BACHELOROPPGAVE:

SIKKERHET I VIRTUELLE LAN – VLAN

FORFATTERE:

ERIK BRENDEN
LARS IHLER
MAGNUS LARSEN MUSTORP
ROBERT RØSTEN

DATO:

20.05.2009

SAMMENDRAG AV BACHELOROPPGAVEN

Tittel:	Sikkerhet i Virtuelle Lan - VLAN	Nr. : 8
		Dato : 20.05.2009
Deltakere:	Erik Brenden	
	Lars Ihler	
	Magnus Larsen Mustorp	
	Robert Røsten	
Veiledere:	Patrick Bours	
Oppdragsgiver:	Kongsberg Maritime AS	
Kontaktperson:	Kai Gustav Palm	
Stikkord	VLAN, sikkerhet, testing, guide	

Antall sider: 149	Antall vedlegg: 6	Tilgjengelighet: Åpen

Kort beskrivelse av bacheloroppgaven:

Grunnet et økende behov for å dele store nettverk inn i flere mindre nettverk, har VLAN blitt en meget aktuell teknologi, særlig i mellomstore til store virksomheter. Dagens teknologi som stadig utvikler seg i retning av mer mobile brukere - samtidig som sikkerhet kanskje er viktigere enn noen gang, har bidratt til å gjøre VLAN mer utbredt. I tillegg har virksomheter blitt oppmerksomme på alle fordelene VLAN teknologien medbringer.

VLAN tar for seg flere av utfordingene i nettverk ved å logisk, i stedet for fysisk, dele opp / separere nettverk. Dermed er man ikke lenger avhengig det fysiske grensesnittet, og et LAN kan bestå av arbeidsstasjoner som ikke lenger er begrenset til et lokalt område.

Oppgaven tar for seg VLAN som en sikkerhetsbarriere mellom ”sikre” og ”usikre” nettverk. Vi har kartlagt og dokumentert de mest kjente angrep mot nettverk generelt og VLAN teknoligen spesielt. De mest relevante angrepene mot VLAN teknologien er gjennomført i kontrollerte former mot et ferdig oppsatt testmiljø.

Med kombinasjonen av praktisk utførelse av angrep og teoretisk dokumentasjonen, gir prosjektet leseren et godt innblikk i emnet VLAN. I tillegg bidrar oppgaven med å bevisstgjøre leseren på hvilke muligheter man har ved å implementerer VLAN i sitt/sine nettverk.

SUMMARY OF THE BACHELOR PROJECT

Title:	Security in Virtuell Lan - VLAN	Nr. : 8
		Date : 20.05.2009
Participants:	Erik Brenden	
	Lars Ihler	
	Magnus Larsen Mustorp	
	Robert Røsten	
Supervisor:	Patrick Bours	
Employer:	Kongsberg Maritime AS	
Contact person:	Kai Gustav Palm	
Keywords	VLAN, security, testing, guide	

Pages: 149	Number of appendices: 6	Availability: Open

A short descrition of the bachelor project:

Because of a growing need to split large networks into smaller networks, VLAN has become a present technology, especially in middle to large sized enterprises. Todays technology, which develops in the direction of more mobile users – at the same time as security is maybe more important than ever, has made VLAN more widespread. In addition, enterprises has become obsequious to all of the advantages the VLAN technology bringes.

VLAN deals with several challenges in network by separating logically, instead of physical. Thereby, you are no longer dependent by the physical topology, and a LAN can consist of workstations which are not in the same local area.

The project takes on the VLAN technology as a securitybarrier between “secure” “and unsecure” network. We have mapped and documendet the most known network and VLAN attacks. The most adequate attacks has been tested in contolled forms in a ready testenvironment.

With the combination of practical execution of attacks and theoretically documentation, the project gives the reader a solid insight in the subject VLAN. In addition the project will make the reader more aware of the possibilities you have by implementing VLAN in a network.

Forord

Allerede før listen med aktuelle bachelor oppgaver ble lagt ut, var vi veldige klare på at vi ønsket å ta for oss en nettverksrelatert oppgave. Vi så dermed ganske tidlig hvilken oppgave som var aktuell for vår del. Ingen av gruppemedlemmene hadde noen spesiell erfaring med VLAN fra tidligere, men i stedet for at dette skulle bli noen hindring for prosjektet, valgte vi heller å vinkle dette til å være en ekstra utfordring, med muligheten til å lære oss en forholdsvis ny, men meget relevant og aktuell teknologi i arbeidslivet.

Målet var ikke bare å øke vår egen kompetanse på området, men også å bidra til at vår oppdragsgiver, Kongsberg Maritime AS, kunne bruke oppgaven til å ta valget om VLAN holder som en sikkerhetsbarriere mellom ulike nettverk, basert på denne rapporten.

Prosjektet, og arbeidet rundt dette, har vært veldig lærerikt. Vi føler vi sitter igjen med ett godt faglig utbytte og vi har fått ett innblikk i hvordan større prosjekter gjennomføres, med alt det innebærer, blant annet hvilke problemer og tilbakefall som kan oppstå underveis.

Vi ønsker å rette en stor takk til vår veileder Patrick Bours, som har vært til stor hjelp under hele prosjektet. Han har alltid vært tilgjengelig, og har kommet med nyttige råd og tilbakemeldinger underveis.

I tillegg vil vi takke vår oppdragsgiver, ved Kai Gustav Palm og Morten Rugland Nilsen, for omvisning på Kongsberg Maritime og ikke minst for utstyret vi har fått låne i forbindelse med prosjektet.

Takk også til vår HP nettverkskonsulent, Arnljot Seem, for hjulpet oss med spørsmål knyttet til HP Procurve switchene og VLAN teknologien, og takk til biblioteket som har skaffet til veie aktuell literatur til prosjektet.

Gjøvik 19.05.2009

Erik Brenden	Lars Ihler
Magnus Larsen Mustorp	Robert Røsten

Innhold

Figurer

Forkortelser

ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BPDU	Bridge Protocol Data Unit
CAM	Content Addressable Memory
CDP	Cisco Discovery Protocol
CFI	Canonical Format Indicator
CLI	Command-Line Interface
CoS	Class of Service
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DTP	Dynamic Trunking Protocol
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
GARP	Generic Attribute Registration Protocol
Gbps	Gigabit per second
GUI	Graphical User Interface
GVRP	GARP VLAN Registration Protocol
HiG	Høgskolen i Gjøvik

HP	Hewlett-Packard
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IMT	Informatikk og medieteknikk
IP	Internet Protocol
ISL	Inter-Switch Link (Cisco)
ITIL	Information Technology Infrastructure Library
L2	Layer 2
LAN	Local Area Network
LANe	LAN emulator
LLDP	Link Layer Discovery Protocol
MAC	Media Access Controll
MITM	Man in the Middle
MSTP	Multiple Spanning Tree Protocol
OSI	Open System Interconnect
PCP	Priority Code Point
QoS	Quality of Service
ROM	Read Only Memory
RSTP	Rapid Spanning Tree Protocol

SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
TC	Topology Change
TCN-BPDU	TC Notification BPDU
ToS	Type of Service
TP	Twisted Pair
TPID	Tag Protocol Identifier
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VID	VLAN Identifier
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WLAN	Wireless Local Area Network
XML	eXtensible Markup Language

Kapittel 1

Innledning

VLAN er en teknologi som brukes til å segmentere et fysisk nettverk til flere logiske nettverk. Det brukes ofte der det er hensiktsmessig at ulike avdelinger i en virksomhet er separert, for eksempel der det er ulike krav til sikkerhet. VLAN er en grunnleggende funksjon i administrerbare switcher. En fysisk switch kan deles i flere logiske nettverk via VLAN teknologien.

Den offisielle betegnelsen på VLAN standarden er IEEE 802.1Q (også kjent som VLAN tagging). Standarden ble utviklet som følge av problemer med oppsplitting av store nettverk til mindre nett. Med VLAN hadde man derimot muligheten til å dele opp nettverk på den samme fysiske linken (switch) uten lekkasje av informasjon mellom de forskjellige nettene. Nettene ble mer håndterbare, broadcast- og multicast-trafikk brukte nå ikke mer båndbredde enn nødvendig.

Vår oppdragsgiver; Kongsberg Maritime leverer produkter og systemer for posisjonering, navigasjon og automasjon til handelsskip og offshoreinstallasjoner, samt produkter og systemer for sjøbunnskartlegging og overvåkning, og til fiskefartøyer og fiskeriforskning. Forretningsområdet er blant markedslederne innen disse områdene. Land med stor offshore-virksomhet og verftsindustri er viktige markeder[1].

1.1 Avgrensninger

Prosjektets hovedoppgave er å levere en grundig risikoanalyse til oppdragsgiver. Denne skal ta for seg VLAN som en sikkerhetsbarriere mellom ulike nettverk. I risikoanalysen vil vi benytte HP ProCurve switcher til testing og angrep. Dette valget er gjort på grunnlag av at det er denne type switcher vi har fått låne av oppdragsgiver, da de benytter disse switchene i sine

nettverk. HP ProCurve er dermed våres referanseprodukt. Dette vil vi gi en mer grundig vurdering av nettopp disse switchene, enn om vi også skulle tatt for oss switcher fra andre leverandører. Vi vil allikevel vinkle rapporten slik at andre som ikke bruker ProCurve også kan dra nytte av deler av denne.

Vi har fokusert på angrep som kun går mot VLANteknologien i dette prosjektet, men vi har også tatt for oss generelle nettverksangrep.

1.2 Oppgavebeskrivelse

VLAN brukes til å dele et fysisk nettverk inn i flere logiske nettverk. Dette gjøres gjerne for å skille ulike avdelinger med forskjellig sikkerhetsnivå i en bedrift. Oppdragsgiver, Kongsberg Maritime AS, "sliter" med en sikkerhetspolicy som sier at VLAN ikke holder som barriere mellom "sikre" og "usikre" nettverk. Dette har sin bakgrunn i en strukturert (men udokumentert) risikoanalyse som ble gjort for anslagsvis 5 år siden. En av gruppens hovedoppgaver blir derfor å levere en dokumentert og grundig risikoanalyse av sikkerheten i VLAN til oppdragsgiver.

I forbindelse med diverse implementeringer ser oppdragsgiver at det ville vårt svært praktisk (og kostnadseffektivt) å kunne bruke VLAN for å segmentere nettverkstrafikk - også fra et sikkerhetsperspektiv. Kvaliteten på arbeidet er helt vesentlig da oppdragsgiver må stå inne for eventuelle valg basert på konklusjoner i dette arbeidet (jf. eventuelle endringer i sikkerhetspolicy).

Kongsberg Maritime har 40 kontorer over hele verden der de benytter seg av HP ProCurve switcher. Det vil derfor bli fokusert på disse switchene, og ikke andre produkter.

Det er i dag mye mer eller mindre kvalifisert synsing på området (særlig VLAN som sikkerhetsbarriere). Oppdragsgiver savner en mer grundig drøfting/ belysning av dette. Vi har derfor kommet fram til følgende problemstillinger som skal belyses:

- Hva er VLAN og ulike anvendelser for dette?
- Angrep på VLAN teknologien.
  - Hvilke angrep finnes?
  - Hvordan blir disse angrepene utført?
  - Eventuelle sikringstiltak som gjør risikoen lavere.
- Implementering av switchene (HP ProCurve).

  - Sette opp best mulig konfigurasjon på HP ProCurve switchene, for så å teste angrep/sikkerhet mot VLAN.

- Vurdere VLAN som sikkerhetsmekanisme.
  - Holder VLAN som sikkerhetsmekanisme for å skille ulike nettverk?
  - Definere ulike faktorer som påvirker VLAN som sikkerhetsmekanisme (ulike implementasjoner, menneskelige feil andre ting?).
  - Hvilke sikkerhetsmekanismer som kan bli implementert og hvilke situasjoner disse metodene egner seg best i?
- Det finnes ulike miljøer/situasjoner hvor VLAN er egnet - noen karakteristika?

1.3 Målgruppe

Målgruppen for dette prosjektet vil hovedsakelig våre vår oppdragsgiver, Kongsberg Maritime AS, som skal dra nytte av oppgaven. Sensor og veileder vil også være en målgruppe, da de skal vurdere oppgaven. I tillegg vil oppgaven være behjelpelig for andre bedrifter som planlegger å dele opp nettverket sitt i virtuelle LAN.

1.4 Prosjektmål

Prosjektmål består av effektmål, resultatmål og læringsmål. Effektmål forteller hva oppdragsgiver ønsker med oppgaven, resultatmål sier hva gruppen skal levere og hva som er gruppens ambisjoner med prosjektet, mens læringsmål er hva gruppen Ønsker å få ut av oppgaven.

1.4.1 Effektmål

Effektmålet med denne oppgaven er å finne ut om VLAN holder som en barriere mellom sikre og usikre nettverk. Det vil være både svært praktisk og kostnadseffektivt for Kongsberg Maritime å kunne bruke VLAN for å segmentere nettverkstrafikk, også fra et sikkerhetsperspektiv.

1.4.2 Resultatmål

Gruppens resultatmål er å analysere/vurdere VLAN som en sikkerhetsmekanisme for å finne ut hvor dette er tilstrekkelig, samt hvor og hvordan

det kan brukes. Målet er at arbeidet vi legger ned skal være et godt nok grunnlag til at Kongsberg Maritime kan ta en avgjørelse basert på våres arbeid.

1.4.3 Læringsmål

Få innsikt og kunnskap om VLAN og konfigurering av switcher. I tillegg til å lære oss arbeidsprosesser og rutiner knyttet til arbeid i større prosjekter.

1.5 Rammer

Underveis i prosjektet vil det være ulike frister vi er nødt til å overholde. På forprosjektet og prosjektavtalen med arbeidsgiver, er det en frist for levering 30.januar. Selve prosjektrapporten skal leveres til kopisentralen innen den 20.mai. Det skal så videreleveres til studenttorget 25.mai. Ved slutten av prosjektet, lages en plakat som skal brukes til å vise arbeidet vi har utført i prosjektperioden og den skal leveres til laminering 28. Mai, så videre til studenttorget 2.juni.

Når prosjektet er ferdig skal det fremøres til andre studenter og ansatte ved HiG. Fremføringen skal finne sted 4.juni. Fristene er satt av IMT. I tillegg er det stilt krav til dokumentasjon og statusmøter underveis i prosjektet.

1.6 Prosjektorganisering

1.6.1 Ansvarsforhold

Erik Brenden er gruppens prosjektleder. Robert Røsten har ansvaret for sammensetting og koordinering av dokumentasjon. Magnus Larsen Mustorp er gruppens sekretær, mens Lars Ihler er testmiljø¸ ansvarlig. Disse rollene følger gruppen gjennom hele prosjektet.

Siden prosjektet strekker seg over en lengre periode har vi i også fordelt inn i mindre roller. På teoridelen skal Erik og Robert ha ansvar for VLAN teknologien, mens Lars og Magnus skal se på angrep og sikkerhetsmekanismer. Når det gjelder den praktiske delen, blander vi de som har jobbet med sikkerhetsdelen sammen med de som har jobbet med teknologidelen. Da får hver av gruppene den nødvendige kompetansen de trenger for å utføre sine respektable oppgaver. Gruppene vil så ta for seg hver sine angrep. Når det gjelder implementering og konfigurering av switchene, vil alle gruppemedlemmene delta aktivt på dette.

1.6.2 Regler og rutiner

- Arbeidsdager fra kl.09:00 - kl.15:00. Unntaket er mandager da vi har forelesning fra 12:30 og ut arbeidsdagen. Fredager er det ikke møteplikt, men det skal fortsatt arbeides med oppgaven.
- Ved fravær skal det gis beskjed til prosjektleder. Fraværet skal begrunnes. Hvis prosjektleder er borte gir han beskjed til et annet gruppemedlem. Selv ved fravær skal gruppemedlemmet være tilgjengelig for de andre gruppemedlemmer, om viktig informasjon må utveksles.
- Alle på gruppa skriver logg over eget arbeid hver dag. Her skal ca timeantall og en grov oversikt over dagens arbeidsoppgaver føres. All logg skal legges på gruppens fellesområde.
- Uenigheter skal i første omgang diskuteres internt i gruppen, og avgjøres ved saklig diskusjon. Hvis vi derimot ikke kommer til noen løsning vil uenigheten bli avgjort i samarbeid med veileder.
- Alt arbeid vil hovedsakelig foregå på grupperom A113. Utstyr vi får tildelt av HiG og oppdragsgiver som er knyttet til oppgaven, skal stå på grupperommet. Slik at testing og konfigurering vil skje her.
- Prosjektdokumentasjon skal lages ut ifra definerte maler. Disse malene er tilgjengelig på gruppens fellesområde.

1.6.3 Øvrige roller og bemanning

Kongsberg Maritime AS er oppdragsgiver ved henholdsvis Kai Gustav Palm som kontaktperson, mens akademisk veileder er Patrick Bours, fra avdelingen IMT.

Kapittel 2

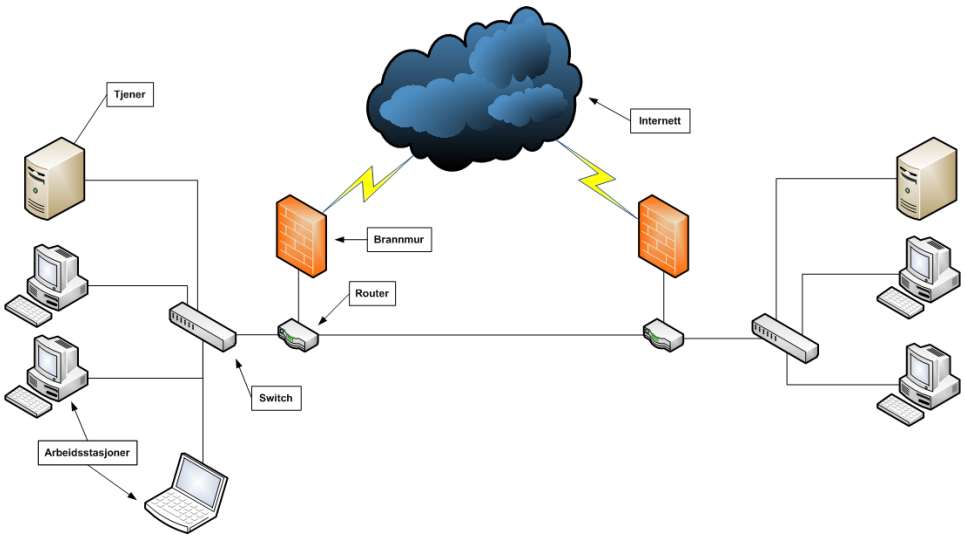
VLAN teknologien

For å få plassert terminologien VLAN i en nettverksstruktur skal vi først ta for oss et par helt sentrale begreper innenfor området nettverk - og med nettverk snakker vi her om datanettverk. Et datanettverk er et system av datamaskiner og periferiutstyr, knyttet sammen ved hjelp av intern kabling og/eller linjesamband, oppkoblingsutstyr samt programvare beregnet på å muliggjøre kommunikasjon mellom tilkoblede enheter[2]. Denne kommunikasjonen er overføring av informasjon i digital form mellom datamaskiner. For at kommunikasjonen mellom ulike digitale systemer skal fungere, benyttes protokoller[3] som definerer regler for hvordan kommunikasjonen skal foregå[4].

