settes til å bruke nåtidsklokke, ikke klokke som refererer til tid siden siste gang svitsjen omstartet.

6.8 NTP

Svitsjen bør settes opp som NTP klient og således få pålitelig klokke. Dette er særlig viktig for presis logging. Flere NTP servere kan med fordel konfigureres for økt robusthet.

Det anbefales at primær NTP kilde bør være nærmeste kjerneruter, evt server i eget campusnett. Disse bør igjen hente klokke fra flere politelige kilder, herunder fra UNINETT.

6.9 Øvrige servertjenester på svitsjen

Ut i fra et generelt og viktig sikkerhetshensyn bør alle tjenester som ikke brukes mot svitsjen skrus av. Dette kan gjelde finger, bootp, udp echo, http (dersom det ikke brukes) m.m.

6.10 Stacking

Enkelte svitsjer kan stackes for å bygge et “virtuelt chassis” der stackingkabelen danner bakplanet. Dette kan kreve noe konfigurasjon. Svitsjer kan også stackes virtuelt og da kun av hensyn til å forenkle management, dvs at man får en ip adresse for å administrere en rekke sviitsjer. Dette krever også spesiell konfigurasjon.

6.11 Fjernkonsol, konsollogg

Mulighet for å logge på konsolporten til svitsjen er gunstig. Dette er lite realistisk for kantsvitsjer og grensvitsjer, men for kjernesvitsjer anbefales en løsning, da spesielt svitsjer som også gjør ruting. Dette kan løses ved å koble serieport til terminalserver i rommet, eller modem, evt kan det løses ved å koble via AUX-port på annen enhet.

En enda bedre løsning er å ha en konsollserver som logger alt som skjer på konsollet. Dette er igjen bare relevant for det mest kritiske utstyret.

7. Vlankonfigurasjon

7.1 Trunkoppsett (vlan tagging)

Trunkoppsett (vlan tagging) skal bruke IEEE 802.1q (ikke ISL eller andre proprietære varianter).

Trunkkonfigurasjon skal ikke basere seg på autokonfigurasjon. Autooppsett skrus av på alle porter. For trunkporter konfigureres trunkoppsett manuelt, da dette gir en større grad av kontroll. Det anses som svært viktig, ut i fra et sikkerthetsperspektiv, at en tilfeldig klientport ikke kan endres til trunk dersom klienten forsøker dette.

Det bør vurderes om man gjennom konfigurasjon skal begrense hvilke vlan som har lov til å traversere en gitt trunk. Enkelte produkter krever dette, andre ikke. Av hensyn til administrativ enkelhet er det fristende å utelate, men det bemerkes at en slik konfigurasjon gir en enda større grad av kontroll.

7.2 Administrasjonsløsning for vlan (GVRP, VTP el.l)

GVRP (GARP, Generic Attribute Registration Protocol, VLAN Registration Protocol) er en standard administrasjonsløsning for vlan over IEEE 802.1q trunker. Flere leverandører støtter denne, Cisco støtter den bare i CatOS per dato. GVRP bør foretrekkes ovenfor proprietære løsninger som Cisco sin VTP (Virual Trunking Protocol).

Det sikreste er uansett å ikke bruke slike administrasjonsløsninger og da i stedet manuelt definere nødvendige vlan på hver svitsj. Leverandørspesifikke egenskaper ved konfigurasjon kan gjøre dette mer eller mindre tungvint.

Dersom vlan administrasjonsløsning benyttes bør man sette opp denne så sikkert som mulig. Dette inkluderer å ha full kontroll på hvilke porter som er trunk, jfr 7.1, samt å benytte delt hemmelighet/passord e.l.

7.3 Vlan på ubrukte porter / vlan 1

Det anbefales av vlan 1 ikke benyttes. Det anbefales at et “dummy” vlan benyttes for ubrukte porter, slik at bruker ved feilkobling/tilfeldig innkobling ikke havner på et nett hun ikke er autorisert for.

Således skal alle ikke-trunk porter ved initiell konfigurasjon settes til en vlan verdi, enten vlanet som her skal benyttes eller “dummy” vlan.

8. Spanningtree konfigurasjon

Spanningtree skal kjøre på svitsjene slik at evt fysiske løkker, bevisste eller ubevisste blir brutt. Merk at en del svitsjer støtter flere vlan enn antall spanning tree instanser, så her må man være bevisst når man konfigurerer.

