CHALMERS

Cisco ISE & Networking

UFUK KONKUR

NASSIR SULEIMAN

Examensarbete

Högskoleingenjörsprogrammet för datateknik

CHALMERS TEKNISKA HÖGSKOLA
Institutionen för data- och informationsteknik
Göteborg 2012

Abstract

More mobile and portable devices are brought to work and school every day. This would in a Utopia mean that it requires a greater development of the networks to provide a fair allocation of the rights and privileges for all new connecting devices. Unfortunately this is not the case. The progress in network development is not going as fast as desired. This puts great pressure on the administrators of the networks that is expected to provide equitable access to justice permissions for the different connecting units. Many companies are today seeking is a good ground to stand on when it comes to construction of a network. Simple network structure is preferred by many companies for its administrators to easily get into the system. The work is an evaluation of a system developed by Cisco Systems, which makes it easier for administrators to manage and control network both in terms of safety, allocation out rights and efficiency. There is a network that is built to be efficient both in secure from intrusion and in operation, but also efficient for end users who do not need to setup before connecting to the network. Mainly the work has been performed in Chalmers lab halls but also in adjacent rooms in the Chalmers premises. The performance of the work is a successful design of networks that are both effective and safe dealing with connecting devices in a way that gives them equitable rights to the network. Cisco ISE that is advanced and effective enough to control and manage different kinds out of rights within the network is the solution to Bring Your Own Device.

Sammanfattning

Fler mobila och bärbara enheter tas med till arbetet och skolan varje dag. Detta kräver en större utveckling utav nätverken för att ge en rättvis tilldelning utav rättigheter samt behörigheter för alla nya anslutande enheter. Tyvärr går inte utvecklingen i samma takt som ökningen utav mobila enheter. Detta sätter en stor press på de administratörer för de nätverk som förväntas kunna tilldela rättvis åtkomst med rättvisa behörigheter för de olika anslutande enheterna. Många företag eftersträvar idag en bra grund att stå på i konstruktion av nätverk. Enkel nätverksuppbyggnad är att föredra av många företag för att dess administratörer enkelt skall kunna sätta sig i systemet. Arbetet är en utvärdering av ett system utvecklat utav Cisco Systems som underlättar för administratörer att styra och kontrollera nätverket både sett i säkerhet och drift samt tilldelning utav rättigheter. Det är ett nätverk som är byggt för att vara effektivt både i säkert mot intrång och i drift, men även effektivt för slutanvändare som inte behöver konfigurera innan anslutning till nätverket. Främst har arbetet utförts i Chalmers labbsalar men även i intilliggande rum i Chalmers lokaler. Resultatet vad gäller arbetet är en lyckad konstruktion av nätverk som är både effektivt och säkert som behandlar anslutande enheter på ett sätt som gör att de får rättvisa rättigheter till nätverket. Cisco ISE som är avancerat och effektivt nog för att kontrollera och styra olika typer utav rättigheter inom nätverket är lösningen till Bring Your Own Device.

Nyckelord

Cisco Identity Service Engine (ISE)

Client

Cisco ISE Policy

Nätverkssäkerhet

Accesspunkt

Policy

Slutanvändare

Ändpunkt

Nod

Identifiering

NAC

Conditions

Förord

Denna rapport omfattar 15 högskolepoäng och är en del av examensarbetet i programmet Dataingenjör 180 p vid Chalmers Tekniska Högskola. Rapporten inriktar sig mot framför allt studenter inom samma kunskapsområde och andra tekniska individer, en viss kunskap inom dator, IT och nätverkssäkerhet bör finnas hos läsaren.

Vi skulle vilja tacka dem som har hjälp oss med examensarbetet genom vägledning, problemlösning och uppmuntran. Framförallt vill vi tacka vår handledare Sakib Sistek som har varit till en stor hjälp samt varit en stor uppmuntran.

Innehållsförteckning

Bilaga

Switch konfiguration

Router konfiguration

1. Inledning

1.1 Bakgrund

I dagens samhälle använder vi oss utav stor mängd av elektroniska apparater.
I princip har varje hem/företag datorer eller andra elektroniska apparater. Datorer är ett kraftfullt verktyg som används hos alla för att utföra sina arbetsuppgifter och andra dylikt. Oftast behöver dessa datorer ett typ av nätverk att koppla upp sig på, dels för att surfa eller för att utföra arbetsuppgifter. Att bygga upp ett säkert och fungerande nätverk blir allt mer komplicerad och efterfrågan för detta ökar.

Detta bidrar till att man strukturerar sitt nätverk mer och mer efter behov. I och med att mycket sker via nätverk idag är det viktigt att det är pålitligt och säkert. Många företag är väldigt beroende utav sina nätverk, detta betyder att utveckling, underhåll och drift har större betydelse än tidigare.
Detta examensarbete leder till förbättrade och säkrare nätverk som är mer pålitliga, speciellt för mindre företag som skall konstruera och implementera ett nytt nätverk.

Idag finns det allt mer program som strukturerar och underhåller ett nätverk. Allt mer folk tror att de idag bara räcker med att ha brandvägg på sina routrar för att känna sig säker, fast det är inte fallet i det riktiga då det går att komma förbi brandväggen. Så med andra ord är det många företag som satsar på att ha ett stabilt nätverk där de känner sig säkra och kan lita på både mjuk-/hårdvaran.

1.2 Problem

År 2015 beräknas över 10 miljarder nya trådlösa enheter att användas ute på marknaden. Detta sätter en väldigt stor press på IT administratörer, nätverkstekniker och IT strateger då fler och fler tar med sig sin bärbara enhet för att koppla upp sig på exempelvis jobbet. Problemet är att kunna identifiera personalens enheter för att kunna tilldela dessa de rättvisa behörigheter, samt filtrera ut de obehöriga. Vår idé är att kunna lösa detta problem för administratörer för olika nätverk genom att utvärdera och rekommendera Cisco ISE som är ett kraftfullt system som kan implementeras i ett nätverk samtidigt som nätverket konstrueras men även för ett nätverk som redan finns.

1.3 Syfte

Syftet är att fördjupa sig i den nätverksbaserade delen, få fördjupande kunskaper och färdigheter i nätverksinstallation och i underhåll utav ett nätverk där även olika typer utav säkerheter ingår. Samla kunskap som senare i livet skall kunna användas för nytta. Utveckla erfarenhet utav implementering och konstruktion utav nätverk, kunskap om nätverkssäkerhet och erfarenhet utav drift utav nätverk samt skydd mot intrång och attacker mot nätverket.

1.4 Mål

Målet är att utveckla ett effektivt, säkert och pålitligt nätverk som kan tillfredställa ett mellanstort företags nätverksbehov. Samt att utveckla olika säkerhets/behörighetspolicys till ett nätverk, med hjälp av program som Cisco har utvecklat som kallas Cisco ISE (Identify Service Engine). Med ett mellanstort företag räknar vi på ungefär 2500 personer. Exempelvis skall olika typer utav rättigheter för olika typer utav människor i företaget kunna delas ut. Oerfarna användare utav nätverk skall själva med en bärbar dator kunna koppla upp sig på nätverket utan problem, inga olika typer utav inställningar skall behöva göras utan allt skall ske automatiskt. Detta kommer att testas i en labbmiljö på Chalmers och konfigureras med den arkitektur som behövs för att uppnå förväntningarna. För att uppnå goda resultat krävs en simulerad arbetsplats bestående utav server, arbetsstationer(datorer) samt en flexibel nätverksutrustning. Ett delmål på vägen är ett arrangerat seminarium där framsteg och resultat av arbetet hittills skall presenteras och debatteras.

1.5 Avgränsningar

Nuvarande hårdvara som stödjer Cisco ISE är begränsad till delar av Cisco Systems produkter, och ett fåtal produkter från andra tillverkare. Det gör att vi blir väldigt begränsade hårdvarumässigt i och med att all hårdvara i stort sett måste vara från Cisco Systems. Anledningen till detta är för att Cisco ISE är ganska nytt (ca 6-12 månader gammalt) och har inte nått ut till många andra tillverkare ännu. Att sedan bygga ett nätverk för att sedan implementera vårt system gör att vi också kommer att hålla oss till Cisco Packet Tracer som är ett program där man konstruerar nätverk med Cisco Systems hårdvaror. Allt eftersom tiden går och Cisco ISE etablerar sig mer och mer i marknaden, kommer systemet att bli mer och mer kompatibelt med nätverk som redan finns uppbyggda idag.

2. Teknisk bakgrund

För att kunna skapa en god förståelse som möjligt för vad detta projekt har innebär krävs det en viss bakgrundsinformation om vad Cisco ISE är och varför det används.
Här förklaras det generellt övergripande om hur Cisco ISE har utvecklats, samt hur det fungerar och vad som är nödvändigt.

Annan bakgrundsinformation som kan vara bra att veta är följande begrepp som använts under arbetet:

ACL
ACL står för Access Control List och är en lista gjord för att antingen blockera eller tillåta tillgång till diverse hemsidor eller olika typer utav uppkopplingar.**[31]**

WAN
WAN står för Wide Area Network. Detta är ett datornätverk för global kommunikation mellan nätverk där det är större avstånd mellan såsom nätverk i olika städer och länder. Med hjälp av WAN kan man koppla ihop LAN och andra olika typer utav nätverk**[32]**.

NAT
Network Address Translation används för nätadressöversättning. Med hjälp av denna teknik blir det möjligt att ansluta flera datorer till en internetanslutning via få gemensamma IP-adresser **[33]**.

VPN
Virtual Private Network är en typ utav säkrare nätverk. VPN kan implementeras i ett större nätverk för att öka säkerheten på nätverket. Det man då ser är i tekniska termer link layer protokollet. Trafiken blir väldigt mycket svårare att läsas av utav obehöriga och VPN är med andra ord en teknik för att använda publika nätverk på ett säkrare sätt**[34]**.

VLSM
Variable-length Subnet masking tillåter så att vi kan dela upp nätverk i olika stora subnät. Man kan ge olika många IP-adresser åt de olika subnäten för det som behovet skulle kräva**[35]**.

DHCP
Dynamic Host Configuration Protocol är ett nätverksprotokoll som används för att kunna tilldela enheter som ansluter en automatisk IP-adress. Varje gång man kopplar bort sig och

kopplar upp sig igen på nätverket så får man en ny ifall den man hade tidigare är upptagen av en annan enhet.**[17]**

VLAN
Virtual Local Area Network är en teknik som används för att dela in grupper/enheter I olika ”nät”. VLAN har samma attribut som ett fysiskt LAN men det tillåter att slutanvändaren kan bli grupperad tillsammans med en annan enhet även om de inte är kopplade till samma switch**[36]**.

WLAN
Wireless Local Area Network är ett trådlöst nätverk. Allt såsom uppkoppling, och all annan kommunikation sker trådlöst. Vad som krävs för detta är att enheten som vill ansluta till ett WLAN måste vara utrustad med ett trådlöst nätverkskort. Det som krävs från nätverket är att det måste vara utrustat med en trådlös Accesspunkt. Kommunikationen som sker trådlöst sker via radio eller mikrovågor. Dessa är dock inte farliga för hälsan. Att tänka på när man bygger ett trådlöst nätverk är att ha tillräckligt många accesspunkter för att alla enheter inte skall vara kopplade till samma accesspunkt. Därefter är det viktigt att de olika accesspunkterna kör på olika kanaler för att de inte skall störa ut varandra**[37]**.

OSPF
Open Shortest Path First är ett protokoll av typen link-state-routing. Med detta protokoll räknas den kortaste vägen ut på nätverket från källan till destinationen och den vägen tas oavsett trafik eller kostnad. Den kortaste vägen räknas ut med hjälp utav Dijktras algoritm. Skulle en länk gå ner upptäcker OSPF detta och en ny väg räknas ut så snabbt som möjligt för att dirigera om trafiken**[38]**.

VTP
VLAN Truking Protocol arbetar på lager 2 och hanterar tillägg, borttagning, namnbyte utav VLAN på hela nätverkets basis. Detta minskar administration för att en switch som oftast agerar som VTP Server skickar ut konfigurationerna via trunk portarna till de andra switcharna som agerar som VTP klienter**[39]**.

FR
Frame Relay är en standardiserad WAN teknologi som specificerar det fysiska och logiska lagret med digital kommunikation som använder paket switching**[40]**.

2.1 Definition

Cisco ISE kan tolkas på följande sätt:

Cisco Identity Service Engine är en benämning av ett säkerhetssystem(program) som är ämnat att upprätthålla integriteten för ändpunkter i ett nätverk.

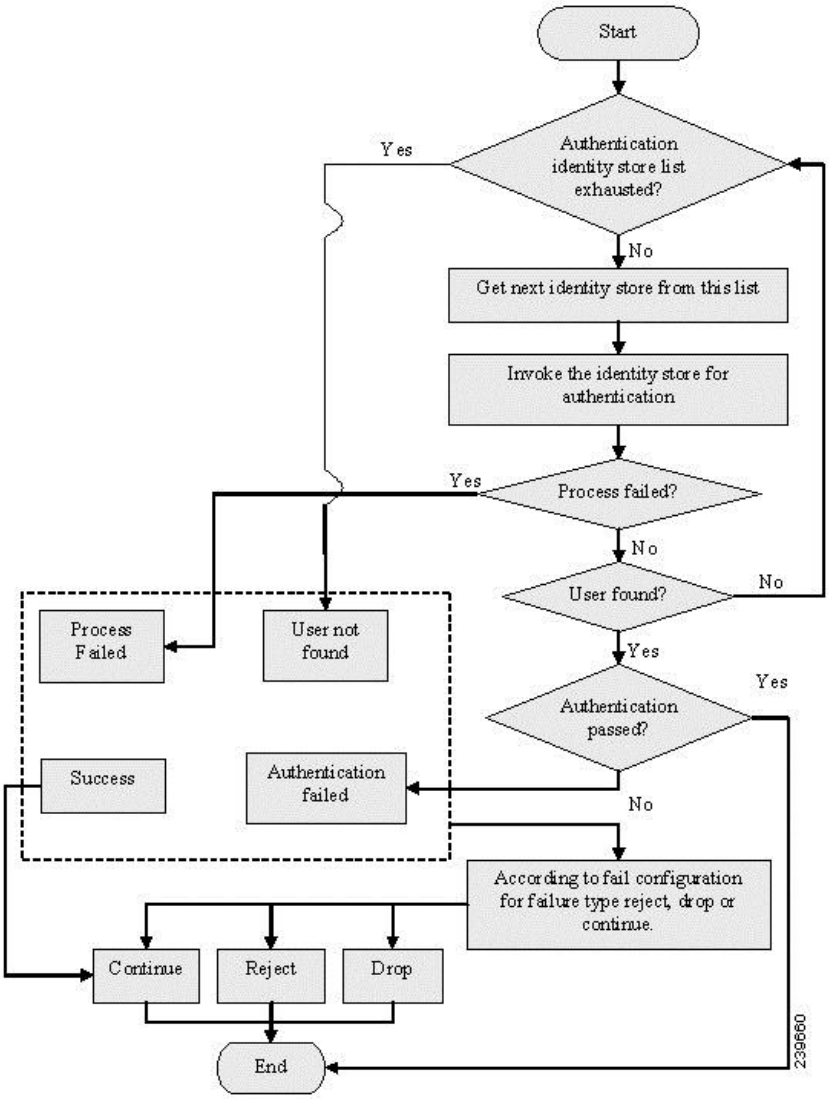
2.2 Tekniken Cisco ISE

I dagens IT samhälle är det flera typer av denna produkt, denna teknik kan användas på två olika sätt. På ena sättet kan du använda tekniken som en fysisk switch där själva programvaran är redan installerad och i stort sätt är det bara att köra en ”plug and play”. På andra sättet kan du installera programvaran på en/flera fysiska datorer som
sedan är ansluten till en vanlig switch. För att kunna utföra det andra sättet så behövs det även en extra fysisk dator som har Vmware installerat.