For å koble sammen enhetene i ett nettverk, samt få de til å kommunisere på best mulig måte, er det vanlig å benytte seg av koblingspunkter. Med koblingspunkter tenker vi her på nettverkskomponenter som switcher og (trådløse)routere, som er de mest brukte i dagens nettverk. Forskjellen på disse er at en router brukes til å binde sammen forskjellige nettverk, samt sørge for å finne den mest velegnede veien å sende informasjonen i nettverket på. En switch derimot, brukes til å binde sammen ett nettverk. Den dirigerer pakker direkte til sitt bestemmelsessted, basert på mottakeradressen til pakken. Routere og switcher befinner seg på forskjellige lag i OSI modellen, noe vi kommer tilbake til i del 2.1.

En bedrift kan bestå av flere LAN. Et LAN er en samling av arbeidsstasjoner og tjenere, kabler, switcher, routere og annet nettverksutstyr, konfigurert til å supportere kommunikasjon innenfor et lokalt område. Bedrifter bruker LAN til å supportere en mengde brukere og nettverksapplikasjoner. De fleste bedrifter ønsker å dele opp nettverkene sine etter avdelinger, prosjekter, applikasjoner, eller lignende. Et eksempel på dette er HiG som har delt inn ansatte og studenter i hvert sine nettverk.

Det vanlige er at hver bruker i nettverket er tilknyttet ett fysisk LAN. Settet, eller samlingen av enheter tilknyttet et gitt LAN er definert av begrensningene på utstyret, for eksempel nummeret av porter på en switch, og/eller tilkoblingsmulighetene konfigurert av nettverksadministrator.



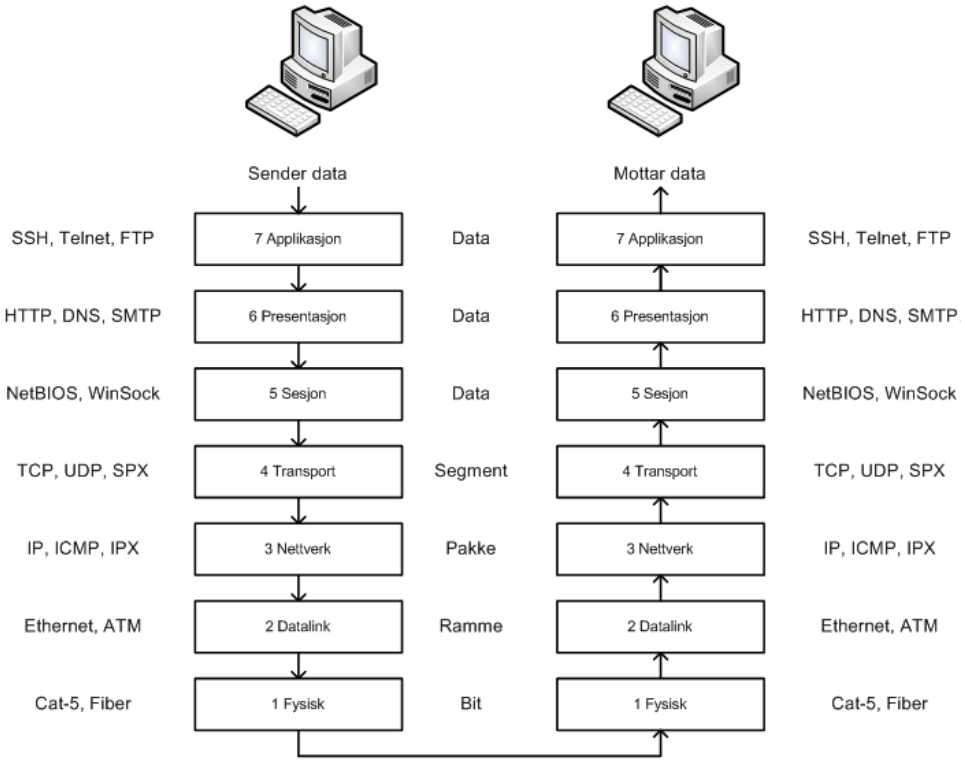
Figur 2.1: *To lokale nettverk*

Så snart man har installert og konfigurert ett LAN, kan man ikke endre på LAN-et's konfigurasjon, med mindre du fysisk endrer på tilkoblinger, altså patcher om. Det er her VLAN kommer inn i bildet. VLAN teknologien tillater deg å separere logisk tilkobling fra fysisk tilkobling, noe du ikke har muligheten til ved LAN, der fysisk tilkobling er den samme som den logiske tilkoblingen. Med VLAN er brukerne fortsatt tilkoblet det samme utstyret - med den samme forbindelsen. Men man er ikke lenger begrenset til den fysiske topologien. I VLAN kan man konfigurere porten på en switch til å tilhøre ett annet LAN. LAN-et er med det virtuelt, da samlingen av arbeidsstasjoner og tjenere er tilknyttet samme fysiske LAN, men faktisk ikke befinner seg innenfor det samme lokale området. For å få til dette må switchene støtte VLAN. De kan da konfigureres til å passe best mulig inn i brukermiljøet.

Grunnet økende behov for å dele store nettverk inn i flere mindre nettverk, har VLAN blitt en meget aktuell teknologi, særlig i større virksomheter hvor det gjerne er flere avdelinger som skal deles opp/skilles ut. VLAN er ingen ny teknologi, men det er først de siste årene den virkelig har blitt utbredt. Før vi dykker dypere inn i VLAN teknologien, skal vi se nærmere på OSI modellen, som vi mener vil gi en grunnleggende forståelse for hvordan nettverksløsninger er bygd opp og hvordan de fungerer.

2.1 OSI modellen

For å bli fortrolig med nettverk er det viktig å ha kjennskap til OSI modellen. OSI modellen er en referansemodell for oppbygning av nettverkskommunikasjon. Den viser og beskriver hvordan kommunikasjon mellom to enheter foregår i ett nettverk, altså hvordan data overføres disse i mellom. Den er delt inn i syv forskjellige lag, der hvert lag har bestemte arbeidsoppgaver. De fire første lagene beskriver selve nettverket og transporten av dataene, mens de tre siste lagene beskriver tjenester og programvare i nettverket. (For mer detaljert beskrivelse av OSI modellen, se ref.[5].)



Figur 2.2: *Lagene på OSI modellen*

På figuren ovenfor ser vi hvordan data fraktes gjennom de forskjellige lagene i OSI modellen, fra det sendes til det mottas. Vi skal nå ta for oss disse lagene, deres funksjoner, tjenester og protokoller. Alle lagene bygger på hverandre, og selv om de er adskilte, kommuniserer de med hverandre gjennom grensesnittene mellom lagene.

2.1.1 Lag 1, Fysiske laget

Dette laget er den fysiske koblingen mellom enhetene i nettverket. Laget har som oppgave å sende og motta rå databits over den fysiske forbindelsen. Det fysiske laget omgjør datastrømmen fra datalink laget til et passende format og sender det ut på nettverket. På et tråd-nettverk blir hver bit omgjort til et elektronisk signal, mens bitene på fiberoptiske nettverk gjøres om til et lyssignal.

2.1.2 Lag 2, Datalink laget

Datalink laget pakker de rå bit-ene inn i datarammer og sørger for feilfri overføring mellom datamaskiner (en dataramme (frame) er en elektronisk konvolutt av informasjon som inkluderer pakken og annen informasjon som legges til av de sju lagene i OSI-modellen). I disse pakkene blir det i tillegg til dataene, lagret adresse til avsender og mottaker. Ved hjelp av dette, kan vi definere hvem som skal kunne motta dataene vi sender. Dette gjøres ved hjelp av MAC-adressen til enhetene.

Andre veien, altså fra datalink laget til det fysiske laget, sendes data som en strøm av bits, altså nullere og enere (1010011). Switcher befinner seg på dette laget.

2.1.3 Lag 3, Nettverkslaget

Nettverkslaget fastslår den fysiske stien for dataene som skal sendes, basert på nettverket's betingelser, prioriteten for tjenesten, samt andre faktorer. Dette er det eneste laget som benytter "logical networking" og kan flytte pakker mellom forskjellige nettverk. Man finner routere på dette laget.

Mens datalink laget har mulighet for adressering innen ett nettverk, har nettverkslaget mulighet for å adressere pakker for sending mellom flere og ulike nettverk. Nettverkslaget bruker routing-algoritmer[6] for å finne korteste sti mellom kilde og destinasjon i nettverket.

2.1.4 Lag 4, Transportlaget

Transportlaget sørger for at pakker blir levert i den tilstanden de blir sendt. Det vil si at de ikke er forandret, tapt eller duplisert. Når dette laget skal sende pakker i nettverket er det ansvarlig for å bryte ned store pakker til mindre pakker, og motsatt når laget mottar pakker, da gjenoppbygger det større pakker ut ifra de mindre.

Dataen på dette laget kalles for segmenter, der hvert segment inneholder ett segmentnummer som brukes for å identifisere rekkefølgen på segmentpakkene fra avsender.

Data kan ta forskjellige veier i ett nettverk og det er ikke sikkert de kommer fram i den samme rekkefølgen de ble sendt i, det er derfor viktig at det blir kontrollert, dette kalles for sekvenskontroll.

2.1.5 Lag 5, Sesjonslaget

Dette laget styrer forbindelse mellom applikasjoner og lar brukere opprette en forbindelse (sesjon). Laget sjekker at sikkerheten er så god som den kan bli for at forbindelsen kan starte. Når kommunikasjonen er i gang, er det sesjonslaget som administrerer dialogen.

2.1.6 Lag 6, Presentasjonslaget

Dersom to maskiner som kommuniserer sammen har forskjellig dataformat, kan presentasjonslaget konvertere begge formatene til ett felles format. Altså sørges det her for at dataen presenteres riktig på det utstyret som det kommuniseres på. Det er også på dette laget at komprimering og dekomprimering foregår, samt kryptering og dekryptering.

2.1.7 Lag 7, Applikasjonslaget

Applikasjonslaget er det øverste laget. Det oppretter forbindelsen mellom applikasjoner og nettverkstjenester samtidig som det tilpasser brukerens programmer til nettverket. Applikasjonslaget gjør at programvaren kan overføre filer, sende e-post og ellers utføre andre tjenester over nettverket. Laget sørger for en program-til-program-kommunikasjon.

2.2 VLAN konseptet

Som nevnt tidligere er VLAN et switchet nettverk, som er logisk- i stedet for fysisk segmentert. Ved å bruke VLAN teknologien kan man ha flere LAN på én switch, i motsetning til fysisk oppdeling hvor man kun kan ha ett LAN på hver switch. Med VLAN kan man også ha ett VLAN over flere switcher. Har du for eksempel arbeidsstasjoner og servere knyttet til ett prosjekt, kan disse være koblet på samme VLAN, uavhengig av fysisk eller geografisk plassering.

Fordi VLAN er en logisk enhet, vil all konfigurasjon/rekonfigurasjon gjøres ved hjelp av software, i motsetning til å måtte fysisk koble til/fra kabler (patching) og/eller flytting av enheter. Men for å få konfigurert VLAN på en switch, må switchen være konfigurerbar. Det vil si at switchen må inneholde hardware som gjør det mulig å bruke VLAN. Om switchen ikke har denne hardwaren innebygget, vil det ikke være mulig å bruke VLAN på den.

Man kan si at VLAN er ett broadcast domene som eksisterer innenfor ett definert sett av switcher. VLAN definerer hvor langt en broadcast pakke kan gå. Antatt at routing ikke er involvert, vil trafikk som kommer inn på en fysisk LAN-port, som igjen er konfigurert til å være medlem av ett VLAN, kun gå til andre medlemmer av dette VLAN-et. VLAN tilbyr dermed en lett og praktisk måte å implementere nettverkssegmentering på lag 2 av OSI modellen.

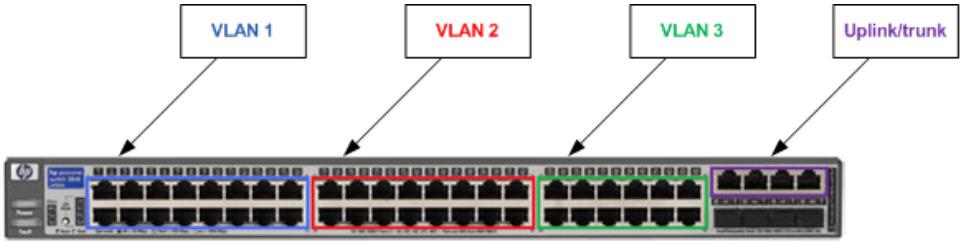
2.3 Hvorfor benytte seg av VLAN?

De aller fleste nettverk består idag av minst én switch. Switchen brukes for å koble sammen datamaskiner, noe som gir en rask og stabil måte for datamaskinene å kommunisere på.

VLAN tillater logiske nettverkstopologier å overlappe fysisk switchet infrastruktur, slik at en vilkårlig gruppe med LAN porter kan kombineres i en egen gruppe, altså eget nettverk. Teknologien segmenterer logisk nettverkene i separate broadcast domener hvor pakkene er switchet mellom portene som er konfigurert til å høre til på samme VLAN. Dermed unngår man å bruke opp unødvendig båndbredde i nettverket, da pakker fra et VLAN ikke går ut til andre enn de som tilhører dette VLANet, i motsetning til tradisjonelle bridgede og switchede nettverk hvor pakkene ofte videresendes til nettverkskomponenter som ikke har bruk for disse pakkene.

Vi kan ta ett eksempel på dette: Har du flere datamaskiner tilkoblet samme switch, vil alle maskinene kunne kommunisere med hverandre, siden de alle er på samme broadcast domene. Hvis én maskin sender ut ett broadcast, vil de resterende motta dette. I ett lite nettverk vil ikke dette være et problem, men i større nettverk vil mangfoldige broadcast etter hvert bli ett problem ettersom nettverket kan bli overfylt av broadcast pakker som sluker båndbredden. I stedet for å bygge ut nettverket med flere switcher og routere for å få delt opp nettverket, gir VLAN deg muligheten til å bruke færre switcher, ved logisk å dele opp i flere nettverk på én switch, altså deles det opp i flere broadcast domener.

Hvert VLAN som blir laget på switchen vil være et separert nettverk. Det betyr at separate broadcast domener blir laget for hvert VLAN. Nettverks



Figur 2.3: *Eksempel på inndeling av tre VLAN på én og samme switch (HP Procurve 2848)*

broadcaster er automatisk filtrert bort fra alle porter på switchen som ikke er medlem av samme VLAN. Som vi kan se utifra figuren over vil dette si at om du har tre VLAN på en switch, vil datamaskinene som sender ut broadcast domene kun sende det til de andre maskinene i samme VLAN. Dette er en av grunnene til at VLAN er blitt mer og mer vanlig i dagens store nettverk, siden de isolerer og separerer nettverkssegmenter.

Men, dette er ikke de eneste fordelene man har ved å implementere VLAN, i tillegg får man:

- Sikkerhet
  VLAN forbedrer sikkerheten ved å isolere grupper. For eksempel kan høy-sikkerhet brukere grupperes i ett VLAN, slik at brukere utenfor dette VLAN-et ikke kan kommunisere med dem. Enkelte virksomheter velger å ikke gå til innkjøp av nye switcher for å dele opp nettverk om de har nok porter på switchen(e) som er i bruk. Dette medfører at alle noder tilkoblet den samme switchen kan se hverandre. Det er en lite idéell situasjon dersom man har servere tilknyttet switchen, eller andre maskiner som krever ulike sikkerhetsnivåer.

- Ytelse og kapasitet
  Logisk gruppering av brukere tillater en brukergruppe å utnytte full bruk av ett nettverkssystem tildelt ett VLAN som inneholder kun denne brukergruppen og dens servere. Denne gruppens arbeid vil ikke ramme andre brukere. VLAN konfigurasjon forbedrer generell nettverkytelse ved å ikke forsinke andre brukere som deler nettverket.

  Arbeidsstasjoner og tjenere kan enkelt flyttes til forskjellige VLAN bare ved å endre tilhørighetsprofilen på switchen. Dette øker kapasiteten i nettverket.

- Kommunikasjon mellom VLAN
  Kommunikasjon mellom VLAN gjøres ved hjelp av routing, slik at de

tradisjonelle sikkerhets- og filtreringsfunksjonene til en router og en firewall kan brukes.

- Skalerbarhet og mobilitet
  Det fine med VLAN er at det gjør nettverket ditt veldig godt egnet for forandringer og utvidelser. Det vil si at implementering av VLAN forbedrer skalerbarheten i nettverket ditt. I stedet for å fysisk måtte patche, eller flytte om på utstyr, kan disse endringene gjøres i softwarekonfigurasjonene på switchene. Du får dermed også utnyttet portene på switchene til det maksimale med VLAN. Dermed kan én fysisk switch gjøres om til flere virtuelle switcher. På mange måter gir VLAN det et software patchepanel.

- Kostnadsbesparende
  For de aller fleste virksomheter vil VLAN være kostnadsbesparende, siden du får utnyttet flere porter på switchen. Det sparer også virksomheten for plass, da flere switcher tar opp mer fysisk plass.

- Nettverksadministrering
  Logisk gruppering av brukere tillater lettere nettverksadministrering. Legge til, endre og flytte gjøres ved å konfigurere en port til å tilhøre det korrekte VLAN.

- Broadcast kontroll
  Switcher isolerer collision domener tilknyttet hoster og videresender relevant trafikk til en spesiell port. VLAN gir komplett isolasjon mellom ulike VLAN. Det er også ett bridget domene med all multicast og broadcast trafikk innesluttet i nettverket.

I bunn og grunn er det veldig få ulemper med VLAN. Det kan være noe forsinkelse eller dårligere ytelse, i og med at man kan ha brukere i samme LAN som ikke befinner seg i samme lokale området. Men med tanke på fleksibiliteten du får med VLAN er dette ett veldig lite minus.

Den største sikkerhetstrusselen i VLAN er ikke VLAN selv, men de som konfigurerer og patcher det. Problemer kan oppstå om noen benytter seg av det, men ikke har den nødvendige kunnskapen, og setter switcher med VLAN i nettverket med default konfigurasjon, dette kan utnyttes og brukes som en svakhet. Men dette er noe vi kommer tilbake til under testmiljø-delen.

Et enkelt spørsmål man kan spørre seg selv, for å finne ut om man har bruk for VLAN er: - Hvor mange brukere i systemet sitter på den samme plassen, bruker det samme utstyret og er tilknyttet de samme enhetene og det samme nettverket som de var for 1-2 år siden? Det er kanskje først da man virkelig ser hvor mange endringer det har vært i nettverket den siste tiden.

2.4 Designe VLAN nettverk

Flere nøkkelspørsmål må vurderes når man designer og bygger switchede nettverk. Blant annet må følgende vurderes:

- LAN Segmentering.
- Sikkerhet.
- Broadcast kontroll.
- Ytelse.
- Skalerbarhet.
- Brukermobilitet.
- Nettverk administrering.
- Endringer og utvidelser i nettverket.
- Kommunikasjon mellom VLAN.

Tradisjonell nettverksdesign bruker routere for å lage broadcast domener og begrense broadcasts mellom subnett. Dette forhindrer oversvømmelse av broadcast i større nettverk, noe som gjør at nettverksressurser ikke konsumeres, eller unødvendige DOS skjer. Men, dessverre har de tradisjonelle nettverksdesignene noen mangler:

- De fokuserer på fysisk lokasjon av utstyr og personell for adressering og LAN-segment plassering.
- Nettverkssegmenter for fysisk usammenhengende organisasjoner kan ikke være del av samme adresseområde. Hver fysisk lokasjon må adresseres hver for seg, og være del av sitt eget broadcast domene. For eksempel kan dette tvinge personell til å lokalisere seg i en sentral lokasjon, eller eventuelt ha forsinkelser eller underskudd på tilkoblinger.
- Relokasjon på personell og avdelinger vil være vanskelig, særlig om den originale lokasjonen beholder nettverkssegmentene. Relokert utstyr må rekonfigureres, avhengig av den nye nettverkskonfigurasjonen. En VLAN løsning kan løse begge disse problemene ved få det samme broadcast domene utover et singelt segment. Et godt VLAN designet nettverk kan forsikre at bare enheter i samme VLAN vil kunne sende og motta pakker ment som kilde eller destinasjonspakker av nettverksflyten.

