

Metoder för trådlös gästaccess

METHODES FOR WIRELESS GUEST ACCESS

Marcus Kallur

MÄLARDALENS HÖGSKOLA | AKADEMIN FÖR INNOVATION, DESIGN OCH TEKNIK

HÖGSKOLEINGENJÖR I NÄTVERKSTEKNIK

HANDLEDARE MDH: HANS BJURGREN & STEFAN LÖFGREN

HANDLEDARE CYGATE AB: SUSANNE COLDE

EXEMINATOR: MATS BJÖRKMAN

DATUM: 2015-06-26

Sammanfattning

Det här arbetet är till för att belysa några av de metoder som finns när ett företag ska implementera trådlös gästaccess i deras nätverk. Du som läsare kommer att få en inblick i tre olika metoder; "Självregistrering", "Besöksmottagare" och metoden "Öppet". Metoden "Självregistrering" är en metod där gästen registrerar sig via en portal som är webbaserad och sedan får ett konto som används för att logga in på nätverket. Metoden "Besöksmottagare" är en metod som använder sig av en företagsanställd som skapar och delar ut konton individuellt till gästerna. Metoden "Öppet" är när gästerna bara behöver ansluta sig till nätverket och då direkt få tillgång till det. Arbetet är till för att ge en djupare analys av de tre metoderna genom att beskriva olika fördelar och nackdelar som varje metod har vid en implementation. Det här arbetet kommer även beskriva användarupplevelsen för gästerna och de konfigureringssvårigheter som metoderna har. För de som är mer intresserade av autentiseringsprocessen för varje metod finns det i det här arbetet en beskrivning om vilka steg enheterna går igenom för att autentisera en användare. Det här arbetet har även kommit fram till några exempel där de olika metoderna skulle kunna passa in; metoden "Självregistrering" passar t.ex. in på ett företag som har många gäster och krav på bra spårbarhet av de enheter som finns i nätverket.

Abstract

This thesis is about a few methods that exist for a company that is in the stage of implementing a solution for wireless guest access. As a reader of this thesis you will be introduced to the three methods; "Self-registration", "Visit receiver" and the method "Open". The method "Self-registration" is a method that uses a web based portal where guests register an account that they will use for access to the network. The method "Visit receiver" uses a company employee that creates and hands out accounts individual for all the guests. "Open" is a method where the guests just connect to the network and right away get access. This thesis will do a deep analyze of these three methods and describe what advantages and disadvantages each method have when chosen to implement. The user experience has also been evaluated in this thesis for all three methods and difficulties with each method have also been mentioned in this report. For those who want to know more about the authentication process this thesis has described the steps that the network devices have to go through to authenticate a user. This thesis have also resulted in a description of what type of situation a method would be preferred to use; method "Self-registration" would fit in a situation when the company have many guests and need for good traceability for all the devices in the network.

Förord

Jag vill tacka mina handledare på Mälardalens Högskola Hans Bjurgren och Stefan Löfgren både för hjälpen med examensarbetet men även för de tre åren på programmet.

Sedan vill jag tacka alla på Cygate som hjälpt mig med både det tekniska och teoretiska under det här arbetet. Framförallt vill jag tacka Susanne Colde och Richard von Essen som agerat handledare på plats.

Avgränsningar

Inga exakta protokoll kommer tas upp eller hur de fungerar i detta arbete. Ingen djupare analys på de olika enheter som kan användas som gästaccess-server i ett nätverk utan ett par nämns bara och används i experimenten. Arbetet kommer inte att ta upp alla delar när ett nätverk ska planeras utan hålla sig till hur autentiseringen och policys för gästerna kan se ut. Arbetet förutsätter att ett företags-LAN finns och fungerar.

Innehållsförteckning

Sammanfattning	1
Abstract	2
Förord.....	3
Avgränsningar	3
1 Inledning	5
1.1 Bakgrund	6
1.1.1 State of Practice (SOP)	7
1.2 Behov/Problem	8
1.3 Metod.....	9
1.4 Material	10
2 Avhandling.....	12
2.1 Vad menas med ett trådlöst nätverk?	12
2.2 Lagring av uppgifter	14
2.3 Olika metoder.....	15
2.3.1 Självregistrering	16
2.3.2 Besöksmottagare	18
2.3.3 Öppet	21
3 Fördjupning	23
3.1 Självregistrering	23
3.1.1 Varför Självregistrering?	24
3.1.2 Hur ser stegen ut?.....	25
3.1.3 Användarupplevelse med självregistrering	26
3.1.4 Var passar självregistrering?.....	27
3.2 Besöksmottagare	28
3.2.1 Varför Besöksmottagare?	29
3.2.2 Hur ser stegen ut för autentisering?	29
3.2.3 Användarupplevelse med besöksmottagare	30
3.2.4 Vart passa besöksmottagare?	31
3.3 Öppet.....	31
3.3.1 Varför Öppet?	32
3.3.2 Hur ser anslutningsstegen ut för Öppet?	32
3.3.3 Användarupplevelsen.....	33
3.3.4 Vart passar ett öppet nätverk?.....	33

4	Resultat.....	34
5	Analys av resultatet	36
6	Avslutning	37
6.1	Framtida arbeten	38
7	Källförteckning	39
8	Bilagor	42

1 Inledning

Syftet med det här examensarbetet är att undersöka några av de olika gästaccessmetoder som idag finns att implementera. De tre metoder som arbetet tar upp kommer att utvärderas med både för- och nackdelar. Metoderna kommer även att utvärderas på ett sådant sätt att rekommendationer kommer ges om vart var och en av dessa metoder kan passa in. De metoder som belyses i det här arbetet är "Självregistrering", "Besöksmottagare" och "Öppet". Då tiden för det här arbetet är åtta veckor kommer inte en djupare analys göras på hur själva flödespaketet ser ut. Istället kommer fokus ligga på hur flödet sker i nätverket när någon ska autentisera sig och hur ett företag ska tänka när de väljer metod för just deras nätverk.

Då gästaccess är ett relativt brett område som även kan innefatta t.ex. hur QoS (Quality of Service) ska byggas upp för ett nätverk och vilka servrar som ska användas, kommer inte detta arbete gå in på djupet av dessa områden utan istället kort beskriva vilka best practices det finns att ta hänsyn till när en företagslösning för gästaccess ska göras. Detta kommer att finnas under rubriken 1.1.1 State of Practice (SOP).

1.1 Bakgrund

Idag ställs det allt högre krav på att en internetanslutning ska erbjudas de personer som kommer som gäster till ett företag. Förr i tiden fanns det bara trådade nätverk och då saknades möjligheten att ansluta enheter utan lämpligt uttag. Med den utveckling som gjorts inom trådlösa alternativ så kan numera enheter som t.ex. telefoner och surfplattor få internetanslutning på ett enkelt sätt. Allt som behövs är ett trådlöst nätverkskort. Denna utveckling gör att företagen får ställa sig frågan hur de ska kunna möta de krav som deras gäster kommer att ställa på nätverket.

Den forskning som hittats angående trådlösa nätverk har mestadels varit på hur trådlösa nätverk fungerar medan det har varit desto svårare att hitta forskning som fokuserat på gästaccess-metoder. Den information som hittats angående gästaccess har varit olika case studies eller best practices från olika personer.

Cisco släppte år 2014 mjukvaruversionen 1.3 till deras enhet ISE (Identity Services Engine) [1]. Med denna uppgradering så möjliggjordes det att kunna ge notifikationer via SMS (Short Message Service) istället för via Epost som tidigare versioner stöder [2]. Det är denna enhet och mjukvaruversionen som större delen av det här arbetet bygger på. Då arbetet inte ska bli för låst till Ciscos produkt ISE så kommer Arubas motsvarighet, ClearPass, att nämnas. Någon djupare analys på hur den produkten fungerar i ett nätverk kommer inte att göras.

1.1.1 State of Practice (SOP)

Best practice står för god praxis och är ett begrepp på riktlinjer som kan följas när ett nätverk ska implementeras. Best practice är inte begränsat bara till nätverk, utan är ett begrepp som används i alla branscher.

Best practice pratas det ofta om när ett nätverk ska byggas. Det är dock inget som måste följas när någon sätter upp och konfigurerar ett nätverk. Best practice i ett nätverk brukar innefatta redundanta vägar så att det inte nätverket går ner ifall någon länk/enhet skulle gå sönder. Det är bra att försöka använda best practice när det finns möjligheten till det, då det är riktlinjer som är utformade att optimera ett nätverk och göra det så stabilt som möjligt. Det finns även nätverk där best practice inte passar in. Ett nätverk kan exempelvis vara tvunget att avvika från best practice och använda sig av den äldre trådlösa standarden IEEE 802.11g i nätverket då företagets trådlösa access-punkt inte stödjer den nyare standarden IEEE 802.11n eller tvingas att inte använda redundanta vägar som rekommenderas. Anledningen skulle kunna vara kostnaden som kommer med att investera i nya enheter.

Olika företag som producerar enheter för nätverk har ofta sina egna åsikter på best practice och hur den ska följas för att ett nätverk med just deras enheter ska fungera optimalt. Sådana företag är Cisco, Aruba och Microsoft. Då best practice inte syftar på saker som måste göras har även enskilda individer egna idéer om detta. Det finns alltså individer som inte tillhör något företag som har sitt eget sätt att implementera best practice på. Dessa personer behöver inte nödvändigtvis ha riktlinjerna dokumenterade, utan kan utgå från erfarenhet och eget tycke.

Det här arbetet kommer att bygga på best practice från olika källor. Arbetet kommer att göra en djupare analys och fokusera på hur själva autentiseringen görs. Utöver det, kommer det att nämnas vilka saker som är bra att tänka på när en gäst har autentiserat sig och börjat använda internet via företaget. Dessa saker kommer kort beskrivas senare i arbetet. De referenser arbetet huvudsakligen kommer att använda är från Cisco och Aruba. Andra referenser från olika avhandlingar och oberoende partners och deras syn på best practice om gästaccess kommer också användas. Det referenserna ska ge svar på

angående best practice är hur de olika metoderna bör sättas upp och vad de ska innehålla samt för- och nackdelar med de olika metoderna.

Som tidigare nämnt så kommer inte fokus ligga på att beskriva QoS och hur det ska sättas upp för att vara så optimalt som möjligt. Dock kan QoS vara en stor del av ett nätverk, så en kort beskrivning av best practice för detta känns ändå nödvändigt. Best practice för QoS kan generellt sammanfattas enligt följande; för att få VoIP (Voice over IP) att fungera optimalt ska det vara högt prioriterat både från gäster och personal. Resterande trafik från gäster ska ha relativt låg prioritet för att inte störa företagets personals trafik [3, sid 88] [4, sid 7].

1.2 Behov/Problem

Det behov som finns av detta arbete är att det idag finns trådlösa nätverk hos nästan alla företag. Personer som kommer på besök till dessa företag förväntar sig att de ska kunna ansluta sina personliga eller arbetsrelaterade enheter till ett nätverk och på så sätt kunna arbeta eller surfa på internet. De nätverk som personerna ansluter sig till förväntas vara säkert för både dem som gäster men även för företaget som tillhandahåller nätverket. Det ska vara säkert så att gästerna inte kan komma åt och göra skadliga saker på företagets nätverk, men de ska samtidigt kunna utföra vardagliga saker samt eventuella arbeten via detta gästnätverk.

Det här arbetet ska ge en förståelse om vilka metoder som finns för ett företag att välja på när de planerar att installera och erbjuda gästaccess. Problemet med gästaccess är att det hela tiden utvecklas. Företag som vill använda gästaccess saknar ofta kunskapen om vilka val de kan göra för att få en lösning som passar just deras företag. Ett stort problem som gästaccess medför är även att företaget öppnar upp nätverket för potentiellt skadliga enheter, och accessen bör därför begränsas ner till endast internetåtkomst [5, sid 32]. Svårigheten med det är att det kan bli en stor utmaning att göra nätverket så säkert som företaget önskar när det inte bara är företagets egna enheter som trafikerar nätverket.