Vmware är en mjukvara (program) som ger en möjlighet att köra flera virtuella maskiner på en fysisk maskin.**[43]**

Cisco ISE är ett ganska komplett och väldigt avancerat program. Dock är det viktigt att veta hur man skall hantera programmet för att få det mest effektiva nätverket. Det finns ingen användning utav Cisco ISE om man inte är påläst och vet hur man hanterar, skapar, redigerar olika typer utav policys, tillstånd eller ansluta en domän till Cisco ISE. Inte heller har man någon användning utav Cisco ISE om man inte är intresserad utav vem som försöker ansluta sig till nätverket och vem som gör vad på nätverket. Cisco ISE - teknik bör alltså konfigureras efter eget behov för vad som intresserar en på ens nätverk men det kräver också sin kunskap.

Cisco ISE kan jobba efter följande modell som liknar följande figur beroende på hur man konfigurerar:



Figur 18 - Anslutningsprocess

Vissa anslutningsprocesser kan man välja att hoppa över så att de inte körs när en enhet försöker att ansluta. Detta är helt upp till administratorn. För att få ett pålitligt system som är säkert i drift krävs det ganska komplexa konfigurationer och det gäller att verkligen veta vad det är man gör för inställningar. Konfigurerar man blint utan vetskap kan systemet bli väldigt sårbart för attacker och liknande. I och med att det inte finns någon standard teknik för Cisco ISE bör tekniken alltid väljas efter behov eller hur det fungerar hos andra företag man exempelvis arbetar med.

Tekniken bygger på att identifiera enheter ända in till dess MAC-adresser för att kunna lagra dessa i en lista för att i efterhand när enheterna ansluter vid senare tillfälle skall kunna kännas igen och identifiering utav enhet skall gå fortare.

När enheterna får sina rättigheter och policys tilldela utav Cisco ISE baseras grunderna mycket på vad för typ utav enhet det handlar om. Det skiljer sig mycket bland enheterna även om enheterna tillhör samma person. Exempelvis så behövs inte fullständiga rättigheter på en telefon som ansluter sig till nätverket även om den tillhör en som är anställd på företaget där Cisco ISE är implementerat.

2.3 Funktioner Cisco ISE

Det finns viktiga steg i hur Cisco ISE funkar när man ansluter bland annat datorer och skrivare till ett nätverk som styrs av ISE. Men allt eftersom man konfigurerar efter behov ser funktionerna olika ut beroende på vad man väljer att konfigurera efter, men detta avsnitt behandlar de övergripande stegen som kan finnas med i Cisco ISE(när man ansluter en enhet till nätverket).

1. Upptäckt av noder
2. Autentisering
3. Kontroll av nodernas säkerhetslösning
4. Kontroll rätigheter
5. Upprätthållande av policy
6. Karantän
7. Efterkontroll

2.3.1 Upptäckt av noder

Denna funktion/steg må vara den viktigaste då man upptäckter nya enheter i ett nätverk. Det finns flertal olika sätt att detektera noder, bland annat med lager 2 och 3 switchar. De vanligaste metoderna att upptäckta en enhet i ett nätverk är:

- ARP
- DHCP
- SNMP
- IEEE 802.1X
- Hårdvara
- Accesspunkt

ARP
Address Resultion Protocol är en metod som jobbar i nätverkslagret i OSI-modellen (Lager 3). ARP står för Address Resolution Protocol och det handlar om att switchen skall lära sig olika enheters MAC-adresser. Switchen lär sig adresserna genom att läsa av och lagra källans MAC-adress från varje paket som skickas via switchen. Switchen läser även av vilken port som paketet kom ifrån. På det sättet skapar switchen en tabell (MAC-adress tabell) med information om vilken MAC-adress som finns på en viss port.

När switchen väl skapat sin tabell skickas den med informationen till Cisco ISE som i sin tur nu får reda vilken enhet som befinner sig vart och på vilken port.

DHCP
Dynamic Host Configuration Protocol är en metod som används i applikationslagret i OSI modellen (lager 7). När en nod kopplar upp sig på nätverket måste den ha en IP-adress för att kommunicera med resterande i nätverket. När detta sker så skickar noden en så kallad DHCP-förfrågan till DHCP-servern(router) om att få tilldelad en IP-adress. Efter kontroll av status på noden tilldelas den en IP-adress och detta sker hos alla noder som tillkommer till nätverket. När detta sker märker Cisco ISE mjukvaran vad som händer och vet vad som är vad i nätverket. Fördelen med denna typ av system är att det är så lättkontrollerat och noderna får IP-adress automatiskt.**[9]**

SNMP
Simple Network Management Protocol är ett protokoll som används i applikationslagret i OSI modellen(lager 7). Detta protokoll som stöds i de flesta lager 3-switchar kan man via Cisco ISE övervaka och hantera nätverket med hjälp utav TCP/IP. Detta hjälper i sin tur upptäckt utav nya enheter när enheter skickar förfrågan om IP-adress.**[27]**

Hårdvara
Hårdvaror I form av switchar som jobbar på lager 2 och 3 i OSI-modellen upptäcker enheter som försöker att ansluta sig till ett nätverk. Dessa upptäcks genom deras MAC – adresser i och med att switcharna jobbar på de lägre lagren 2 och 3. Switchen samlar även information om på vilken port enheten kopplats in på. Det är det första som händer i en process där en enhet försöker att ansluta sig. Det är först då förfrågan om bland annat IP-adress skickas till servern, men först och främst upptäcks enheten via switchar.

IEEE 802.1X
Är ett protokoll som används för att upptäcka/identifiera nya noder i ett nätverk via switchar, routrar och trådlösa accesspunkter. Detta protokoll används även utanför Cisco ISE för att autentisering av enheter. För noder som inte uppfyller kraven om anslutning av nya noder som sätts av Cisco ISE begränsar den 802.1X-enheter noderna att komma åt nätverket.

Protokollet använder sig utav EAP(Extensible Authentication Protocol) och dessa kommer i olika varianter. En av de vanligaste metoderna att autentisera är(stegvis):

- När en 802.1X-enhet känner av en ny nod nätverket skickar den ut en identifikations-fråga till noden.
- Noden skickar ut EAP-paket över UDP med autentiseringsinformation via enheten som ansluter som sedan skickar den vidare till en RADIUS-Server.
- Nu svarar servern tillbaka en förfrågan till noden om ett lösenord.
- Noden svarar nu på förfrågan och skickar den vidare till RADIUS-Servern
- Om klienten har bifogat rätt information för att autentisera sig skickar RADIUS-Servern ett meddelande till noden om att inloggningen har lyckats.
  [28]

Accesspunkt
En accesspunkt är en enhet som man kan koppla upp sig på trådlöst. Dessa är komplement till trådlösa routrar som är de som ger internet tillgång. Dess uppgift är främst att brygga de radio och mikrovågor som skickas över nätverket. Trådlösa accesspunkter och routrar kör på olika kanaler för att inte störa ut varandra. Därför är det viktigt att även konfigurera dessa så att två accesspunkter som finns nära varandra så att de kör på olika kanaler för att de inte skall störa ut varandra. Fördelen med trådlöst nätverk är främst smidigheten. Nackdelarna är dock fler, säkerheten är inte den högsta, enklare att störa ut ett trådlöst nätverk.**[26]**

2.3.2 Autentisering

Ett system som Cisco ISE bör vara konfigurerat så att det finns möjlighet för alla användare att autentisera sig när de begärs för att ansluta till nätverket. Detta kan göras på flera olika sätt som nämnt tidigare fast de mest använda är:

- DHCP(som förklarad innan)
- IPsec
- VPN
- HTTPS
- IEEE 802.1X(som förklarad innan)

IPsec
Internet Protocol Security, är ett säkerhetsprotokoll som jobbar på nätverkslagret. IPsec används vid autentisering och kryptering av varje IP-paket som skickas över nätverket. IPsec jobbar så effektivt att nästintill alla system kan använda sig utav denna teknik för att autentisera enheter, så med andra ord behöver man även inte strukturera eller bygga om de paket som skickas över nätverket. IPsec är den mest effektiva sättet att begränsa

kommunikationen mellan noder i ett nätverk. Noder som har kopplat upp sig till nätverket och inte har fått godkännande kan med andra ord inte kommunicera med de som har kopplat upp sig och är konstaterade fria från hot mot nätverket. **[18][19]**

VPN

Virutal Private Network, är en säkerhetsåtgärd som mesta dels används av stora nätverk. Företag som har kontor i olika städer har en VPN-uppkoppling genom internet. VPN är en tunnel mellan två platser där allt färdas i ett krypterat och autentiserat sätt. VPN är inte bara för att skapa en tunnel eller säkerhetsåtgärd för ett nätverk utan även för att kunna skapa olika policys med hjälp av att skapa olika grupper.
Ett exempel på detta kan vara att man delar upp ett lokalt nätverk i olika grupper där de har olika åtkomsträttigheter. Cisco ISE kan använda både VPN policyservern och VPN servern för att styra de inkommande anslutningarna.**[21][22]**

HTTPS

Hypertext Transfer Protocol Secure är en teknologi som används på internet. Denna typ av teknologi verifierar om noden/klienten är den dem utger sig att vara i nätverket. Det finns en liknande teknologi som heter HTTP som är i stort sätt samma sak, skillnaden är att HTTPS är en säkrare version som är kombinerad med SSL/TLS.**[23]**

2.3.3 Kontroll av noderna

I detta steg görs bland annat kontroller på den eller de enheter som försöker att ansluta sig till nätverket. Detta kan jämföras ungefär som en liten snabb scanning utav datorerna efter skadlig mjukvara som är eller skulle kunna vara ett hot mot nätverket eller andra slutanvändare på nätverket. Skulle det vara så att enheterna som försöker att ansluta sig till nätverket är skadade eller innehåller skadlig mjukvara som skulle vara skadlig mot nätverket på något sätt, tillåts inte anslutningen att fullbordas och enheterna förlorar sin uppkoppling från nätverket.**[10]**

2.3.4 Kontroll rättigheter

En sak som Cisco ISE utför när den skall identifiera och kommunicera med enheter är att kontrollera nodens mjukvara och hårdvara.Cisco ISE kan med hjälp av identifiering avgöra om en nod skall ha tillgång till nätverket eller inte.
Ett scenario kan vara då en nod skall ansluta till nätverket och inte har den senaste uppdateringen på någon specifik mjukvara får noden inte tillgång till nätverket, tills då åtgärden är utförd och noden försöker ansluta igen.

Detta sker inte bara en gång utan testet utförs kontinuerligt medan noden är ansluten. Denna typ av testning görs hela tiden och informationen jämförs med en policyserver hela tiden för att kontrollera att noden har rättigheten att ansluta till nätverket.
Sedan finns de ytterligare andra tester som Cisco ISE utför för att säkerställa vad noden egentligen är, bland annat testas:

- Vilket typ av operativsystem(OS) noden kör
- Farliga programvaror som kan vara skada för nätverket
- Säkerhetsuppdateringar på t.ex. antivirus, OS
- Om noden har tillgång till nätverket, rättigheter
- Hårdvaruenheten

[24]

2.3.5 Upprätthållande policy

I detta steg har Cisco ISE kommit till den punkt att autentiseringen och verifieringen av noden är genomförd och skall sätta fingret på vad för policys nätverket skall genomdriva. Väldigt övergripande kan man dela upp säkerhetsnivåerna i tre delar:

- full åtkomst(som en administratör, tillgång till allt)
- karantän(som förklaras nedan)
- begränsad åtkomst(som kan redigeras som de önskas efter behov som oftast administratören kan utföra).

Eventuellt kan man även ta hjälp av mjukvaror för att upprätthålla policys, detta kan man göra med hjälp av dessa metoder:

- ACL som står för Access Control List, som innebär att man kan rada upp flera spalter av regler om vad, hur en användare/nod kan blockera eller ge tillgång till nätverket.

- VLAN Virutal Local Area Network är ett sätt att skapa lokala nätverk som har olika typer av rättigheter. Noder kan hamna i olika VLAN som har olika åtkomstmöjligheter till nätverket.

[25]

2.3.6 Karantän

Detta kan ses som en lista som skapas då misstanke om infekterade enheter försöker att ansluta till nätverket. Enheternas MAC-adress lagras i en lista och blockeras från att ansluta till nätverket. När en enhets MAC-adress lagras i karantän brukar administratorn få denna information och därefter vidtar administratorn lämpliga åtgärder för detta.
Detta är en säkerhetsåtgärd som görs för att upprätthålla säkerheten i nätverket. Ifall en enhet hamnar i karantän av systemet och administratorn löst problemet med enheten kan denne tillåta enheten att få begränsad åtkomst till nätverket under tiden alla anslutningssteg gås igenom igen, det vill säga trippel A (Authentication, Authorization, Accounting). Hela Trippel A processen börjar vid punkt 2.3.2 som nämnts tidigare med autentisering. När alla steg körts igenom av systemet på enheten kan enheten efteråt få full tillgång till nätverket.**[20]**

2.4 Komponenter i Cisco ISE

För att kunna installera och köra samt driva och underhålla ett nätverk med Cisco ISE behövs följande komponenter bortsett från mjukvarorna. Cisco ISE är ganska nytt så det är tyvärr inte kompatibelt med så mycket mer än bara Cisco komponenter såsom switchar och routrar.**[2]**

1. Klienter
2. Upprätthållande komponenter
3. Policykontrollerande Switch
4. VMWare Server
5. Domänserver & DNS server

2.4.1 Klienter

Med klienter i detta fall menas ändpunkter som har en viss applikation eller mjukvara installerad för att kunna nå servern för att kontrollera och se vad som händer på nätverket. Med andra ord skiljer sig klienter från vanliga slutanvändare genom att ha annan mjukvara installerad och brukar oftast vara direkt kopplad till någon server eller liknande. Det är via klienten som administrator kan styra och ställa hela nätverket genom att göra ändringar och inställningar i exempelvis servern eller i olika switchar eller liknande.

Från klienten kan även olika typer utav rättigheter delas ut samt även begränsas eller utökas. Olika typer utav policyer kan också redigeras. Förutom rättighetshantering kan klienterna användas för att övervaka nätverket. Detta medför att administratorn som sitter och övervakar nätverket via klienten ser vem som gör vad i hela nätverket.

I vårt fall av klienter har vi två stycken datorer. En som är kopplad till Cisco ISE där all konfiguration av nätverket sker, och en dator som är kopplad till switchen där vi kan konfigurera och styra trafiken som sker på nätverket. I switchen kan vi styra vad som exempelvis skall skickas till Cisco ISE eller vad som inte behöver skickas till ISE på grund av att vissa funktioner kanske är inaktiverade av administratorn.**[3]**

2.4.2 Upprätthållande komponenter

En komponent som är upprätthållande är en komponent som en klient eller slutanvändare använder sig utav för att ansluta sig till nätverket. Dessa är oftast konfigurerade utav en administratör i förväg när nätverket byggs upp. Bortsett från våra klienter har vi använt oss utav följande komponenter som vi har upprättat:

- **Switch –** Vi använder endast en switch för att koppla ihop de upprätthållande komponenterna. Switchen är utav märket Cisco och modellen heter 2960.