2.5 VLAN links: VLAN access link og VLAN Trunk

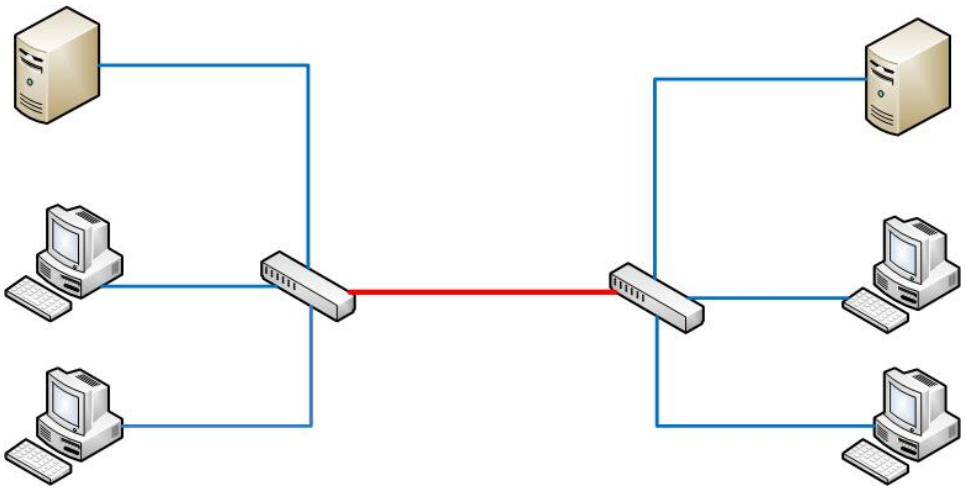
Når man snakker om VLAN-forbindelser er det to hovedtyper man bruker, nemlig VLAN access link og VLAN trunk[7]. VLAN access link er forbindelsen mellom en switch og en arbeidsstasjon, mens en Trunk link er forbindelsen mellom ulike switcher, routere og annet nettverksutstyr. HP sin terminologi på området beskriver access link som untagged, og trunk link som tagged.

2.5.1 VLAN access link

Som nevnt ovenfor er dette forbindelsen fra en switch til arbeidsstasjoner. Trafikken på disse linkene går som vanlig nettverkstrafikk, uten noe ekstra VLAN-tagging. Arbeidsstasjonene oppfatter derfor ikke at de er tilkoblet ett VLAN, og oppfører seg derfor som om de er koblet til ett vanlig nettverk med ett broadcast domain.

2.5.2 VLAN trunk

VLAN trunk er forbindelsen mellom switcher, routere og annet nettverksutstyr. På disse linkene blir ethernet pakkene modifisert med en ekstra VLAN tagg (se punkt 2.6), slik at switchene vet hvilke pakker som hører til hvilke VLAN. For å få til VLAN trunk forbindelsen, må man konfigurere en trunk port på switchen,



Figur 2.4: *Access links i blått og Trunk links i rødt*

2.6 IEEE 802.1Q (VLAN Tagging)

Standarden som gjelder for VLAN heter IEEE 802.1Q[8]. Den ble godkjent av IEEE, 8.desember 1998. Standarden tar for seg hvordan VLAN skal implementeres som en standard, slik at det kan brukes mellom utstyr levert av forskjellige leverandører.

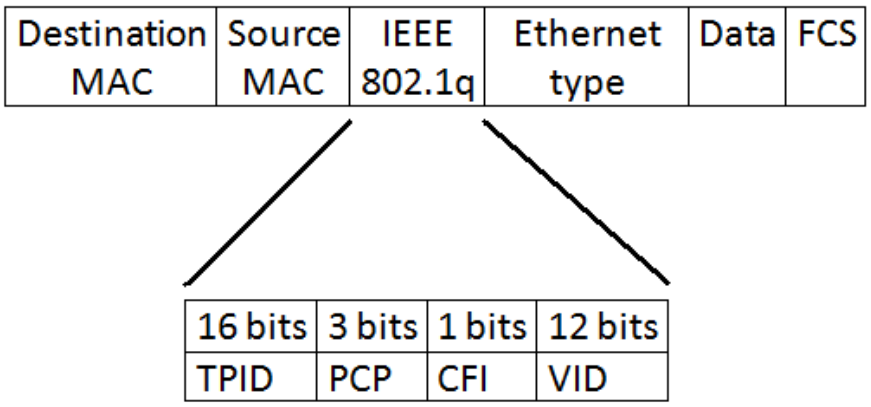
Initiativet til IEEE 802.1Q standarden ble tatt allerede i juli 1995, hvor innledende møter ble holdt. Det første offisielle møtet ble holdt i mars 1996, men det skulle likevel gå over to år og totalt 11 utkast til, før standarden ble godkjent. IEEE 802.1Q ble utviklet som en del av IEEE 802.1. IEEE 802.1 er igjen en del av IEEE 802 familien, som består av en rekke standarder som definerer forskjellige nettverksteknologier, blant annet LAN (802.1) Ethernet (802.3), WLAN (802.11) og Bluetooth (802.15). Selve navnet, 802, stammer fra grunnleggelsen, nemlig februar 1980 (80 fra årstallet og 2 fra februar, som er den 2.måneden i året).

Målet med IEEE 802.1Q var å gjøre store nettverk mer håndterbare, ved å dele de opp i flere og mindre nettverk. I tillegg skulle forskjellige nettverk kunne dele samme fysiske nettverkslink uten tap av informasjon mellom nettverkene. Store nettverk kan bruke opp mer båndbredde enn nødvendig, slik at ved å dele de opp i flere og mindre nettverk, vil broadcast og multicast ta opp mindre båndbredde. Ved å dele opp LAN ved hjelp av denne protokollen, har du i tillegg ett mye sikrere miljø for den interne trafikken, ved at det du får et høyere sikkerhetsnivå mellom nettverkene.

Spesifikasjonene i IEEE 802.1Q etablerer en standard metode for tagging av Ethernet rammer med informasjon om VLAN tilhørighet. IEEE 802.1Q standarden gir definisjon, operasjon og administrasjon av VLAN topologier i en bridget LAN infrastruktur. Nøkkelen til alle fordeler IEEE 802.1Q medfører, er dens tagging. Et tagget felt som inneholder VLAN informasjon kan settes inn i en Ethernet ramme. Hvis en port har en 802.1Q mottakelig enhet tilknyttet, for eksempel en switch, vil de taggede rammene kunne bære VLAN tilhørighetsinformasjon mellom switcher, slik at VLAN kan ha en spennvidde over flere switcher. Men det er viktig å forsikre seg om at porter, med utstyr tilknyttet som ikke er mottakelig for taggede pakker, er konfigurert til å sende untagged rammer. Mange datamaskiner eller printere er ikke mottakelige for taggede pakker, og om de da mottar en tagged ramme vil de ikke skjønne VLAN taggen og de vil miste rammen. Den maksimalt tillate lengden på en tagged ethernet ramme er på 1522 byte. Det betyr at nettverkskort eller eldre typer switcher kan miste taggede rammer om rammene er for store.

2.6.1 Tagged Ethernet ramme

VLAN blir integrert i Ethernet 2 pakkene ved å legge til et 32 bits felt mellom "Source MAC address" og "Ethertype/Length" feltene. Dette feltet kalles, som nevnt ovenfor, for VLAN tagg og har følgende oppbygning:



Figur 2.5: *Viser hvor VLAN taggen plasseres i ethernet pakken, og dens oppbygning*

- TPID
  16 bits felt med verdien 0x8100 for å gjenkjenne at Ethernet 2 rammen er en IEEE 802.1Q tagget ramme.
- PCP
  3 bits felt som referer til standarden IEEE 802.1P prioritet. Dette feltet kan ha en verdi fra 0(laveste) til 7(høyeste), og blir brukt til å prioritere forskjellig typer trafikk som tale, video, data osv.
- CFI
  1 bit felt som angir formatet på MAC adressen. CFI brukes for kompabilitet mellom ethernet og token ring nettverk. For ethernet switcher skal denne verdien alltid være satt til 0.
- VID
  12 bit felts som spesifiserer hvilket VLAN rammen hører til. Hvis verdien er 0 hører ikke rammen til noe VLAN, altså er 802.1Q taggen der bare for å angi prioritet og kalles da en prioritets tagg. Hex verdien FFF er reservert for implementerings bruk, alle andre verdier kan brukes som VLAN identifiserer som gjøre at man kan ha opptil 4094 VLAN.

2.6.2 Funksjonaliteter i 802.1Q

IEEE 802.1D standarden, eller MAC Bridges, spesifiserer arkitektur og protokoll for sammenkobling av IEEE 802 LAN under MAC service grensene.Forholdet mellom 802.1D og 802.1Q er slik at 802.1Q har utvidet konseptet av MAC bridging og filtreringsservicene for å supportere definisjonen og administrasjonen av VLAN. De to standardene henger ikke sammen, det er to forskjellige standarder, men 802.1Q bruker mange av funksjonalitetene til 802.1D, blant annet:

- Bridge arkitektur
  Arkitektur for bridging blant et vilkårlig nummer av porter tilknyttet MAC teknologi som supporterer 48-bit addresser (Ethernet, Token Ring, osv.).
- Filtreringsarkitektur
  Arkitektur for å filtrere databaser, altså en datastruktur som vet mappingen av enheter til porter.
- Prosesser for videresending
  Algoritmer for filtrering og videresending av rammer mellom porter, basert på innholdet av filtreringsdatabasen.
- RSTP
  Spesifikasjon for STP slik at aktive looper forhindres.

I tillegg, for å supportere VLAN relaterte operasjoner på en switch, inneholder 802.1Q funksjoner 802.1D ikke har, som blant annet:

- Filtreringsdatabase
  802.1D sin filtreringsdatabase gir kun mulighet til 48-bit adressering til porter. For 802.1Q er det slik at filtreringsdatabasen er utvidet til å inkludere muligheter til å kartlegge adresser til VLAN og VLAN til porter.
- Ramme tagging
  Her har man en metode for å tagge rammer med VLAN identifikasjon.
- Prioritetsoperasjon
  Prioriteringskoding av VLAN taggede rammer.
- Automatisk distribuering av VLAN konfigurasjons informasjon
  Automatisk distribuering av VLAN tilhørighets informasjon mellom switcher og endestasjoner. GARP VLAN tillater switcher til å automatisk lære å kartlegge VLAN på switch porter uten å måtte konfigurere hver eneste switch.

- Switch administrering
  802.1Q gir muligheten til å administre switcher. Som med de fleste IEEE 802 standarder er administrasjon valgfritt. Men det er, ut ifra brukerbehov, sikkerhet og produktforutsetninger, ikke anbefalt.

- MSTP
  MSTP, som bruker RSTP for hurtig konvergens, gjør det mulig for VLAN å bli gruppert i en spanning tree instans, hvor hver spanning tree topologi er uavhengig av andre spanning tree instanser. Denne arkitekturen gir flere stier for videresending av data trafikk og reduserer nummeret av spanning tree instanser nødvendig for å supportere mange VLAN.

2.7 Noen Cisco-proprietære VLAN protokoller

Som nevnt tidligere skal vi i dette prosjektet hovedsakelig konsentrere oss om HP Procurve, men vi vil også nevne noen Cisco-proprietære protokoller i dette avsnittet.

2.7.1 VTP

VTP[7] er en Cisco-proprietær lag 2 protokoll for administrasjon av VLAN på Cisco's switcher. Med VTP kan man sentralisere administrasjonen av VLAN på Cicso's switcher, man kan da legge til, slette eller gi nytt navn til VLAN fra en VTP server og det vil oppdatere seg på alle svitcher som er tilkoblet. Switcher kan operere i 4 forskjellige VTP metoder:

- Server
  I server mode kan man lage, endre eller slette VLAN samt spesifisere andre konfigurasjons parametere, som VTP versjon og VTP pruning for hele VTP domenet. VTP servere annonserer sin VLAN-konfigurasjon til andre svitcher i samme VTP domene og synkroniserer VLAN-konfigurasjonen sin med de andre svitchene. VTP server er standard modus når VTP er på.

- Client
  En client kan ikke gjøre endringer. Den bare mottar oppdateringer fra switcher som er VTP servere og oppdaterer seg etter dette.

- Transparent
  En switch i "transparent mode" annonserer ikke sin VLAN-konfigurasjon, den gjør bryr seg heller ikke om mottatte VTP oppdateringer. Det eneste den gjør er og videresende VTP informasjon den mottar.

- Off
  En switch med VTP off oppfører seg som en switch i transperent mode, bortsett fra at den ikke videresender VTP pakker.

VTP er jo en Cisco proprietær protokoll, men finnes det også ett åpent alternativ i 802.1P og 802.1Q standarden, som kalles GVRP. GVRP fungerer på mange måter likt som DTP, ved at switcher kan dynamisk utveksle VLAN-konfigurasjon med hverandre over 802.1Q trunk linker.

2.7.2 DTP

DTP er også en Cisco proprietær lag 2 protokoll. DTP[7] brukes til å opprette trunk linker mellom to switcher med støtte for VLAN. Switchene diskuteret ved hjelp av DTP, seg i mellom om hvordan trunk som skal brukes, enten med en 802.1Q-tagg eller Cisco's egen ISL-protokoll. DTP kan operere i følgende modus:

- Auto
  I auto modus lytter porten etter DTP pakker og er da villig til å konvertere til trunk hvis det skulle være ønskelig av nabosvitchen. Auto tar aldri initiativ til å konvertere til trunk men gjør det bare hvis den blir bedt om det av andre svitcher.

- Desirable
  Når en port opererer i desirable modus prøver den alltid og bli en trunk, hvis da utstyret i andre enden av porten har støtte for dette, konverteres de til trunk.

- On
  I on modus er porten en trunk uansett hva som er andre enden, untatt hvis den får en DTP beskjed om at den ikke kan være trunk.

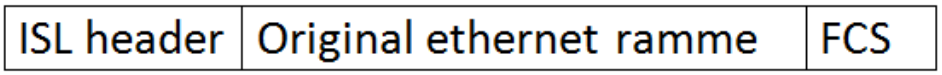
- Nonegotiate
  En port som står i nonegotiate DTP modus er uansett en trunk, samme hva slags DTP beskjeder den skulle motta.

- Off
  Hvis en port står i DTP off modus kan den ikke bli en trunk uansett hva slags DTP beskjeder den mottar.

Det som er viktig å huske på ved bruk av DTP, er å ikke sette access porter i Auto DTP mode, men hardkode dem som access porter i ett statisk VLAN med DTP off. Dette for å unngå at angripere kan utnytte DTP svakheter.

2.7.3 ISL

ISL[7] er nok en proprietær protokoll fra Cisco. ISL er Cisco sitt svar på 802.1Q tagging. ISL brukes til å vedlikeholde VLAN informasjon i ethernet pakker mellom switcher. Måten ISL gjør dette er ved å innkapsulerer ethernet rammene med en 26 bytes header som inneholder VLAN informasjon, og en 4 bits FCS etter den originale ethernet pakken. ISL kan hold styr på opptil 1000 VLAN i et nettverk.



Figur 2.6: *Viser hvordan ISL innkapsulerer en ethernet ramme*

2.8 VLAN typer

Det finnes to typer VLAN, nemlig Cell-based og Frame-based. Cell based VLAN blir brukt i ATM nettverk med LANE. LANE tillater vanlig nettverksutstyr å kommunisere over ATM nettverk uten behov for noen spesiell software eller hardware. Frame based VLAN blir brukt i ethernet nettverk og baserer seg på tagging av ethernet rammene (se del 2.5). I dette prosjektet vil vi fokusere på Frame based nettverk siden det er ethernet utstyr vi skal teste på og det er det mest vanlige nettverksmiljøet.

Selve inndelingen av VLAN på switchene, kan gjøres på tre forskjellige måter. Du har port baserte VLAN, MAC baserte VLAN og du har forskjellige lag 3 baserte VLAN. For å oppnå optimal funksjonalitet kan det være aktuelt å kombinere flere metodene vi nå skal ta for oss[5].

2.8.1 Port-basert VLAN

Dette er den enkleste og mest brukte måten å opprette et VLAN på. Port baserte VLAN baserer seg på at hver enkelt port er medlem av et VLAN, eller sagt på en annen måte, brukerne i et VLAN er tilknyttet bestemte porter i switchen. Hver enkelt port (untagged porter) som kommuniserer med arbeidsstasjoner kan kun være untagged i et VLAN, mens uplink porter (tagged porter) som kommuniserer med annet nettverksutstyr kan være medlemmer av flere VLAN. En port kan altså være unntagged i et VLAN mens den er tagged i et andre VLAN, dette for å ha muligheten til å kunne sende flere VLAN på en enkelt port. Som for eksempel ethernet

trafikk og VoIP trafikk på samme kabel, ved slik kommunikasjon er man avhengig av at utstyret som skal hente ut den taggede infoen støtter 802.1Q standarden. Alt nettverksutstyr innenfor ett VLAN kommuniserer fritt seg i mellom med enten unicast, broadcast eller multicast adressering. Dette gjør at port-baserte VLAN er veldig enkle å sette opp og administrere, men de er samtidig lite fleksible, siden man må være koblet på en port som er medlem av riktig VLAN for å få tilgang til det man skal.

2.8.2 MAC-basert VLAN

MAC-baserte VLAN baserer seg på den unike MAC-adressen alt nettverksutstyr har. MAC-adresser hører til lag 2 i OSI modellen og denne typen VLAN kalles derfor også ofte for lag 2 baserte VLAN. Ved konfigurasjon av MAC-baserte VLAN settes det opp en liste i switchene over hvilke MAC-adresser som tilhører hvilke VLAN. Slik at når man kobler til en arbeidsstasjon vil switchen sjekke MAC-adressen til arbeidsstasjonen og assosiere den med riktig VLAN, om MAC-adressen er konfigurert til ett VLAN. Hvis ikke, vil ikke arbeidsstasjonen få tilgang til noen nettverksressurser. Dette gjør MAC-baserte VLAN veldig fleksible i forhold til at det ikke spiller noen rolle hvor man kobler seg til så lenge MAC-adressen er registrert i forhold til ett VLAN.

Ulempen med MAC-basert VLAN er at det er en god del mer arbeid å sette opp og vedlikeholde et MAC-basert VLAN med registrering av MAC adresser. Spesielt vedlikeholdet, etterhvert som folk begynner og slutter, eller bytter arbeidsstasjoner. Og om det er snakk om store nettverk krever MAC-baserte VLAN mye kapasitet av switchene for å finne frem til riktig VLAN for hver MAC-adresse.