Detta arbete kommer ge svar på vilka sorters enheter som behövs för att lösa detta problem. Vilka konfigureringsvårigheter som kan finnas när företaget valt att installera en viss metod.

1.3 Metod

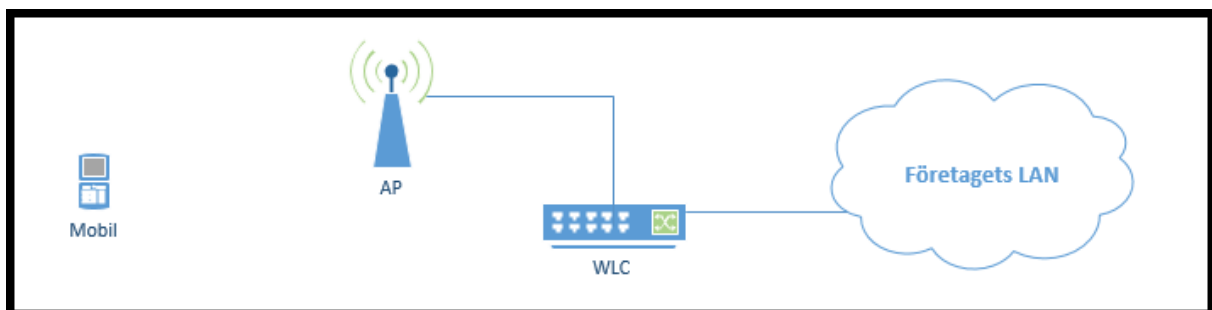
För att undersöka gästaccess på ett sätt som ger ett bra resultat kommer arbetet att genomföras med hjälp av några olika metoder. Då arbetet görs i samarbete med nätverksföretaget Cygate AB, vilket är ett stort företag med stora kunskaper inom ämnet, kommer en metod att utgå från deras expertis inom området och hur de brukar anpassa en lösning till ett projekt. På så sätt kommer arbetet kunna ge tillförlitliga och bra svar på hur en lösning kan se ut. En annan metod som kommer att användas är att läsa material från de olika tillverkarna av de enheter som behövs för en sådan lösning. Detta då de som producerat enheten förhoppningsvis har god kunskap om varför en viss metod ska användas och hur den ska sättas upp för att fungera på bästa sätt. Den tredje metoden kommer vara att läsa tidigare studier och avhandlingar på områden som belyser intressanta delar för detta arbete. Den sista metoden som arbetet kommer att använda sig av är att genomföra egna tester om hur metoderna konfigureras samt se hur de skulle kunna passa in på olika sorters företag.

1.4 Material

För att kunna göra detta arbete kommer det att behövas olika komponenter så att de metoder som arbetet tar upp kan sättas upp, testas och undersökas på rätt sätt.

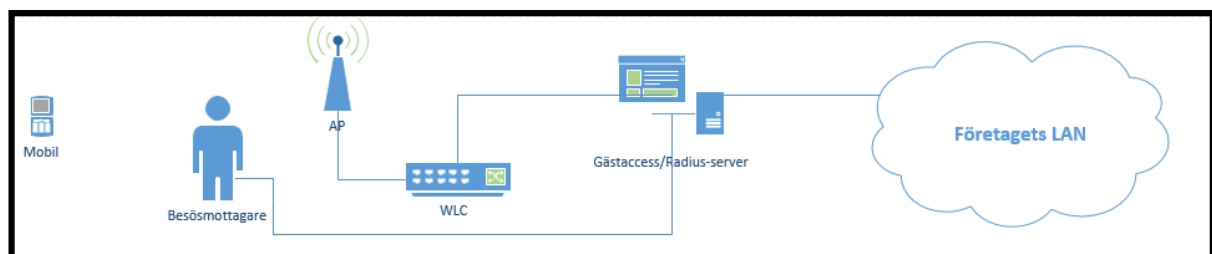
För att kunna sätta upp metoden "Öppet" kommer följande komponenter att behövas och sättas upp på följande sätt:

- En Wireless Lan Controller (WLC)
- En Accesspunkt (AP)
- En PC/Mobil



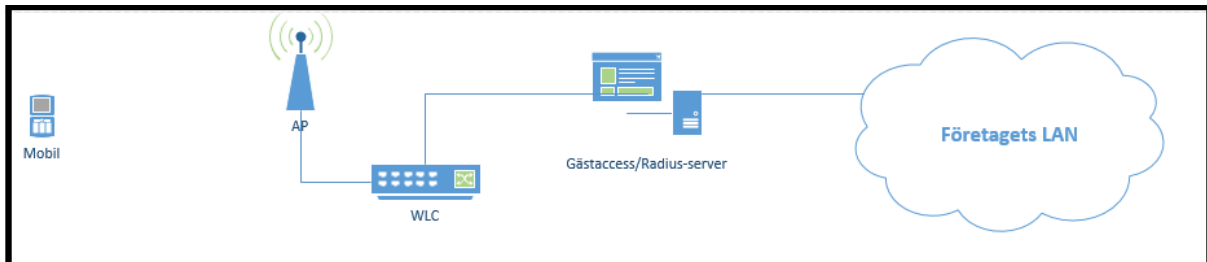
För att sätta upp metoden "Besöksmottagare" kommer följande komponenter att behövas och sättas upp på följande sätt:

- En WLC
- En AP
- En Gästaccess-server
- En Besöksmottagare
- En PC/Mobil



För metoden "Självregistrering" kommer följande komponenter att behövas och sättas upp på följande sätt:

- En WLC
- En AP
- En Gästaccess-server
- En PC/Mobil



De material som behövs för detta arbete kommer att tillhandahållas av Cygate AB. Materialet finns i Cygates labb och kan nås både via internet och på plats hos företaget. Som gästaccess-server kommer en Cisco ISE användas, Cisco 5508 agerar WLC och Cisco 600 Aironet agerar AP.

2 Avhandling

I följande del av rapporten kommer mer av det arbete och undersökningar som gjort presenteras.

2.1 Vad menas med ett trådlöst nätverk?

Med ett trådlöst nätverk, även kallat WLAN (Wireless Local Area Network) menas ett nätverk som saknar kablar. Det betyder inte att hela nätverket är trådlöst för t.ex. ett företag utan själva trådlösa delen sker mellan datornheten och en access-punkt. Trafiken mellan de olika nätverksenheterna som routrar och switchar sker via trådade förbindelser.

Det finns många fördelar med att använda sig av ett trådlöst nätverk för ett företag. Den största fördelen med ett trådlöst nätverk är att de anställda och alla andra personer som ansluter sig till nätverk har möjligheten att röra sig runt i lokalerna samtidigt som de är uppkopplade till nätverket. Det finns många olika enheter som kan använda sig av trådlösa nätverk. Som tidigare nämnt under rubriken "1.1 Bakgrund" så räknas enheter med ett trådlöst nätverkskort t.ex. surfplatta eller bärbara PC (Personal Computer) till sådana.

Då trådlös kommunikation inte använder kablar så måste kommunikationen ske via andra tekniker. Trådlösa nätverk använder sig av radiovågor eller infrarött ljus [6, sid 8].

Då personer som använder sig av trådlösa nätverk kan röra sig på olika stora områden finns det olika kategorier som definierar vad ett trådlöst nätverk ska klassas som. De tre kategorierna är [7]:

- PAN (Personal Area Network)
- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

Ett trådlöst PAN räknas som ett nätverk med ganska kort räckvidd, ungefär 10 meters avstånd mellan enheterna [8]. I ett PAN används ofta tekniker som infrarött och Bluetooth för att kommunicera mellan enheterna. Infrarött är en teknik som använder sig av ljus medan Bluetooth använder sig av radiovågor [6, sid 224].

Ett LAN är ett nätverk som sträcker sig utöver en plats, oftast en byggnad. I ett LAN kan det finnas allt från några enstaka enheter till flera tusen enheter. Ofta byggs olika LAN upp med enheter som switchar, routrar och accesspunkter. Ett LAN gör det enkelt för företaget och personalen att dela filer mellan varandra och inte med resterande internet [7].

Men ett MAN menas ett nätverk som sträcker sig över flera byggnader t.ex. över en hel stad eller mellan ett universitets olika fastigheter. Ett MAN kopplar ofta ihop mindre LAN för att skapa ett större nätverk, som kan sträcka sig allt från några kilometer till flertalet mil [7].

Med ett WAN så räknas mycket större nätverk. Ett WAN kan innefatta ett helt lands nätverk eller en kontinent. Ett väldigt bra exempel på ett WAN som är publikt att få åtkomst till är internet [7]. Internet sträcker sig över större delen av jorden och är världens största WAN [9].

Det här arbetet har valt att fokusera på hur gästaccess kan se ut i ett företags-WLAN då det är oftast där nya implementationer sker av gästaccess.

2.2 Lagring av uppgifter

Eftersom att detta arbete behandlar två gästaccess-metoder som kan användas för att registrera personuppgifter kommer denna rubrik att ta upp lite kort om vad det finns för lag att förhålla sig till angående personuppgifter.

Den lag som finns för lagring av personuppgifter heter Personuppgiftslagen (PuL). Det är inte bara namn och personnummer som kan räknas in till personuppgifter. Utan enligt lagen kan alla uppgifter som kan kopplas till en fysisk person räknas som en personuppgift. Personuppgiftslagen behandlar även elektroniska uppgifter t.ex. bilder, ljudupptagningar som lagrats i datorer. Även krypterade uppgifter och IP-adresser kan klassas som personuppgifter om de kan kopplas till en fysisk person [10].

Då en gästaccess-server sparar personuppgifterna i en databas räknas de som strukturerade, d.v.s. ordnade efter en viss ordning. Om den personen som uppgifterna handlar om inte vill att uppgifterna ska användas i marknadsföring kan den personen skicka in en skriftlig anmälan till personuppgiftslagraren t.ex. via Epost [11].

För mer information angående PuL och hur den beskriver hur personuppgifter ska och får hanteras hänvisas läsare till följande referenser [12] [13].

2.3 Olika metoder

Som titeln på det här arbetet avslöjar, så är det meningen att arbetet ska ta upp några av alla de metoder som finns att välja på när ett företag ska välja att implementera gästaccess till deras nätverk. Arbetet är fokuserat på tre av de metoder som finns i nuläget. De metoderna är "Självregistrering", "Öppet" och "Besöksmottagare". Anledningen till detta är att skillnaden mellan de olika metoderna är ganska stora; både uppsättning och hur användaren upplever åtkomsten till nätverket.

Här visas en tabell med de tre olika metoderna samt kortfattad information om hur de kategoriseras.

Metod	Administration	Kostnad	Säkerhet	Spårbarhet
Öppet	Låg	Låg	Låg	Låg
Besöksmottagare	Medel	Medel	Hög	Hög
Självregistrering	Hög	Hög	Hög	Medel/Hög

Det här arbetet kommer att använda sig mycket av Ciscos enheter när det kommer till experiment samt olika konfigurationsexempel. Med hjälp av en Cisco ISE, en WLC samt en AP kan du sätta upp alla de tre metoder som belyses i arbetet. Men då Cisco inte är det enda företaget som producerar nätverksenheter är det viktigt att veta att andra företag som Aruba har liknande enheter som i slutändan ger samma möjlighet att sätta upp gästaccess. Ett exempel på detta är ClearPass.