- **Domänserver –** Denna server är upprättad med operativsystemet Windows Server 2008 och i denna har vi upprättat bland annat en domänserver, DNS server och NTPserver.**[1]**

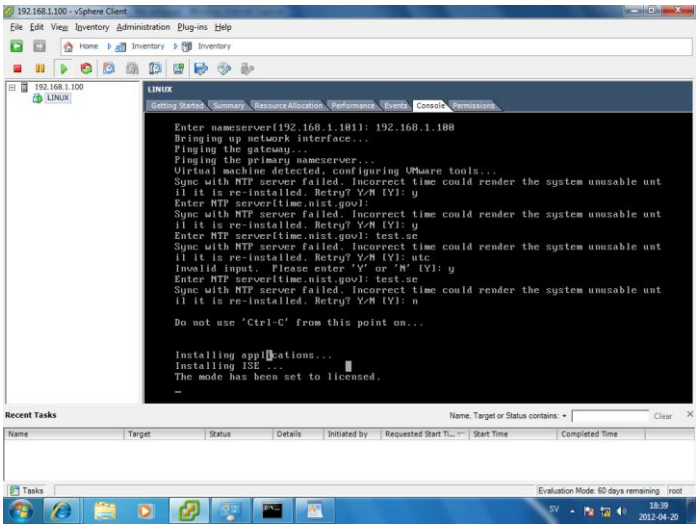
2.4.3 Policykontrollerande Switch/Cisco ISE

Här defineras den policy som har satts upp för att få en åtkomst till nätverket. Policyn är skapad av regler som t.ex. att man har den senaste uppdateringen till en viss mjukvara, att man har ett specifikt antivirusprogram installerat på slutanvändaren eller att man bara kan komma åt nätverket med ett specifik slutanvändare som har ”rätt” operativsystem installerad. Utifrån dessa regler sätts det olika *conditions* på den anslutade klienten, *conditions* innerbär att man sätter upp olika krav på vad slutanvändaren måste ha för att få tillgång till hela nätverket. Dessa kan vara allt ifrån vilket operativsystem klienten kör och vad för användarnamn klienten använder, utifrån dessa samlar Cisco ISE information och avgör vilket typ av åtkomst klienten skall ha till nätverket. Uppfyller denna klient inte kraven så får den inte åtkomst åt nätverket, men däremot om klienten uppfyller vissa krav så kanske den får policyn som en gäst på nätverket. **[4]**

2.4.4 VMware server

För att kunna simulera och installera programvaran Cisco ISE behöver man en viss typ av server. Den här typen av server är en virtuell maskin som simulerar ett specifikt operativsystem som man väljer att installera. För att kunna installera Cisco ISE på en VMware server behöver man en hårddisk där hela utrymmet är ledigt. Minimala kravet för att installera Ciscos mjukvara behöver man följande**[5]**:

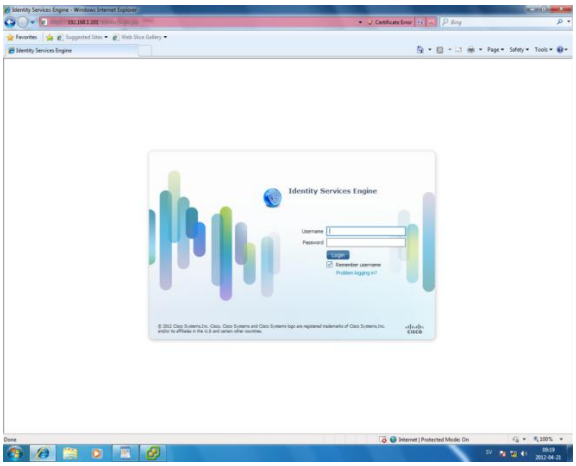
- Processor : Intel Dual-Core: 2.13 GHz or faster
- Ram minne: 4 GB
- Hårddisk : singel på minst 60 GB
- Nätverkskort: 1 GB
- VMware: Hypervisor ESX 4.x or ESXI 4.x



Figur 1 - Installera Cisco ISE med VMware Server ESXI 5 och vSphere Client

När dessa krav är uppfyllda kan man installera mjukvaran på en dator och därefter med hjälp av en klient komma åt mjukvaran med en webbläsare eller med VMware vSphere client. VMware vSphere är en mjukvara som VMware har utvecklat och det är en klient server som kopplar upp sig till VMware servern, med hjälp av detta kan man styra operativsystemet eller mjukvaran som är installerad. För att kunna komma åt Cisco ISE kan man göra det genom en webbläsare. Även här finns de krav på vilka webbläsare som kan simulera mjukvaran, för att kunna komma åt den behöver man en av dessa webbläsare**[6]**:

- Microsoft Internet Explorer, version 8 (även senare webbläsare fungerar)
- Firefox, version 3.6.x
- Google Chrome



Figur2 – Webbåtkomst med hjälp av Internet Explorer

2.4.5 Domänserver & DNS server

En domänserver och en DNS server är viktiga att konfigurera när man skall konstruera ett nätverk med ISE. Med hjälp av en DNSserver kan du nå en ändpunkt via exempelvis enheters namn. Adressen till en viss enhet blir enhetens namn plus domännamnet. Det är där domänserver kommer in och spelar roll. Med hjälp av att ansluta sig till domänservern kan DNSservern nå dig via en adress och inte bara via en IP-adress.
För att kunna köra både domänserver och DNSserver på en maskin krävs en viss maskinvara. Rekommenderat är att man åtminstone skall ha en dator med en processor på 400 MHz, ramminne på 512 MB och minst 4 GB ledigt på hårddisken. Nätverkskort är givetvis ett krav. **[7]**

För att senare kunna styra och ställa över servrarna med hjälp av ISE så kommer ISE även att ansluta sig till domänen. På detta sätt kan man även nå ISE med hjälp av en adress också.

2.5 Implementeringsteknik för Cisco ISE

2.5.1 Mjukvarubaserad

Cisco ISE finns även som hårdvara. Det vi kör är en annan version virtuellt med VMWare. Med en helt mjukvarubaserad kontroll krävs endast en policykontrollerande server, där regler sätts upp samt efterföljs tillsammans med agentmjukvara som installeras på samtliga noder som ämnas upprätthållas.

Det är väldigt viktigt att redan i början av planeringsstadiet veta hur man skall upprätta ett nätverk med ISE. Det är som med allt annat, ju bättre man planerat och gjort rätt utan att fuska i början desto enklare blir det att jobba vidare på det och utveckla det vidare.
I detta fall handlar det ganska mycket om säkerhet. ISE kan konfigureras så att det fungerar väldigt flexibelt, men det kräver en viss erfarenhet och ganska mycket tänk bakom det hela. Man skulle exempelvis kunna göra det väldigt lätt och bekvämt för sig genom att låta mycket ske automatiskt, men det skulle leda till större risk för exempelvis attack mot nätverket eller att man inte har lika stor koll på vad som sker på nätverket i och med att ISE automatiserar och kör allt i en bakgrund där man inte ser.

På så sätt kan även oinbjudna enheter eller gäster få tillgång och nå nätverket vilket inte är önskvärt. Man kan även göra ganska mycket (eller det mesta) manuellt. Allt har givetvis sina för och nackdelar. Men beroende på vad som ligger i fokus borde man tänka efter på vad som bör ske automatiskt och vad man borde hantera manuellt på nätverket. Att installera Cisco ISE är ett stort ingrepp i den nätverksstrukturen som tidigare är uppbyggd.

Efteråt konfigureras allt via Cisco ISE och inte via hårdvarorna såsom routrar och switchar på nätverket. När dessa väl en gång blivit konfigurerade sker all annan konfiguration utav policy, behörighet, tillgång, rättighet osv. via ISE. Det är viktigt att konfigurera på rätt sätt för att få ett så säkert system som möjligt.
Är man heller inte så påläst på hur ISE fungerar kan man missuppfatta allt och missa ganska mycket som händer på nätverket.
Om man exempelvis konstruerar ett nätverk för enheter med ett visst operativsystem är det viktigt att styra och ställa olika rättigheter och tillgångar för de enheter som inte har det eller de operativsystem som man konstruerar nätverket för.

Gör man inte detta kan enheter få olika typer av tillgångar till nätverket i och med att ISE inte agerar mot enheter som inte har det/de operativsystem man jobbat mot och nätverket blir således inte så säkert som man önskat sig. Viktigt är också att konfigurera ISE så att enheter som inte kan identifieras klassas som gäster på nätverket och får bara en viss tillgång till nätverket, dvs. gäster borde inte få full tillgång till nätverket. Hur trådlösa respektive trådbundna enheter skall hanteras är också viktigt att konfigurera och om det skall vara skillnad på dessa.**[8] [42]**

2.6 Produkten Cisco ISE

Med öppnare nätverk och tillgänglighet krävs större underhållning, kontroll och tilldelning utav rättigheter. Cisco är en av de ledande jättarna på marknaden när det har med säkerhet att göra. Allt från struktur, säkerhet, utveckling, underhållning är Cisco ett av de större företagen

som leder utvecklingen. Nätverk växer och utvecklas hela tiden. Detta leder till att kontroll redan vid första gången enheter ansluter får större betydelse. En avläsning för att få ut information som sedan loggas är viktigt för säkerheten. En vanlig avläsning ger information om följande:

- Enhetstyp
- Hur enheten har anslutit till nätverk (trådlöst eller trådbundet)
- Vart enheten befinner sig (vilken hårdvara samt port och på så sätt veta vart även geografikskt)
- Om enheten tillhör företaget eller inte
- Om enheten är skadlig mot nätverket eller inte
- När enheten anslöt sig till nätverket

Identifiering utav en enhet sker på olika sätt, till exempel lyssnar skrivare på en viss port och har den MAC-adress tillhörande ett märke (så som Hewlett Packard som tillvekar skrivare) så är sannolikheten stor att det är just en skrivare man kopplat in. Skulle det dock vara så att en enhet lyssnar på exempelvis JetDirect-porten där skrivare oftast lyssnar men enheten kör på operativsystem exempelvis Windows 7 och begär saker och till från nätet, samt har en MAC-adress som är från en tillverkare som inte tillverkar skrivare, tillåts inte anslutning genomföras och enheten kommer inte att nå nätverket.**[11]**.

Det finns egentligen en färdig produkt Cisco ISE att köpa som hårdvara. Den liknar vilken annan switch/router som helst men den är ganska dyr.

Men för att utföra detta utan den hårdvaran har vi via mjukvaran Cisco ISE och kör den på en virtuell maskin istället. Det fungerar, fast inte lika smidigt. Det leder till att man kan konfigurera men inte testa vissa saker. Exempelvis kan man inte testa anslutningen när man har trådlösa enheter. Detta just för att vår switch som vi är kopplade till inte är trådlös utan trådbunden. Man kan då ställa sig frågan “vad händer om man kopplar in en trådlös accesspunkt till switchen?”. De enheterna skulle lyckas ansluta sig till nätverket och dyka upp i Cisco ISE. Men de skulle visas som att de ansluter trådbundet, detta just för att de ansluter via en accesspunkt som är kopplad till switchen på en viss port och det är bara switchen som Cisco ISE lyssnar på just för att det bara är den som skickar information. Det hade gått om vi hade haft en mer avancerad switch att konfigurera så att både switchen och Cisco ISE vet om att på vissa specifika portar är det trådlösa accesspunkter kopplade och alla enheter som ansluter via de portarna är med andra ord trådlösa. Tyvärr har vi inte en såpass avancerad switch.

Hade vi däremot haft den riktiga Cisco ISE hårdvaran så hade det inte varit några problem i och med att den fungerar både trådlöst och trådbundet. Det hade förenklat en hel del men den

fick utebli för att den var såpass dyr. Principerna är desamma för både trådlöst och trådbundet nätverk. Vill man konfigurera och begränsa/tilldela trådlösa enheter specifika rättigheter är det lika enkelt att göra det som konfiguration av trådbundna enheter som kopplas och ansluter till nätverket.

Själva systemet Cisco ISE är väldigt komplext. Systemet är oftast väldigt avancerat att implementera. Lyckas man dock implementera detta på rätt sätt får man ett väldigt stabilt system som erbjuder dig väldigt hög säkerhet och smidighet att neka obehöriga från nätverket.

3. Nätverk

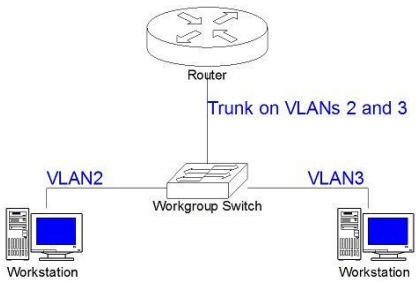
Att bygga ett nytt nätverk från grunden är inte alltid helt enkelt. Det krävs mycket planering i början både hårdvarumässigt och mjukvarumässigt för att få en optimal struktur med enheter som är kopplade mellan varandra genom noder som tillsammans bildar ett nätverk. Frågor man måste ha klart för sig är även vem som skall använda sig utav nätverket. En annan faktor att tänka på är även om företaget kommer att utvecklas och bli större eller om det har nått sin gräns i storlek. Detta är viktigt att veta för att kunna på rätt sätt dela in IP-adresser, skapa olika VLAN, administratörer etc.

På detta sätt vet man i förväg hur stort nätverket ungefär kommer att bli, vad man skall satsa på för hårdvara, hur viktig säkerheten är osv. Idén med de hela är att bygga ett nätverk som är bra i grunden och har stora möjligheter att byggas på med tiden. Ju mer stabilt ett nätverk är ifrån grunden via bland annat indelning utav subnät desto enklare blir det att bygga vidare på det ifall det skulle behövas.

Parallellt med utvärderingen utav Cisco ISE utvecklar vi även en nätverksmodell som är lämplig för medelstora företag. Med medelstora företag syftar vi på företag med ca 2500 anställda. Det finns då olika modeller på nätverk som man kan rekommendera. Mycket beror på hur nätverket ser ut, vem som skall implementera nätverket (företag, skola, sjukhus, etc), hur stort man vill ha nätverket och hur kunnig personalen är för att kunna hantera nätverket. Ju större nätverket är desto kunnigare personal behöver man för att kunna driva nätverket. Bland olika nätverksmodeller finns följande:

3.1 Router on a stick

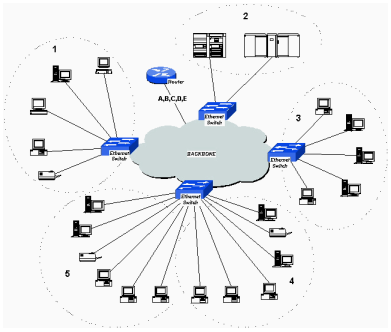
I hela nätverket finns det en router längst upp i hierarkin. Denna routern är kopplad ut till internet och neråt i hierarkin finns det enkelt kopplade switchar. Till dessa switchar kan datorer vara kopplade i olika VLAN och ändå nå varandra i och med att routern känner till och kan dirigera trafik mellan de olika VLAN. Önskas inte detta kan man blockera trafik med bland annat ACL och på så sätt göra de VLAN man vill oåtkomliga för specifika VLAN, en sådan topologi kan se ut såhär**[41]**:



Figur 4 - ”Router on a stick”

3.2 Switchnät lösning med lager 3 switchar

Denna modell liknar Router on a stick till en början då det även på denna modell är en router längst upp i hierarkin som är kopplad mot internet. Skillnaden är det som sker neråt. Denna modell har ett sofistikerat switchnät som består utav tre olika nivåer: access, distribution och core. Denna modell är att föredra om man har ett företag exempelvis i en byggnad med många olika våningar då man bara smidigt kan ha en switch per våning eller liknande, en sådan topologi kan se ut såhär**[29]**:

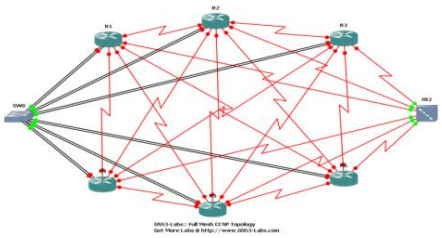


Figur 5 - ” Switched network”

3.3 Router stjärnnät

Denna modell är den mest effektiva men även den dyraste i drift. Längst upp i hierarkin finns det två routrar som det finns internet tillgång till på varje router. Med andra ord är det två separata anslutningar till internet, en på varje router. Router stjärnnät bygger på Switchnät lösning med lager 3 switchar då router stjärnnät också har ett sofistikerat switchnät men med flera coreswitchar som bildar ett ringnät.