2.8.3 Lag 3-basert VLAN (Protokoll basert VLAN)

I likhet med ett VLAN som er basert på MAC-adresser, kan også brukere i lag 3-baserte VLAN flyttes rundt i nettverket uten å endre sin logiske adresse. Lag 3-baserte VLAN bruker adresseformatet på lag 3 av OSI modellen for å definere hvilke arbeidsstasjoner som danner et VLAN. For eksempel kan alle arbeidsstasjoner i ett IP-subnett danne ett VLAN, og en serie med IPX-adresser danne et annet VLAN, altså deles det opp etter protokoller. Brukerne får tildelt lag 3 adresser dynamisk, og følgelig en ny adresse ved hver innlogging. Ulempen med lag 3 baserte VLAN er at de kan være mer ressurskrevende enn de to metodene over, i og med at det tar lenger tid å behandle lag 3 informasjon i forhold til lag 2 informasjon.

2.8.4 IP-multicast basert VLAN

Denne typen VLAN går ut på at én pakke sendes rundt til en gruppe med mottakere som er medlem i en aktuell multicast-gruppe. Denne gruppen (av IP-adresser) blir definert dynamisk ved at klientene svarer "ja" på en invitasjon som opplyser om at multicast-gruppen finnes. Ved å opprette et VLAN med denne metoden, vil også endringene for de ulike medlemmene skje dynamisk. Dette gir rom for stor fleksibilitet. Ved å involvere flere routere kan slike multicast ha en stor rekkevidde ved å ta i bruk for eksempel WAN.

Kapittel 3

Angrep

Det finnes mange forskjellige angrep som kan ramme et datanettverk. Vi har i forbindelse med dette satt opp en oversikt over noen av de mest vanlige angrepene nettverk kan være sårbare for. Dette spenner fra vanlige ARP angrep til et mer spesifisert angrep som VLAN hopping. Det er lagt inn generell statistikk for sikkerhet i bedrifter for å se hyppigheten av slike angrep mot deres datasystemer.

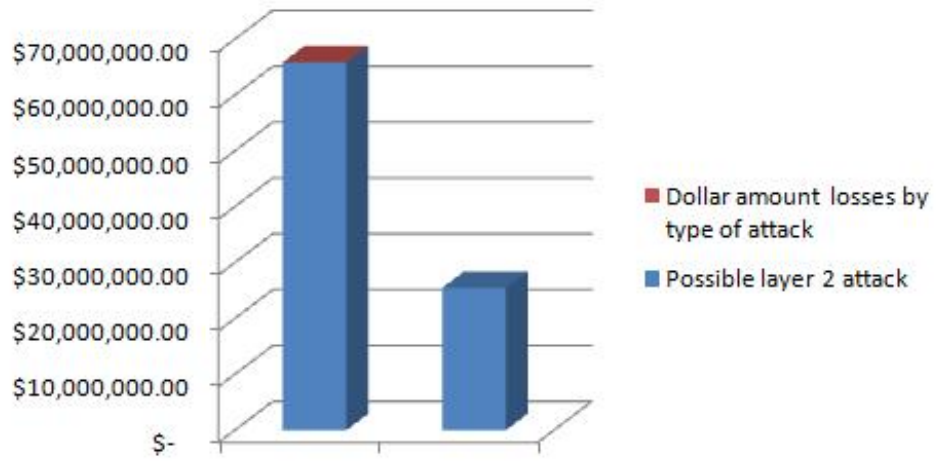
Før vi tar for de forskjellige angrepstypene, skal vi se på en sikkerhetsundersøkelse rettet mot lag 2 sikkerhet.

3.1 Sikkerhet blant bedrifter

Sikkerhet har i mange år vært noe som har blitt nedprioritert fremfor ytelse og pris i mange bedrifter. I følge en undersøkelse gjort av CSI(Computer Security Institute) og FBI(Federal Bureau of Investigation) ser man tap som følge av angrep utført for 2008[9]. Av disse er da 9 av 19 mulige lag 2 angrep. Altså angrep som kan ha blitt rettet mot switcher.

I denne undersøkelsen har CSI og FBI sett mot Karachi, Pakistan, fordi dette er et veldig stort nettverksmiljø. Her ble det oppdaget at av de 25 nettverkene undersøkt, virket det som om 67% var ubeskyttet, altså uten VLAN. 8% brukte lavnivå-beskyttelse som SSH, STP (se del 3.4), Auto-Trunking/Auto-Tagging. Rundt 25% benyttet seg av mer sikker "beskyttet lag 2" sikkerhet (som for eksempel HP's "Port Security" ved MAC-flooding). Med andre ord var faktisk 75% av de nettverkene med VLAN sårbare for VLAN-hopping angrep innenfor det samme subnettet. Undersøkelsen viste også at en VTP broadcast storm kan bli generert i 32% av nettverkene.

Det er en voldsom vekst innen kablet og trådløst nettverksutstyr, uten lik



Figur 3.1: *Tap i forbindelse med angrep*

øking i bevisstheten rundt lag 2 sikkerhet. Dette er et voksende problem innenfor både små- og store bedrifter. På samme tid er det spillerom for å forbedre sikkerheten rundt usikrede nettverk. Den største trusselen man kan bli utsatt for er uatoriserte brukere som kan få tilgang til usikrede nettverk og dermed ha muligheten til å bruke påfølgende nettverksresursser. Dette vil ikke bare øke trafikken, men det tilrettelegger for muligheten til å utføre et angrep mot lag 2 delen av nettverket.

Da undersøkelsen ble foretatt hadde CSI og FBI sett på det overordnede målet med å øke sikkerheten i det 2. laget på nettverks-systemene i Karachi. De kom frem til at de skulle inkludere følgende "Layer 2 Network Security Good Practices" i Annexure I:

- Forhindre MAC Flooding angrep
  - Port sikkerhet
  - Å gi tillatelse til å undersøke MAC-adressene til alle portene, eller å lære visse MAC-adresser per port.
  - Ved funn av ugyldig MAC-adresse, blokkere selve MAC-adressen eller slå av hele porten.
  - Smart CAM-tabell
    - Aldri overskrive eksisterende oppføringer
    - Aldri overskrive aktive verter.
    - Bare gi time-out til inaktive oppføringer.
- Snakk først

  - Krev at en vert sender trafikk før den kan motta.

- Forhindre VLAN Hopping Angrep
  - Bruk nyere switcher.
  - Deaktiver Auto-tagging/trunking
  - Aldri plasser en vert i et Native/Default VLAN
  - Sett ubrukte porter til å tillhøre ubrukte VLAN

- Forhindre Spanning Tree Angrep
  - Deaktiver STP(Trenger ikke STP i loop-frie topologier)

- BPDU Guard
  - Deaktiverer porter ved detektering av en BPDU melding på porten.

- Root Guard
  - Deaktiverer porter som kan bli root bro som følge av BPDU annonsering

3.2 VLAN hopping

VLAN-hopping er en av de vanligste former for angrep på VLAN platformen. Denne type angrep benyttes til å infiltrere nettverksikkerheten som hjelper til med å skille de ulike logiske nettverkene i et VLAN-system. Et slikt angrep blir vanligvis utført ved å sende pakker til en port på nettverket som normalt ikke er tilgjengelig på grunn av VLAN oppdeling.

Et VLAN-hoppangrep kan skje på to forskjellige måter:

1. Switch Spoofing
   Hvis en nettverksswitch er stilt inn på "Autotrunking" eller "Autotagging"[7] så kan en angriper konfigurere et system slik at det utgir seg for å være en switch. Ved å gjøre dette så kan angriperen få mulighet til å emulere enten ISL eller 802.1Q signaler sammen med DTP-signaler. Dersom dette lykkes, får angriperen tilgang til alle de tillatte VLANene på den tiltenkte porten.

2. Double Tagging
   Denne formen for VLAN-hopping[7] skjer ved at en hacker overfører data gjennom en switch til en annen ved å sende rammer med to 802.1Q tagger, der den ene taggen er for angrepsswitchen og den andre er for offer switchen. Dette "lurer" offer-switchen til å tro at bitrammen er tiltenkt den, dermed vil den utpekte switchen sende infoen videre til offer-porten.

3.2.1 Konsekvenser

VLAN-hopping kan deaktivere hvilke som helst sikkerhetstiltak som brukere har satt på enheten som legger opp rutinger mellom ulike VLAN. VLAN-hopping kan brukes for å stjele passord og annen sensitiv informasjon fra en klient på nettverket. Det kan også brukes til å forplante ormer virus og trojaner, samt endre, ødelegge eller slette data, installere ondsinnet programkode gjennom hele lokalnettverket.

3.2.2 Sikkerhetstiltak

I Cisco sin DTP, så kan mottageligheten for et VLAN-hopp stilles til et minimun ved at en slår av autotrunking-innstillingene på alle switchene som ikke trenger å sende VLAN-koblinger til andre switcher. Det samme gjelder for HP's Procurve switcher ved tagging av pakker som går fra en switch til en annen. Ved å følge anbefalingene fra leverandørene av switchene hjelper det veldig mye på sikkerheten. Aldri bruk standard VLAN-et som er satt opp fra start!

3.3 Mac-flooding og ARP angrep

I switcher finner man en liste som kalles Translation table. Translation table inneholder MAC-adresser som sier hvilke maskiner som er knyttet til hvilke porter på switchen. Den sier også hvilke data som skal sendes til hvilke porter der destinasjonsmaskinen finnes. Dette er forskjellen mellom en switch og en hub. En hub vil sende alle pakker til alle maskinene knyttet til portene på huben, mens en switch finner frem riktig port og maskin den vil derfor sende data kun til den ene datamaskinen.

For å kunne sende data til riktig maskin trengs det en unik identitet for hver maskin. Denne unike identiteten får man ved hjelp av MAC-adresser. Alle nettverkskort, porter og liknende hardware har dette som en unik identifikator. En MAC-adresse består av 6 byte med data og er permanente. Det vil

si at de er hardkodede i ROM-et på nettverkskortet. Når en maskin sender en pakke med data over en port på en switch er det med en header med en destinasjo

Et MAC-flooding[7] angrep kan lede videre til et ARP angrep[7]. Dette angrepet brukermange av de samme mekanismene til et MAC-spoofing. Dette er protokollen som vet hvilke IP-adresser og MAC-adresser som hører sammen i translation list. Når en angriper sender ut falske adresser legges disse i denne tabellen. Dette brukes i et angrep der man legger inn falske adresser slik at brukerens maskin tror angriperens adresse er switchen i nettverket eller andre. På denne måten kan man utføre et Man in the Middle angrep der all trafikk går fra brukeren til angriper slik at man kan sniffe trafikken med en pakkesniffer.

3.3.1 Konsekvenser

Et MAC-flooding angrep er laget slik at det sendes mange pakker til en switch hvor alle pakker inneholder falske MAC avsenderadresser. Målet med dette angrepet er å fylle opp minnet som translation table har fått tilmålt. Når dette skjer vil switchen aktivere failopen mode. Denne mekanismen ser bort ifra translation table slik at switchen da fungerer som en hub. Dermed blir alle pakkene som er ment til å gå til en bestemt MAC-adresse sendt ut til alle portene på switchen. Dette betyr at alle kan få tak i dataene som blir sendt over nettverket. Dette en betydelig sikkerhetsrisiko.

Angriperen får tilgang til data som han han/hun ikke normalt sett skulle hatt tilgang til. Dette kan være passord, beskyttede filer, e-post og samtaler over lynmeldingstjenester. Noe som gjør dette angrepet veldig farlig, da man kan snappe opp bedriftshemmeligheter og annen viktig data som kan brukes mot en bedrift, enten som et konkurranse fortrinn eller som utpressingsmiddel.

3.3.2 Sikkerhetstiltak

For å sikre seg mot slike angrep kan man begrense hvor mange MAC-adresser man kan ha på en port. Dette vil redusere risikoen for en flooding angrep. Ulempen med dette er man kun kan koble til et vist antall maskiner.

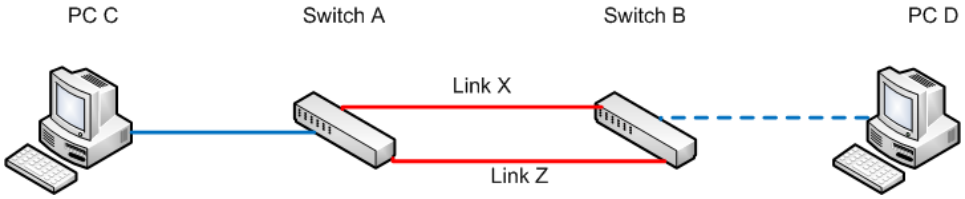
Et annet sikkerhetstiltak kan være at man gir ekstra sikkerhet til enkelte MAC-adresser eller man kan slå av switchen helt når et angrep inntreffer, selv om dette ikke er å anbefale.

For å sikre seg at en angriper ikke kan lese trafikken som går over nettet ditt, selv om han har fått gjennomført et vellykket MAC-flooding angrep og sniffet pakkeflyten, kan man kryptere dataene som sendes over nettverket

slik at disse er uleselige for en som ikke har de rette krypteringsnøkklene.

3.4 STP

STP[7] brukes i nettverk der det kan oppstå redundante linker. I disse nettverkene finner STP den korteste sti fra en maskin til en annen ved å deaktivere linker på nettverksutstyr som har flere tilkoblinger mellom seg. Tenk deg at du har et nettverk med to switcher A og B. Switchene er koblet sammen ved hjelp av to linker X og Z mellom switch A og B. Maskin C er koblet til switch A og Maskin D er koblet til switch B. Problemer oppstår når maskin C og D skal kommunisere med hverandre.



Figur 3.2: *Viser et nettverk med doble linker*

Det som skjer er:

- PC C sender en pakke til switch A på port 1. Denne inneholder en destinasjonsadresse som er MAC-adressen til PC D.
- Switch A har ikke lagret MAC-adressen til PC A i forward table. MAC-adressen og porten som maskinen er tilkoblet på blir lagret i forward table i switchen.
- Switch A finner ikke noe oppføring i sin forward table for MAC-adressen til D
- Switch A sender da ut en frame på til alle portene på hele nettverket også til switchen B på link X og Z
- Switch B mottar denne rammen både på link X og på link Z. Når dette skjer vil forward table bli overskrevet to ganger. Først med avsender-adressen fra link X (eller den linken som rammen kommer først frem på) og deretter link Z.
- Switch B slår opp MAC-adressen til B og finner ingen oppføring av denne fordi B ikke har snakket til noen på nettverket enda.

Rammene i dette nettverket vil gå i en evig rundgang mellom de to switchene. Det finnes ingen maksimumstid for en ramme i et slikt nettverk. Det eneste som kan få pakkene til å slutte å sirkulere rundt er et strømbrudd som forårsaker en omstart av switchene. Dette terminerer all trafikk som går mellom enhetene.

For å løse dette problemet bruker man STP. Oppgaven til denne protokollen er å fjerne redundante linker slik at man har kun én vei fra switch A til B. Det som vil skje i eksempelet over er at den ene linken vil bli brukt til datatrafikk, mens den andre blir deaktivert og ligger som en redundant link. Denne tas i bruk hvis en link mellom switchene blir terminert. For å utføre et angrep må man skjønne hvordan STP funker. Nettverket blir satt opp som et tre. Dette vil si at man har en root som bestemmes av switchene. Dette gjøres ved at switchene har en brige ID og den switchen som har den laveste bridge ID vinner og blir da root i nettverket. Når en switch mottar en brige ID vil disse bli sammenlignet med sin egen. Hvis den har en lavere brige ID vil switchen som mottar signalet slutte å sende ut sin bridge ID.

Når STP skal bygge sin loopfrie topologi så benyttes det payloads ved hver enkelt swtich. Det vil si at når en switch mottar en BPDU så legges det til en verdi for stien den har gått mellom mottakeren og den forrige switchen. Root switchen setter verdien 0 i BPDU og sender denne videre til de andre switchene som legger til sin verdi i pakken. Hvis en switch mottar flere BPDU vil den med minst verdi bli valgt og den andre vil bli lagt i noe som heter "blocked mode". In blocked mode vil en switch ikke godta andre pakker enn BPDU-er.

Field	Value
Destination MAC	**01 80 c2 00 00 00** IEEE reserved BPDU MAC
Source MAC	**00 00 0c a0 01 96** Port's MAC address
LENGHT	**00 26**
LLC HEADER	
Destination Service Access Point	**42**
Source Service Access Point	**42**
Unnumbered Information	**03**
PROTOCOL	**00 00**
PROTOCOL VERSION	**00**
BPDU TYPE	**00**
BPDU FLAGS	**00**
ROOT ID	**20 00 00 d0 00 f6 ba 04**
PATH COST	**00 00 00 00**
BRIDGE ID	**20 00 00 d0 00 f6 ba 04**
PORT	**81 14**
MESSAGE AGE	**00 00**
MAXIMUM AGE	**14 00**
HELLO TIME	**02 00**
FORWARD DELAY	**0f 00**

Figur 3.3: *Viser innholdet i en BPDU pakke [7]*

De viktigske dataene her er Hello, Forward Delay, Message Age og Maximum Age.

- Hello er de dataene som sier noe om hvor lang tid der er mellom Hello forespørslene som blir gitt på en port.
- Forward delay er hvor lang tid som brukes på å være i Listening og Learning staten til switchen. I Listening staten lytter switchen etter BPDUer og i Learning staten settes det opp forwardingtabeller.
- Message Age er den tiden en BPDU har brukt fra den ble sendt ifra root bridge til den er mottat i switchen. Alle switcher som BPDUen har vert innom legger til 1 i Message Age. Ved hjelp av denne kan man finne ut hvilken plassering man har i nettverkstreet.
- Maximum Age er hvor lang tid det tar før konfigurasjonen fra en BPDU blir lagret i switchen.

En BPDU sendes ut av switchen hvert andre sekund med en Max Age på 20. BPDUer kan være ustabile og komme "for sent" frem til mottakeren. Det som skjer da er at switchen vil begynne hele runden på nytt med og bygge opp nettverket og dermed skape mye trafikk som kan hemme nettverket.

BPDUer brukes også til å gi varsler om nye tilkoblinger i nettverket slik at de forskjellige switchene vet når porter blir aktive/innaktive. Dette gjøres ved

å sende en verdi i Flag feltene. Denne verdien kan enten være 1000 0000 eller 0000 0001. Hvis den lave biten er satt vil dette utgjøre en TCN-BPDU. Dette går helt opp til root switchen og skjer når en port går opp eller ned. Denne beskjeden blir godtatt av alle switchene i nettverket uten at root switchen har godtatt denne. Når root switchen mottar beskjeden vil den sende tilbake et ACK ved å sette "high-order bit" i BPDU-en som den sender ut. De forskjellige funksjonene forklart hjelper STP med å bygge og vedlikeholde nettverkstreet slik at man hele tiden har en loop fri nettverksoppbygging[7].

3.5 STP angrep

Dette angrepet går ut på å overta som root bridge slik at man kan kontollere nettverket. Det som skjer er at man sender ut BPDUer som har en lavere MAC-adresse enn det root bridge har. For å gjennomføre dette angrepet kan man bruke Yersinia. Yersinia genererer en BPDU pakke som har lavere MAC-adresse enn det root bridgen har. Hvis root bridge har MAC-adressen 00:60:3e:05:9c:00 vil Yersinia generere en MAC adresse som kan se slik ut 00:60:3e:04:9c:00. Dersom fem tallet blir byttet ut med fire tallet av Yersinia vil man få en lavere MAC-adresse. Dette vil gjøre at angriperen blir root bridge og kan se trafikken som går over nettverket. Når angriperen sniffer pakkene i nettverket kan han/hun se alle dataene som flyter mellom arbeidsstasjoner.[7]

En annen variant av dette angrepet er at man trekker tilbake sin BPDU med den laveste adressen slik at STP må kjøre på switchene igjen. Ved å repetere denne handlingen med å ta over og gi ifra seg kravet på å være root bridge, vil man skape høy CPU bruk. På grunn av dette kan nettverket arbeide saktere eller skape et DOS angrep[7].