Den enhet som anses vara den som sköter gästaccessen i ett nätverk är antingen Ciscos ISE eller Arubas ClearPass. Då en utförligare beskrivning på hur dessa enheter fungerar, funktioner och kapacitet inte kommer göras i arbetet så finns en utförligare dokumentation om dessa på följande dokument: Cisco [14][15] Aruba [16][17].

2.3.1 Självregistrering

Den här metoden är den nyaste av de tre som tas upp i arbetet. I det här avsnittet kommer "Självregistrering" beskrivas och sedan följer för- och nackdelar med just den här metoden. Senare i rapporten kommer en fördjupning på "Självregistrering" där metoden kommer att granskas mer på djupet.

Självregistrering fungerar på det sätt att när en gäst kommer till ett företag så ansluter personen till ett SSID (Service Set Identifier) som är till för gäster. När personen sedan ska börja använda nätverket så kommer den bli skickad till en portal där en registrering ska göras. Registreringen brukar bestå av att personen måste godkänna ett licensavtal, skriva in ett användarnamn, ange sitt namn och ange antingen en Epost-adress eller ett telefonnummer. När personen fyllt i alla dessa fält kommer ett SMS eller ett Epost-meddelande innehållande ett lösenord att skickas ut. När personen fått detta surfar den in på internet igen och väljer att logga in. Då använder personen den information som den mottagit i meddelandet för att få åtkomst till nätverket.

Den här metoden kommer mestadels beskrivas och analyseras från ett perspektiv då en Cisco ISE (1.3) använts samt andra enheter från Cisco. Under rubriken "3 Fördjupning" kommer flödet för denna metod att beskrivas djupare och visas hur det går till. Användarupplevelsen kommer även att beskrivas samt hur personer har upplevt hur självregistrering fungerar.

Fördelar

Vad har då metoden "Självregistrering" för fördelar? Den stora fördelen är att företaget kommer att få tillgång till en Epost-adress eller ett mobilnummer, eller både och. Med hjälp av dessa kan företaget sedan få mer uppgifter om vem det är som använt nätverket. Ett mobilnummer är ofta kopplat till ett abonnemang som någon står och betalar för [18]. På så sätt kan företaget genom en tredje part t.ex. företaget 118118 få reda på vem numret är registrerat på och då kontakta den personen om den brutit mot någon policy eller kanske bara glömt något på företaget [19]. Fördelen med att ange en Epost är inte lika stor som ett mobilnummer då det är lättare att skapa en Epost-adress med falska uppgifter. Epost ger dock en liten spårbarhet även om den är äkta.

Enligt Richard von Essen [20] på Cygate AB så är en annan fördel med just den här metoden är att företagets gäster inte behöver gå till någon person som har behörighet att skapa ett konto för att få tillgång till nätverket. Detta gör att de anställda inte behöver avbryta en eventuell arbetsuppgift för att ta sig tiden att släppa in en person på nätverket.

Det finns fortsatta fördelar med just "Självregistrering". En av dessa är att om du måste använda dig av en anställd med tillstånd att godkänna gäster till nätverket så kanske denne måste ha tillgång till enheter som kan vara kritiska för nätverket. Detta slipper företaget oroa sig för med självregistrering då registreringen och autentiseringen görs helt själv av gästen [21].

Nackdelar

Alla metoder medför vissa nackdelar. Självregistrering är inget undantag. En av de nackdelar som finns är att företaget ger tillgång till vem som helst att försöka registrera ett konto om personen ansluter sig till nätverket via portalen [22, sid 3]. Hade du haft en anställd som sköter utdelningen av konton så hade den personen kunnat göra en personbedömning på gästen och på så sätt se om gästen är lämplig att tillåtas internetaccess.

En annan nackdel är att företagets investering blir lite dyrare om självregistrering väljs att implementeras då mer avancerad utrustning krävs; som t.ex. en investering i en Cisco ISE eller i Aruba CleaPass. Eftersom det här arbetet bygger på att det finns en separat enhet som sköter autentiseringen och policyn för gästaccess och inte en eventuellt redan installerad server så måste en sådan investering göras.

Den tredje nackdelen är att företaget litar på att gästen i nätverket förhåller sig till den nätverkspolicy som den accepterade under registreringen. Skulle gästen inte förhålla sig till den policyn så har företaget rätt att kontakta denne med hjälp av det mobilnummer och epost som registrerats [23].

Ytterligare en nackdel är den att då en gäst ska kunna registrera sig själv så måste personens enhet ha en webbläsare installerad. Har den inte det, blir det omöjligt för enheten att registrera sig via portalen [24, sid 18].

2.3.2 Besöksmottagare

Metoden "Besöksmottagare" fungerar på det sätt att när en gäst till företaget vill komma åt nätverket, så måste personen gå till en anställd som har tillåtelse att ge denne tillgång till nätverket. Oftast brukar den anställde som agerar besöksmottagare vara en receptionist, men det kan även vara den personen som gästen är där för att träffa. Om besöksmottagaren bedömer att gästen ska få tillgång till nätverket kommer denne att gå in på en enhet och skapa ett konto som gästen sedan använder för att autentisera sig eller ge gästen ett fördefinierat konto som används av alla gäster.

Den enhet som gästen ansluter sig mot kommer att skicka en förfrågan till en Radius- eller Tacacs-server som checkar om det finns en användare som har tillåtelse att ansluta sig. Om besöksmottagaren har skapat ett konto eller att det redan finns ett konto med dessa uppgifter som gästen använt när den försöker logga in kommer servern att svara med att det är okej för enheten att släppas in i nätverket. Den enhet som i detta arbete agerar Radius-server är Ciscos enhet ISE (1.3).

Besöksmottagaren som skapat kontot kommer även få välja vilken sorts tillgång till nätverket gäst användaren kommer få. Exempelvis så kan gästen ges tillåtelse att bara använda TCP-protokollen HTTP och HTTPS samt UDP-protokollet DNS. Om användaren enbart skulle få tillgång till dessa tre protokoll så räknas det som en som bara fått tillgång till internet. Besöksmottagaren kan även välja att ge gästen tillgång till flera olika protokoll men det är inte rekommenderat för en person som bara gästar nätverket tillfälligt då den kan sprida skadliga koder till företagets enheter [25].

Fördelar

Vad ger då den här metoden för fördelar till företaget? En av de fördelar som kommer med det här valet av metod är att receptionisten eller den anställda som bedömer ifall en person ska få tillgång till nätverket kan göra en personlighetsbedömning på individen och fatta beslutet på den informationen men även på informationen gästen uppger om vem hen ska träffa, vilken tid den har ett möte med den personen samt hur läge hen har tänkt att stanna. Den som agerar sponsor kan använda sig av sunt förnuft för att göra dessa bedömningar [26].

En annan fördel med metoden är att besöksmottagaren kan ha möjligheten att skapa ett konto som passar bra in på den typ av gäst det handlar om. Personen som skapar kontot kan alltså göra ett visst konto som ger tillgång till vissa delar och på så sätt får gästen ett konto som passar mer in på behovet den individen har för nätverket [27].

Den tredje fördelen med just den här metoden är även att företaget som tillhandahåller möjligheten för gästaccess kan ge vissa personer som skulle kunna agera sponsor behörigheten att skapa flera typer av konton som har olika tillåtelser i nätverket medan andra eventuella besöksmottagare kan bara skapa ett väldigt begränsat konto t.ex. bara tillgång till internet [28].

Nackdelar

Som tidigare sagt i det här arbetet så finns det alltid någon nackdel med varje metod. En nackdel som följer metoden besöksmottagare är att den person som agerar besöksmottagare kan utsättas för någonting som kallas "Phishing". Phishing är en metod som hackare använder sig av för att komma åt t.ex. ett lösenord till något. Det går ut på att hackaren uppger sig för att vara en normal individ och spelar ett socialt spel för att komma åt dessa uppgifter [29, sid 2].

En annan nackdel med metoden är den extra arbetsuppgiften som en person kan få. Personen som arbetar på företaget måste eventuellt avbryta sina uppgifter för att kunna ge gästen åtkomst till nätverket vilket minskar produktiviteten [21].

Ännu en nackdel är att den administrativa bördan för de personer som har tillåtelse att ge åtkomst till nätverket ökar. De personer som agerar besöksmottagare måste både skapa ett konto, men även ta bort kontot från databasen efter att gästen gått för att inte ta upp onödiga resurser på enheten [30].

2.3.3 Öppet

När ett nätverk klassas som öppet betyder det att nätverket saknar en autentiseringsmetod för användare när de vill ansluta sig till företagets nätverk. Om en individ kommer till ett sådant företag som använder ett "öppet" nätverk, så kommer den personen att kunna välja att ansluta sin eller sina enheter via det trådlösa nätverket utan några problem. Om nätverket saknar någon typ av säkerhet kommer den nya enheten att få tillgång till alla resurser som nätverket har att erbjuda. Metoden "Öppet" är den metod som klassas som äldst, då internet från början saknade säkerhetstänk. Det är även den metod som används minst av olika företag idag. Det ställe där metoden oftast påträffas är i privatpersoners nätverk.

Metoden "Öppet" är också den metod som företaget kan välja för att utesluta en investering i en ISE/ClearPass enhet. Då ingen autentisering behövs så är en accesspunkt den enda enhet som behövs för att metoden ska fungera. Detta för att det SSID som gästerna ska ansluta sig till måste vara näbart för gästernas dataenheter.

Fördelar

Vad finns det då för fördelar med en metod där nätverket är öppet för alla? Det finns faktiskt ett fåtal fördelar med just en sådan metod. En av dessa fördelar är att det blir billigare för företaget att sätta upp nätverket och när det sedan ska administreras. Detta då den här metoden inte kräver någon extra säkerhetsenhet samt kräver minimal administration.

En annan fördel är att företagets personal kan fokusera på sina egna arbetsuppgifter och inte lägga ner tid för att se till så att gäster får tillgång till nätverket.

Ett öppet nätverk ger även fördelen att gästerna kan få tillgång till alla protokoll som t.ex. FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) och POP3 (Post Office Protocol version 3). FTP är ett protokoll som ger möjligheten att ladda ner filer, medan SMTP och POP3 är protokoll för att kunna använda sina Epost-applikationer [31][32][33]. Med dessa protokoll kan gäst användaren

komma åt sina filer och Epost som ligger på den personens företagsservrar, vilket kan underlätta för det arbetet som personen ska utföra.

Nackdelar

En av nackdelarna med att välja att ha ett "Öppet" nätverk är att personalen som styr nätverket inte kan hålla koll på vilka enheter som finns för närvarande i nätverket. Det kan medföra att olika säkerhetsbrott kan göras i nätverket som leda till katastrofala konsekvenser för företaget. Ett exempel på en sådan konsekvens kan vara att känsliga uppgifter på företagets anställda kan hamna i fel händer [34, sid 4]. Ett annat exempel kan vara att företaget slutar att fungera och därmed förlora inkomster.

En annan nackdel med användningen av ett öppet och okrypterat nätverk är även att du som gäst kan bli utsatt för olika attacker. En sådan attack kan vara en MitM (Man in the middle) attack [35] Vilket kan leda till att oönskade personliga uppgifter kan läcka ut till fel sorters personer. När vem som helst kan ansluta sig till nätverket ökar även risken för att den som använder nätverket kan skapa en DoS (Denial of Service) attack. En sådan attack kan leda till att ett nätverk och dess enheter blir överbelastade och fungerar sämre [36, sid 11].

3 Fördjupning

Under följande avsnitt kommer en fördjupning göras på de tre olika metoderna. Det som tas upp i denna del är:

- Varför metoden ska användas.
- Hur metodernas flöde ser ut för en autentisering.
- Användarupplevelse.
- Var metoderna passar in någonstans.