Alla dessa modeller är implementerade med ACL, WAN, NAT/PAT, VPN, VLSM, DHCP, VLAN, WLAN, OSPF, VTP, FR. Detta skall testas på en labbmiljö på Chalmers för att säkerställa att allt fungerar, konfigurationerna kommer att implementeras i Cisco routrar och switchar. I ovanstående modeller finns det två olika topologier man strukturera efter. Full mesh som innebär att man kopplar alla switchar och routrar till varandra för att få en låg redundans, Partial mesh innebär att man kopplar åtminstone en av dessa centrala routrar eller switchar till alla andra. En Router stjärnnät topologi kan se ut såhär**[30]**:



Figur 6 - ”Router stjärnnät”

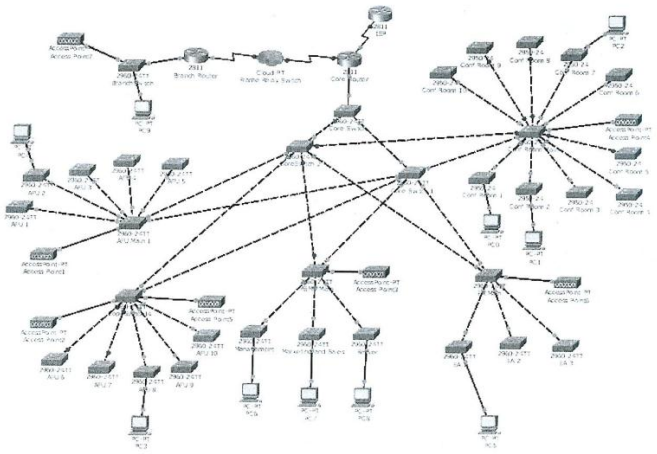
3.4 Uppbygnad av nätverket

Nätverket skall som tidigare nämnts byggas så att det finns möjligheter att utöka eller minska slutanvändare om det nu skulle vara att företaget bestämmer sig för att anställa/sparka personal. För att göra det både simpelt och effektivt delas olika avdelingar/användare i olika VLAN, om man t.ex. är med i VLAN 10 så verifierar numret 10 på vilket VLAN du är med på och vart slutanvändaren har för avdelning.

På detta sätt kan man dela in flera olika avdelningar i olika VLAN för att höja säkerheten och veta vad som händer i nätverket.
Sedan implementeras ACL på alla routrar för att skilja IP-adresser och höja säkerheten mellan avdelningarna så att inga intrång sker.

Vårt nätverk som vi byggt upp ser ut som det gör nedan. Det är lite av en blandning utav de tre modeller som vi presenterat tidigare. Förutsättningarna för alla nätverk är olika och därför är den ena lösningen inte bättre än den andra för alla situationer. Målet är att ha det så optimerat och säkert som möjligt med liten risk för attacker, intrång, och driftfel.

Routing med VLSM, VLAN, DHCP, VPN, tunnel samt ACL



Figur 8 - Topologi över nätverket

4. Metod

Metoden som användes för att uppnå målet var att läsa lite på tidigare examensarbeten då Cisco ISE inte är något som har slagit igenom riktigt på marknaden än och därmed inte finns mycket information om hur man hanterar ett sådant avancerat program/system. Främst när vi väl startade med genomförandet kom vi fram genom testning utav en hel del. Det var mycket att vi skulle ”få ett känn” på själva systemet, hur det fungerar, vad det gör osv. Då vi inte kunnat ansluta vårt nätverk till internet har vi inte kunnat testa hela systemet fullt ut med exempelvis access control lists när man kommer ut på internet och liknande. Vid sökning av information presenterar ofta de som har något med Cisco ISE att göra deras färdiga produkt (system) med alla konfigurationer gjorda som körs i bakgrunden. På så sätt ser vi bara hur kraftfullt systemet är och inte hur man kan konstruera ett så stabilt system.

Vi har arbetat och tagit oss framåt genom att hela tiden sätta delmål för att vi skall komma någon vart. Vi försökte att hålla oss till schemat vi hade satt upp innan när vi befann oss i planeringsstadiet. Vår planering föll efter cirka två veckors arbete när vi stötte på problem efter problem.

Med hänsyn till detta har en väsentlig del av arbetet inneburit felsökning, trial-and-error och mycket arbetstid som lagts ner utanför den faktiska uppgiften. Det man dock positivt kan nämna är att vi tagit lärdom utav hur systemet fungerar, problematiken hänger ihop och hur man kan lösa problem som uppstår i och med att vi stött på dessa och själva klurat ut hur dessa löses.

5. Genomförande

I början var det ganska mycket hårdvaruproblem som begränsade oss till vår handledare som var ganska upptagen i början med att få igång alla examensarbeten. Därför blev hela arbetet trögstartat. Allt från klena datorer, kassa CD läsare, för lite RAM minnen, switchar som inte var kompatibla med Cisco ISE m.m. var anledningar till att vi inte kom igång på riktigt som vi önskat.

Vårt arbetssätt var att beta av det största och svåraste först som vi aldrig hållit på med innan, dvs. Cisco ISE. Parallellt med detta har vi jobbat vi med Cisco Packet Tracer där vi konstruerat ett nätverk som vi sedan byggt upp i Chalmers labbsal bland annat med de datorer vi använt för Cisco ISE. I och med att vi har erfarenhet av att konstruera och konfigurera ett nätverk just i programmet Cisco Packet Tracer tog detta inte lång tid alls. Det ledde till att arbetet som egentligen var tänkt att arbetas med parallellt blev mest fokuserat på Cisco ISE då det var där vi stötte på alla problem. Att konstruera ett nätverk i Cisco Packet Tracer gick smärtfritt och väldigt smidigt.

5.1 Val av Cisco ISE

Under projektets planeringsfas var det lämpligt att använda den stabila versionen av mjukvaran. De inledande 2 veckorna bestod utav att lära känna mjukvaran och kunna hantera programmet på ett effektivt sätt.
Den versionen som vi fick tillhandahållit var en test version så det fanns inga uppdateringsmöjligheter. Versionen som vi fick jobba med var *Cisco ISE 1.1* och det bestod av en ISO fil som man fick installera genom VMware servern.

5.2 Upprättande av testsystem

För att kunna testa detta i realtid finns det specifika hårdvaror som måste ingå för att kunna testa och se resultat.

5.2.1 Servrar

Under projektets gång insåg vi att det behövs servrar för att kunna dela upp resurserna som krävdes för att kunna testa systemet.
Två datorer utrustades med hårdvara tillräckligt för att kunna köra Windows Server 2008 32bit och VMware Server ESXI 5.0. Den ena krävde mer än den andra så det fick bli olika hårdvara på båda serverna.
Hårdvara på Windows Server 2008 32bit: Intel Celeron CPU 2.7 GHz och ramminne på 512 MB.
Hårdvara på VMware Server ESXI 5.0 : Intel Core Duo 2 2.5 GHz och ramminne på 4 GB, kör på VMwares egna operativsystem.

Server #1 **Windows Server 2009** **DNS & Domain Controller** **Active Directory**	**Server #2** **VMware Server ESXI 5.0** **Cisco ISE** **Virtual Machines**
DNS-server(Doman Name Server) Domänkontroller för test.test.se Active Directory som beskrivs längre fram är kopplad till test.test.se	Hanterar Virtuella maskiner som skapas på klientsidan. Servern agerar passivt då den i stort sett bara Cisco ISE mjukvaran installerad på sin hårddisk.

5.2.2 Klienter

För att skapa ett nätverk där olika användarroller och policyer skall simuleras i olika operativsystem och så vidare, valde vi att köra labbmiljön på 2 klientdatorer.
Datorerna anslöts till en switch som i sin tur hade en direkt koppling till Cisco ISE mjukvaran.
Utöver detta hade vi en trådlösrouter kopplad till switchen för att kunna göra uppgiften bredare så att även trådlösa enheter kan koppla sig till nätverket.

Hårdvara på klientdatorerna bestod i Intel Core 2 Duo processorer och 512-2056 MB ram.

2 st Klientdatorer

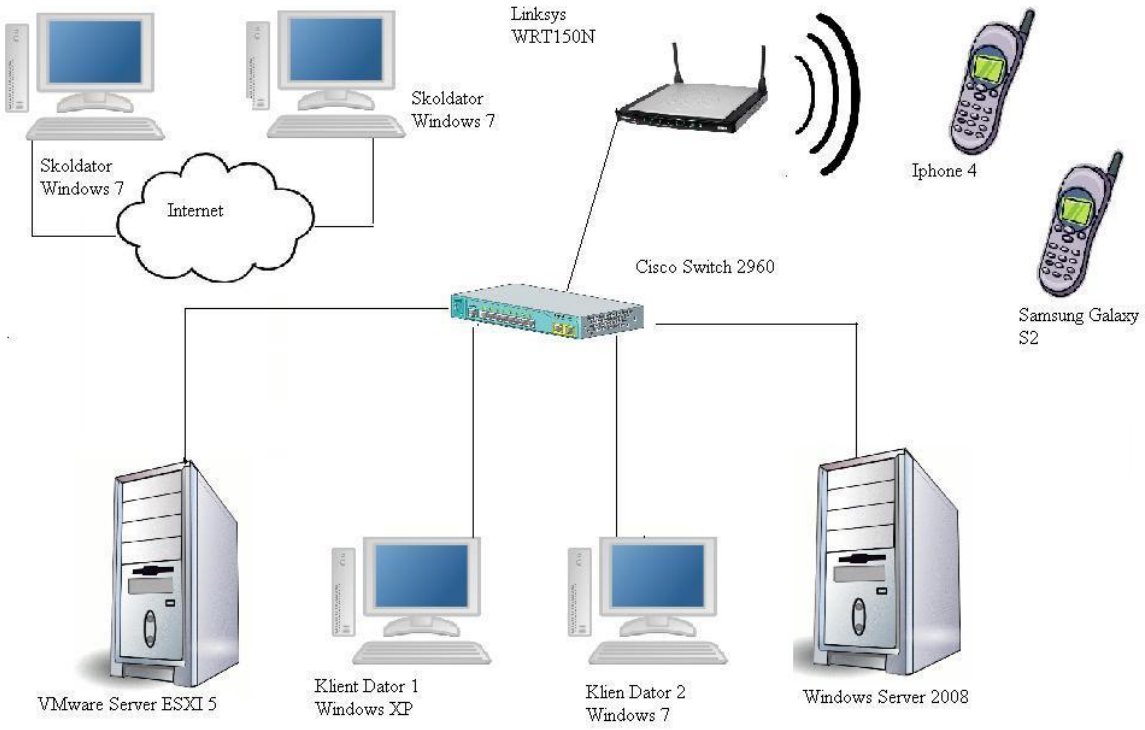
De viktigaste labbdatorerna som vi i huvudsakligen baserade alla våra tester på.
Det som var så fiffigt här var att ena klientdatorn kördes på Windows XP(32 bitars) och den andra på Windows 7(64 bitars) vilket gav oss större bredd och se vilken enhet som var mest kompatibel gentemot Cisco ISE.

1 st Trådlös Router (Linksys)

För att kunna testa trådlösa klienter installerade vi en linksys trådlös router på switchen så även trådlösa enheter kan ansluta sig, framförallt så vi kan simulera trådlösa enheter och se hur de agerar i nätverket. Vi hade *två st* trådlösa enheter som var ansluta till nätverket och dessa enheter var mobila enheter. Den första var en Iphone 4 som kör IOS 4.3.3 som är Apples egna operativsystem, den andra var en Samsung Galaxy S2 som kör ICS(4.0.3) som är Androids egna operativsystem.

2 st Internetanslutna datorer, mot Chalmers-Nätverk

Utöver de vi nämnde innan hade vi 2 st ”skoldatorer” som var kopplade till Chalmers nätverk och dessa enheter användes endast för att kunna söka information på internet. Anledningen till detta var att vi ville skilja våra labbdatorer från internet.



Figur 7 - Topologi över labbmiljön

5.2.3 Hårdvara

De hårdvaror som vi använt i detta arbete är datorer, switchar och en trådlös router, allt tillhörande Chalmers labbsalar. Vår Cisco switch som vi nu använder och som är kompatibel med Cisco ISE är utav modell Catalyst 2960 series. Den har 24 fast Ethernet portar, två gigabit ethernet portar samt en console port. Switchen är konfigurerad via console porten kopplad till en dator på dess COM port.

5.3 Konfigurering utav nätverket

5.3.1 Servrar

Domänkontroller

En domänkontroll är en dator som lagrar kopior av domänens konto och säkerhetsinformation. Vi installerade en Active Directory på vår domänkontroll där vi har Windows server 2008 som operativsystem. När vi installerat och konfigurerat denna kunde enheter ansluta sig till den. Det effektiva med en domänkontroll är att de enheter som är anslutna till den ingår i ett ”separat” nätverk där de kan dela information som inte är tillgänglig för enheter som inte är anslutna till just den domänen. Vi valde att kalla vår domän för ”test.test.se”. Förutom Active Directory har vi installerat DNS (Domain Name System) på domänkontrollen.**[12]**

Active Directory är utvecklat av Microsoft och är en katalogtjänst där man kan lagra uppgifter och som innehåller information om olika resurser i en domän. Med resurser menas datorer, skrivare, användare osv. Active Directory är ett ca 16 år gammalt system många använder för att hantera och lagra exempelvis information, resurser m.m. Active Directory gör det väldigt enkelt att styra över fler användare på nätverket.

Det finns olika tjänster som kan sammankopplas med Active Directory och som kan implementeras med Active Directory. Bland andra är LDAP, Kerberos, DNS några exempel.**[13]**

LDAP

LDAP står för Lightweight Directory Access Protocol. Det är som man hör på namnet ett protokoll där man definierar en datamodell för att kunna kommunicera med en LDAP-server. LDAP är standard i vårt arbete och därför har vi inte behövt konfigurera det. Vid snabba sökningar på katalogservrar används LDAP. Lightweight Directory Access Protocol jobbar med TCP/IP modellen.**[14]**

DNS

DNS står för Domain Name System och detta system jobbar från domänkontrollen. Denna teknik utvecklades år 1983. Den har för uppgift att översätta enheternas olika användarnamn till IP-adresser. Detta gör det mycket enklare för avläsning, identifiering m.m. Skall man ut på internet och exempelvis skriver ”www.google.se” jobbar DNS med att översätta ”www.google.se” till en IP adress som är kopplad till ”www.google.se” som enheten därefter ansluter sig till.

Det finns med andra ord servrar (DNS servrar) med information om vad för olika webbsidor har för IP-adress. På detta sätt slipper man arbeta med IP adresser som kan vara jobbiga att ha i minnet när det kommer till många användare i ett nätverk. Det vi använder vår DNS till i vårt nätverk är att kunna namnge de enheter som ansluter sig i Cisco ISE. Detta underlättar avläsning för Administratörer i och med att de får upp enheters användarnamn istället för IP-adresser.**[16]**

DHCP
Detta är ett protokoll som ger en möjligheten att kunna tilldela IP-adresser som ansluter sig till nätverket automatiskt. Med andra ord behövs inte detta göra manuellt utav en administrator eller liknande. Det är ett väldigt smidigt system, speciellt när man bygger nätverk för större ändamål. Detta protokoll gör det även mycket enklare för användaren som försöker att ansluta med sin enhet då denne inte behöver göra några som helst inställningar innan anslutning till nätverket.

Bekvämlighet och säkerhet går dock tyvärr inte alltid hand i hand. När mycket sker automatiskt har man inte lika stor koll på vad det är som egentligen händer på nätverket. Det leder till att oönskade enheter skulle kunna få en IP-adress så fort de skickar en förfrågan till DHCP servern.
Vi har dock valt att inte använda oss utav en DHCP server. Anledningarna till det är vi först och främst prioriterar säkerheten på nätverket, och sedan lär vi oss mer av att hantera datorer manuellt genom att ge de statisk IP-adress. Självklart kan man ändra detta och implementera en DHCP server som delar ut IP-adresser till enheter men nu känner vi att vi vill få känslan av att kunna kontrollera hela systemet manuellt.**[17]**

VMWare server
Förutom vår domänkontroll med tjänster implementerade har vi även vår VMWare server där vi installerat hela Cisco ISE systemet med hjälp utav VMWare. Detta är motsvarigheten till den riktiga Cisco ISE hårdvara som vi undvek att köpa på grund av priset.