Man kan også ha en variasjon på dette angrepet der man er root bridge og mottar en TCN-BPDU fra en av de andre switchene som kan la være å sende TC-ACK tilbake. Dette vil gjøre at forwarding table ikke blir oppdatert og flooding kan oppstå når man sender pakker over nettverket med utdaterte adresser til porter som ikke lenger er aktive[7].

Flooding angrep med BPDUer og TCN-BPDU er ganske enkelt. Det går fortsatt ut på å bruke BPDU pakkene. I dette angrepet sendes det ut veldig mange BPDU, ikke bare noen få som det ble gjort i forrige angrep. Med den store mengden slike pakker vil en nettverks switch få problemer med å behandle pakkene. Dermed har man et DOS angrep. En angriper kan ved å sende mange TCN-BPDU også skape et DOS angrep. Disse må root bridgen godta, dermed brukes all CPU kraften på å behandle dissa pakkene. Når en root bridge godtar disse pakkene og setter high bit i BPDUen vil også de andre nettverksenhetene se disse pakkene og justere forwarding tabellen sin.

På grunn av dette vil angrepet ha et større omfang enn bare root bridge som i det forrige angrepet.

3.5.1 Sikkerhetstiltak

Det finnes mange forskjellige tiltak for å forhindre angrep mot nettverksenheter. Disse egenskapene er vanligvis lagt inn i switchen fra produsenten sin side. Noen av disse egenskapene kan være Root Guard, BPDU-Guard og BPDU-Filtering[7].

Root Guard overvåker portene for å sjekke om det kommer BPDU-er fra en kilde det ikke skal komme fra. La oss si at vi har Swtichene A, B, C og D. A er root brige, mens B og C er koblet til denne. D blir da koblet til B og begynner og sende ut BPDU-er. Det som skjer et at B blokkerer porten D er koblet til, dermed kommer ikke BPDU-ene frem til A og et angrep der man prøver og ta over som root brige er avverget. C gjør dette helt til D slutter å sende ut BPDU-er og åpner så opp porten igjen.

BPDU-Guard virker på en liknende måte som Root guard. Den overvåker porten som den er aktivert på. Den stopper BPDU-ene ved å blokkere porten. Forskjellen er at denne funksjonen ser etter alle typer BPDU-er, ikke bare de som prøver og ta over som root bridge.

BPDU-filtrering filtrerer ut alle BPDU-er uten og lukke eller åpne noen porter slik som de andre sikkerhetsmekanismene gjør. Den filtrerer enkelt ut disse pakkene slik at de ikke har noen virkning. Denne innstillingen kan være spesielt interessant når det kommer til å forhindre DOS-angrep. Det som imidlertid er ulempen med denne egenskapen er at man stopper absolutt all trafikk også de BPDU-ene som blir generert av systemet for å holde STP vedlike. Dette kan føre til looping i nettverket noe som igjen kan føre til overflødig bruk av CPU i switchene.

3.6 VoIP Hopping

Når det gjelder angrep på VLAN så er det nok ikke VoIP(Voice over IP) eller IP-telefoni som er det første man tenker på innen sårbarheter i VLAN.

IP-telefoni er veldig aktuelt om dagen for bedrifter. Både store og små bedrifter velger å benytte seg av dette i sine systemer. Mest fordi dette gir lavere kostnader, men også fordi det også gir økt kvalitet og er enklere å administrere. Når dette blir kombinert med VLAN teknologien så kan det allikevel by på problemer. Da med tanke på sårbarheter.

SecurityFocus[10] fant i slutten av 2007 at det var og er kanskje fortsatt

veldig lav bevissthet gjennom bedrifts-amerika når det kommer til de forskjellige sårbarhetene og risikoene som kommer fra å konvergere IP-telefonisystemer. I et konvergert IP-telefonisystem så er det som regel samme type kabel(RJ45 Ethernetkabel) som tilbys til både IP-telefoni tjenesten og datamaskintilkoblingen. Siden det er samme type kabel som på en vanlig datamaskin, kan dette føre til kostnadsbesparelser på både kjøp og trekking av TP-kabel. Men da er vi igjen inne på sikkerhetsproblemene, fordi det at når det er samme funksjonalitet så byr dette også på problemer. Den største bekymringen er rettigheter som kommer på avveie gjennom offentlig tilgjengelige IP-telefoner, som de plassert i hotelrom, konferanserom og lobbier. Dette åpner for muligheten for at uatoriserte personer får tilgang til steder som ikkke er tiltenkt dem.

3.6.1 Konsekvenser

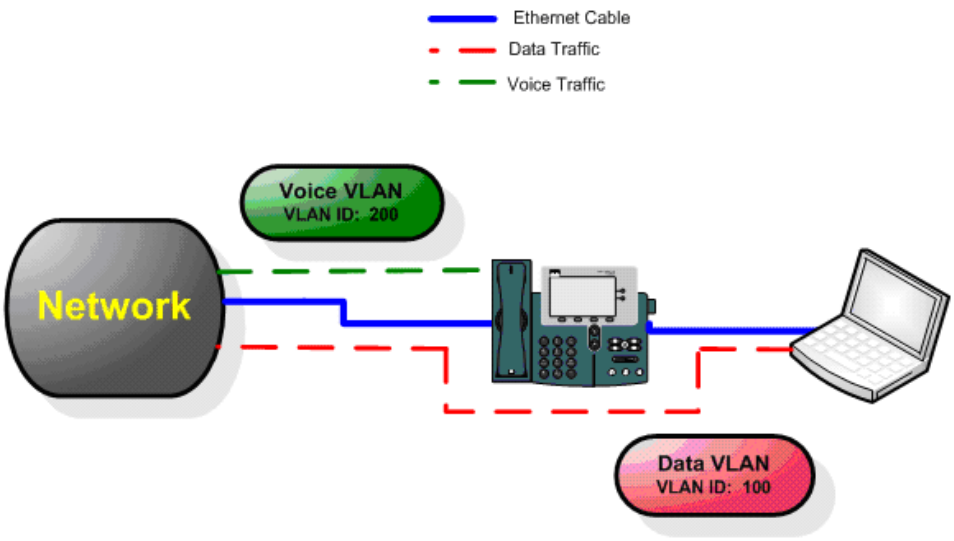
"Voice-VLAN" er en spesiell egenskap/tilgangsport som gir mulighet for IP-telefoni til å autokonfigurere og enkelt knytte seg til ett logisk separat VLAN. Denne tjenesten tilbyr ulike fordeler, der en som skiller seg ut er når Voice VLAN-et er aktivert på en port som også er aktivert til å tillate samtidig tilgang for en vanlig PC. Denne funksjonen gir en PC muligheten til å bli koblet til en switch via IP-telefonen. Tilkoblingen for både PC-en og IP-telefonen kan da bli trunket gjennom den samme fysiske TP-kabelen.

Aktivering av Voice VLAN øker kompleksiteten med å sikre de fysiske ethernet portene. Aktivering av porter uten tilstrekkelig sikkerhetskontroll på plass kan øke risikoen for angrep mot organisasjonen. Når implementeringen av VoIP nettverk utføres, bør man ikke anta at sikkerheten til IP-telefoner og selve Voice VLAN-et er bra nok i en standard installasjon. På grunn av enkele angrep og kritiske tap som kan oppstå, burde de som setter opp VoIP gjøre følgende:

- Implementere den strengeste formen for sikkerhetsmekanisme til de portene det gjelder.
- Teste portene til de tilkoblede IP-telefonene for å forsikre at de passer overens med omgivelsene.

3.6.2 Potensielle angrep

Når IP-telefoner er plassert på pysiske steder utenfor avlukkede bedriftsnettverk, så er angrepstruslen vedr. VoIP hopping mye større. Grunnen til dette er fordi mange bedrifter implementerer konfigurasjoner for stemme



Figur 3.4: *VoIP tilkobling*

og data VLAN ved disse eksterne nettverkene på samme måte som de har ved de interne nettverkene. Istedet for dette burde de eksterne plassene bli behandlet som det de er. Eksterne, utrygge nettverksegmenter. På disse plassene vil en angriper enkelt få tilgang til en IP-telefon som kan gi direkte tilgang til det interne nettverket.

Et eksempel er at SecurityFocus hadde observert muligheten til å VoIP-hoppe på hotellrom og lobbier, noe som tillot en backend trunk til det interne bedriftsnettet. I dette tilfellet ble det utnyttet en av over 200 rom der tilgang til IP-telefoni gjorde slik at det ble mulig å få koble til datasenteret gjennom VoIP-hoppet. Etter at testmaskinen hadde fått en IP-adresse som tilhørte Voice VLAN-et, så har den dermed tilgang til intern-nettet fordi det ikke var noen brannmurer som skilte Voice VLAN-et fra de andre VLAN-ene. Det var dermed mulig å få administratortilgang til flere ulike servere, så vel som å utføre andre angrep mot IP-telefoni nettverket. Hadde noen av disse testene blitt utført av en person med onde hensikter, kunne det ha resultert i tap av data som er kritiske for den daglige driften av bedriftens systemer som for eksempel ulike interne prosjekter og finansielle applikasjoner.

3.6.3 Sikkerhetstiltak

Ved hjelp av å konfigurere de eksterne områdene av VoIP-nettverk slik at de får det høye sikkerhetsnivået de trenger for å forhindre potensielle angrep mot det interne bedriftsnettet. Det altså selvfølgelig viktig å skille mellom

private og offentlige nettene.

Kapittel 4

Angrepsverktøy

I dette kapittelet vil vi beskrive de angrepsverktøyene vi har benyttet oss av under den praktiske utføringen av angrep.

4.1 Yersinia

Yersinia[7] er et nettverksverktøy oppkalt etter bakterien som forårsaket svartedøden. Yersinia er laget for å utnytte svakhetene i ulike nettverksprotokoller. Den utgir seg for å være et solid rammeverk for analysering og testing av implementerte systemer og nettverk. Verktøyet benytter seg av svakheter i det 2. laget i OSI modellen (se punkt 2.2). Dette laget er en av de svakeste delene når det kommer til å forsikre seg om sikkerheten i en organisasjon. I tillegg til dette, er det også et av de vanligst ignorerte lagene, fordi det ikke finnes så mange offentlig implementerte angrep mot dette nivået. Det betyr allikevel ikke at et slikt angrep er mindre farlig enn andre angrep.

Når man tester et angrep med Yersinia så har man mange forskjellige angrep å velge mellom. Det vi har fokusert på er et såkalt "Double nested VLAN attack"(punkt 3.2.1).

Det er noen nettverksprotokoller som er implementert per tidspunkt, og i følge programmets nettside skal det komme flere - uten at noen navn blir nevnt.

Implementerte protokoller[11]:

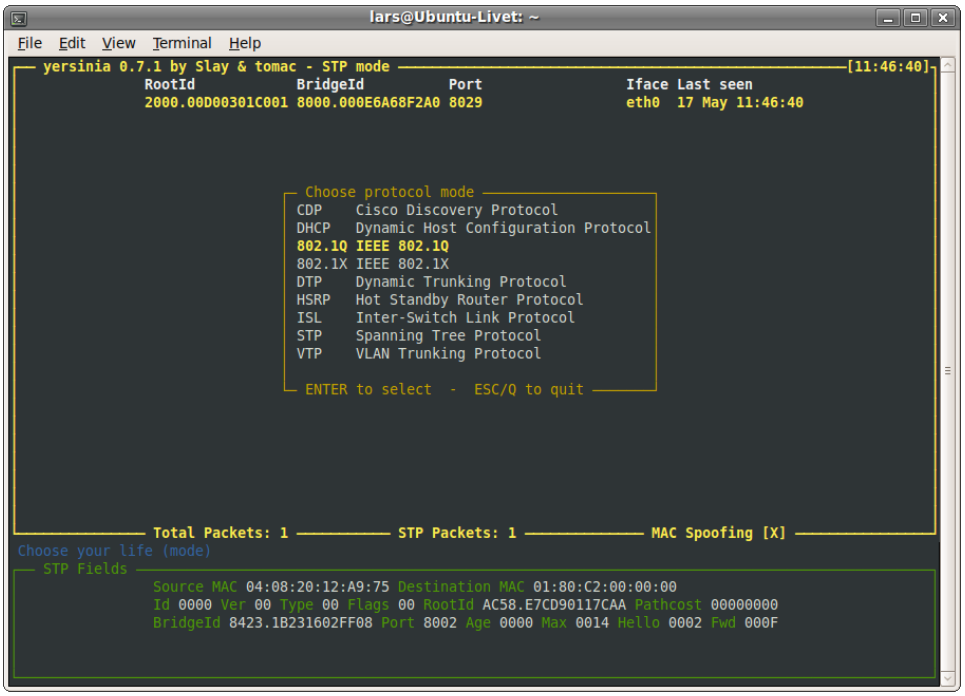
- Spanning Tree Protocol
  - Sending RAW Configuration BPDU
  - Sending RAW TCN BPDU

- DoS sending RAW Configuration BPDU
- DoS sending RAW TCN BPDU
- Claiming Root Role
- Claiming Other Role
- Claiming Root Role dual home (MITM)

- Cisco Discovery Protocol
  - Sending RAW CDP packet
  - DoS flooding CDP neighbors table
  - Setting up a virtual device
- Dynamic Host Configuration Protocol
  - Sending RAW DHCP packet
  - DoS sending DISCOVER packet (exhausting ip pool)
  - Setting up rogue DHCP server
  - DoS sending RELEASE packet (releasing assigned ip)
- Hot Standby Router Protocol
  - Sending RAW HSRP packet
  - Becoming active router
  - Becoming active router (MITM)
- Dynamic Trunking Protocol
  - Sending RAW DTP packet
  - Enabling trunking
- 802.1Q
  - Sending RAW 802.1Q packet
  - Sending double encapsulated 802.1Q packet
  - Sending 802.1Q ARP Poisoning
- 802.1X
  - Sending RAW 802.1X packet
  - Mitm 802.1X with 2 interfaces
- VLAN Trunking Protocol
  - Sending RAW VTP packet
  - Deleting ALL VLANs

- Deleting selected VLAN
- Adding one VLAN
- Catalyst crash

Vi har i dette prosjektet brukt Yersinia til å utføre et VLAN-hopping angrep (kapittel 6.1).



Figur 4.1: *Bilde av Yersinia, hvor man ser de ulike hovedkategoriene*

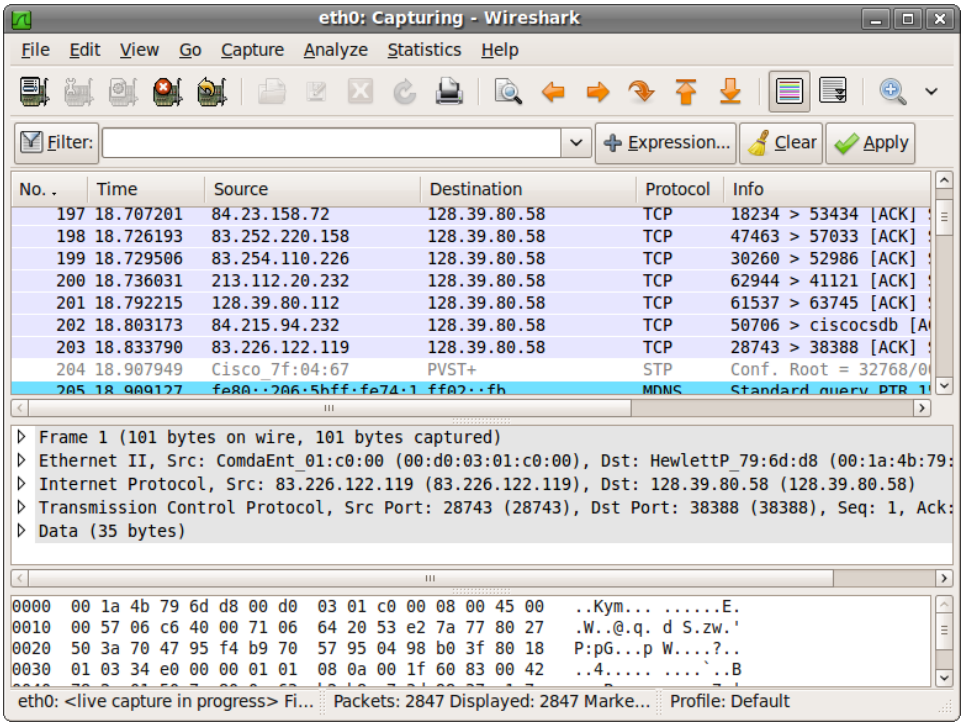
4.2 Wireshark

Wireshark[7] er et nettverksprotokoll analyse program, som blir brukt til nettverksfeilsøking, nettverksanalyse, programvare og protokoll utvikling.

Wireshark sine funksjoner[12]:

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platfrom)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript®, CSV, or plain text

Vi vil bruke Wireshark til å se på nettverkstrafikken hos angriper og offer. Gjennom å se på pakkene sendt fra angriper og pakkene mottatt av offeret, kan vi verifisere om et angrep er vellykket eller ikke.



Figur 4.2: *Bilde av wireshark, man ser her hvordan wireshark fanger opp nettverkspakkene og viser hva dem inneholder*

4.3 Macof

Macof[7] er ett angrepsverktøy som brukes i nettverksangrep. Verktøyet lager mange pakker som inneholder falske MAC adresser. Disse pakkene blir sendt ut på nettverket til switchene og kan skape en state i switchene som kalles for "failopen mode". Dermed er det mulig for en angriper å sniffe pakkene som blir sendt på nettverket. For å starte Macof brukes kommandoen

```
sudo macof -i eth0
```

i linuxterminalen, da sender Macof ut MAC-adresser på nettverket.

Du har også andre konfigurasjonsmuligheter[13] i Macof, blant annet:

- Hvilket interface som skal brukes for å sende ut pakkene.
- Bestemme hvor mange pakker som skal sendes ut.
- Definere mottakerens og avsenders IP adresse.
- Bestemme hvilken macadresse pakkene skal sendes til.
- Definere kilde og målport for pakkene.

Med de forskjellige mulighetene kan man rette et MAC flooding angrep mot et ønsket offer (switch, router, brannmur) i et nettverk.

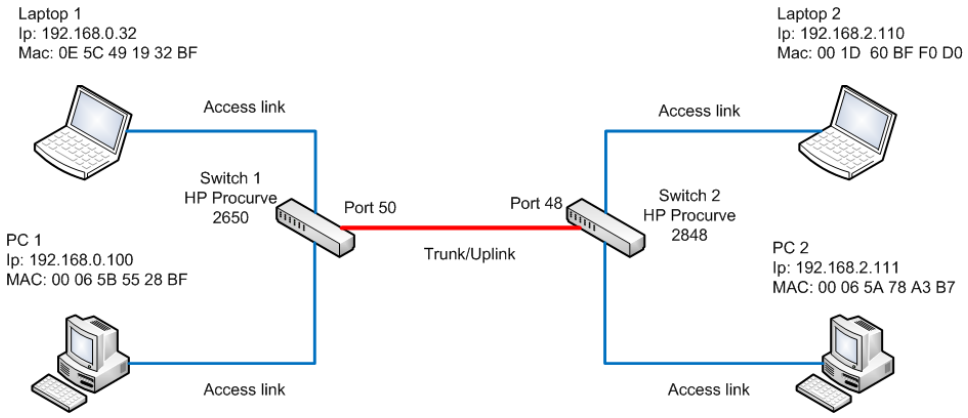
Kapittel 5

Testmiljø

Vi har satt opp et testmiljø for testing av VLAN teknologien og dens sikkerhet. Testmiljøet består av to switcher vi har fått låne av Kongsberg Maritime AS, et par PC-er vi har fått låne av IT-avdelingen på HiG, samt våre egne bærbare PC-er.