3.1 Självregistrering

Självregistrering är den metod som används mer frekvent i nätverk som anser sig ha ett gästantal som överstiger den godtagbara administrativa bördan som en anställd skulle ha vid besöksmottagare-metoden. Självregistrering väljs före ett öppet nätverk då självregistrering ger möjligheten till bättre spårbarhet samt övervakning av trafiken som en specifik enhet genererar och därmed ökad säkerhet för företaget. Med mer avancerade funktioner som en gästaccess-server erbjuder medföljer ett högre pris. Företaget som vill implementera självregistrering måste lägga in mer pengar samt planering när de väljer den metoden. Då företaget har fått implementationen på plats och de olika policys som ska användas beroende på typ av gäst är konfigurerade så är självregistrering en metod som inte behöver så mycket administration. Det som kan behövas administreras är borttagningen av konton. Detta behövs dock inte göras så ofta, då en gästaccess-server beroende på kapacitet stödjer ett stort antal konton.

En svårighet med konfigurationen av självregistrering är att skapa de olika policys som gästerna har möjlighet att få tillgång till. Desto flera olika typer av gäster som företaget väljer att erbjuda tillgång till nätverk för så ökar antalet policys som ska skapas. Det behövs en policy för varje typ av gäst. En annan svårighet är att skicka rätt policy till rätt sorts gäst. Även konfigurationen av de olika ACLerna kan vara problematiskt då en sådan lista snabbt kan växa till många rader och lätt bli överväldigande för de som administrerar.

Om företaget väljer att använda sig av Epost och SMS kan en ny svårighet uppstå. Cisco ISE kommer förinstallerad med ett antal SMS-gateways t.ex. Verizon, men företaget kanske inte vill använda några av dessa. Då måste en egen lösning skapas vilket kan leda till att mer tid måste läggas ner och nya investeringar måste göras. Det är även en svårighet att få notifieringsmeddelanden att se snyggt uppställda ut då alla Epost och SMS-gateways hanterar meddelanden på olika sätt.

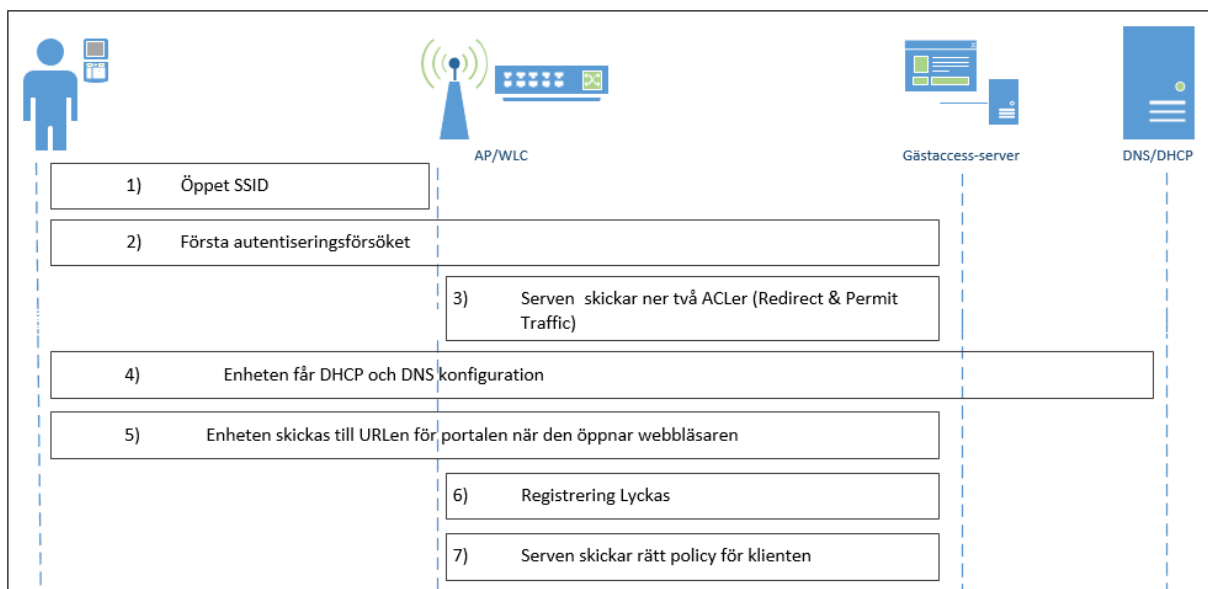
3.1.1 Varför Självregistrering?

Frågan som många kommer ställa sig när de ska välja vilken gästaccess-metod som företaget ska använda sig av kommer vara varför de ska välja just metoden "Självregistrering".

Som tidigare beskrivits under rubrikerna "2.3.1 Självregistrering" så har metoden vissa för- och nackdelar som självklart måste vägas in när beslutet ska göras. Som IT-administratör så kan fördelarna med självregistrering väga väldigt tungt. Att ha möjligheten att kräva ett telefonnummer samt en Epost-adress under registreringen kan visa sig vara väldigt värdefullt i slutändan. När företaget fått tillgång till ett telefonnummer som kan kopplas till en viss användare så har de mycket större koll på personen och vem det är även efter att personen lämnat nätverket. Detta då gästaccess-servern lagrar dessa uppgifter i en databas som är lättåtkomlig för personalen.

3.1.2 Hur ser stegen ut?

För att en enhet ska kunna autentisera sig måste först en paketutväxling göras mellan de enheter som är inblandade i metoden. Detta resulterar antingen i ett godkännande eller nekande av tillgång till nätverket. Det här flödesschemat beskriver vilka steg som metoden gör för att autentisera en ny användare. Det beskriver dock inte vilka protokoll som trafiken transporteras med då detta är en avgränsning som gjorts för det här arbetet.



Steg 1) Klienten väljer att ansluta till det SSID som är ämnat för gäst användare.

Steg 2) Gästaccess-servern ser att klienten inte finns lagrad i serverns databas. Istället för att neka användaren access direkt så skickar servern istället ett Radius-meddelande med "access-accept".

Steg 3) Tillsammans med meddelandet access-accept skickar även servern med en eller flera ACLer som tillåter att DHCP ska fungera för klienten samt att klienten ska kunna skickas till portalen för registrering via en URL.

Steg 4) Klienten får en IP-adress, Subnätmask, Default-gateway och DNS tilldelad.

Steg 5) När klienten öppnar sin webbläsare skickas den direkt till den URL som servern skickade med till klienten. Den URL:en leder till själva portalen för självregistrering.

Steg 6) Klienten går igenom registreringen och lämnar ett visst antal uppgifter. Efter att klienten registrerat sig så loggar användaren in med det nyskapade kontot.

Steg 7) Gästaccess-servern skickar ner den rätta policyn för användaren som säger vad gästen får göra i nätverket när autentiseringen lyckats.

3.1.3 Användarupplevelse med självregistrering

Hur användare upplever den här metoden kan variera från person till person. Det finns självklart personer som tycker att metoden flyter på smidigt och bra då de kan göra allt själva för att få gästaccess. De slipper vara beroende av en annan person innan de får access. Det finns även personer som tycker att metoden inte är så användarvänlig. Dessa kan vara personer som saknar tillgång till en webbläsare i sin enhet. Då enda sättet att registrera sin enhet i metoden "Självregistrering" är via en portal som öppnas i en webbläsare, blir detta omöjligt för dessa personer.

Användargränssnittet på den här metoden kan du som administratör skapa och koda själv. Du kan då få sidorna som gästen måste gå igenom att se stilrent ut medan portalen uppfyller de önskade kraven som företaget har på den. Förutom möjligheten att skraddarsy sin egen portal via kodning i språket HTML så finns det även fördefinierade teman som företaget kan använda sig av. Sidan blir då väldigt enkel men fyller sin funktion samtidigt som portalen hålls väldigt snygg och enkel.

Om användaren saknar konto för inloggning och väljer att skapa ett nytt konto så kommer personen gå igenom allt från 1-4 olika sidor där olika godkännanden och registreringar ska göras. Vissa av dessa sidor är inte nödvändiga att gå igenom manuellt utan kan göras automatiskt av gästaccess-servern. Det minimala som behöver göras i metoden "Självregistrering" är att användaren måste registrera några uppgifter som t.ex. namn, telefonnummer, Epost och

personen som användaren ska hälsa på. Dessa fyra uppgifter kommer, som tidigare sagt, även kunna ge en bra spårbarhet för företaget om de skulle vilja komma i kontakt med personen efter att något hänt eller av någon annan anledning.

3.1.4 Var passar självregistrering?

Det finns väldigt många olika företag i världen. De flesta av dessa företag erbjuder någon form av gästaccess för besökare. Eftersom alla företag inte sysslar med exakt samma saker så krävs det olika lösningar för olika företag.

Ett företag som använder sig av självregistreringsmetoden är Sundsvall flygplats (Midlanda). Där får gästen ansluta sig till ett SSID och sedan lämna sitt mobilnummer under registreringen. Sedan får gästen en bekräftelse skickad till sitt mobilnummer.

Något som måste betänkas när ett företag ska välja att implementera självregistrering är att besökaren saknar internetanslutning och då åtkomst till internet innan gästen har registrerat sig och uppfyllt alla krav. Företagets accessmetod kan gå ut på att gästaccess-servern genererar ett slumpat lösenord för användaren. Företaget kan sedan välja att det slumpade lösenordet bara ska skickas till den Epost-adress som användaren registrerat. Detta medför att användaren måste ha åtkomst till internet för att komma åt sin Epost, vilket saknas då användaren inte loggat in via portalen än. En lösning på det problemet kan då vara att välja att användaren registrerar ett telefonnummer och ett SMS skickas ut med lösenordet istället för att det skickas via Epost. Då kan ett problem för de företag som har många internationella gäster uppstå. Det är att de saknar svensk mobilnummer och då kanske inte SMS notifieringen kommer fram till gästen. För att säkra att dessa problem inte ska kunna uppstå, kan en lösning vara att det direkt efter registreringen visas en ny sida med de uppgifter som gästen angivit plus det slumpade lösenordet. Om lösningen även har så att Epost skickas ut så kommer gäst användaren nu komma åt sina Epost-meddelanden eftersom lösenordet visats och inloggningen kan göras. Självfallet

finns även möjligheten att de som registrerar sig kan välja ett eget lösenord direkt under registreringen.

Ovanstående är därför en väldigt viktig del när ett företag ska planera sin gästaccess. Företaget måste tänka på vad för typer av personer som kan komma att röra sig i deras nätverk. Om det finns risk för att många personer kommer att ansluta sig via företagets nätverk så gäller det att företaget har skapat en bra policy som begränsar gästernas möjligheter att komma åt känslig data. Metoden "Självregistrering" tycks passa bäst in på de företag som har många gäster, men även gäster som inte är inplanerade utan bara råkar vara i behov av ett nätverk och ansluter sig på grund av detta. Företag som har en stor koppling till allmänheten, t.ex. Sundsvall flygplats eller olika caféer, där det sker en stor genomströmning av gäster lämpar sig därför för självregistreringsmetoden. Vidare kan varje företag välja att registrera olika sorters uppgifter som de anser sig behöva för spårbarhet eller för eventuella nyhetsutskick till kunder samt hur de ska lösa problemet med hur lösenordet ska presenteras för användaren.

3.2 Besöksmottagare

Här kommer en fördjupning göras på metoden "Besöksmottagare". Det finns kort beskrivet under rubriken "2.3.2 Besöksmottagare" hur metoden fungerar samt för- och nackdelar med att använda sig av den här metoden.