Denna står och kör för sig själv och med hjälp av en klientdator är det enkelt att komma åt själva mjukvaran Cisco ISE för att konfigurera. Det är denna maskin tillsammans med domänkontrollen som är de centrala och viktiga pjäserna i vårt nätverk.
Även switchen som båda dessa maskiner är kopplade till är en viktig del i systemet. Skulle någon utav dessa maskiner ge upp kan inte bara dessa ersättas utan nya konfigurationer måste göras och för att nätverket skall fungera som innan, dvs. felfritt. Till skillnad från domänkontrollen som vi inte kan komma åt genom en annan dator utan måste fysiskt ha tillgång till datorn så behövs inte det med Cisco ISE eller VMWare när det kommer till VMWare servern.

Den har två IP-adresser som man kan komma åt servern med, ena IP-adressen är till VMWare servern och den andra för att komma åt själva Cisco ISE mjukvaran för att kunna logga in på servern. Den har även några virtuella maskiner som kör Windows 7 som operativsystem. På så sätt kan vi ansluta fler enheter till vårt nätverk för att kunna se hur allt fungerar.

Genom att använda virtuella maskiner sparar vi plats i vår labbsal. Vi sparar även tid som annars hade gått åt för att installera operativsystem på datorer samt uppdatera drivrutiner och liknande för att få de körklara.

5.3.2 Klienter

De klienter som vi använder i vårt system har vi konfigurerat själva. Vi började med att först se till att de hade den hårdvara som krävs för att den skall fungera felfritt och kunna ansluta till nätverket. Därefter formaterades hårddiskarna på alla datorer, installerade operativsystem på dem och uppdaterade dem till deras senaste service pack. Uppdateringen var egentligen inte alls nödvändig så sätt men vi ville att datorerna skall vara så verkliga som möjligt. Finns det en uppdatering brukar användare uppdatera till det senaste. När de var körklara kopplade vi upp dem på nätverket och mot domänen test.test.se som vår domän heter.

En av datorerna som vi kopplade upp med verkade det dock vara något fel på. Vi kunde inte förstå varför det inte gick att använda två olika nätverkskort i den utan att det skulle bli konflikt mellan dessa. Efter den del felsökning bytte vi båda nätverkskorten utan bättre resultat. Det resulterade i att vi bytte dator helt.

5.4 Nätverk

Tidigare nämnt att utöver utvärderingen av Cisco ISE byggs det ett nätverk för ett medelstort företag på 2500 anställda. Genomförandet utfördes på Chalmers labbsalar och testades för att verifiera att förarbetet var korrekt genomtänkt och att alla förväntningar på nätverket uppfylldes. Hela genomförandet av nätverket skedde på Chalmers labbsalar och då användes de Cisco routrar och Cisco switchar. Hårdvaran som användes var Cisco Catalyst 2800 series(som är routern) och Cisco Catalyst 2960 series(som är switchen). Det mest effektiva sättet att genomföra detta bygge var att konfigurera routrar och switchar parallellt för att sedan kunna testa och verifiera att allt fungerar.

6. Resultat

6.1 Labbresultat

Efter att konfigurationerna var klara i packet tracer och våra tester på Cisco ISE i vårt lilla nätverk vi byggt upp i examensarbetssalen flyttade vi över till labbsalen för att testa allt på hårdvara. Vi använde oss utav Cisco Switchar och Routrar för att bygga upp de nätverk vi utvecklade i Cisco Packet Tracer. På så sätt fick vi svar på hur våra utvecklade modeller i simuleringsprogrammet fungerar på hårdvara. Tester som utfördes var anslutning utav datorer till nätverket. Skapande utav olika VLAN, studera hur de olika slutanvändarna fick olika IP-adresser. Vi testade även vår DHCP server som såg till att vi fick olika IP-adresser varje gång vi anslöt oss till nätverket. OSPF testade vi med hjälp utav routrarna som har det som protokoll mellan varandra och vi kunde se trafiken mellan dessa.

I labbmiljön lyckades vi få allt att fungera med en viss konflikt utav vissa datorer som inte riktigt ville med. Om det berodde på datorernas nätverkskort eller annan hårdvara/mjukvara i datorn vet vi inte riktigt då vår felsökning inte ledde till någon lösning. Det vi dock kunde utesluta var switcharna och routrarna då dessa fungerade felfritt för alla datorer förutom de tre datorer som krånglade. Switchar som användes i labbsalarna skiljde sig lite från den vi använde när vi själva satt och konfigurerade. De switchar vi använde var utav modell Catalyst 2950.

Utöver Cisco ISE testades och konfigurerades ett nätverk som tillfredställer ett företag på ungefär 2500 anställda, som tidigare nämnt testades även detta på Packet tracer för att säkerställa att allt fungerar och är i sin ordning. Efter testningen på simuleringsprogrammet så var det dags att implementera dessa på hårdvara. Under konfigurationerna stötte vi på små problem som till exempel att DHCP servern inte fungerat rätt och att man inte kunnat skicka echo meddelande (ping) till varandra. Men efter små korrigeringar och lite mer testning på routrarna och switcharna blev resultatet som tänkt, testningarna gjordes genom att pinga olika VLAN.

6.1.1 Begränsning

Det som var mindre tråkigt var att testning inte kunde göras fullt ut. Detta för att Cisco ISE hanterar både trådlösa och trådbundna nätverk och enheter. För detta krävs dock att man har en switch som stödjer trådlös kommunikation eller att man har den riktiga Cisco ISE hårdvaran vilket vi saknade. Därför kunde bara testning utav trådbundna enheter testas.

En annan variant man skulle kunna köra är att man kan koppla in trådlösa accesspunkter till switchen där Cisco ISE är kopplad till och konfigurera i switchen att alla enheter som ansluter via den eller de portar som man har accesspunkter kopplade till är trådlösa. Detta gick dock inte att konfigurera på vår switch, den är inte tillräckligt avancerad för det.

6.1.2 Ingen testning utav infekterade datorer

Vi lyckades aldrig att testa att ansluta till nätverket där Cisco ISE var implementerad. Anledningen var att vi saknade datorer som har virus. Meningen var att se hur Cisco ISE hanterar infekterade datorer med skadlig mjuk eller hårdvara. I teorin skall dessa enheter inte få full tillgång till nätverket innan de söks av och åtgärd vidtas för de enheter som anses vara hot mot nätverket.

6.2 Analys av Cisco ISE

Vilka krav bör sättas på Cisco ISE?

I och med att Cisco ISE är ett kraftfullt och väldigt avancerat program är det rättvist att ställa relativt höga krav på systemet. Dock är det viktigt att ha kunskapen för det vid implementering.

- Säkerhet skall vara högsta prioritet

- Anslutningsprocess skall gå relativt snabbt

- Alla olika enheter skall kunna identifieras
    1. Med eller utan någon mjukvara installerad
    2. Kunna tilldelas administrativa rättigheter eller endast användarrättigheter
    3. Oavsett vilken domän de tillhör. Allt som kopplas upp skall Cisco ISE kunna hantera

- Konfigurerbart. Administratörer skall enkelt kunna hantera systemet och forma det på de sätt de önskar.

Vilka komponenter bör finnas?

DOMÄNER
För att få ut så mycket som möjligt utav möjligheterna i Cisco ISE bör man åtminstone ha en domän installerad.
Detta för att försäkra sig om att en majoritet utav datorerna som är ansluta till nätverket skall följa nätverkets säkerhetspolicy.

ANSLUTNINGSENHETER
Cisco ISE hanterar både trådlösa och trådbundna enheter och därför bör man ha enheter som ansluter på olika sätt till nätverket. Man kan efteråt i Cisco ISE se hur kontroll görs efter att en nod ansluter till nätverket.

DNS SERVER
För att optimera ett nätverk bör man ha en DNS server installerad för att kunna översätta IP-adresser inom och utanför nätverket. Denna kan placeras vart man än önskar men för att rekommendera borde den vara placerad centralt i nätverket tillsammans med domänservern. Detta just för att Det är källan till alla anslutande enheter oavsett anslutningssätt

7.Slutsats och disskussion

Detta examensarbete har genomförts i syfte av att lära och fördjupa kunskaperna, utvärdera och analysera tekniken Cisco ISE - Networking. Att göra sig bekväm i en miljö att utveckla och konstruera nätverk där det krävs mycket planering från grunden är också ett syfte vi strävat efter.
Studier i ämnet har genomförts i ett tillvägagångssätt där delmål sätts upp, information samlas, problem stöts på, problem löses, lärdom och lösningar antecknas och nya delmål sätts upp. Med andra ord har mycket varit teoretiskt men parallellt har även experiment tillvägagångssätt utförts. I labbmiljö har en Cisco ISE från Cisco Systems, som är en av de större utvecklarna installerats och testats för att studera vilka funktioner som tekniken besitter och vad detta system bör innefatta. Därefter har produkter inom samma segment och från samma utvecklare teoretiskt studerats, konfigurerats, jobbats med och sammanställts i avsikt att ge en så klar bild som möjligt om av vad Cisco ISE är och vad som kan krävas från produkten. De punkter som framgår i resultatdelen är också våra egna slutsatser kring dessa frågeställningar.

Under arbetets gång har vi gjort massvis av tester med ett system bestående utav Cisco ISE och dess kringliggande produktportfölj. Hela examensarbetet har på grund av olika anledningar gått ganska långsamt och genom många "trial-and-error" och ominstallationer har vissa slutsatser kunnat dras kring just denna produkt.

Vi har även haft lite strul med Packet tracer, idén var att testa och simulera hela nätverket vi har byggt på Packet Tracer. Men det gick inte som förväntat på grund av versionshanteringen och oberäkneliga strul fast när vi testade samma sak på hårdvaran så fungerade allting galant. Värt att notera är att själva simuleringen på Packet Tracer inte gick så bra men själva testningen på hårdvara gick bra.

Vi har kommit fram till att Cisco ISE som är ett komplext system är lätt att sätta sig in i och använda för kontroll av nätverket för administratörer. Trots att systemet är väldigt avancerat och kräver mycket arbetskraft av datorer och en del av nätverkets andra hårdvaror i form av switchar blir systemet säkrare och mer effektivt.

7.1 Disskussion kring arbetet

Cisco System tillverkar komponenter som är utav väldigt hög kvalitet. Deras hårdvaror är stabila och fungerar utmärkt tillsammans med både varandra och med hårdvaror utav andra märken. Dem är väldigt stabila och krånglar aldrig. Det mer krångliga är att kunna hantera och konfigurera dessa på rätt sätt, och i och med att alla hårdvaror skiljer sig vet man aldrig hur ”standard konfigurerade” hårdvaror egentligen är konfigurerade dvs. om vissa funktioner är aktiverade eller inte exempelvis.

Vad har varit komplikationerna?

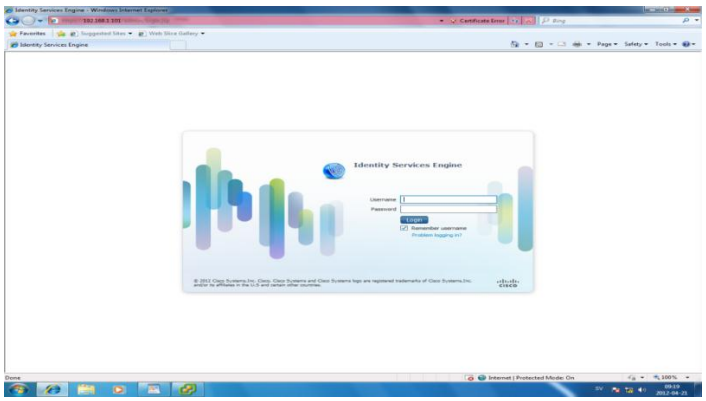
Detta examensarbete och labbutförande har varit mycket tidsödande arbete som inneburit problem som inte varit relaterade till uppgiften. Inledningsvis samlade vi mycket information om vad Cisco ISE är, vad som krävs för att köra detta samt hur man arbetar med det. Problemet var att den information vi samlade in var till de äldre versionerna utav Cisco ISE. Den Cisco ISE version vi hade fått av vår handledare var den senaste där många nya uppdateringar skett och därmed hjälpte inte den informationen vi hade samlat in mycket alls. Därför rekommenderades vi av vår handledare att testa oss fram, träffa på problem, lösa dessa, ta lärdom och testa nytt. Det ledde till att vi lärde oss ganska mycket om programmet ändå även om det inte gick i den takt vi önskade från början. Grundsyftet var ifrån början att konstruera ett nätverk och implementera Cisco ISE i detta. Själva konstruktionen var det inga större problem med då vi har erfarenhet utav det sedan tidigare. Därför lades det mycket fokus på Cisco ISE i och med att det var där alla problem uppstod. När vi testade oss fram togs många steg framåt i blindo. Detta för att det inte finns någon guide på hur man implementerar Cisco ISE i ett nätverk. Med den kunskap som vi nu besitter angående Cisco ISE och med hjälp utav dokumentation vi fört kan vi konstatera att utgången utav detta arbete förmodligen varit annorlunda. Om inte annat hade genomförandet gått mycket smidigare och fler djupdykningar i tekniken hade hunnits med.

Tidsbristen blev lite utav ett problem då mycket utav det inledande arbetet som bestod utav upprättande utav en stabil labbmiljö och erhållning utav rätt utrustning att testa på tog mycket längre tid än väntat. Anledningarna till detta var främst de klena datorer vi hade ifrån början. När vi hade samlat information om vad vi behövde för hårdvara angående datorer tog det tid att få fram detta samt att hitta en miljö att kunna labba i då dessa hårdvaror inte är bärbara.

De tidigare versionerna utav Cisco ISE gick att köra på äldre version utav VMWare. Det fanns inga krav på internet om att den senaste versionen utav VMWare behövdes för att köra den senaste Cisco ISE som finns ute idag. Därför fastnade vi väldigt länge just vid installation utav systemet. I och med att vi aldrig tidigare kört mjukvaror virtuellt blev även detta något nytt för oss som vi tog lärdom utav. Vid installationen utav Cisco ISE gick mycket fel och vi saknade allt ifrån RAM-minne, hårddiskar, rätt operativsystem.

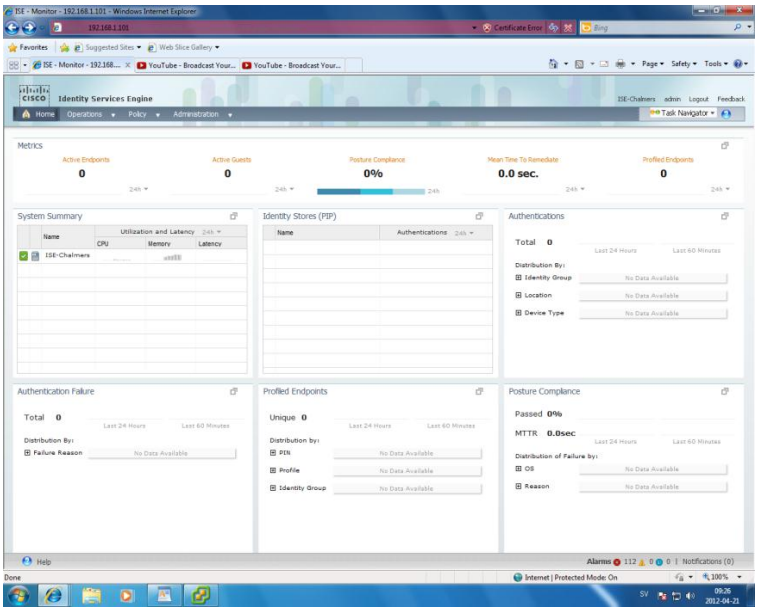
Cisco ISE är ett ganska komplext system och har många olika funktioner. En av alla dess funktioner är NAC som står för Network Access Control. NAC jobbar på ett sätt så att de enheter som försöker att ansluta till nätverket söks av efter skadlig mjukvara. På så sätt får man ett säkert system där enheter inte smittar varandra över nätverket. På grund utav tidsbrist fick vi aldrig ihop NAC att fungera och på så sätt kunde vi inte testa NAC funktionen.

Målet var att nå den webbaserade delen utav Cisco ISE som man kan nå via webbläsaren som är enklast och effektivast där man får logga in för att kunna konfigurera.