Switchene vi har fått låne er en HP Procurve 2650 og en HP Procurve 2848. Begge er lag 3 switcher med mye funksjonalitet. De er forholdsvis like, forskjellen er at 2848 bare har gigabit porter, mens 2650 kun har to gigabit porter for uplink. Derav har 2848 større kapasitet når det gjelder båndbredde.

Under følger en illustrasjon av testmiljøet. Switchenes spesifikasjoner og egenskaper finner du i Vedlegg F[14].



Figur 5.1: *Illustrasjon av testmiljø*

Kapittel 6

Praktisk utføring av angrep

6.1 Double nested VLAN attack

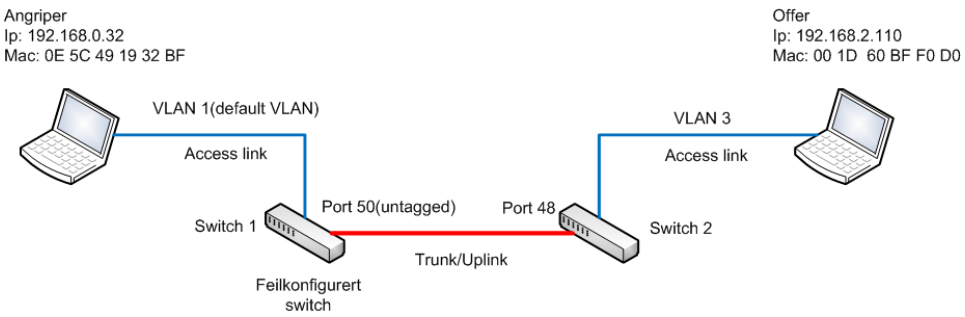
"Double nested VLAN attack"[7] er et angrep som utnytter svakheter i switcher utstyrt med 802.1Q standarden (VLAN). Det fungerer ved at en angriper sender en dobbel-tagget ethernet-pakke (se del 3.2) til en switch. Denne switchen må være feilkonfigurert, slik at uplink porten står som untagged i default VLAN. Offeret må være koblet til en annen switchen, denne trenger ikkenødvendigvis å være feilkonfigurert, siden feilen bare trenger å være på switchen angrepet blir utført fra. Dette gjør at man kan sende pakker fra ett VLAN til ett annet, som man egentlig ikke har tilgang til. Det er dermed mulig å sende ondsinnet programvare til offer-maskinen på det andre VLAN-et på den andre switchen. Det er viktig og presisere at dette angrepet kun får sendt pakker med enveis kommunikasjon, slik at det bare kan brukes til å få sendt ondsinnet kode til offeret.

6.1.1 Forutsetninger for et vellykket angrep

For å kunne utføre dette angrepet må angriperen vite enten MAC- eller IP-addressen til offeret. Uplink porten i default VLAN på angrepsswitchen må være i en untagged modus. Offeret må være på en annen switch og i ett annet VLAN. Switchen som offeret er koblet til trenger ikke å være feilkonfigurert.

6.1.2 Gjennomføring av angrepet

Figur 6.1 viser at angriperen er koblet til VLAN 1: Default VLAN på switch 1 i IP-range 192.168.0.xxx. Offerets maskin er koblet i VLAN 3 på switch 2 i IP-range 192.168.2.xxx.



Figur 6.1: *Testoppsett for double nested VLAN attack*

6.1.3 Switchkonfigurasjoner

Forklaring på uttrykkene i switch konfigurasjonene[15]:

- Untagged porter betyr at portene er medldem av VLAN-et som access porter, altså porter som kobles til arbeidsstasjoner.
- Tagged porter er uplink/trunk porter som brukes som linker mellom forskjellig nettverksutstyr.
- No untagged er et uttrykk som brukes kun i Default VLAN, og betyr at portene ikke er medlem i dette VLAN-et.

Switchene kjørte med følgende oppsett:

Switch 1 HP Procuve 2650
Running configuration:
J4899B Configuration Editor Created on release H.10.74
hostname “ProCurve Switch 2650”
mirror-port 5
ip routing
snmp-server community “public” Unrestricted

VLAN 1
    name “DEFAULT-VLAN”
    untagged 1-16,49-50
    ip address 192.168.0.10 255.255.255.0
    no untagged 17-48
    exit
VLAN 2
    name “VLAN2”

untagged 17-32
ip address 192.168.1.10 255.255.255.0
tagged 50
exit
VLAN 3
name “VLAN3”
untagged 33-48
ip address 192.168.2.10 255.255.255.0
tagged 50
exit

password manager

I konfigurasjonen av switch 1 over, ser man at VLAN 1: Default VLAN har en feilkonfigurasjon. Port 50 står som untagged, altså som en vanlig access port selv om dette er trunk porten til switchen. VLAN 1: Default VLAN har standard oppsett, så det er egentlig ikke en feilkonfigurasjon, men mer at man har glemt å endre på det. Dette er alt som skal til for at angrepet kan lykkes.

Switch 2 HP Procurve 2848
Running configuration:
J4904A Configuration Editor; Created on release I.10.43
hostname “ProCurve Switch 2848”
ip default-gateway 192.168.1.100
snmp-server community “public”Unrestricted

VLAN 1
name “DEFAULT-VLAN”
untagged 1-16,46-47
ip address 192.168.0.11 255.255.255.0
tagged 48
no untagged 17-45
exit
VLAN 2
name “VLAN2”
untagged 17-32
ip address 192.168.1.11 255.255.255.0
tagged 48
exit
VLAN 3
name “VLAN3”

```
untagged 33-45
ip address 192.168.2.11 255.255.255.0
tagged 48
exit
```

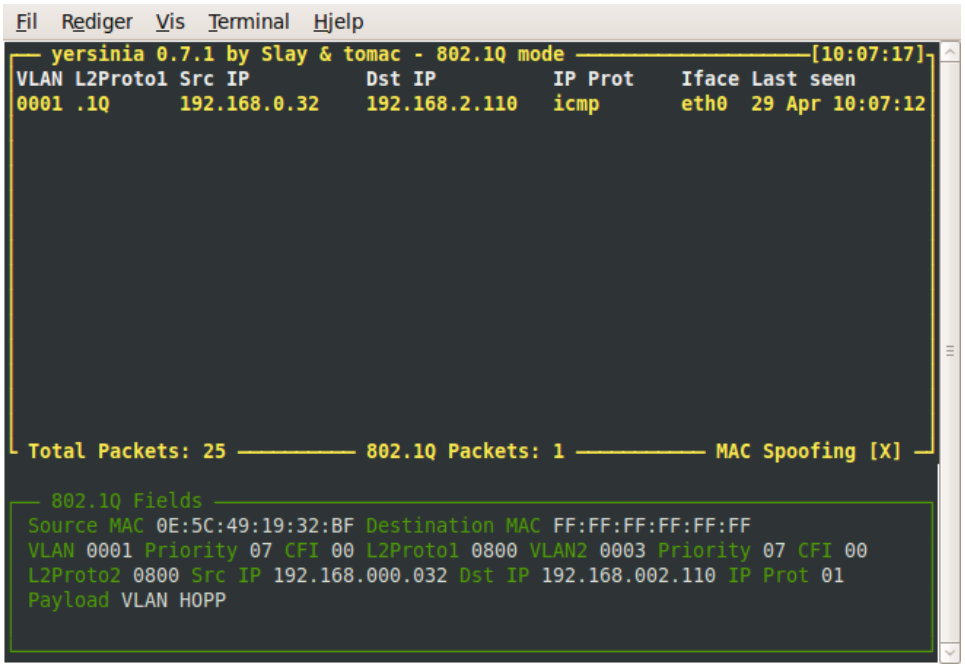
password manager

Over ser man oppsettet på switch 2. Denne kjører med korrekt oppsett ved at port 48, som i dette tilfellet er trunk porten, er tagged i alle VLAN.

Neste steg blir å lage en dobbel tagged ethernet pakke, til det bruker vi Yersinia. Vi forsøkte å utføre angrepet på to forskjellige måter; en der vi visste IP-adressen til offeret og en der vi visste MAC-adressen.

6.1.4 Angrep med kjent IP

Først testet vi angrep der vi vet IP-adressen til offeret. Vi bruker da yersinia til å lage en dobbel tagged ethernet pakke. Første tagg har VID 1 og andre tagg har VID 3. Vi hopper fra VLAN 1 på switch 1 til VLAN 3 på switch 2 som i utgangspunktet skal være umulig. Offeret har IP 192.168.2.110, denne skal vi nå med payloaden VLAN HOPP.



Figur 6.2: *Her vises yersinia oppsettet der vi vet IP adressen til offeret og sender med payloaden ´´VLAN HOPP"*

Pakken som Yersinia generer, er en ethernet pakke med to 802.1Q tagger.

Destination MAC	Source MAC	IEEE 802.1q Tagg 1 med VID 1	IEEE 802.1q Tagg 2 med VID 3	Ethernet type	Data	FCS

Figur 6.3: *Pakken som blir sendt fra angriper til switch 1 med to VLAN tagger*

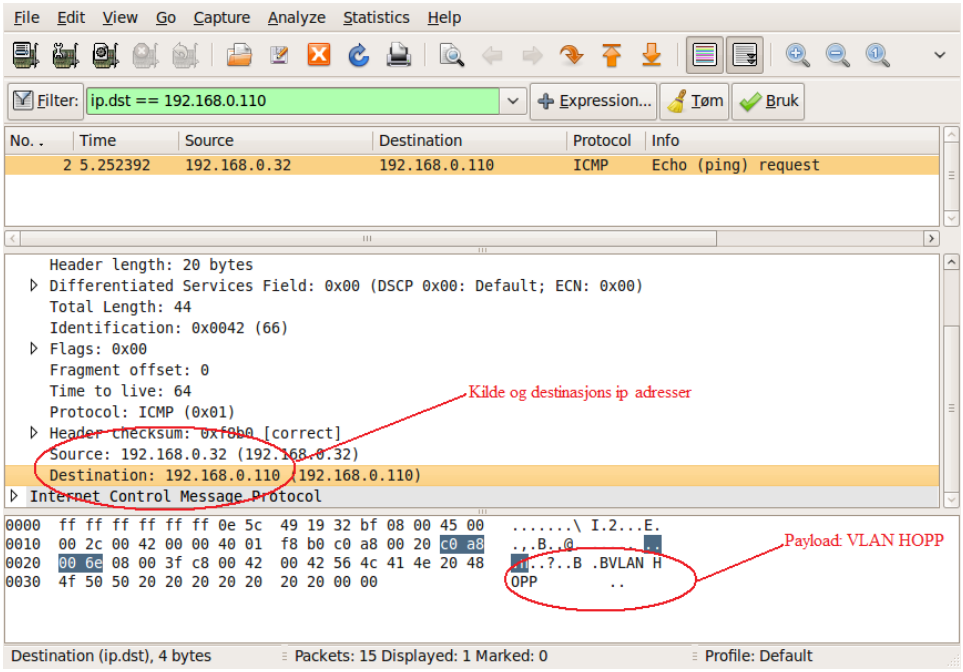
Destination MAC	Source MAC	IEEE 802.1q Tagg 2 med VID 3	Ethernet type	Data	FCS

Figur 6.4: *Pakken da den kommer frem til switch 2, Tagg 1 er da fjernet pga feilkonfigurasjonen i switch 1*

Destination MAC	Source MAC	Ethernet type	Data	FCS

Figur 6.5: *Pakken som kommer frem til offeret ser da ut som en helt vanlig ethernet pakke, siden switch 2 mottar pakken som vist i figur 6.4 og fjerner siste VLAN tagg før den sendes ut til mottaker*

På offerets maskin kjører vi Wireshark for å overvåke all nettverkstrafikk.

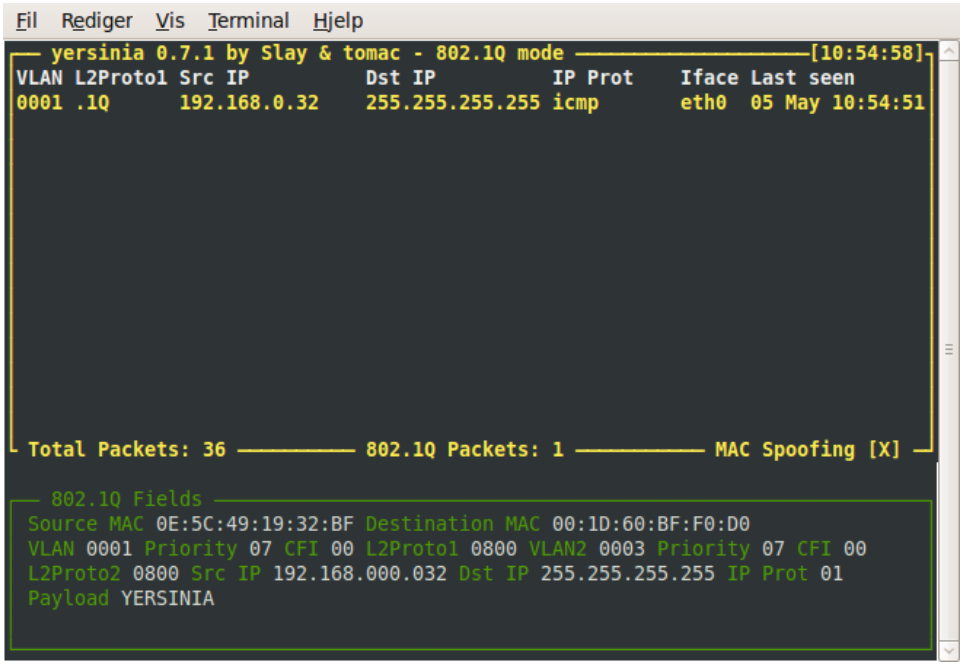


Figur 6.6: *Pakken vi mottok på offeret viser at pakken er sendt fra angriperen med payloaden VLAN HOPP*

Dette viser at angrepet med kjent IP var vellykket.

6.1.5 Angrep med kjent MAC-adresse

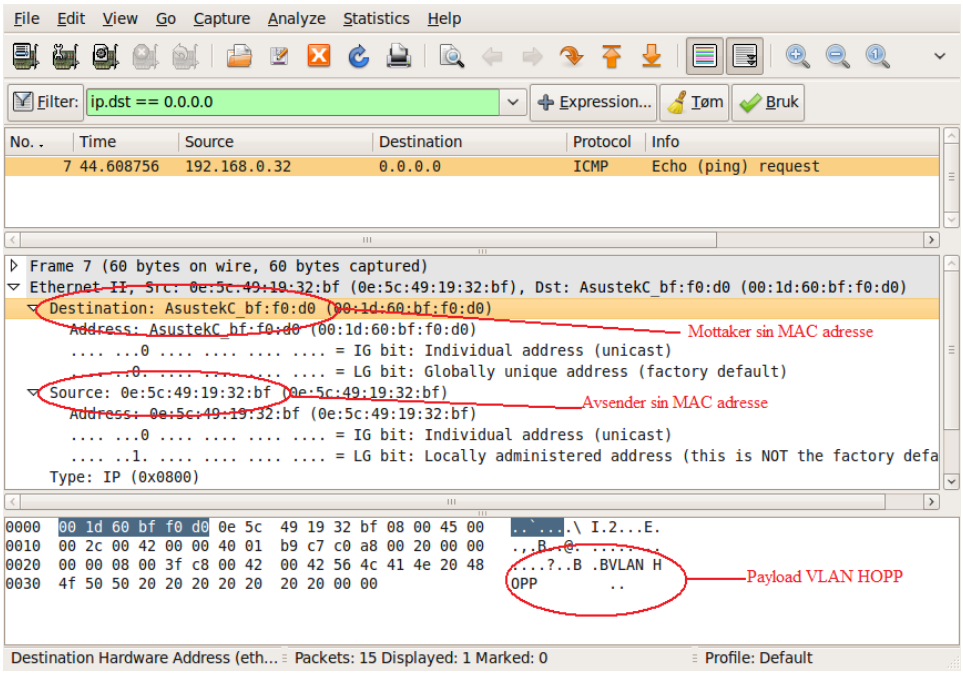
Neste steg er å teste samme angrepet der vi kjenner til MAC-adressen til offeret i steden for IP-adressen. Fremgangsmåten blir akkurat den samme bare at her fyller vi inn MAC-adressen til offeret i stedet for IP-adressen.



Figur 6.7: *Yersinia oppsett der vi vet MAC-adressen til offeret*

Den dobbelt taggede pakken vil i angrepet med kjent MAC oppføre seg likt som pakken i angrepet med kjent IP. Se derfor figur 6.3 til 6.5 for forløpet til pakken.

På offeret kjører vi som før wireshark for å overvåke nettverkstraffiken på offeret.



Figur 6.8: *Pakken vi mottar på offeret viser at VLAN hoppingen er vellykket med kjent MAC-adresse*

6.1.6 Hvordan forhindre angrepet

Alt man trenger å endre for å forhindre dette angrepet er å tagge port 50 på switch 1 i VLAN 1: Default VLAN. Konfigurasjonen blir dermed følgende:

Running configuration: (Korrekt konfigurert):
J4899B Configuration Editor; Created on release H.10.74
hostname ProCurve Switch 2650”
mirror-port 5
ip routing
snmp-server community “public”Unrestricted

VLAN 1
name “DEFAULT-VLAN”
untagged 1-16,49
ip address 192.168.0.10 255.255.255.0

```
        tagged 50
        no untagged 17-48
        exit
VLAN 2
        name “VLAN2”
        untagged 17-32
        ip address 192.168.1.10 255.255.255.0
        tagged 50
        exit
VLAN 3
        name “VLAN3”
        untagged 33-48
        ip address 192.168.2.10 255.255.255.0
        tagged 50
        exit
```

password manager

Med dette oppsettet vil ikke switchen lenger fjerne første tagg i ethernet pakken når den kommer inn på VLAN 1: Default VLAN. Dette fordi port 50 nå er tagged i VLAN1: Default VLAN. Double nested VLAN attack vil ikke lengre kunne lykkes.

Alt i alt viser dette hvor lite feilkonfigurasjon som skal til for at et Double nested VLAN attack skal vellykkes, og at det i utgangspunktet heller ikke er feilkonfigurasjon, men standard oppsett levert fra leverandør. Dette belyser bare hvor viktig det er å ha gode rutiner på utrulling av nytt utstyr, ikke bare koble en ny ukonfigurert switch til nettverket uten å sikre den.