8.1 Rapid spanning tree / MSTP

Vanling spanning tree har lang kovergenstid hvilket er uheldig. Merk at dette også kan virke uheldig i scenarioer der design er løkkefri, altså i en ren trestruktur. Dersom man her ubevisst lager løkke så vil dette lamme trafikk i unødvendig lang tid dersom vanlig spanning tree er implementert. Man bør derfor vurdere løsninger som gir raskere konvergens. IEEE 802.1w, også kalt RSTP (Rapid Spanning Tree), er en standard som addresserer dette. Dersom alle svitsjene i broadcastdomenet støtter RSTP, så bør det benyttes. MSTP bør også vurderes. MSTP muliggjør multiple vlan å bli håndtert av den same spanning tree instansen. MSTP har også støtte for lastdeling og raskere konvergens da redundante veier er operative i utgangpuntet MSTP øker kompleksiteten, så man bør nøye vurdere fordelene opp i mot ulempene.

8.2 Rot i spanningtree

Rot i spanningtree bør settes på kjernesvitsj, så nært ruterporten som mulig.

Roten bør beskyttes (root guard) dersom dette er mulig.

8.3 Portfast

Sluttbrukerporter bør konfigureres med “portfast” slik at man kan få link før komplett rekalkulering av spanning tree er gjennomført.

8.4 BPDU guard

Dersom svitsjen støtter dette, bør det konfigureres, da på alle klientporter, altså porter som er satt til portfast. Hensikten er å stoppe trafikk dersom det viser seg å være en svitsj bak en klientport.

9. Trafikkegenskaper

9.1 Hastighet, dupleks, autokryssing

Alle porter bør settes til auto. Videre bør alle klienter settes til auto. Dette forenkler administrasjon og gir mindre sjanse for duplekskonflikter.

Dersom gitt klient ikke støtter automodus settes fart og dupleks manuelt. Man må da ha rutiner for å rydde opp i dette når aktuell maskin ikke lenger er bak porten.

Tilfeller av autokonfigurasjon der dupleks ender på half bør man følge særskilt med på. Dette indikerer ofte duplekskonflikt grunnet ikke-auto-oppsett i klientenden.

Noen porter støtter autokryssing, i noen tilfeller må dette eksplisitt konfigureres.

9.2 Jumboframes

Porter som støtter jumboframes bør konfigureres for dette. Jumboframes vil si at MTU økes fra 1500 byte til 9000byte noe som øker overføringskapasitet på gigabit, spesielt over avstand.

9.3 Bundling av porter (ether channel) /lastbalansering

Det kan i gitte tilfeller være nyttig å doble eller flerdoble kapasiteten på en link ved å samle multiple fast ethernet eller gigabit ethernet porter. Cisco har en proprietær løsning, etherchannel. En standard for dette er IEEE 803.ad (link aggregation).

9.4 Trafikkadministrasjon / tjenestekvalitet

Ved behov kan tjenestekvalitetsfunksjoner konfigureres, herunder støtte for ulike tjenesteklasser, policing og shaping.

9.5 Strøm over ethernet

Dersom svitsjeporten skal kobles mot IP-telefon, basestasjon eller annen enhet som baserer seg på strømforsyning over nettverkskabelen, må dette konfigureres. Motsatt er det et poeng å skru dette av der slik bruk ikke er ønsket.

9.6 Beskyttelse av kontrollplanet

For å beskyttes CPUen (mest relevant på kjernesvitsjer) bør tiltak gjøres for å styre og sikre ressursbruken og tilgangen på denne.

9.7 Fysisk link monitorering

Dersom svitsjen støtter mekanismer for å monitorere den fysiske kabelen en gitt port er tilkoblet, så bør slike funskjoner skrus på.

10.Multicast snooping

Svitsjen må støtte for både IGMP snooping versjon 2 og 3. Versjon 3 er viktig for å håndtere SSM (single source multicast), noe som blir stadig mer utbredt. IGMP snopping bør være påskrudd på alle porter.

11. Sikkerhetsfunksjoner

11.1 Port security

For bedre kontroll med adgangen til en gitt svitsjeport kan port security funksjonaliteten benyttes. Denne tillater kun et gitt antall maskiner (macadresser) bak en gitt port. Konfigurasjon bør være slik at tillatte maskiner fortsatt får nett etter at evt tilleggsmaskiner er koblet til. Kun tilleggsmaskinene sperres. Funksjonaliteten anbefales spesielt mot skrivere i åpne areal slik at disse svitsjeportene ikke blir tatt/misbrukt.

Alle klientporter bør som et minimum konfigureres med en høy verdi her som overgår praktisk bruk. Dette for å hindre flooding av cam-tabellen. Merk at nettverksporter (porter mot annet nettutstyr) ikke må ha en slik konfigurasjon.

11.2 IEEE 802.1X

IEEE 802.1X gir en bedre kontroll med hvem som kobler seg til nettverket. Ulempen er at dette krever mer av klienten ved at den må ha konfigurert støtte. Videre må brukeren logge seg på ved hver tilkobling til nettverket.