Figur 9 - Cisco ISE

För att sedan kunna logga in och få följande miljö:

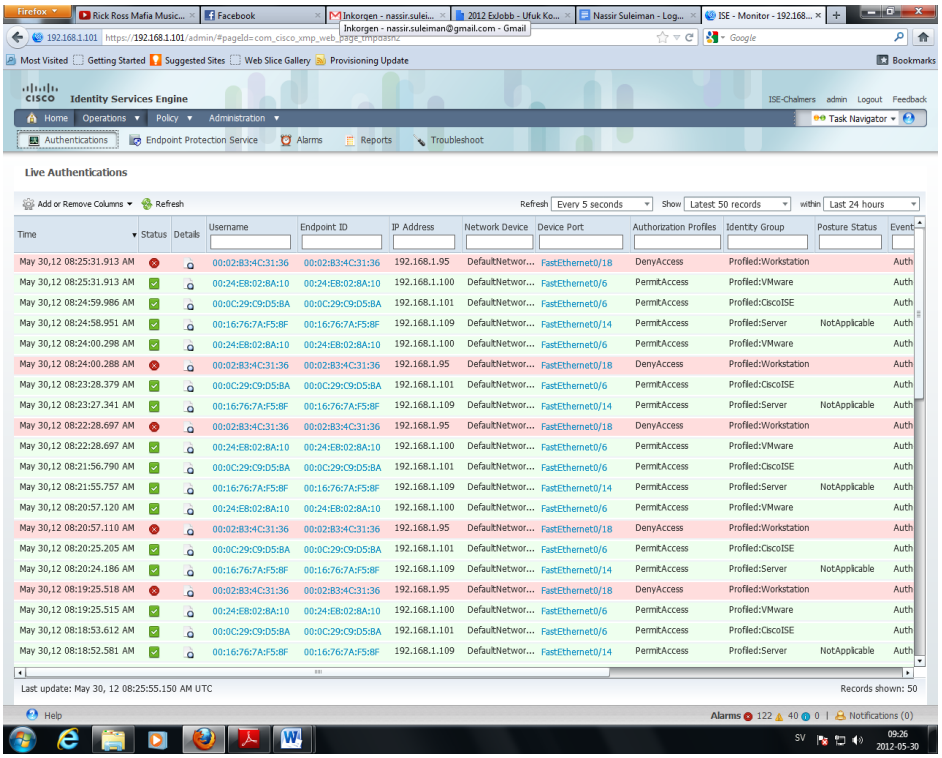


Figur 10 - Cisco ISE

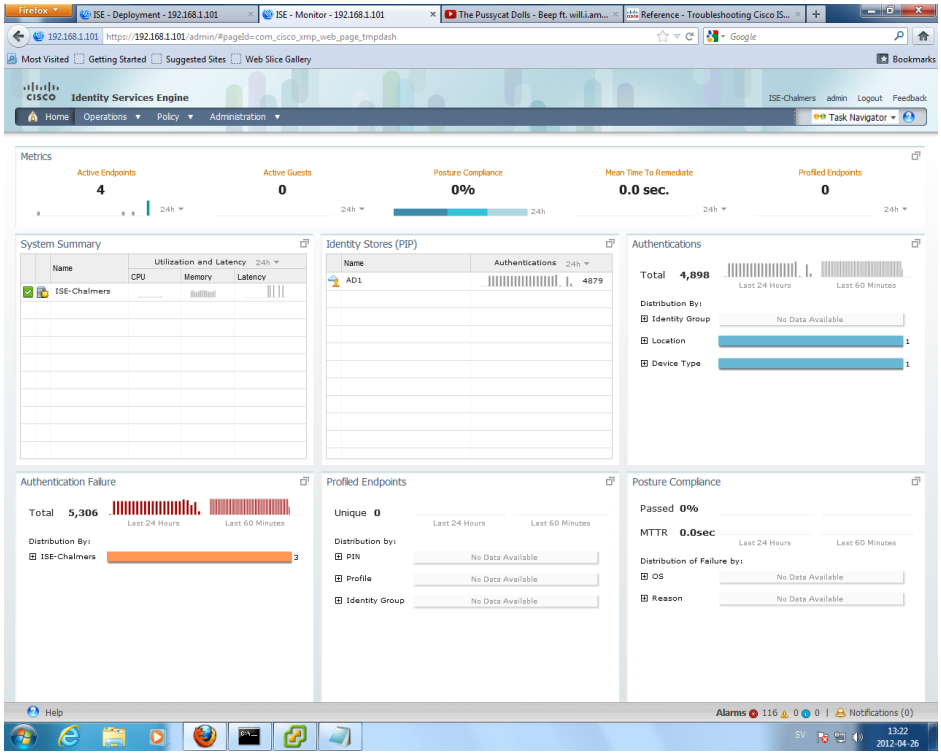
Väl inne i den webbaserade delen som vi nått som tog mycket längre tid än väntat stötte vi på ännu fler problem som tog tid att lösa. Tanken med Cisco ISE är att systemet skall upptäcka nya enheter som ansluter till nätverket. I början gjordes inte detta, vi jobbade med felsökning väldigt länge och kom fram till att switchen som vi fick inte var kompatibel med den Cisco ISE version vi fått.

Då skulle en ny switch beställas och tid slösades på att vänta på den och eftersom att vi redan konstruerat ett nätverk blev vi sittandes i väntan på den nya switchen som beställdes. När denna väl kom löstes vårt problem efter att switchen konfigurerades så att den skickar information om vad som händer på nätverket till Cisco ISE.

Det skulle dock dyka upp fler problem. På nätet finns mycket information men inte om hur man ställer in och konfigurerar olika policys och identifieringar. Därför nekades all trafik ifrån början då systemet var inställt på att göra det. Därför fick vi testa oss fram med att tillåta olika anslutningsförsök. Då det inte står mycket om olika hot mot Cisco ISE på nätet kan vi inte vara helt säkra på att vi konfigurerat rätt och säkert i systemet men vi lyckades att konfigurera så att vi kan tillåta de enheter som vi vill skall kunna ansluta och neka de oönskade enheterna.



Figur 11 – Anslutningsförsök utav diverse enheter



Figur 12 - Cisco ISE

Nästa problem skulle dyka upp, ansluta Cisco ISE till domän. Vi hade en dator där vi installerade Windows Server 2008, Active Directory domain och DNS server för att kunna nå enheter via dess användarnamn och inte bara via dess IP-adress. Problemet kunde vi dock inte sätta fingret på då vi konfigurerat DNS servern på rätt sätt i och med att det gått att pinga datorer med hjälp utav deras användarnamn och domännamn. Cisco ISE gav ändå ett felmeddelande om att DNS inte fungerar. Många omstartningar utav hela systemet gjordes utan framgång. DNS och Active Directory konfigurerades om och External Identity Sources konfigurerades om i Cisco ISE. Till slut fick vi inte bara anslutningen att fungera utan även uppkopplingen.

Vissa komplikationer som vi hade på servern där Cisco ISE är installerad (VMWare servern) var att vi inte lyckades att installera flera virtuella maskiner som vi hade hoppats på att kunna testa att ansluta till nätverket med. Det hade varit mycket smidigare med det istället för att dra in flera datorer i labbmiljön för att testa och se hur Cisco ISE hanterar nya enheter som försöker att ansluta. Vår idé ville sig dock inte så vi anslöt en trådlös accesspunkt till switchen och anslöt oss till nätverket via våra telefoner och bärbara enheter istället.

Kritisk diskussion
Det finns många saker vi hade kunnat förbättra i efterhand för att klara av uppgiften bättre. Arbetet med att skriva rapport har skjutits upp en del på grund av alla problem som stöttes på, därför blev rapporten inte riktigt som vi önskat oss. Målet är att skriva klart rapporten för att bara kunna fokusera på att förebereda inför presentation utav vårt examensarbete plus förberedelse utav opponering utav andra examensarbeten.

Vi hade kunnat vara mer förberedda och läst på mer om just Cisco ISE i och med att det var något helt nytt som vi gav oss in på som vi aldrig hört talas om innan. Man kan aldrig förbereda sig för mycket. Vi hade kunnat förbereda och ha fler frågeställningar som vi ville ha svar på innan vi började med arbetet. Det vi hade som mål innan vi började med arbetet var att kunna konstruera, konfigurera och driva ett nätverk med hjälp utav Cisco ISE. Istället för en frågeställning blev det mer att vi testade och utvärderade en produkt framställt utav Cisco Systems.

Vid kontroll av vad vi behöver för komponenter och liknande så hade vi kunnat söka efter mer noggrant för att inte slösa tid på att i efterhand komma på att vi behöver fler/mer stabila komponenter. Vi hade kunnat sitta fler timmar i skolan även om vi gick till skolan varje dag och satt ca 6-7 timmar per dag i skolan.

Dokumentationen i google docs hade också kunnat bli bättre samt loggboksskrivandet. Även om kontakten med vår handledare varit god och han funnits tillgänglig ofta blir det svårt för honom att sätta sig i och ta del av vårt arbete för att hjälpa oss när vi inte lägger upp nytt på google docs hela tiden utan bara sparar det lokalt på våra arbetsstationer.

Slutligen är vi mycket nöjda med det arbete vi utfört samt med de slutsatser vi nått. Genom arbetet med Cisco ISE och Cisco Systems produkter och studier har vi inte bara lärt oss mycket kring produkten Cisco ISE utan mycket om nätverkssäkerhet i allmänhet och om ändpunktssäkerhet i synnerhet samt profilering, rättigheter, behörigheter och policys.

Vi känner att vi kommit långt på de 10 veckor som vi jobbat med produkten. Från att inte veta något om produkten till att känna till den väl, kunna konfigurera, implementera och använda produkten är för oss ett väldigt stort steg framåt.

Referenslista

[1] (2012) *Cisco Identity Service Engine* [WWW Dokument]
http://www.cisco.com/en/US/products/ps11640/index.html
(använd 23 maj)

[2] Cisco (Mars2012) *Cisco Identity Engine Network Component Compatibility, Release 1.1* [WWW Dokument]
http://www.cisco.com/en/US/docs/security/ise/1.1/compatibility/ise_sdt.html
(använd 2 maj)

[3] Cisco (2012) *Overview of Cisco ISE* [WWW Dokument]
http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_overview.html
(använd 1 maj)

[4] Gavin McBain (Dec 2011) *Introducing Cisco Identity Service Engine (ISE) Profiling* [WWW Dokument] http://packetpushers.net/introducing-cisco-identity-services-engine-ise-profiling/ (använd 2 Maj 2012)

[5] Cisco (2012) *Installing the Cisco ISE System Software on a VMware Virtual Machine* [WWW Dokument]
http://www.cisco.com/en/US/docs/security/ise/1.0.4/install_guide/ise104_vmware.html

(använd 3 maj)
[6] Cisco (tid?) *Performing Post Installation Tasks* [WWW Dokument]
http://www.cisco.com/en/US/docs/security/ise/1.0/install_guide/ise10_postins.html
(använd 3 maj)

[7] (2012) Microsoft Windows Server. *Översikt över DNS Server* [WWW Dokument]
http://technet.microsoft.com/sv-se/library/cc770392(v=ws.10).aspx
(använd 3 maj)

[8] (2012) Cisco. *Management* [WWW Dokument]
http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_guest_pol.html
(använd 4 maj)

[9] (3 januari 2012) *Switch* [WWW Dokument]
http://sv.wikipedia.org/wiki/Switch
använd (4maj)

[10] (6 december 2011) *Cisco ISE Fundamentals* [Youtube]
http://www.youtube.com/watch?v=sel1F7mKdtI
använd (10maj)

[11] (18 april 2012) *Cisco TrustSec - Lösningen på BYOD* [WWW Dokument]
http://blogg.atea.se/post/Cisco-ISE.aspx
använd (14maj)

[12] Christian Mård & Sebastian Ahlman (20 mars 2008) *Active Directory* [WWW Dokument]
http://www.google.se/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0CIMBEBYwBA&url=http%3A%2F%2Fpeople.arcada.fi%2F~mardc%2Fnetos%2Fad_rapport.doc&ei=NIi1T4iIJueL4gTS4O2aDg&usg=AFQjCNEcNETG8xNzL2e0r7xeZlwOs1yAvQ&sig2=OmqCoVaCx4fp5oMHkyBRNQ
(använd 18 maj)

[13] (2 maj 2012) *Active Directory* [WWW Dokument]
http://sv.wikipedia.org/wiki/Active_Directory
(använd 18 maj)

[14] (15 december 2011) *LDAP* [WWW Dokument]
http://sv.wikipedia.org/wiki/LDAP
(använd 18 maj)

[15] (27 maj 2011) *Kerberos* [WWW Dokument]
http://sv.wikipedia.org/wiki/Kerberos_%28datas%C3%A4kerhet%29
(använd 19 maj)

[16] (15 april 2012) *DNS* [WWW Dokument]
http://sv.wikipedia.org/wiki/DNS
(använd 19 maj)

[17] (9 maj 2012) *DHCP* [WWW Dokument]
http://sv.wikipedia.org/wiki/DHCP
(använd 19 maj)

[18] (18 maj 2012) *IPsec* [WWW Dokument]
http://en.wikipedia.org/wiki/IPsec
(använd 20 maj)

[19] (6 mars 2012) *Cisco Systems* [WWW Dokument]
http://www.securityie.com/cgi-bin/ultimatebb.cgi?ubb=get_topic;f=10;t=003877
(använd 20 maj)

[20] (2 februari 2012) *Karantän* [WWW Dokument]
http://sv.wikipedia.org/wiki/Karant%C3%A4n
(använd 20 maj)

[21] (30 mars 2012) *VPN* [WWW Dokument]
http://sv.wikipedia.org/wiki/Virtual_private_network
(använd 21 maj)

[22] (14 maj 2012) *VPN inline Posture using IPEP ISE and Cisco ASA* [WWW Dokument]
https://supportforums.cisco.com/docs/DOC-24412
(använd 21 maj)

[23] (2012) *HTTPS* [WWW Dokument]
http://en.wikipedia.org/wiki/HTTP_Secure
(använd 22 maj)

[24] (2012) *Configuring Authentication Policies* [WWW Dokument]
http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_auth_pol.html#wp1089046
(använd 24 maj)

[25] (2012) *Integration of ISE* [WWW Dokument]
https://supportforums.cisco.com/docs/DOC-18121
(använd 24 maj)

[26] (2012) *Accesspunkt och Accespunkter* [WWW Dokument]
http://accesspunkt.se/
(använd 24 maj)

[27] (11 maj 2012) *SNMP* [WWW Dokument]
http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
(använd 25 maj)

[28] (17 aug 2010) *Whats is 802.1x?* [WWW Dokument]
http://www.networkworld.com/news/2010/0506whatisit.html
(använd 25 maj)

[29] (2012) *Fully Switched Networks by* ***Jeff Tyson*** [WWW Dokument]
http://computer.howstuffworks.com/lan-switch5.htm
(använd 28 maj)

[30] (2012) *Network Topologies by* ***Bradley Mitchell*** [WWW Dokument]
http://compnetworking.about.com/od/networkdesign/a/topologies.htm
(använd 28 maj)

[31] (5 maj 2012) *Access Control lists* [WWW Dokument]
http://msdn.microsoft.com/en-us/library/windows/desktop/aa374872(v=vs.85).aspx
(använd 28 maj)

[32] (5 maj 2012) *WAN* [WWW Dokument]
http://sv.wikipedia.org/wiki/Wide_Area_Network
(använd 28 maj)

[33] (2 mars 2012) *NAT* [WWW Dokument]
http://sv.wikipedia.org/wiki/Network_Address_Translation
(använd 29 maj)

[34] (30 mars 2012) *VPN* [WWW Dokument]
http://sv.wikipedia.org/wiki/Virtual_private_network
(använd 29 maj)

[35] (2012) *VLSM* [WWW Dokument]
http://www.orbit-computer-solutions.com/VLSM.php
(använd 30 maj)