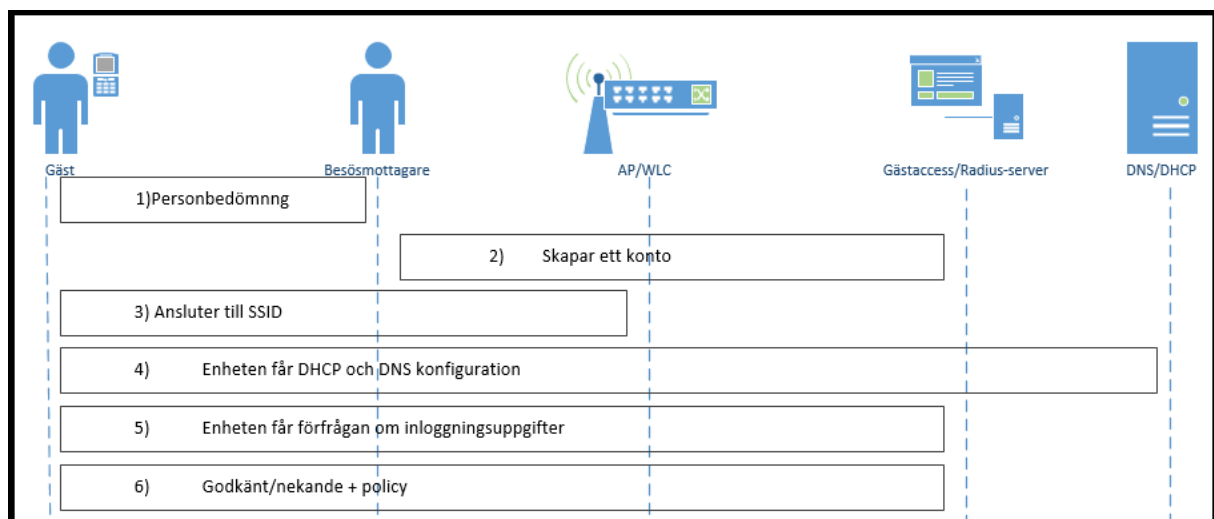
De svårigheter som finns med den här metoden är att bestämma vilken sort konton/policy som ska vara möjliga att skapa för gästerna samt ifall företaget ska använda sig av ett konto åt alla gäster eller individuella konton eller en mix av de båda versionerna.

3.2.1 Varför Besöksmottagare?

Då metoden "Besöksmottagare" kommer med både för- och nackdelar för det företag som väljer att implementera metoden är det viktigt att ha ett starkt argument för att använda metoden. Metoden "Besöksmottagare" skall användas när företaget tycker att det finns risk att gäster med onda avsikter ansluter sig till nätverket. Med hjälp av en "Besöksmottagare" kan företaget identifiera en person som inte borde ha tillåtelse till nätverket samt personer som inte borde via olika personbedömningar. Att välja rätt sorts version på "Besöksmottagare" är även en viktig del i varför metoden ska användas. Då det finns möjligheten att skapa ett konto till varje gäst för att på lättare sätt kunna spåra den enskilda personen. Eller så kan ett konto delas ut till alla gäster och då minska spårbarheten på individuell nivå och den administrativa delen blir mindre.

3.2.2 Hur ser stegen ut för autentisering?

Även i den här metoden måste en viss informations- och paketutväxling göras innan gästen får tillgång eller nekad tillträde in i nätverket. Det som skiljer sig i metoden "Besöksmottagare" i jämförelse med de andra metoderna är att här kan potentiella gäster nekas tillgång direkt innan någon paketutväxling gjorts.



Steg 1) Gästen frågar "Besöksmottagaren" ifall hen skulle kunna få tillgång till nätverket och en snabb personlighetsbedömning görs då på individen. Här kan personen nekas tillgång.

Steg 2) "Besöksmottagaren" väljer att skapa ett konto som är anpassat för individen eller så ger hen ut ett konto som är tillför alla de gäster som kommer till nätverket.

Steg 3) Gästen ansluter till det SSID som är tillför gäster.

Steg 4) Tilldelas IP-adress, subnätmask, default-gateway och DNS-server.

Steg 5) Gästen blir antingen skickad till en portal eller får upp en ruta där inloggningsuppgifterna ska skrivas in. Här skickas ett access-request meddelande till Radius-servern (gästaccess-servern) som frågar ifall uppgifterna ger tillgång till nätverket.

Steg 6) Om kontot finns skickas Radius-servern ett access-accept tillbaka som ger tillgång till nätverket samt den policy som ska gälla för klienten. Finns inte kontot så nekas klienten tillträde till nätverket.

3.2.3 Användarupplevelse med besöksmottagare

Det finns olika typer av "Besöksmottagare". Antingen kan ett konto skapas för varje gäst som kommer till nätverket eller så kan företaget ha ett konto som alla gäster använder. De olika versionerna tillför olika användarupplevelser.

Upplevelsen för de personer som får ett individuellt konto skapat är att under en personbedömning kan mer frågor ställas om vad personen gör här och vad den ska göra för att kunna skapa ett så bra anpassat konto som möjligt.

Personbedömningen kan alltså bli för personlig och kanske uppfattas som kränkande när "Besöksmottagaren" vill ha reda på information angående personen.

Användarupplevelsen för de personer som får tillgång till ett sådant konto som alla gäster använder kan personbedömningen vara väldigt kort och inte alls lika djupgående som den andra versionen. Det kan vara avsiktligt gjort att hålla bedömningen på ytligare nivå då företaget vet att de konto gästerna får tillgång till redan är bra begränsat.

3.2.4 Vart passa besöksmottagare?

Den här metoden passar bäst in på de företag som tycker att administrering av gästaccess inte behöver vara en nackdel för företaget. Även här gäller det att skapa en lösning som är bäst anpassad för just det företag som ska implementera metoden.

Det företag som väljer att använda sig av metoden "Besöksmottagare" och skapa individuella konton för alla gäster är de företag som känner att de måste ha full kontroll på vad för sorts personer som rör sig i nätverket samt att de får rätt och anpassad behörighet för vad de ska göra. Ett sådant företag skulle kunna vara t.ex. Forsvarsmaktens eller skatteverkets nätverk då det rör sig om mycket känslig information som kan läcka ut.

De företag som skulle kunna mer passa in på den kategorin med att ha ett konto som alla gäster använder sig av är t.ex. de som inte vill att vem som helst kan ansluta sig utan företaget vill ha någorlunda koll på vem som finns i nätverket. Ett sådant företag som använder den här versionen är Cygate AB. De har alltså ett konto som delas ut till alla gäster efter att de bedömt att personen ska ha tillgång till nätverket.

3.3 Öppet

Här kommer en fördjupning göras på metoden "Öppet" Under rubriken "2.3.3 Öppet" finns en förklaring hur metoden fungerar samt de för- och nackdelar metoden har.

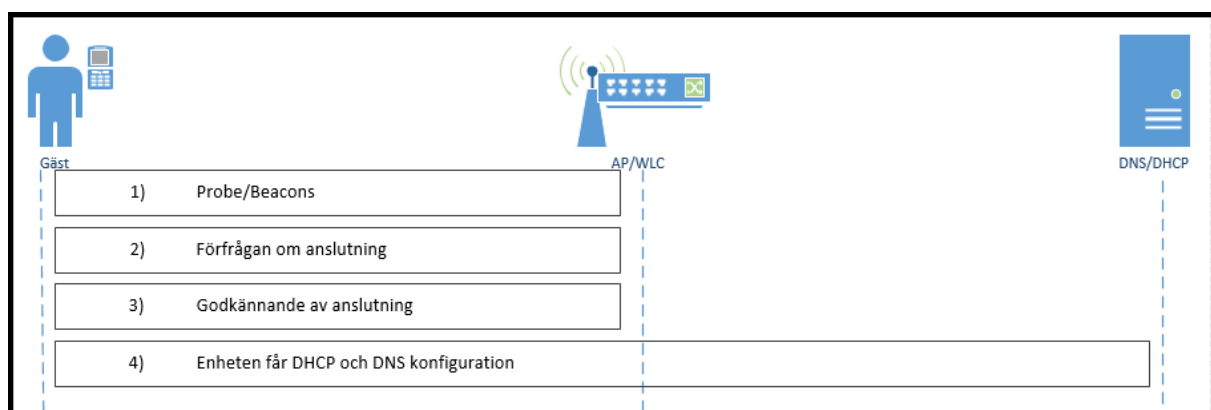
Då den här metoden är enkel att använda sig av och behöver knappt någon konfiguration så det finns inga konfigureringsvårigheter att nämna i detta arbete.

3.3.1 Varför Öppet?

Det kan kännas dumt att i dagens samhälle välja att använda sig av ett nätverk som är öppet för alla att ansluta sig till. Men som tidigare beskrivits har metoden ett par fördelar som kan visa sig vara avgörande när metod ska väljas. Känner ett företag att det inte är i behov av någon speciell säkerhet mot de gäster som ska vara i nätverket samt avsaknaden av spårbarhet är "Öppet" ett val som skulle kunna vara aktuellt. Är företaget litet kanske de inte vill lägga ner en stor summa för att ha egna servrar som de lagrar information på utan de använder sig av en molntjänst där all data sparas i. Om de använder sig av en molntjänst så kan de anställda ofta nå sina dokument från vilket nätverk som helst. De kan skapa krypterade tunnlar från deras egna klienter när de ska nå molntjänsten och på så sätt kommer ingen som avlyssnar nätverket att få tillgång till känslig information. Därför skulle företagets nätverk kunna vara "Öppet" för alla men den information som de anställda använder sig av är krypterad och ej läsbar för avlyssnare.

3.3.2 Hur ser anslutningsstegen ut för Öppet?

Då ett "Öppet" nätverk egentligen saknar någon form av autentisering är det inte många steg som behövs för att en gäst ska få tillgång till nätverket. De steg som görs i den här metoden görs även i alla andra metoder då gästen ska ansluta till ett SSID, därav kommer en beskrivning av denna autentisering. Det finns en aktiv och en passiv metod för att upptäcka olika SSID i ett nätverk.



Steg 1) Klienten skickar ut "probe" meddelande för att ta reda på vilka SSID som finns tillgängliga (aktiva metoden). Eller så lyssnar klienten på "beacons" som access-punkten skickar ut för att ta reda på olika SSID (passiva metoden).

Steg 2) Klienten skickar en förfrågan om den får ansluta sig till det SSID.

Steg 3) Access-punkten tillåter klienten att ansluta till det SSID.

Steg 4) Klienten får DHCP-konfiguration.

Notis: Stegen 1 – 3 görs även på metoderna "Självregistrering" och "Besöksmottagare".

3.3.3 Användarupplevelsen

Metoden "Öppet" är den metod som går enklast och snabbast för gäster att ansluta sig via. Det är inga portaler eller personer som gästen måste gå igenom för att få tillåtelse att använda nätverket. Det gör att uppfattningen och användarupplevelsen känns enkel och smidig och ger såklart önskat resultat med tillgång till nätverket. En annan användarupplevelse med ett "Öppet" nätverk är att gästerna slipper ge ut personlig information för att få tillgång till nätverket vilket kan vara skönt för att individens integritet.

3.3.4 Vart passar ett öppet nätverk?

Den här metoden skulle kunna passa in på företag som är nystartade och inte har de möjligheter att ha sina egna servrar och enheter antingen på grund av höga investeringskostnader eller att företaget inte har tillräckligt med plats i sina lokaler. Ett exempel på ett sådant företag skulle kunna vara är en konsultfirma med en anställd. Den konsulten kanske har ett litet kontor med ofta befinner sig ute hos kunder och arbetar. Att då inte har allt för mycket investerat i enheter bara för att lösa gästaccess kan ett öppet nätverk vara en bra lösning då det inte används så ofta ändå.