6.2 MAC-flodding

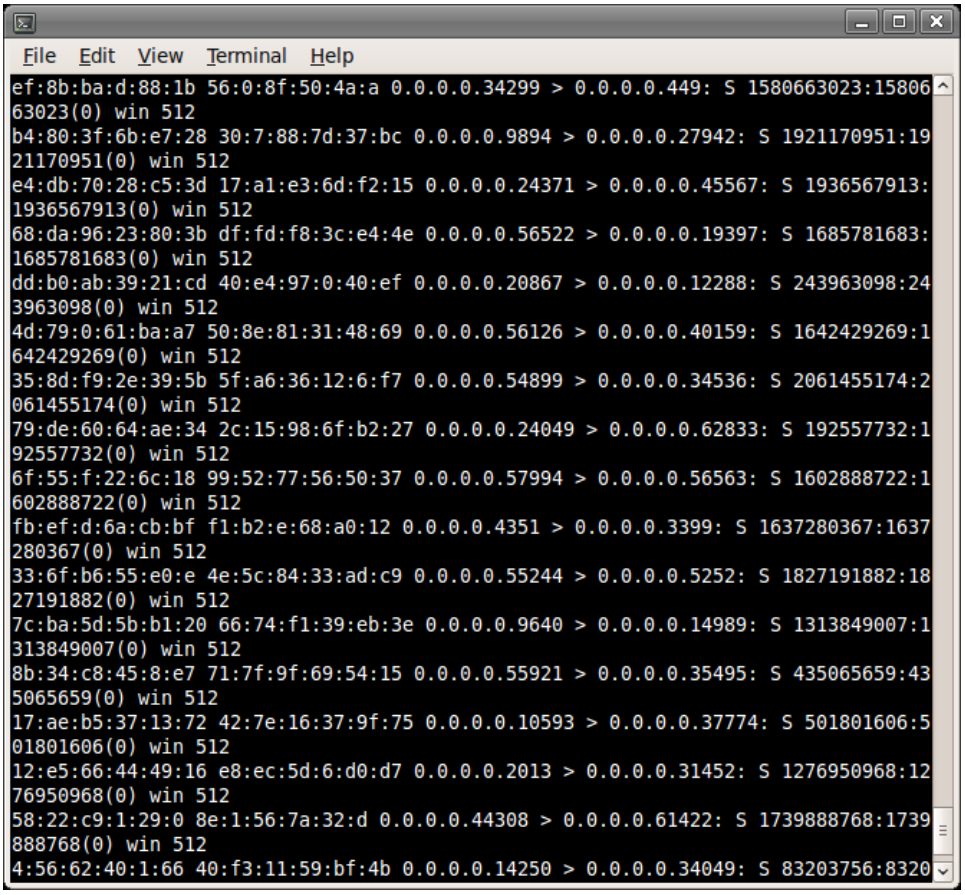
MAC-flodding er et angrep som utføres ved at det sendes mange pakker som inneholder falske MAC-adresser. Disse pakkene sendes til den tilkoblede switchen. Dette gjøres fordi vi ønsker å fylle opp minnet som translation table. Noe som gjør at switchen forhåpentligvis går i en “failopen mode”.

6.2.1 Forutsetninger for vellykket angrep

For å kunne utføre dette angrepet trenger man kun å være tilkoblet en switch som også har andre klienter tilkoblet til seg igjen.

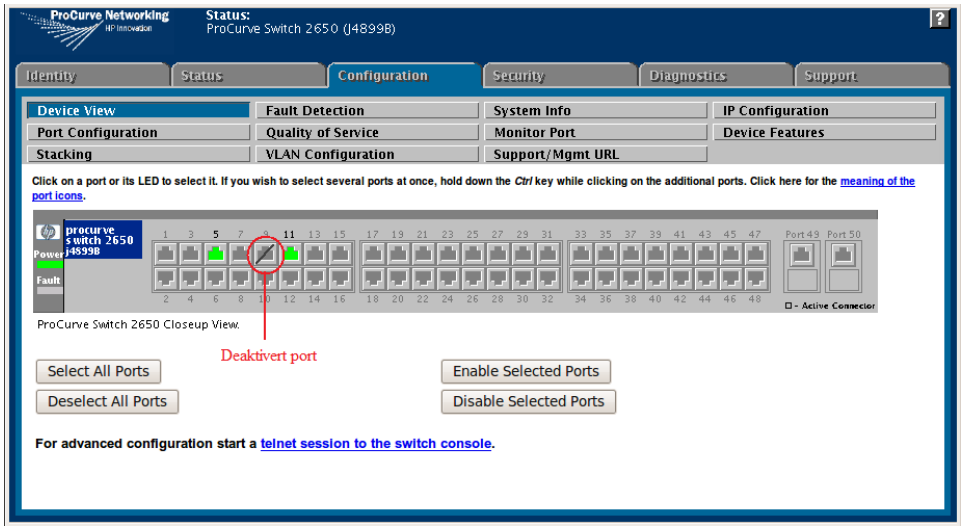
Vi ønsker å ha flere klienter tilkoblet switchen, slik at når den går i “failopen

mode" kan angriper fange opp trafikk mellom andre klienter.



Figur 6.9: *Falske MAC-adresser blir massesendt til switchen*

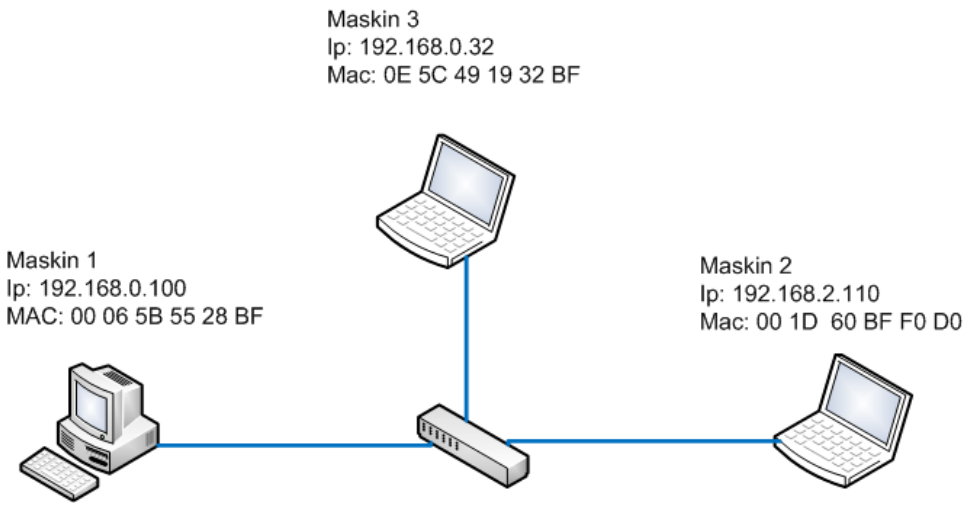
I Procurve Switchene må "Port Security" være avslått. Dersom denne er på og MAC-flodding angrep blir utført(Figur 6.9), vil porten som angrepsmaskinen er koblet til automatisk bli deaktivert(Figur 6.10). Siden funksjonen "Port Security" ikke er aktivert ved standard konfigurasjon, kan dette angrepet skape problemer på nettverket.



Figur 6.10: *Port 9 etter at den har blitt automatisk deaktivert på switchen*

6.2.2 Switchkonfigurasjoner

Switchene har vært konfigurert på samme måte som ved utføring av VLAN-hopping.



Figur 6.11: *Testoppsettet ved utføring av MAC flooding angrepet*

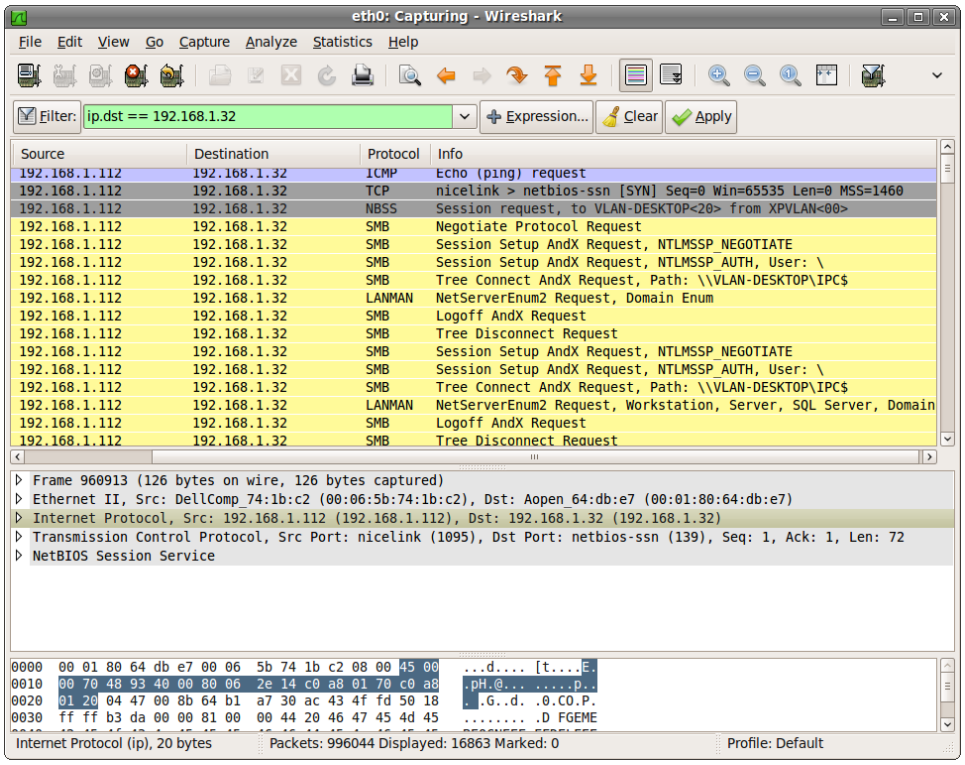
6.2.3 Utføring av angrep

Når vi utførte angrepet hadde vi tre maskiner koblet til den ene switchen (Figur 6.11). De to første maskinene (A og B) brukte vi til å kommunisere med hverandre. Dette gjorde vi ved hjelp at Maskin A kontinuerlig pinget Maskin B. Den tredje maskinen, Maskin C, stod på "utsiden" og lyttet etter meldinger som gikk over nettverket mellom Maskin A og Maskin B.

Vi installerte Macof (Del 4.3) og startet å oversvømme CAM-tabellen.

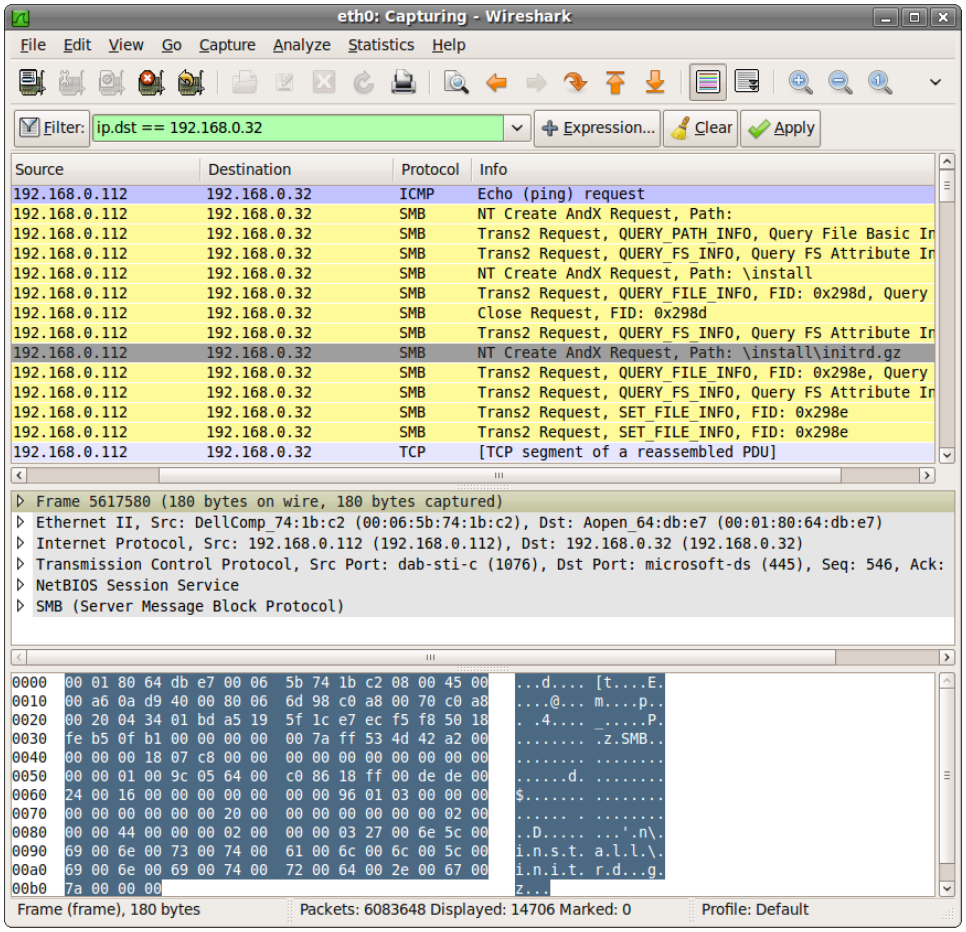
Da dette programmet hadde startet, ble switchen's CAM-tabell til slutt oversvømt av falske MAC-adresser. Ved kun å gjør dette, skjedde det ingen ting. Siden vi da trodde angrepet var mislykket, koblet vi fra Maskin B som vi pinget mot. Det som så skjedde var at Wireshark begynte å fange opp ping-requests opprinnelig ment for Maskin B som vi nå hadde koblet fra nettverket. Vi koblet denne raskt tilbake på nettverket og fikk fortsatt inn ping-requestene på Maskin C.

Vi kunne nå se fra Maskin C, ved hjelp av Wireshark, at Maskin A prøvde å koble seg til Maskin B sine delte mapper. Wireshark snappet opp en "Session request" som gikk fra Maskin A til Maskin B (Figur 6.12).



Figur 6.12: *Pakkesniffing ved bruk av Wireshark 1*

Når vi testet med å sende ulike filer fra Maskin A til Maskin B så ble dataen sendt på vanlig måte fra Maskin A, men det som var spesielt nå var at Maskin C kunne overvåke alt som skjedde inn mot Maskin B (Figur 6.13). Dataene fra Maskin A blir sendt til switchen som videre sender det ut til alle portene på nettverket.



Figur 6.13: *Pakkesniffing ved bruk av Wireshark 2*

Vi sendte en mappe som het "install" over fra Maskin A til Maskin B. Som vist i Figur 6.13 ser man på linje 5 i oversikten at Maskin A ber om å få sende denne mappen over til Maskin B. Under har vi merket av en linje i grått som viser at Maskin A også har bedt om å sende over en fil ved navn initrd.gz som hører til i install-mappen.

6.2.4 MAC-flooding over ulike VLAN

Nå som vi har testet MAC-flooding på et og samme nettverk, fant vi det naturlig å teste det samme over forskjellige VLAN. Utførelsen var stort sett den samme, bortsett fra at Maskin C var koblet til VLAN2, mens Maskinene A og B var koblet til VLAN3. Testen viste at MAC-floodingen blir isolert i det VLAN-et det blir utført i. Vi kan dermed konkludere med at sikkerheten mellom VLAN ikke blir påvirket av angrepet.

6.2.5 Forhindre MAC-flooding

For å forhindre MAC-flooding har HP (og andre produsenter) implementert en funksjon som lar deg bestemme hvor mange MAC-adresser som kan sendes til en port på switchen over en gitt tid. Hvis denne grensen overskrides vil porten bli deaktivert og ubrukelig frem til en systemadministrator aktiverer den igjen.

Det bør være tillatt å undersøke MAC-adressene til alle portene. Dersom dette ikke er tillatt, bør switchen lære seg visse MAC-adresser per port.

Smart CAM-tabell bør implementeres, slik at man:

1. Bare gir “time-out” til inaktive oppføringer
2. Aldri overskriver eksisterende oppføringer.
3. Aldri overskrive aktive verter.

Kapittel 7

Best Practices

I dette kapittelet vil vi ta for oss tips og råd ved bruk av VLAN, både våre egne, i form av en "best practises" sjekkliste, samt datatilsynets anbefalinger.

7.1 Oppsett/drift av VLAN

Den største faren ved bruk av VLAN er den som konfigurerer og kobler opp, derfor er den menneskelige faktoren den største trusselen mot sikkerheten i VLAN. En ukonfigurert switch har standard oppsett som er usikkert, hvis man kobler inn en switch før man har konfigurert den, utgjør det en sikkerhetstrussel. Også patching kan utgjøre en stor risiko om porter på switcher ikke er logisk inndelt i VLAN, og/eller ikke er godt nok merket. Det vil da være veldig lett å koble en port feil, slik at for eksempel et offentlig gjestenett får tilgang til servernettet eller et annet sensitivt nett. Det er derfor veldig viktig at man er nøye med rutiner og dokumentasjon, nettopp for å unngå slike feil. Under følger en liste over tips på oppsett og drift av VLAN:

- Bruk logiske inndelinger av porter til VLAN, bruk derfor porter som utgjør en fysisk port gruppe eller rekke. Husk god merking og dokumentasjon.
- Unngå å bruke VLAN1: Default VLAN. Hvis det må brukes, husk å fjerne trunk linker som untagged i VLAN1, og bytt default VLAN til en annen VID enn 1.
- Aldri sett inn en ukonfigurert switch i et nettverk. En ukonfigurert switch kan være sårbar for ulike angrep med standard innstillinger. Det er derfor viktig med gode rutiner på utrulling av nytt nettverksutstyr.

- Vær nøye med rutiner på patching.
- Hold dokumentasjon oppdatert til enhver tid.
- Deaktiver alle ubrukte porter og sett dem til et ubrukt VLAN.

7.2 Anbefalinger fra datatilsynet

Datatilsynet[16] har laget en rekke anbefalinger til kommuner som skal etablere god struktur for informasjonssikkerhet i sin bedrift og nettverk. Dette kan også brukes i bedrifter der man skal etablere eller gjennomgå sikkerhetsrutiner ved behandling av sensitive opplysninger. I denne anbefalingen viser Datatilsynet de forskjellige elementene som skal være tilfredstilt etter §13 i personopplysningsloven og §16 i Helseregisterloven.

Det det blir lagt vekt på av datatilsynet i denne anbefalingen er:

- Elektronisk behandling av personopplysninger i virksomhetens informasjonssystem
- Tilkobling av virksomhetens datasystem til eksterne datanett
- Ekstern kommunikasjon - herunder ekstern datakommunikasjon av sensitive personopplysninger

Disse sikkerhetsanbefalingene kan brukes i andre sammenhenger også. For å kunne opprette en god rutine for informasjonssikkerhet på datanivå må man ikke bare konsentrere seg om det tekniske, man må gjøre gode forberedelser før man setter i gang med å sette opp utstyr og implementere maskinvare.