[36] (8 januari 2012) *VLAN* [WWW Dokument]
http://sv.wikipedia.org/wiki/VLAN
(använd 30 maj)

[37] (18 april 2012) *WLAN* [WWW Dokument]
http://sv.wikipedia.org/wiki/Tr%C3%A5dl%C3%B6st_LAN
(använd 30 maj)

[38] (30 januari 2012) *OSPF* [WWW Dokument]
http://sv.wikipedia.org/wiki/Open_Shortest_Path_First
(använd 30 maj)

[39] (15 april 2012) *VTP* [WWW Dokument]
http://en.wikipedia.org/wiki/VLAN_Trunking_Protocol
(använd 30 maj)

[40] (4 juli 2012) *Frame Relay* [WWW Dokument]
http://sv.wikipedia.org/wiki/Frame_Relay
(använd 30 maj)

[41] (2012) *CCNA Certification Exam Training by* ***Chris Bryant*** [WWW Dokument]
http://www.thebryantadvantage.com/RouterOnAStickCCNACertificationExamTutorial.htm
(använd 28 maj)

[42] (2012) *Cisco* Setting Up Cisco ISE in a Distributed Environment [WWW Dokument]
http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_dis_deploy.html#wp1123466
(använd 29 maj)

[43] (10 juni 2012) *VMWare* [WWW Dokument]
http://sv.wikipedia.org/wiki/VMware
(använd 15 juni)

Bilaga

Switch konfiguration

```
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.2.3
ip http server
ip http secure-server
username Kalle password cisco123
ntp server 192.168.1.109
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting dot1x default start-stop group radius
aaa session-id common
aaa accounting update periodic 5
aaa accounting system default start-stop group radius
aaa server radius dynamic-author
client 192.168.1.101 server-key cisco123
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 30 tries 3
radius-server host 192.168.1.101 auth-port 1812 acct-port 1813 test username
Kalle key cisco123
radius-server vsa send accounting
radius-server vsa send authentication
ip radius source-interface vlan 1
aaa server radius dynamic-author
client 192.168.1.101 server-key cisco123
ip dhcp snooping
ip device tracking
dot1x system-auth-control
dot1x critical eapol
authentication critical recovery delay 1000
vlan 1
name VLAN1
int vlan 1
ip address 192.168.1.103 255.255.255.0
ip helper-address 192.168.1.101
ip access-list extended ACL-ALLOW
```

```
 permit ip any any
ip access-list extended ACL-DEFAULT
  remark DHCP
  permit udp any eq bootpc any eq bootps
  remark DNS
  permit udp any any eq domain
  remark Ping
  permit icmp any any
  remark Ping
  permit icmp any any
  remark PXE / TFTP
  permit udp any any eq tftp
  remark Allow HTTP/S to ISE and WebAuth portal
permit tcp any host 192.168.1.101 eq www
permit tcp any host 192.168.1.101 eq 443
permit tcp any host 192.168.1.101 eq 8443
remark Drop all the rest
  deny   ip any any log
ip access-list extended ACL-WEBAUTH-REDIRECT
deny   ip any host 192.168.1.101
permit ip any any
interface range FastEthernet0/1-24
switchport mode access
switchport access vlan 1
authentication open
ip access-group ACL-ALLOW in
authentication host-mode multi-auth
authentication periodic
authentication timer reauthenticate server
authentication event fail action next-method
authentication event server dead action authorize vlan 1
authentication event server alive action reinitialize
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
logging monitor informational
logging origin-id ip
logging source-interface vlan 1
logging host 192.168.1.101 transport udp port 20514
```

```
epm logging
snmp-server community public RO
snmp-server trap-source vlan 1
mac address-table notification change
mac address-table notification mac-move
```

Nätverk

Appendix #1 – Core Network

Innehåll

- Core Router
- Core Switch
- Core Switch #1
- Core Switch #2

Core Router

```
Hostname CoreRouter
!
line console 0
password cisco
loggin synchronous
login
!
enable secret class
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.0.0.1
ip dhcp excluded-address 10.0.4.1
ip dhcp excluded-address 10.0.6.1
ip dhcp excluded-address 10.0.7.1
ip dhcp excluded-address 10.0.9.1 10.0.9.44
ip dhcp excluded-address 10.0.9.1 10.0.9.127
ip dhcp excluded-address 10.0.9.129
ip dhcp excluded-address 10.0.9.123
!
ip dhcp pool AFU
Network 10.0.0.0 255.255.252.0
default-router 10.0.0.1
!
Ip dhcp pool EA
Network 10.0.4.0 255.255.254.0
default-router 10.0.4.1
!
Ip dhcp pool WLAN
Network 10.0.6.0 255.255.255.0
Default-router 10.0.6.1
!
Ip dhcp pool ConfRoom
Network 10.0.7.0 255.255.255.0
Default-router 10.0.7.1
!
Ip dhcp pool MS
Network 10.0.8.128 255.255.255.128
Default-router 10.0.8.129
!
Ip dhcp pool Management
```

```
Network 10.0.9.128 255.255.255.192
Default-router 10.0.9.129
!
No ip domain lookup
!
Interface fastethernet0/0
No ip address
Ip access-group company in
Ip access-group MainBuilding out
Ip nat inside
Duplex auto
Speed auto
No shutdown
!
Interface fastethernet0/0.10
Encapsulation dot1Q 10
Ip address 10.0.0.1 255.255.252.0
Ip nat inside
!
Interface fastethernet0/0.20
Encapsulation dot1Q 20
Ip address 10.0.4.1 255.255.254.0
Ip nat inside
!
Interface fastethernet0/0.30
Encapsulation dot1Q 30
Ip address 10.0.6.1 255.255.255.0
Ip nat inside
!
Interface fastethernet0/0.40
Encapsulation dot1Q 40
Ip address 10.0.8.129 255.255.255.128
Ip nat inside
!
Interface fastethernet0/0.50
Encapsulation dot1Q 50
Ip address 10.0.9.193 255.255.255.192
Ip nat inside
!
Interface fastethernet0/0.60
Encapsulation dot1Q 60
Ip address 10.0.7.1 255.255.255.0
```

```
Ip nat inside
!
Interface fastethernet0/0.70
Encapsulation dot1Q 70
Ip address 10.0.9.129 255.255.255.192
Ip nat inside
!
Interface fastethernet0/0.99
Encapsulation dot1Q 99
Ip address 10.0.9.1 255.255.255.128
!
Interface Serial0/3/0
Ip address 203.202.201.201 255.255.255.252
Ip access-group ISP out
Ip nat outside
No shutdown
!
Interface serial0/3/1
Ip address 10.0.10.1 255.255.255.252
Ip access-group BranchOffice out
Ip nat inside
Encapsulation frame-relay
Ip ospf network point-to-point frame-relay map ip 10.0.10.2 201 broadcast
No shutdown
!
Router ospf 1
Log-adjency-changes
Network 10.0.0.0 0.0.3.255 area 0
Network 10.0.4.0 0.0.1.255 area 0
Network 10.0.8.128 0.0.0.127 area 0
Network 10.0.9.0 0.0.0.127 area 0
Network 10.0.9.128 0.0.0.63 area 0
Network 10.0.9.192 0.0.0.63 area 0
Network 10.0.10.0 0.0.0.3 area 0
Default-information originate
!
Ip route 0.0.0.0 0.0.0.0 serial 0/1/0
!
Ip http server
Ip nat source static tcp 10.0.9.195 80 interface serial0/1/0 80
Ip nat inside source list NAT interface serial 0/1/0 overload
```

```
Ip nat inside source static tcp 10.0.9.194 20 203.202.201.201 20
Ip nat inside source static tcp 10.0.9.194 21 203.202.201.201 21
Ip nat inside source static tcp 10.0.9.194 23 203.202.201.201 23
Ip nat inside source static tcp 10.0.9.197 110 203.202.201.201 110
Ip nat inside source static tcp 10.0.9.197 25 203.202.201.201 25
Ip nat inside source static tcp 10.0.9.204 10011 203.202.201.201 10011
Ip nat inside source static tcp 10.0.9.203 9987 203.202.201.201 9987
Ip nat inside source static tcp 10.0.9.202 3784 203.202.201.201 3784
Ip nat inside source static tcp 10.0.9.201 995 203.202.201.201 995
Ip nat inside source static tcp 10.0.9.200 993 203.202.201.201 993
Ip nat inside source static tcp 10.0.9.199 443 203.202.201.201 443
Ip nat inside source static tcp 10.0.9.198 143 203.202.201.201 143
Ip nat inside source static tcp 10.0.9.196 8000 203.202.201.201 8000
Ip nat inside source static tcp 10.0.9.195 80 203.202.201.201 80
Ip nat inside source static tcp 10.0.9.194 1723 203.202.201.201 1723
!
Ip access-list extended BranchOffice
Permit icmp anu anu echo-reply
Permit tcp any any eq www
Permit tcp any any eq 8000
Permit icmp 10.0.0.0 0.0.3.255 any
Permit icmp 10.0.4.0 0.0.1.255 any
Permit icmp 10.0.7.0 0.0.0.255 any
Permit icmp 10.0.8.128 0.0.0.127 any
Permit icmp 10.0.9.0 0.0.0.127 any
Permit icmp 10.0.9.128 0.0.0.63 any
Permit icmp 10.0.9.192 0.0.0.63 any
Permit icmp 10.0.9.128 0.0.0.63 10.0.8.0 0.0.0.127
Permit tcp any any established
Ip access-list extended ISP
Permit ip any any echo-reply
Permit ip 10.0.0.0 0.0.3.255 10.0.9.192 0.0.0.63
Permit ip 10.0.4.0 0.0.1.255 10.0.9.192 0.0.0.63
Permit ip 10.0.6.0 0.0.0.255 10.0.9.192 0.0.0.63
Permit ip 10.0.7.0 0.0.0.255 10.0.9.192 0.0.0.63
Permit ip 10.0.8.0 0.0.0.255 10.0.9.192 0.0.0.63
Permit ip 10.0.9.0 0.0.0.127 10.0.9.192 0.0.0.63
Permit ip 10.0.9.128 0.0.0.63 10.0.9.192 0.0.0.63
Permit icmp any 10.0.9.192 0.0.0.63
Permit tcp any any eq 8000
Permit tcp any any eq www
Permit tcp any 10.0.9.192 0.0.0.63 eq ftp
```

Permit tcp any 10.0.9.192 0.0.0.63 eq ftp-data
Permit tcp any 10.0.9.192 0.0.0.63 eq smtp
Permit tcp any 10.0.9.192 0.0.0.63 eq pop3
Permit tcp any 10.0.9.192 0.0.0.63 eq 143
Permit tcp any 10.0.9.192 0.0.0.63 eq 443
Permit tcp any 10.0.9.192 0.0.0.63 eq 22
Permit tcp any 10.0.9.192 0.0.0.63 eq telnet
Permit tcp any 10.0.9.192 0.0.0.63 eq 993
Permit tcp any 10.0.9.192 0.0.0.63 eq 995
Permit tcp any 10.0.9.192 0.0.0.63 eq 3784
Permit tcp any 10.0.9.192 0.0.0.63 eq 9987
Permit tcp any 10.0.9.192 0.0.0.63 eq 10011
Permit tcp any 10.0.9.192 0.0.0.63 eq 1723
Permit ip 10.0.4.0 0.0.1.255 10.0.8.128 0.0.0.127
Permit ip 10.0.8.128 0.0.0.127 10.0.4.0 0.0.1.255
Permit ip 10.0.9.128 0.0.0.63 any
Permit tcp any 10.0.9.192 0.0.0.63 range 40000 45000
Permit tcp any 10.0.9.128 0.0.0.63 www
Permit tcp any a ny established
Ip access-list extended NAT
Permit ip 10.0.0.0 0.0.3.255 any
Permit ip 10.0.4.0 0.0.1.255 any
Permit ip 10.0.6.0 0.0.0.255 any
Permit ip 10.0.7.0 0.0.0.255 any
Permit ip 10.0.9.128 0.0.0.63 any
Permit ip 10.0.9.192 0.0.0.63 any
Permit ip 10.0.8.128 0.0.0.127 any
Permit ip 10.0.9.0 0.0.0.127 any
Permit ip 10.0.8.0 0.0.0.127 any
!
Bannes motd &
****
Welcome to Core Router
Unauthorized access is
Strictly prohibited
****
&
!
Line aux 0
Line vty 0 4
Password cisco
Logging synchronous

Login
!
End

Core Switch

```
Hostname CoreSwitch
!
Enable secret class
!
Vtp mode server
Vtp domain company
Ctp password cisco
!
Vlan 10
name AFU
Exit
!
Vlan 20
name EA
Exit
!
Vlan 30
name WLAN
Exit
!
Vlan 40
name MS
Exit
!
Vlan 50
name Servers
Exit
!
Vlan 60
name ConfRoom
Exit
!
Vlan 70
name Management
Exit
!
Vlan 99
name SwitchManagement
Exit
!
```

```
No ip domain-lookup
Ip name-server 0.0.0.0
!
Interface range fastethernet0/1-24
Switchport mode trunk
Switchport trunk native vlan 99
!
Interface range gigabitethernet0/1-2
Switchport trunk native vlan 99
Switchoport mode trunk
!
Interface vlan 99
Ip address 10.0.9.2 255.255.255.128
!
Banner motd &
**************************
Welcome to CoreSwitch
Unauthorized access is
Strictly prohibited
**************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Lone vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Core Switch #1

```
Hostname CoreSwitch1
!
Enable secret class
!
Vtp mode client
Vtp domain company
Vtp password cisco
!
No ip domain-lookup
Ip name-server 0.0.0.0
!
Interface range fastethernet0/1-24
Switchport trunk native vlan 99
Switchport mode trunk
!
Interface range gigabitethernet0/1-2
Switchport trunk native vlan 99
Switchport mode trunk
!
Interface vlan 99
Ip address 10.0.9.3 255.255.255.128
!
Banner motd &
**************************
Welcome to CoreSwitch1
Unauthorized access is
Strictly prohibited
**************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Lone vty 5 15
Password cisco
Logging synchronous
```

Login
!
End

Appendix #2 – Branch Office

Innehåll

- Branch Router

Branch Router

Hostnamt Branch
!
Enable secret class
!
No ip dhcp use vrf connected
Ip dhcp excluded-address 10.0.8.1 10.0.8.3
!
Ip dhcp pool Branch
Network 10.0.8.0 255.255.255.128
Default-router 10.0.8.1
!
No ip domain-lookup
!
Interface fastethernet0/0
Ip address 10.0.8.1 255 255 255.128
Speed auto
No shutdown
!
Interface serial0/1/1
Ip address 10.0.10.2 255.255.255.252
Encapsulation frame-relay
Ip ospf network point-to-point
Frame-relay map ip 10.0.10.1 102 broadcast
No shutdown
!
Router ospf 1
Log-adjency-changes
Network 10.0.8.0 0.0.0.127 area 0
Network 10.0.10.0 0.0.0.3 area 0
Default-information originate
!
Banner motd &
****
BRANCH OFFICE
****
&
!
Line console 0
Password cisco
Logging synchronous

Login
Line vty 0 4
Password cisco
Login
!
End

Appendix #3 – Avdelning för Forskning och Utveckling

Innehåll

Avdelning för Forskning och Utveckling Distribution Switch #1