4 Resultat

Det resultat som det här arbetet har kommit fram till är att varje företag har sina egna behov som måste vägas in när det kommer till valet av metod för gästaccess. Det finns ingen självklar metod som är given att använda på ett företag, utan alla metoder kan egentligen användas på alla sorters företag. Varje företag som väljer att implementera gästaccess kan skapa sin egen version av alla metoder och på så sätt se till att gästaccessen blir så bra anpassad för företaget som möjligt.

Resultatet av detta arbete har även gett en inblick till för- och nackdelar som varje metod har.

Metod	Fördelar	Nackdelar
Självregistrering	<ul style="list-style-type: none"> • Ökad spårbarhet • Allt sköts av användaren vid registrering • Företaget slipper ge personal behörighet för åtkomst till gästaccess-servern 	<ul style="list-style-type: none"> • Risk att oönskade personer får tillgång till nätverket • Större investeringskostnad • Litar på att användaren förhåller sig till policyn • Krävs en webbläsare
Besöksmottagare	<ul style="list-style-type: none"> • Individuella bedömningar på gäster kan göras • Kan skapa mer personligt anpassade konton • Olika nivåer på sponsorer 	<ul style="list-style-type: none"> • Risk för Phishing • Extra arbetsuppgifter för besöksmottagaren • Mer administrativ börda vid hantering av konton

Öppet	<ul style="list-style-type: none"> • Billig lösning • Personal kan fokusera på sina arbetsuppgifter • Gäster kan göra alla sina arbetsuppgifter utan begränsningar 	<ul style="list-style-type: none"> • Personliga uppgifter kan lättare hamna i fel händer • Spårbarheten är låg • DoS attacker kan lättare utföras på och från nätverket
--------------	---	--

Arbetet har även lett fram till ett resultat som gett en bra förståelse om hur de olika metoderna fungerar samt vad företagens gäst-användare och anställda kan vänta sig för upplevelse när de använder metoden. Arbetet har även gett en bra bild på vilka typer av företag och situationer de olika metoderna passar in på.

Metod	Användarvänlighet	Konfigurering svårigheter	Passar in
Självregistrering	Enkel registrering	De olika policyn	Många gäster
Besöksmottagare	Enkel eller svår registrering	Skapandet av alla konton och policys	Fåtal gäster samtidigt vid registrering
Öppet	Väldigt simpel registrering	Inga svårigheter	Både många och få gäster

Innan arbetet genomfördes var det förväntade resultatet att de olika metoderna skulle skilja sig ganska mycket i förhållande till varandra på flera olika punkter; som t.ex. konfiguration samt vilket företag som metoden skulle kunna passa bäst in på. Det resultat som arbetet lett fram till är i linje med det förväntade

resultatet när de kommer till dessa punkter samt vilka olika fördelar och nackdelar det finns med varje metod.

5 Analys av resultatet

Det här arbetet har fungerat bra på det sättet att metoderna som använts i arbetet har gett en bra inblick i hur gästaccess fungerar samt vad som bör tänkas på när en implementation ska göras av någon metod. Att göra detta arbete tillsammans med ett företag som innehar både kunskap och expertis inom gästaccess samt andra områden har haft en stor positiv påverkan på hur arbetet förlöpt. Att kunna diskutera olika delar av arbetet med personalen från Cygate har varit en väldigt stor fördel. Även att veta att kunskap om dessa områden finns nära tillhands om någon del skulle visa sig krångla har känts som en enorm trygghet för mig personligen och för att arbetet skulle kunna genomföras.

När det kommer till metoden som gått ut på att söka upp referenser från antingen avhandlingar eller företagssidor så är jag antingen kritisk. Det har visat sig väldigt svårt att hitta vetenskapliga referenser som handlar om gästaccess. Större delen av alla de referenser som hittats är antingen från företag eller från andra sorters sidor där påståenden gjorts. Jag hade gärna sett att flera avhandlingar gjorts på den här typen av arbete så att flera vetenskapliga referenser på avhandlingar om gästaccess hade kunnat användas. Egna tester och slutsatser har gjorts på vilken metod som skulle kunna passa in på olika typer av nätverk. Detta har känts som en bra metod för att skaffa sig en uppfattning om vart personer skulle kunna stöta på en viss typ av lösning. Jag hade gärna sett att intervjuer och möten med företag gjorts och på dessa möten diskuterat deras tankesätt angående metod för gästaccess.

Resultatet som det här arbetet kommit fram till har den betydelsen att om ett företag funderar på att implementera gästaccess så ger det här arbetet en bra grund till vad de ska ha i åtanke när de väljer metod. Arbetet kommer även att bidra till att ge en grov bild av vilka enhetsinvesteringar som behöver göras för att få metoderna att fungera samt vad som senare kommer krävas av organisationen för att underhålla och administrera metoden.

Resultatet som arbetet gett kommer att ge en tankeställare för de företag som ska välja gästaccess-metod. De konsekvenser som presenterats kan göra att företag inser att den metod de tänkt sig egentligen inte passar in på deras behov och de personer som ska röra sig i deras nätverk.

Relationen till aktuell forskning

Då det varit väldigt svårt, nästintill omöjligt, att hitta aktuell forskning om området gästaccess så har det här arbetet ingen relation med någon aktuell forskning för området gästaccess. Det här arbetet relaterar ändå en liten del till forskning som gjort inom trådlösa nätverk samt säkerhet i ett trådlöst nätverk [29][37].

6 Avslutning

Önskan är att det här arbetet ska vara givande för er läsare som är intresserade av att veta mer om vad ett företag har för möjligheter när det kommer till olika typer av gästaccess-metoder. Det har förhoppningsvis gett en bra beskrivning på vilka olika för- och nackdelar som varje metod kommer att ge ett företag. Även att det inte finns någon metod som är det självklara valet för någon typ av företag, utan att varje företag måste göra en individuell plan och anpassning för hur deras lösning ska se ut.

Arbetet har även gett undertecknad ett nytt perspektiv på hur olika lösningar kan se ut och vad som krävs både administrativt och enhetsmässigt för att få varje metod att fungera. Det har varit ett roligt arbete att genomföra och jag hoppas att det ger er läsare en bra förståelse om gästaccess samt förhoppningsvis väckt ett litet intresse om hur nätverk fungerar.

6.1 Framtida arbeten

Ny forskning som kan göras på detta område skulle kunna vara att jämföra de olika företagens lösningar på gästaccess. Ett annat arbete som skulle kunna göras efter det här är att djupare undersöka olika personers syn på vilka sorters uppgifter som är lämpliga att ge ut för en registrering, samt hur de skulle få användas av företaget så länge de håller sig inom PuL. Ytterligare ett arbete hade kunnat göras på vad för sorters trafik och paket som skickas i ett nätverk med gäst-access samt vad de innehåller.

7 Källförteckning

- [1] Chrostoffer, Tibbelin. "Välkommen – Cisco ISE 1.3". [Online], november 10 2014. <https://www.cygate.se/-/valkommen-cisco-ise-1-3> [Hämtad 2015-04-7]
- [2] Jesse, Wiener. "Cisco Identity Services Engine (ISE) 1.3 – Should You Bite the Bullet and Update?". [Online], februari 17, 2015. <http://blog.cdw.com/cisco-identity-services-engine-ise-1-3-should-you-bite-the-bullet-and-update/#.VTjqiSHtmko> [Hämtad 2015-04-10]
- [3] Vikrant S, Kaulgud. "IP Quality of Service: Theory and best practices". [Pdf], [Hämtad 2015-05-04].
- [4] Aruba. "WLAN Secure Guest Access". Aruba. [Pdf], 2005-2006.
- [5] Fredrik, Larsson. Michael, Ben-Zur. "Trådlösa nätverk – analys av förutsättningar och förslag på utformning", Tekniska Högskolan i Jönköping. [Pdf], 2009.
- [6] David D, Coleman. David A, Westcott. *CWNA: Certified Wireless Network Administrator*, Tredje Upplagan, John Wiley & Sons Inc, [Bok], 2012.
- [7] Paul, Zandbergen. "Types of Networks: LAN, MAN, WLAN, MAN, SAN, PAN, EPN & VPN". [Online], <http://study.com/academy/lesson/types-of-networks-lan-wan-wlan-man-san-pan-epn-vpn.html> [Hämtad 2015-05-06]
- [8] Cory, Janssen. "Personal Area Network (PAN)". [Online], 2010-2015, <http://www.techopedia.com/definition/5079/personal-area-network-pan> [Hämtad 2015-06-05]
- [9] GFC. "What is the Internet: Wide area network (WAN)". Februari 25, 2015. [Online], <http://www.gcflearnfree.org/internet101/1.3> [Hämtad 2015-05-06]
- [10] Datainspektionen. "Vad är en personuppgift?" [Online]. <http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-ar-en-personuppgift/> [Hämtad 2015-05-10]
- [11] Datainspektionen. "Dina rättigheter enligt personuppgiftslagen". [Online] <http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/dina-rattigheter/> [Hämtad 2015-05-10]

- [12] Justitiedepartementet. "Behandling av personuppgifter" [Pdf]. 2006.
- [13] Datainspektionen. "Personuppgiftslagen" [Online]
<http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/> [Hämtad 2015-05.10]
- [14] Cisco Systems, Inc. "Cisco Identity Services Engine". [Online],
<http://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html> [Hämtad 2015-05-08]
- [15] Cisco Systems, Inc. "Cisco Identity Services Engine Administrator Guide, Release 1.3". [Pdf], oktober 31, 2014.
- [16] Aruba Networks. "ClearPass Policy Management platform". [Online],
<http://www.arubanetworks.com/products/security/policy-management/> [Hämtad 2015-05-08]
- [17] Aruba Networks. "THE CLEARPASS ACCESS MANAGEMENT SYSTEM". [Pdf], 2014.
- [18] Wikipedia. "Telefonnummer". [Online], mars 17, 2015.
<http://sv.wikipedia.org/wiki/Telefonnummer>. [Hämtad 2015-04-27]
- [19] Eniro. "Välkommen till Eniro 118 118". [Online],
<http://www.eniro.se/118118/> [Hämtad 2015-05-04]
- [20] Richard von, Essen. Business Area Manager – Networking. Cisco CCIE 10851, Cygate AB. [Muntlig], maj 12.
- [21] Zoho Corp. "Employ your Resources for better tasks". [Online], 2015.
<https://www.manageengine.com/products/self-service-password/benefits.html>
[Hämtad 2015-05-04]
- [22] Cisco Meraki, "Captive Portal Configuration Guide: What is a Captive Portal?" [Pdf], juni, 2014.
- [23] Philip, Wegner. "WHY IS CAPTIVE PORTAL IMPORTANT FOR WIRELESS GUEST ACCESS?". [Online], <http://www.securedgenetworks.com/security-blog/Why-is-captive-portal-important-for-wireless-guest-access> [Hämtad 2015-06-07]

- [24] Rustam, Jemurzinov. "Authentication and authorization service for a community network". [Pdf], oktober 13, 2008.
- [25] Bradley, Mitchell. "What is a Guest Network". [Online], 2015.
<http://compnetworking.about.com/b/2009/03/03/what-is-a-guest-network.htm>
[Hämtad 2015-05-06]
- [26] Michael, Kassner. "Technology can't stop phishing perhaps common sense can". [Online], <http://www.techrepublic.com/blog/it-security/technology-cant-stop-phishing-perhaps-common-sense-can/>. [Hämtad 2015-05-06]
- [27] Se bilagor, "Experiment 1", Steg 15.
- [28] Se bilagor, "Experiment 2", Steg 3-7.
- [29] Xun, Dong. "Defending Against Phishing Attacks", The University of York, Department of Computer Science. [Pdf], September, 2009.
- [30] Se bilagor, "Experiment 3", Steg 5-6
- [31] J. Postel. J, Reynolds. "FILE TRANSPORT PROTOCOL (FTP)". [Online], oktober, 1985. <https://www.ietf.org/rfc/rfc959.txt> [Hämtad 2015-05-07]
- [32] Jonathan B, Postel. "SIMPLE MAIL TRANSFER PROTOCOL". [Online], augusti, 1982. <https://tools.ietf.org/html/rfc821> [Hämtad 2015-05-07]
- [33] J, Myers. Carnegie, Mellon. "Post Office Protocol – Version 3". [Online], maj, 1996. <https://www.ietf.org/rfc/rfc1939.txt> [Hämtad 2015-05-07]
- [34] Daan, Stakenburg. Jason, Crampton. "Underexposed risks of public Wi-Fi hotspots". [Pdf].
- [35] Michael, Kassner. "Convenience or security: You can't have both when it comes to Wi-Fi". [Online], juni 24, 2013. <http://www.techrepublic.com/blog/it-security/convenience-or-security-you-cant-have-both-when-it-comes-to-wi-fi/>
[Hämtad 2015-05-04]
- [36] Huda Bader, Hubboub. "Denial of Service Attack in Wireless Sensor Networks", Islamic University-Gaza. [Pdf], 1431H, 2010.
- [37] Oh Khoon, Wee. "WIRELESS NETWORK SECURITY: DESIGN CONSIDERATIONS FOR AN ENTERPRISE NETWORK", Naval Postgraduate School, Monterey, Kalifornien. [Pdf] december 2004.