IEEE 802.1X anbefales spesielt for det trådløse nettet, men kan med fordel også anvendes i fastnettet. Man kan velge å implementere det for enkelte brukergrupper, som f.eks. på studentby.

11.3 Traffic storm control

Man bør konfigurere porten slik at broadcast trafikk stoppes når mengden er over en definert uakseptabel terskel (f.eks. 10 %).

11.4 DHCP snooping

På kantsvitsjer bør DHCP snooping være konfigurert (gitt at svitsjen støtter dette). Hensikten er at malkonfigurerte klienter ikke kan opptre som DHCP-server og da dele ut falske IP-adresser til øvrige klienter. Dette har blitt et problem og unngås ved at DHCP snooping og dertil blokkering er implementert. Det er viktig at funksjonaliteten kun er satt på klientporter, ikke trunk/nettverksporter.

11.5 IP source guard / dynamic IP lockdown

Dette er en mekanisme som hindrer forfalskning av IP-adresser fra klientmaskinen. Kun den IP-adressen klienten har fått med DHCP eller evt en statisk registert adresse kan benyttes bak porten.

Dersom svitsjen støtter dette, anbefales det påskrudd på klientporter. Funksjonaliteten kan kreve at DHCP snooping også er tatt i bruk.

11.6 Dynamic arp inspection

Denne mekanismen beskytter oss mot man-in-the-midle som sender falske ARP pakker for å opptre som ruter. Dersom svitsjen vet hvilke IP-adresser som skal høre hjemme bak hvilke porter kan den effektivt blokkere forsøk på å gjennom ARP utgi seg for å være noen andre. Funksjonaliteten bør absolutt vurderes, den kan imidlertid kreve at DHCP snooping også er tatt i bruk.

11.7 Port unicast og multicast flood blocking

Ved å sende pakker til nye, falske macadresser vil disse alltid gå ut på alle porter på en svitsj. Et regissert angrep kan således degradere ytelsen for hele miljøet bak svitsjen. Dette kan forhindres ved å konfigurere denne funksjonaliteten. Dersom svitsjen støtter egenskapen, bør man vurdere å ta i bruk dette på alle klientporter.

11.8 Mac address notification

Dette er en mekanisme som sender SNMP trap når en ny macadresse er oppdaget eller eldet ut på svitsjen. Dersom SNMP trap mottak tolker dette kan man få et nøyaktig bilde av klientmaskinene i nettverket. Dette kan også kartlegged ved å regelmessig SNMP polle svitsjene, noe som dog gir et litt grovere bildet. Dersom svitsjen støtter dette, bør funksjonaliteten benyttes.

12. Nyttige funksjoner ved daglig drift

12.1 Portspeiling

Portspeiling er nyttig å sette opp ved behov. Portspeilking speiler all trafikk fra en port ut på en annen port. På lyttende port kan man kjøre en sniffer, tcpdump eller tilsvarende og analysere trafikken.

12.2 Sperre en mac adresse

En macadresse kan effektivt sperres ved å konfigurere dette i svitsjen. Alternativ tilnærming er å bruke et nettadministrasjonssystem som har støtte for maskinsperrnig. Det er også mulig å sperre en IP-adresse med lag3 filter.

12.3 Statisk binding av mac adresse til port

Samme funksjon kan oppnås med port security, men man kan altså definere statiske brotabellinslag dersom man ønsker dette.

13. Intellektuelt eierskap

UNINETT står ansvarlig for innholdet i dette dokument. Arbeidet er utført som et samarbeidsprosjekt i UH-sektoren. Dokumentet ble endelig godkjent etter en åpen høringsperiode på 4 uker.

14. Forfatterenes adresse

Børge Brunes
IT-avdelingen
Universitetet i Tromsø
9037 Tromsø
Telefon: 77644113
Epost: borge.brunes@cc.uit.no

Vidar Faltinsen
UNINETT
Abels gt 5 - Teknobyen
7465 Trondheim
Norway
Telefon: 735 57825
Epost : faltin@uninett.no

Einar Lillebrygfjeld
UNINETT
Abels gt 5 - Teknobyen
7465 Trondheim
Norway
Telefon: 735 57942
Epost : Einar.Lillebrygfjeld@uninett.no

Knut-Helge Vindheim
IT-seksjonen (ITEA)
NTNU
7491 Trondheim
Telefon: 73597610
Epost: knut-helge.vindheim@ntnu.no

Ved spørsmål omkring denne eller andre UFSer – kontakt campus@uninett.no
Andre UFSer er tilgjengelige på www.uninett.no/ufs