```
Hostname AFUMain1
!
Enable secret class
!
Vtp mode client
Vtp domain company
Vtp password cisco
!
No ip domain-lookup
Ip name-server
0.0.0.0
!
Interface range fastethernet0/1-23
Switchport trunk native vlan 99
Switchport mode trunk
!
Interface fastethernet0/24
Switchport mode access
Switchport access vlan 30
!
Interface range Gigabitethernet0/1-2
Switchport trunk native vlan 99
Switchport mode trunk
!
Interface vlan 99
Ip address 10.0.9.5 255.255.255.128
!
Banner motd &
**************************
Welcome to AFUMain1
Unauthorized access is
Strictly prohibited
**************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
```

Line vty 5 15
Password
Logging synchronous
Login
!
End

Avdelning för Forskning och Utveckling Distribution Switch #2

Hostname AFUMain2
!
Enable secret class
!
Vtp mode client
Vtp domain company
Vtp password cisco
!
No ip domain-lookup
Ip name-server 0.0.0.0
!
Interface range fastethernet0/1-23
Switchport trunk native vlan 99
Switchport mode trunk
!
Interface fastethernet0/24
Switchport mode access
Switchport access vlan 30
!
Interface range Gigabitethernet0/1-2
Switchport trunk native vlan 99
Switchport mode trunk
!
Interface vlan 99
Ip address 10.0.9.6 255.255.255.128
!
Banner motd &
****
Welcome to AFUMain2
Unauthorized access is
Strictly prohibited
****
&
!

Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 5 15
Password
Logging synchronous
Login
!
End

Avdelning för Forskning och Utveckling Access Switch #2

Hostname AFU1
!
Enable secret class
!
Vtp mode client
Vtp domain company
Vtp password cisco
!
No ip domain-lookup
!
Interface range fastethernet0/1-24
Switchport mode access
Switchport access vlan 10
!
Interface range gigabitethernet0/1-2
Switchport trunk native vlan 99
Switchport mode trunk
!
Interface vlan 99
Ip address 10.0.9.11 255.255.255.128
!
Banner motd &
****
Welcome to AFU 1
Unauthorized access is
Strictly prohibited
****
&

```
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Avdelning för Forskning och Utveckling Access Switch #2

```
Hostname AFU2
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 10
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.12 255.255.255.128
!
```

```
banner motd &

******************************
Welcome to AFU 2
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Avdelning för Forskning och Utveckling Access Switch #3

```
Hostname AFU3
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 10
!
interface range GigabitEthernet 1/1-2
```

```
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.13 255.255.255.128
!
banner motd &

******************************
Welcome to AFU 3
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Avdelning för Forskning och Utveckling Access Switch #4

```
Hostname AFU4
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
```

```
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 10
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.14 255.255.255.128
!
banner motd &

******************************
Welcome to AFU 4
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Avdelning för Forskning och Utveckling Access Switch #5

```
Hostname AFU5
!
enable secret class
```

```
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 10
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.15 255.255.255.128
!
banner motd &

******************************
Welcome to AFU 5
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Avdelning för Forskning och Utveckling Access Switch #6

```
Hostname AFU6
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 10
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.16 255.255.255.128
!
banner motd &

******************************
Welcome to AFU 6
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
```

Logging synchronous
Login
!
End

Avdelning för Forskning och Utveckling Access Switch #7

Hostname AFU7
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 10
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.17 255.255.255.128
!
banner motd &

****
Welcome to AFU 7
Unauthorized access is
Strictly prohibited
****
&
!
Line console 0
Password cisco
Logging synchronous

```
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Avdelning för Forskning och Utveckling Access Switch #8

```
Hostname AFU8
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 10
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.18 255.255.255.128
!
banner motd &

******************************
Welcome to AFU 8
Unauthorized access is
Strictly prohibited
```

****
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End

Avdelning för Forskning och Utveckling Access Switch #9

Hostname AFU9
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 10
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.19 255.255.255.128
!

```
banner motd &

******************************
Welcome to AFU 9
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Avdelning för Forskning och Utveckling Access Switch #10

```
Hostname AFU10
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 10
!
interface range GigabitEthernet 1/1-2
```

```
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.20 255.255.255.128
!
banner motd &

******************************
Welcome to AFU 10
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Appendix #4 – Ekonomi och administration (EA)

Innehåll

- Ekonomi och administration Distribution Switch
- Ekonomi och administration Access Switch #1
- Ekonomi och administration Access Switch #2
- Ekonomi och administration Access Switch #3

Ekonomi och administration Distribution Switch

```
Hostname EAMain
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
ip name-server 0.0.0.0
!
interface range fastEthernet 0/1-23
switchport trunk native vlan 99
switchport mode trunk
!
interface fastEthernet 0/24
switchport mode access
switchport access vlan 30
!
interface GigabitEthernet 1/1-2
switchport mode trunk
switchport trunk native vlan 99
!
interface vlan 99
ip address 10.0.9.8 255.255.255.128
!
banner motd &
*****************************
Welcome to EAMaIn
Unauthorized access is
Strictly prohibited
*****************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 5 15
Password cisco
```

```
Logging synchronous
Login
!
End
```

Ekonomi och administration Access Switch #1

```
hostname EA1
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 20
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.21 255.255.255.128
!
banner motd &

******************************
Welcome to EA1
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
```

```
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Ekonomi och administration Access Switch #2

```
hostname EA2
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 20
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.22 255.255.255.128
!
banner motd &

******************************
Welcome to EA2
Unauthorized access is
Strictly prohibited
******************************
&
```

```
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Ekonomi och administration Access Switch #3

```
hostname EA3
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 20
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.23 255.255.255.128
!
banner motd &

**********
```

Welcome to EA3
Unauthorized access is
Strictly prohibited
****
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End

Appendix #5 – Marknad och försäljning /server/Management (MSSM)

Innehåll

- MSSM Distribution Switch
- Marknad och försäljning Access Switch
- Server Access Switch
- Management Access Switch

MSSM Distrubution Switch

```
Hostname MSSM
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
ip name-server 0.0.0.0
!
interface range fastEthernet 0/1-23
switchport trunk native vlan 99
switchport mode trunk
!
interface fastEthernet 0/24
switchport mode access
switchport access vlan 30
!
interface GigabitEthernet 1/1-2
switchport mode trunk
switchport trunk native vlan 99
!
interface vlan 99
ip address 10.0.9.7 255.255.255.128
!
banner motd &
******************************
Welcome to MSSM
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 5 15
Password cisco
```

Logging synchronous
Login
!
End

Marknad och Försäljning Access Switch

hostname MS
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 40
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.24 255.255.255.128
!
banner motd &

****
Welcome to MS
Unauthorized access is
Strictly prohibited
****
&
!
Line console 0
Password cisco
Logging synchronous
Login

!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End

Server Access Switch

hostname Server
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 50
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.26 255.255.255.128
!
banner motd &

****
Welcome to Server
Unauthorized access is
Strictly prohibited
****

&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End

Management Access Server

hostname Management
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 70
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
interface vlan 99
ip address 10.0.9.25 255.255.255.128
!

banner motd &

****
Welcome to Management
Unauthorized access is
Strictly prohibited
****
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End

Appendix #6 – Konferensrum

Innehåll

- Konferens Distribution Switch
- Konferens Access Switch #1
- Konferens Access Switch #2
- Konferens Access Switch #3
- Konferens Access Switch #4
- Konferens Access Switch #5
- Konferens Access Switch #6
- Konferens Access Switch #7
- Konferens Access Switch #8
- Konferens Access Switch #9

- Konferens Access Switch #10

Konferens Distrubution Switch

```
Hostname ConfRoomMain
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
ip name-server 0.0.0.0
!
interface range fastEthernet 0/1-23
switchport trunk native vlan 99
switchport mode trunk
!
interface fastEthernet 0/24
switchport mode access
switchport access vlan 30
!
interface GigabitEthernet 1/1-2
switchport mode trunk
switchport trunk native vlan 99
!
interface vlan 99
ip address 10.0.9.9 255.255.255.128
!
banner motd &
*****************************
Welcome to ConfRoomMain
Unauthorized access is
Strictly prohibited
*****************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 5 15
Password cisco
```

Logging synchronous
Login
!
End

Konferens Access Switch #1

hostname ConfRoom1
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 60
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
banner motd &

****
Welcome to ConfRoom1
Unauthorized access is
Strictly prohibited
****
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15

Password cisco
Logging synchronous
Login
!
End

Konferens Access Switch #2

hostname ConfRoom2
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 60
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
banner motd &
****
Welcome to ConfRoom2
Unauthorized access is
Strictly prohibited
****
&
!
Line console 0
Password cisco
Logging synchronous
Login

!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End

Konferens Access Switch #3

hostname ConfRoom3
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 60
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
banner motd &

****
Welcome to ConfRoom3
Unauthorized access is
Strictly prohibited
****

&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End

Konferens Access Switch #4

```
hostname ConfRoom4
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 60
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
banner motd &

******************************
Welcome to ConfRoom4
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Konferens Access Switch #5

```
hostname ConfRoom5
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 60
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
banner motd &

******************************
Welcome to ConfRoom5
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Konferens Access Switch #6

```
hostname ConfRoom6
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 60
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
banner motd &

******************************
Welcome to ConfRoom6
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Konferens Access Switch #7

```
hostname ConfRoom7
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 60
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
banner motd &

******************************
Welcome to ConfRoom7
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Konferens Access Switch #8

```
hostname ConfRoom8
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 60
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
banner motd &

******************************
Welcome to ConfRoom8
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Konferens Access Switch #9

```
hostname ConfRoom9
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 60
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
banner motd &

******************************
Welcome to ConfRoom9
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

Konferens Access Switch #10

```
hostname ConfRoom10
!
enable secret class
!
vtp mode client
vtp domain company
vtp password cisco
!
no ip domain-lookup
!
interface range fastEthernet 0/1-24
switchport mode access
switchport access vlan 60
!
interface range GigabitEthernet 1/1-2
switchport trunk native vlan 99
switchport mode trunk
!
banner motd &

******************************
Welcome to ConfRoom10
Unauthorized access is
Strictly prohibited
******************************
&
!
Line console 0
Password cisco
Logging synchronous
Login
!
Line vty 0 4
Login
Line vty 5 15
Password cisco
Logging synchronous
Login
!
End
```

VLSM - Tabell

Name	Type	IP	IP assignement	Net mask	Vlan	Interface	Interface type
CoreRouter	Router	10.0.9.1	Static	255.255.255.128		Gi	Trunk
CoreSwitch	Switch	10.0.9.2	Static	255.255.255.128	Vlan 99		
CoreSwitch1	Switch	10.0.9.3	Static	255.255.255.128	Vlan 99	Gi	Trunk
CoreSwitch2	Switch	10.0.9.4	Static	255.255.255.128	Vlan 99	Gi	Trunk
AFUMain	Switch	10.0.9.5	Static	255.255.255.128	Vlan 99	Gi	Trunk
AFUMain2	Switch	10.0.9.6	Static	255.255.255.128	Vlan 99	Gi	Trunk
Administration	Switch	10.0.9.7	Static	255.255.255.128	Vlan 99	Gi	Trunk
E&A	Switch	10.0.9.8	Static	255.255.255.128	Vlan 99	Gi	Trunk
ConfRoom	Switch	10.0.9.9	Static	255.255.255.128	Vlan 99	Gi	Trunk
BranchOffice	Switch	10.0.9.10	Static	255.255.255.128	Vlan 99	Gi	Trunk
AFU1	Switch	10.0.9.11	Static	255.255.255.128	Vlan 99	Fe	Access
AFU2	Switch	10.0.9.12	Static	255.255.255.128	Vlan 99	Fe	Access
AFU3	Switch	10.0.9.13	Static	255.255.255.128	Vlan 99	Fe	Access
AFU4	Switch	10.0.9.14	Static	255.255.255.128	Vlan 99	Fe	Access
AFU5	Switch	10.0.9.15	Static	255.255.255.128	Vlan 99	Fe	Access
AFU6	Switch	10.0.9.16	Static	255.255.255.128	Vlan 99	Fe	Access
AFU7	Switch	10.0.9.17	Static	255.255.255.128	Vlan 99	Fe	Access
AFU8	Switch	10.0.9.18	Static	255.255.255.128	Vlan 99	Fe	Access
AFU9	Switch	10.0.9.19	Static	255.255.255.128	Vlan 99	Fe	Access
AFU10	Switch	10.0.9.20	Static	255.255.255.128	Vlan 99	Fe	Access

Name	Type	IP	IP assignement	Net mask	Vlan	Interface	Interface type
E&A1	Switch	10.0.9.21	Static	255.255.255.128	Vlan 99	Fe	Access
E&A2	Switch	10.0.9.22	Static	255.255.255.128	Vlan 99	Fe	Access
E&A3	Switch	10.0.9.23	Static	255.255.255.128	Vlan 99	Fe	Access
M&S	Switch	10.0.9.24	Static	255.255.255.128	Vlan 99	Fe	Access
Management	Switch	10.0.9.25	Static	255.255.255.128	Vlan 99	Fe	Access
Server	Switch	10.0.9.26	Static	255.255.255.128	Vlan 99	Fe	Access
AFUAP1	AP	10.0.9.27	Static	255.255.255.128	Vlan 99	802.11.g	Access
AFUAP2	AP	10.0.9.28	Static	255.255.255.128	Vlan 99	802.11.g	Access
AFUAP3	AP	10.0.9.29	Static	255.255.255.128	Vlan 99	802.11.g	Access
AFUAP4	AP	10.0.9.30	Static	255.255.255.128	Vlan 99	802.11.g	Access
ADMINAP	AP	10.0.9.31	Static	255.255.255.128	Vlan 99	802.11.g	Access
E&AAP	AP	10.0.9.32	Static	255.255.255.128	Vlan 99	802.11.g	Access
CONFAP	AP	10.0.9.33	Static	255.255.255.128	Vlan 99	802.11.g	Access
BRANCHAP	AP	10.0.9.34	Static	255.255.255.128	Vlan 99	802.11.g	Access
ConfRoom1	Switch	10.0.9.35	Static	255.255.255.128	Vlan 99	Fe	Access
ConfRoom2	Switch	10.0.9.36	Static	255.255.255.128	Vlan 99	Fe	Access
ConfRoom3	Switch	10.0.9.37	Static	255.255.255.128	Vlan 99	Fe	Access
ConfRoom4	Switch	10.0.9.38	Static	255.255.255.128	Vlan 99	Fe	Access
ConfRoom5	Switch	10.0.9.39	Static	255.255.255.128	Vlan 99	Fe	Access
ConfRoom6	Switch	10.0.9.40	Static	255.255.255.128	Vlan 99	Fe	Access
ConfRoom7	Switch	10.0.9.41	Static	255.255.255.128	Vlan 99	Fe	Access
ConfRoom8	Switch	10.0.9.42	Static	255.255.255.128	Vlan 99	Fe	Access
ConfRoom9	Switch	10.0.9.43	Static	255.255.255.128	Vlan 99	Fe	Access
ConfRoom10	Switch	10.0.9.44	Static	255.255.255.128	Vlan 99	Fe	Access

Name	IP	Assignable Addreses	Subnet	Subnet mask	Broadcast	Total address	Total addresses	Router IP	VLAN
AFU	10.0.0.0	10.0.0.1 – 10.0.3.254	/22	**255.255.252.0**	10.0.3.255	742	1024	10.0.0.1	Vlan 10
E & A	10.0.4.0	10.0.4.1 – 10.0.5.254	/23	**255.255.254.0**	10.0.5.255	272	512	10.0.4.1	Vlan 20
WLAN	10.0.6.0	10.0.6.1 – 10.0.6.254	/24	**255.255.255.0**	10.0.6.255	200	256	10.0.6.1	Vlan 30
Conf Rooms	10.0.7.0	10.0.7.1 – 10.0.7.254	/24	**255.255.255.0**	10.0.7.255	140	256	10.0.7.1	Vlan 60
Branch	10.0.8.0	10.0.8.1 – 10.0.8.126	/25	**255.255.255.128**	10.0.8.127	107	128		
M&S	10.0.8.128	10.0.8.129 – 10.0.8.254	/25	**255.255.255.128**	10.0.8.255	66	128	10.0.8.129	Vlan 40
SwitchMng	10.0.9.0	10.0.9.1 - 10.0.9.126	/25	**255.255.255.128**	10.0.9.127	34	128	10.0.9.1	Vlan 99
Management	10.0.9.128	10.0.9.129 - 10.0.9.188	/26	**255.255.255.192**	10.0.9.189	31	64	10.0.9.129	Vlan 70
Servers	10.0.9.192	10.0.9.193 - 10.0.9.254	/26	**255.255.255.192**	10.0.9.255	42	64	10.0.9.193	Vlan 50
External IP	**201.202.203.204**								