8 Bilagor

Förkortningar

AP	Access-point
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ISE	Identity Services Engine
LAN	Local Area Network
MAN	Metropolitan Area Network
MitM	Man in the middle
PAN	Personal Area Network
PC	Personal Computer
POP3	Post Office Protocol version 3
PuL	Personuppgiftslagen
QoS	Quality of Services
SMTP	Simple Mail Transfer Protocol
SMS	Short Message Service
SOP	State Of practices
SSID	Service Set Identifier
VoIP	Voice over IP
WAN	Wide Area Network
Wi-Fi	Trådlös nätverksteknik
WLAN	Wireless Local Area Network
WLC	Wireless Lan Controller

Experiment 1

Då Cygate har tillhandahållit en Cisco ISE med mjukvara 1.3 så ska detta experiment illustrera hur en besöksmottagare kan välja att ändra på attribut när personen ska skapa ett konto för att det ska passa gästen senare.

Bilderna som kommer användas är print screens från den riktiga ISEn som Cygate fixat.

För att sätta upp ett konto via Sponsorportalen måste följande steg först göras. Dessa steg förutsätter att en ISE (1.3) är installerad med basic-konfig för IP-adresser och subnet-maskar samt även en Cisco WLC med en AP ansluten till sig med ett VLAN och ett interface skapat som fungerar, samt att WLCen är konfigurerad att använda ISEn som AAA-server.

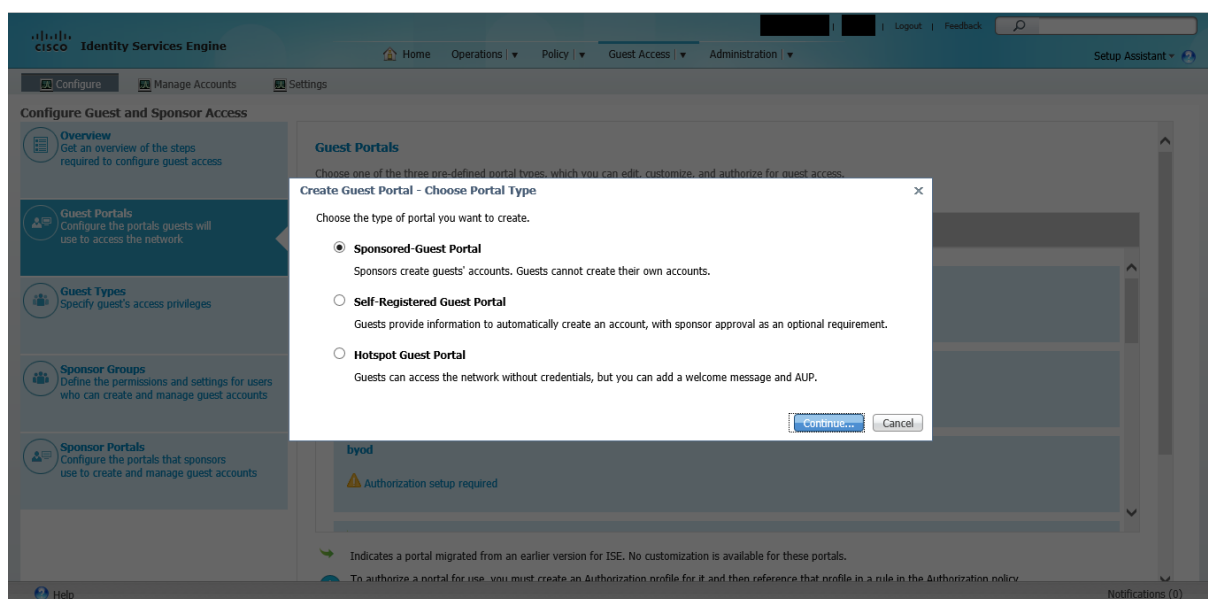
Steg 1)

Logga in på Cisco ISE enheten.

Steg 2)

Skapa en sponsorportal i Cisco ISE genom att gå via:

Guest Access -> Configure -> Guest Portals -> Create -> Sponsored-Guest Portal



Steg 3)

Gå in på den nyss skapade portalen och kopiera portalens URL

Steg 4)

Logga in på WLC

Steg 5)

Gå in på Access Control Lists och skapa en ny ACL genom: Security -> Access Control Lists -> Access Control Lists -> New...

Steg 6

För att gästen ska kunna bli skickad till portalen för att logga in behövs följande rader i den skapade ACLen.

1. Permit, source = Any, destination = Any, Dest Port = DNS
2. Permit, source = Any, destination = Any, Source Port = DNS
3. Permit, source = Any, destination = IP för ISE
4. Permit, source = IP för ISE, destination = Any
5. Deny, source = Any, destination = Any

Steg 7)

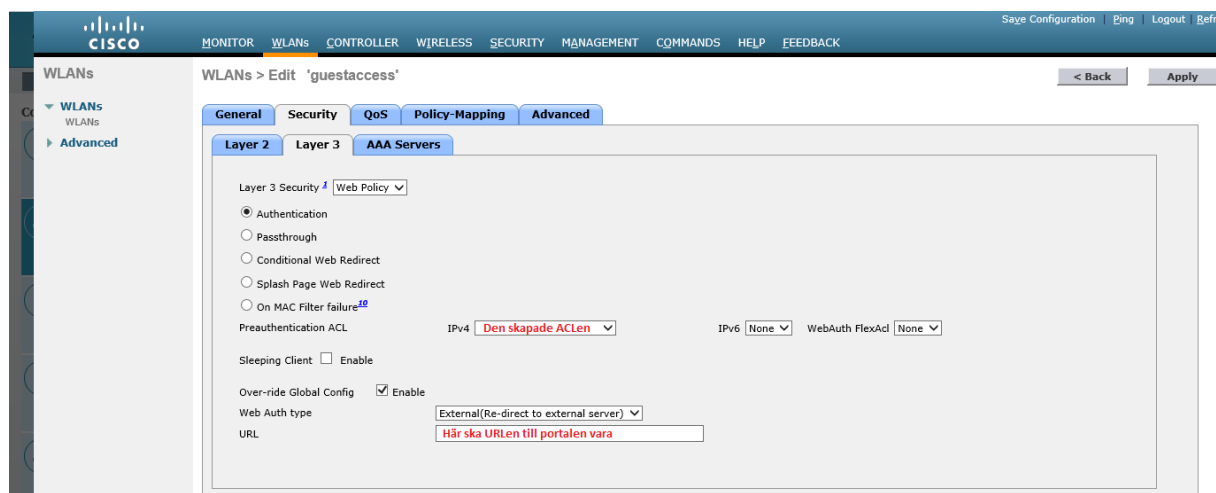
Gå in på det VLAN som är tänkt att användas: WLANs -> (Ditt VLAN).

Steg 8)

För att möjliggöra så att gästen skickas till portalen av går du först in på: Security -> Layer 3 (När du är inne på ditt VLAN).

Steg 9)

Här ska följande konfiguration göras:



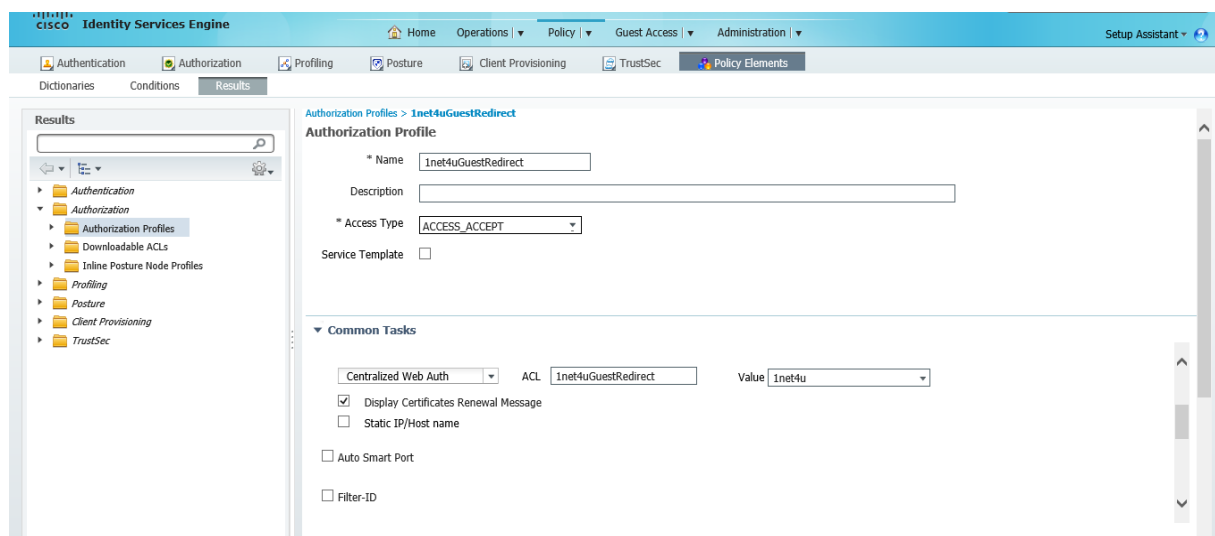
Steg 10)

Skapa authorization profiles som ska gälla för de gäster som autentiserar sig.

Logga in på ISE: Policy -> Policy Elements -> Results -> Authorization Profiles
-> Add

Steg 11)

Välj "Web Redirection (CWA, MDM, NSP, CPP)" sen "Centralized Web Auth" samt den ACL som skapades I WLCn, och I "Value" ska den portal du skapat.



Steg 12)

Skapa sedan en ny ACL I WLC som tillåter den trafik företaget vill att gästerna ska ha tillgång till.

Steg 13)

Skapa en ny Authorization Profile:

I den ska Airespace ACL Name väljas och den nya ACLen ska användas.

Steg 14)

Skapa två nya Authorization Policies: Policies -> Authorization

Ena policyn ska ha "Condition = Radius:Called-Station-ID CONTAINS GÄST-SSID" och "Permissions = Den profile med Web Redirection"

Den andra policyn ska ha "Condition = GuestType_Daily (default)"
och "Permissions = Den profile med Airespace ACL"

Steg 14)

Som sponsor kan du antingen skapa ett konto genom att logga in på ISEn och gå via: Guest Access -> Manage Accounts -> Manage Accounts

Eller via en sparad länk till den sidan direkt då hanteringen av konton sker av en separat databas i ISEn.