I sin anbefaling har datatilsynet laget punkter som burde følges for å oppnå god sikkerhet. De anbefaler at man setter ansvarsområder, sikkerhetsmål, sikkerhetsstrategi og utfører en risikoanalyse før man begynner med det tekniske. Videre bør man se på ledelsens ansvar, organisering og sikkerhet. Under sikkerhet har de tatt for seg personellsikkerhet, fysisk sikkerhet, systemteknisk sikkerhet, datakommunikasjon og eksempler på tilgangs- og overføringssikkerhet. Det er systemteknisk sikkerhet og datakommunikasjon som er interessant. Systemteknisk sikkerhet gjelder sikring av bedriftens datanettverk. Datatilsynet mener alle tjenester som finnes på nettverket i utgangspunktet skal være utilgjengelige, og informasjon kun skal gis etter behov. For å kunne gjennomføre en inndeling benytter man forskjellige soner ettersom hvilken grad av sensitivitet som skal benyttes i forhold til det man jobber med. En sone etter datatilsynes definisjon er "En sone er de deler av et informasjonssystem som tillates å kommunisere ved datakommunikasjon."[16]

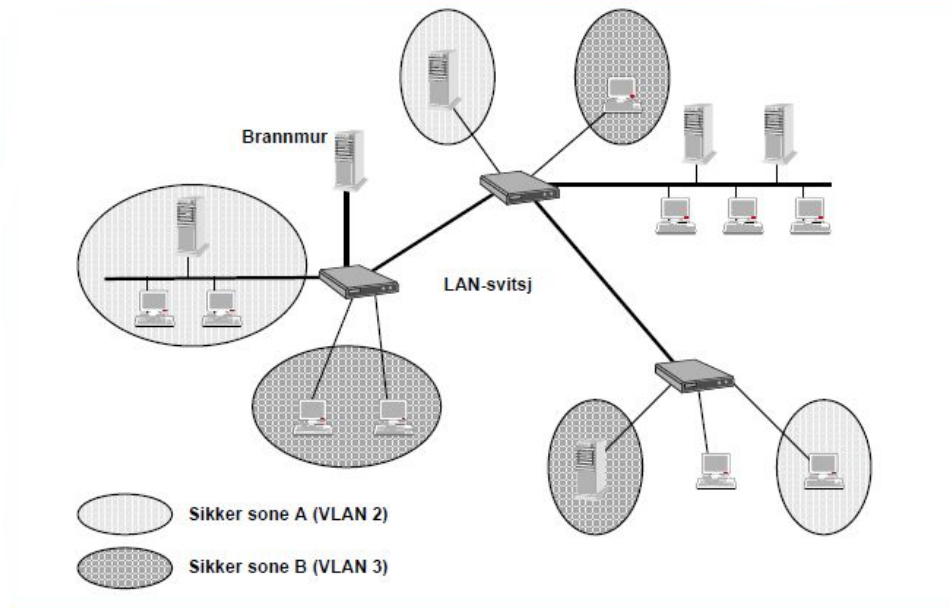
For å dele inn systemer kan det på enklest mulig måte deles inn i to soner. Dette er henholdsvis sikker og intern sone. I den sikrede sonen vil sensitive opplysninger behandles, mens i den interne sonen vil de forskjellige normale bedriftshendelsene utføres. Her kan det også være andre opplysninger som ikke skal komme videre fra den interne sonen. De forskjellige sonene bør være adskilt ved hjelp av brannmurer slik at man får en teknisk sikkerhetsbarriere mellom de forskjellige sonene. Sikkerhetsbarrieren skal inneholde:

- "Nettverkskontroll; som regulerer informasjonsflyten mellom eksternt nettverk og virksomhetens ulike soner, herunder hvilke nettverks- og applikasjonsprotokoller som kan benyttes
- Applikasjonskontroll; som muliggjr kontroll og begrensning på applikasjonsniv med formål : verifisere at det er den tillatte tjenesten som faktisk benyttes hindre at tjenesten benyttes for initiering av aktiviteter som ikke er tillatt og ikke er del av tjenesten selv kontrollere og begrense funksjonaliteten i tjenestene etter behov forhindre utnyttelse av kjente svakheter i tjenestene kontrollere og filtrere ut komplekse datastrukturer slik at datadrevne angrep og tilstedeværelse av ødeleggende program hindres (f.eks. Active X komponenter, viruskontroll) ivareta autentisering og autorisering av brukeren før tjenesten aktiveres
- Redusere virkningen av "denial of service" angrep, det vil si uautorisert utilgjengeliggjøring av tjenester."[16]

Man bør fokusere på å ha et samlet system for å sikre bedriften. Dette gjøres gjennom brannmurer, viruskontroller med mer. Alt dette behøver ikke å ligge på samme maskin eller sted, men samlet bør det utgjøre en sammensatt sikkerhetsbarriere. I tillegg til sikkerhetsbarrierenes alarmer skal bedriften også ha Intrusion Detection Systems (IDS) som generer alarmer ved mistenkelig trafikk over nettverket. Dette skal logges for å kunne gi en eksakt gjengivelse av hendelser, samt gi nettverksansvarlig muligheten til å gjøre sikkerheten bedre på dette området. Slike logger kan også brukes til å gi et estimat om bedriften bør investere i nye og bedre sikkerhetssystemer.

Datatilsynet foreslår også å bruke VLAN for å dele opp det interne nettverket i sikker og usikker sone. Her vil de forskjellige brukerne bli koblet til forskjellige VLAN etter hvilken tilgang de skal ha. Brukeren kan sitte på forskjellige lokasjoner, men være i samme nettverk. Datatilsynet foreslår å bruke brannmurer for å sikre de forskjellige sonene med forskjellig sikkerhetsnivå slik at de områdene som skal være sikker sone er på ett VLAN med en brannmur, mens de som sitter i en intern sone er på et annet VLAN.

De forskjellige innedelingene skal sikre at nettveket:



Figur 7.1: *Bildet viser hvordan Datatilsynet vil bruke VLAN med routing på hver switch for å bygge opp ett Nettverk med forskjellige sikre soner*

- Ikke sender data mellom de forskjellige nettverksnivåene innad i bedriften, eller ut av bedriften.
- Hindre at uønskede applikasjoner kjører på nettverket, og at kun autoriserte har mulighet til å kommunisere med hverandre og ut av bedriten. Det skal forsikres at kun den funksjonaliteten i applikasjoner som brukeren trenger er tilgjengelig, slik at brukeren ikke har tilgang til mer enn det man trenger for å utføre arbeidsoppgavene sine.
- Forhindre at svakheter i nettverket utnyttes av interne og eksterne kilder.
- Redusere virkningen av målrettede angrep slik som DOS angrep.
- Forhindre at uvedkommende endrer tilhørighet i VLAN, lager nye VLAN eller fjerner eksisterende VLAN. Dette oppnås ved å ha en arbeidsplass hvor dette er mulig. Det skal også benyttes identifisering og autentisering på applikasjonen for og vite hvem som har utført hvilke endringer.

Datatilsynet har flere anbefalinger i sitt dokument om anbefalinger for Informasjonssikkerhet. Dette er et kort utdrag av hva vi synes er viktigst og hva datatilsynet mener skal være med når det gjelder informasjonssikkerhet.

Kapittel 8

Risikoanalyse

Utfra oppgavebeskrivelsen kommer det fram at vi skal lage en grundig risikoanalyse av VLAN. I denne analysen har vi ikke tatt med angrep som går mot nettverk generelt, eller VLAN angrep som retter seg mot Cisco. Vi har ikke den nødvendig kunnskapen for å inkludere angrep mot Cisco da vi ikke har testet dette. Generelle angrep mot nettverk er ikke relevant i denne risikoanalysen.

Vi kom fram til 5 forskjellige risikoer, som utgjør en trussel mot VLAN. Hver risiko er satt inn i Figur 9.1, hvor de er evaluert etter lav, middels og høy risiko. Sannsynligheten for de ulike risikoene er tatt på ett generelt grunnlag, da det vil variere fra bedrift til bedrift.

1. VLAN hopping
   Risiko middelslav. For at VLAN hopping skal inntreffe er det veldig mange faktorer som må ligge til rette. Angriperen må være tilkoblet et default VLAN på en usikret switch. I tillegg må angriperen vite offerets VLAN ID og MAC eller IP-adresse. Dermed anser vi sannsynligheten som lav. Konsekvensen derimot, hvis det skulle inntreffe, vil være høy. Angripern kan få sendt ondsinnet kode til offeret. Denne koden kan utføre uønskede handlinger som kan være skadelig for offerets nettverk.

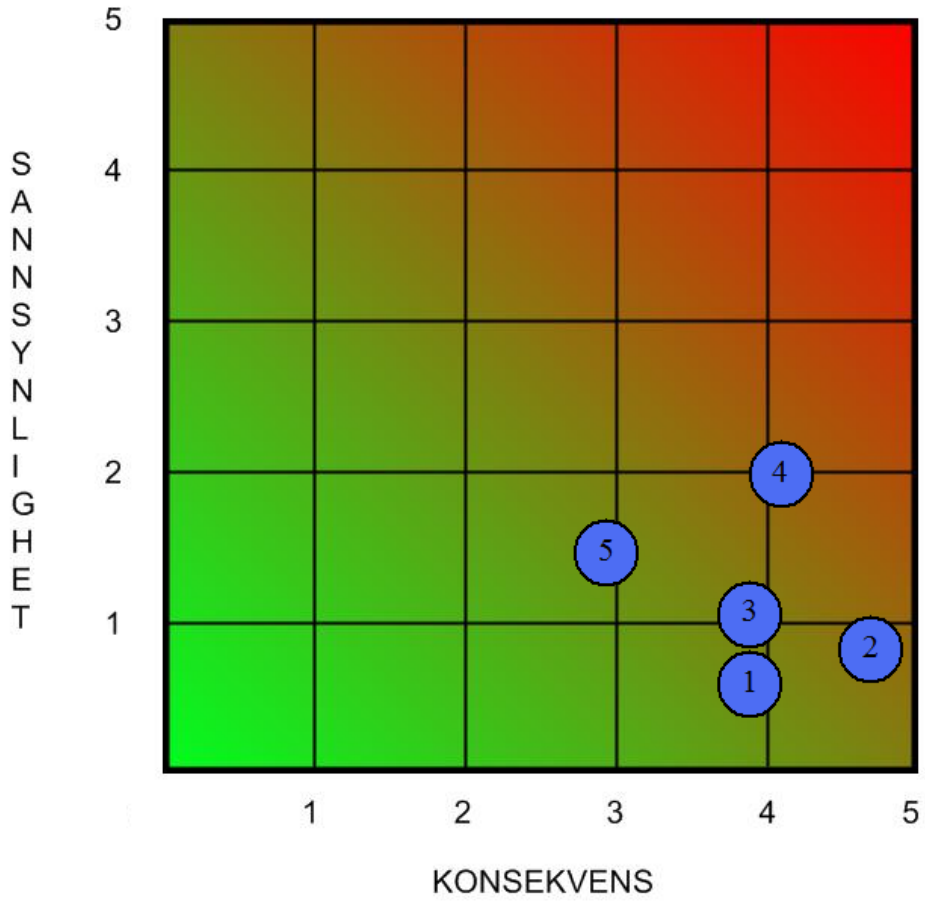
2. Feilkobling
   Risiko middels. Sannsynlighet kommer ann på om dokumentasjonen er oppdatert til enhver tid, og at det er gode rutiner på bruk av dokumentasjon ved patching. Logisk inndeling av porter på switcher, samt merking av disse, er også viktig. Derfor har vi satt sannsynligheten til lav. Om det skulle inntreffer, vil konsekvens være høy. F.eks. kan en port i et gjestenettverk kobles inn et nettverk med sensitive opplysninger.

3. Feilkonfigurasjon
   Risiko middels. Sannsynligheten avhenger av teknisk kompetanse til den som konfigurerer, vi har derfor satt den til lav. Bruk av fagpersonel, leverandører, samt ha dokumentasjon av konfigurasjonen i orden. Konsekvensen er høy siden det gjør nettverket sårbart for angrep av typen VLAN hopping.

4. Ufullstendig dokumentasjon
   Risiko middelshøy. Her er det viktig med gode rutiner, slik at dokumentasjonen alltid er oppdatert. Sannsynligheten for at dokumentasjonen ikke er 100% oppdatert ligger mellom middelslav. Rutiner og dokumentasjon er noe som bare har blitt viktigere de siste årene. IT syndet ofte på dette punktet før, men rammeverk som blant annet ITIL, har rettet fokuset på dette og bidratt til at det har blitt mer og mer integrert i virksomheter. Mangelfull dokumentasjon kan føre til både feilkobling og feilkonfigurasjon. Konsekvensen setter vil derfor bli høy.

5. Mangel på rutiner
   Risiko middelslav. Sannsynligheten for at en virksomhet mangler, eller har dårlige rutiner for alt fra patching, dokumentasjon, installasjon og endring av hardware/software er middelslav. Veldig ofte i virksomheter med mindre IT-avdelinger. Store IT-avdelinger er avhengig av gode rutiner og dermed er det større sjanser for at de har nettopp det. Konsekvensen av mangel på rutiner har vi satt til middelshøy, da det inndirekte kan føre til alle punktene over.

De grønne feltene i risikoanalysen på figuren tilsier lav risiko, de gule feltene tilsier middels risiko, mens det på de røde feltene er høy risiko. Vi har satt inn de 5 punktene fra risikoevalueringen for å få en oversikt over risikoene VLAN teknologien står ovenfor.



Figur 8.1: *Risikoanalyse*

Kapittel 9

Evaluering

9.1 Prosjektevaluering

Ved å kombinere teoretisk dokumentasjon av VLAN teknologien og angrep mot den, sammen med praktisk testing av angrep, har vi på en god måte kvalitetssikret vårt teoretiske arbeid. Vi får resultater vi kan bruke til å trekke en konklusjon basert på egne resultater og ikke på andre sitt arbeid. I prosjektet har vi testet to av angrepene som er funnet. Dermed kan dette brukes til å si at gruppen ikke har en fullstendig analyse av alle sikkerhetstrusler som kan ramme et VLAN. Å foreta en komplett sikkerhetsanalyse av alle kjente angrep er veldig vanskelig, fordi det oppdages nye sårbarheter hele tiden. Derfor valgte gruppen å holde seg til de mest kjente angrepene. Vi kunne tenkt oss å jobbe videre med testing av flere forskjellige angrep for å forbedre resultatene, men dette er ikke mulig på grunn av tidsbegrensningen i prosjektet.

Oppgavebeskrivelsen har gitt oss klare retningslinjer for hva prosjektet skulle inneholde. Disse ble videreført gjennom valget av prosjektmodell og oppgavebeskrivelse. Gruppemedlemmene har samarbeidet i andre prosjekter tidligere og det var derfor uproblematisk å fordele roller internt i gruppen. Gruppemedlemmene har hatt nytte av reglementet når det gjelder å løse saker til alles beste.

I prosjektperioden har gruppen hatt jevnlig kontakt med veileder for å få tilbakemeldinger på arbeidet vi har utført. Oppdragsgiver har også vært tilstedet for å gi oss informasjon når vi har kommet til utfordringer der vi trengte deres hjelp. Vi er under den oppfatning at de har tatt oss seriøst når vi har hatt spørsmål og vi har fått svar på det vi har spurt om. De har også vært meget hjelpsomme med teknisk utstyr og litteratur.

9.1.1 Evaluering av testede verktøy

I denne seksjonen evaluerer vi verktøyene benyttet under testingen. Evalueringen er satt opp i henhold til rekkefølgen det er brukt under testingen. Alle resultater og vurderinger i denne delen er basert på erfaringer med verktøyene gjort i kapittel 6.

9.1.2 Yersinia

Dette er et fint angrepsverktøy for penetrasjonstesting av sikkerhetsmekanismer i nettverk. Yersinia gjør det veldig enkelt å konstruere nettverkspakker for utføring av angrep, slik at man slipper å skrive programmer for å konstruere disse. Ulempen med Yersinia er at det er noe uoversiktelig og rotete i bruk. En annen ting er at Yersinia, på samme måte som Wireshark, må kjøres som root(administrator).

9.1.3 Wireshark

Wireshark er et generelt bra og kostnadsfritt verktøy som er veldig utbredt i akademiske miljøer. Wireshark hadde all funksjonalitet vi trengte for å dokumentere angrep i dette prosjektet. Eneste ulempen vi fant ved bruk av Wireshark er at man i Linux må kjøre det som root(Administrator).

9.1.4 Macof

Macof har kun én oppgave, det er å sende ut mest mulig MAC adresser på kort tid. Til dette fungerer det bra, men det har mange forbedringspunkter. Det mangler brukergrensesnitt hvor man kan få en bedre oversikt over hvor mange MAC adresser som er sendt og tid brukt til dette. Når det gjelder dette programmet ser vi det som en fordel at det må kjøres som root, slik at vanlige brukere ikke kan starte et angrep da det kun er én kommando som må til for at angrepet utføres.

9.2 Veien videre

Når vi ser de forskjellige switchleverandørene satt opp mot hverandre, er vi av den oppfatning at HP har veldig god hardware i sine switcher. De har allikevel en vei å gå når det gjelder software. HP er nødt til å publisere mer om sine egne produkter. Cisco for eksempel har flere "best practises" rettet mot sine produkter tilgjengelig på sine nettsider. Dette finner vi ikke på

HP sine hjemmesider. Det kan være en oppgave for fremtidige studenter og utvikle et sett med ´´best practises" for forskjellige bedrifter som vurderer å ta i bruk VLAN, eller som allerede bruker VLAN i sine systemer.

Kapittel 10

Konklusjon

Prosjektet har resultert i en grunnleggende innføring i VLAN teknologien og dens muligheter. Vi har kartlagt de mest VLAN relevante angrep gjennom fordypning i teknisk litteratur og praktisk sikkerhetstesting. Her har vi kommet frem til en "best practises" guide med hvordan man bør konfigurere sikre VLAN på switcher.

Vi har kommet frem til at VLAN holder et meget høyt sikkerhetsnivå - dersom det er riktig konfigurert. Det holder ikke at kun VLAN er sikkert, all teknologi rundt må også være satt opp med tanke på sikkerhet. Selv om en switch er konfigurert med et høyt sikkerhetsnivå, hjelper det lite om man har en router eller brannmur som er åpen for sårbarheter.

Datatilsynet godkjenner VLAN som en sikkerhetsbarriere mellom sikre og usikre soner i et kommunalt nettverk, dette er vi enig i utifra vårt arbeid med oppgaven. Det gjør allikevel ikke VLAN 100% sikkert. Det vil alltid være en liten, dog usannsynlig mulighet for et vellykket angrep mot ulike VLAN sikkerhetsmekanismer, da VLAN ikke innebærer fysisk adskilte nettverk. Dermed vil ikke denne sikkerheten være høy nok i nettverk hvor gradert informasjon om militære hemmeligheter/nasjonalsensitive opplysninger er lagret.

Bibliografi

[1] Kongsberg Maritime - Om oss http://www.kongsberg.com/nb-NO/KOG/AboutUs.aspx

[2] Store Norsk Leksikon http://snl.no/datanett/IT

[3] Store Norsk Leksikon http://snl.no/protokoll/IT

[4] Store Norsk Leksikon http://snl.no/datakommunikasjon/IT

[5] Rich Seifert and Jim Edwards. *The All-New Switch Book – The Complete Guide to LAN Switching Technology*, Wiley, Indianapolis, 2nd edition, 2008.

[6] James F. Kurose and Keith W. Ross. *Computer Networking – A top-down approach featuring the internet*, Addison Wesley, 3rd edition, 2005.

[7] Eric Vyncke and Cristopher Paggen. *LAN Switch Security – What Hackers Know About Your Switches*, Cisco Press, Indianapolis, 2008.

[8] IEEE Computer Society. *IEEE Std 802.1Q - 2005*, IEEE, New York, 2006.

[9] SooperTotutorials Nettverksundersøkelse - Karachi http://www.soopertutorials.com/technology/networks/2405-layer-2-security-attacks.html

[10] Jason Ostrom and John Kindervag. *VoIP Hopping: A Method of Testing VoIP security or Voice VLANs*, http://www.securityfocus.com/infocus/1892, 2007.

[11] *Yersinia, angrepsverktøy* http://www.yersinia.net/attacks.htm

[12] *Wireshark, nettverksprotokoll analyse program* http://www.wireshark.org/about.html

[13] *Macof, MAC-floodingsverktøy* http://www.irongeek.com/i.php?page=backtrack-3-man/macof

[14] Procurve HP Procurve
http://www.procurve.com

[15] HP development Company. *Student guide – ProCurve Networking by HP*, HP development Company, 2006.

[16] Datatilsynet *Datatilsynet's Veiledning i informasjonssikkerhet for kommuner og fylker*
http://www.datatilsynet.no/upload%5Ctv202_2005_1.pdf