Steg 15)

The screenshot shows the 'Create Accounts' page in ISE. At the top, there are four buttons: 'Create Accounts' (highlighted in blue), 'Manage Accounts (3)', 'Pending Accounts (0)', and 'Notices (0)'. Below the buttons, the 'Guest type' is set to 'Daily (default)'. A note states: 'Maximum devices that can be connected: 5' and 'Maximum access duration: 5 days'. The 'Guest Information' section has three tabs: 'Known' (selected), 'Random', and 'Import'. It contains input fields for 'First name', 'Last name', 'Email address', 'Phone number', 'Company', and 'Person being visited (email)'. The 'Access Information' section includes 'Duration:*' (1), 'From Date (yyyy-mm-dd)*' (2015-05-06), 'From Time*' (20:40), 'To Date (yyyy-mm-dd)*' (2015-05-06), and 'To Time*' (23:59). A 'Location' dropdown is set to 'CET'. A blue 'Create' button is at the bottom right.

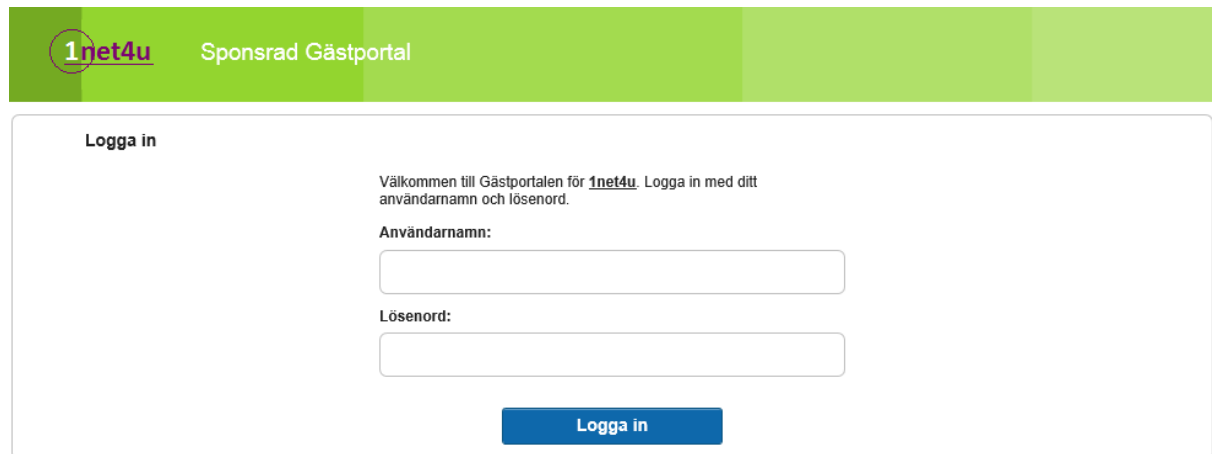
Här skapas kontot för gästen. Du som sponsor kan välja att skapa ett konto med en specifik giltighetstid samt fylla i den personliga informationen om gästen.

Steg 16)

När kontot är skapat så ges informationen för användarnamn och lösenord till gästen.

Steg 17)

När gästen sedan ansluter sig till *Gäst-SSID* och öppnar webbläsaren så kommer hen till portalen där användarnamnet och lösenordet ska skrivas in.



Logga in

Välkommen till Gästportalen för **1net4u**. Logga in med ditt användarnamn och lösenord.

Användarnamn:

Lösenord:

Logga in

Efter gästen loggat in kommer den få tillgång till det som tidigare definierades i ACLen för Airespace.

Slutsats experiment 1

Det här experimentet har bevisat att ett konto kan skapas och få olika policys tilldelade sig. På så sätt kan besöksmottagaren välja vad gästen kan få tillgång till genom att skapa eller redigera olika ACLer som kopplas till olika policys som gästernas konton matchar när de försöker logga in. Det här experimentet har även bevisat att det kan lätt bli stora konfigurationer när policys ska skapas och anpassas för olika gäster.

Experiment 2

Det här experimentet går ut på att stödja referens [28] och visa hur en gästaccess-server (ISE) kan göra så att vissa sponsorer kan skapa olika konton beroende på hur mycket behörighet som ska ges ut till gästen.

För att demonstrera detta experiment så behövs en PC och en gästaccess-server (I det här experimentet används Cisco ISE) som är konfigurerade med IP-adresser samt anslutna till ett nätverk så enheterna kan nå varandra.

Steg 1)

Öppna webbläsaren på PC och skriv in IP-adressen till ISE som URL.

Steg 2)

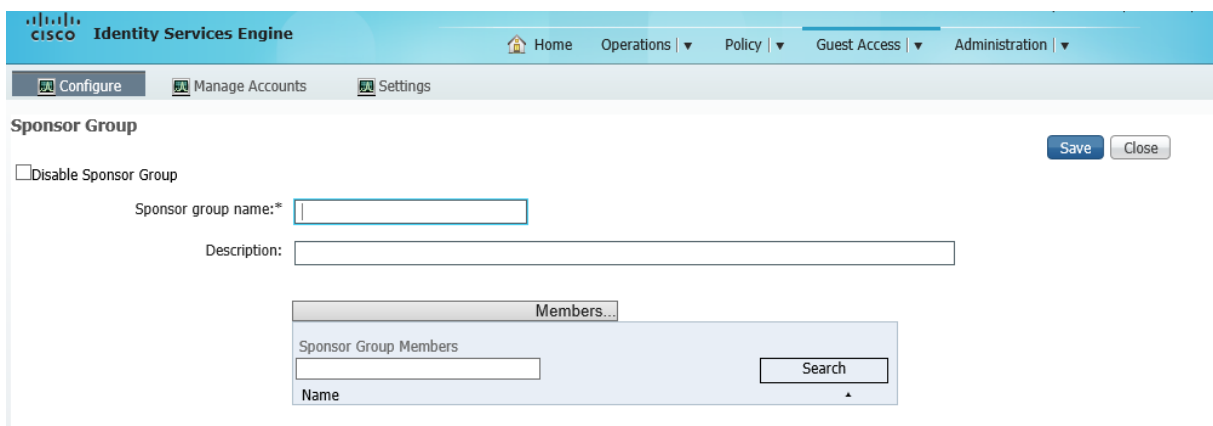
Logga in med ett giltigt konto på ISE.

Steg 3)

Skapa en ny "Sponsor Groups" genom att gå via flikarna: Guest Access -> Configure -> Sponsor Groups -> Create

Steg 4)

Välj lämpligt namn på den nyskapade "Sponsor Groups" för att förenkla senare i konfigurationen.

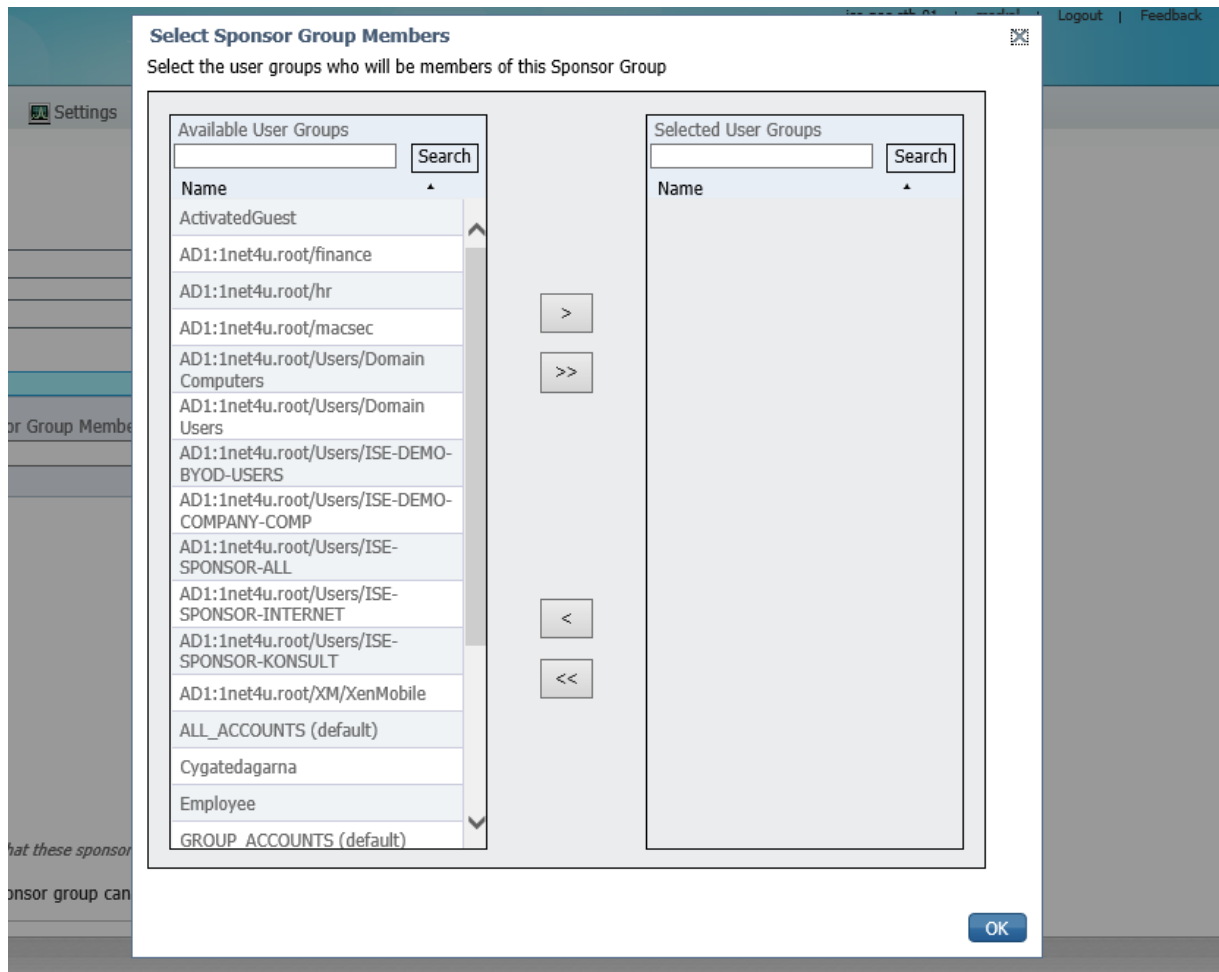


The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a Sponsor Group. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The main menu has 'Configure', 'Manage Accounts', and 'Settings'. The 'Sponsor Group' configuration page includes a 'Disable Sponsor Group' checkbox, a 'Sponsor group name:*' text input field, and a 'Description:' text input field. Below these is a 'Members...' section with a search bar and a 'Search' button. The page also features 'Save' and 'Close' buttons.

Välj sedan "Members..."

Steg 5)

Här läggs de konton eller grupper som ska räknas till den här "Sponsor Groups"



För att välja ett konto eller grupp: Flytta önskade konton till höger sida för att de ska väljas.

Tryck sedan "OK" och sedan "Save".

Steg 6)

Välj "Guest Types" och sedan "Create" för att skapa en ny sorts gästkonto.

Steg 7)

Guest Type Save Close

Guest type name: *

Description:

Language File

Collect Additional Data

Maximum Access Time

Maximum account duration
 days (1-999)

Allow access only on these days and times:
 From To Sun Mon Tue Wed Thu Fri Sat

Login Options

Maximum simultaneous logins (1-999)

When guest exceeds limit:
 Remove the oldest connection
 Don't connect

Maximum devices guests can register: (1-999)

Store device information in endpoint identity group:

Configure endpoint identity groups at: Administration > Identity > Management > Groups > Endpoint Identity Groups

Purge endpoints in this identity group: As Per EndPoint Purge Policy

Configure endpoint purge at Administration > Identity Management > Settings > Endpoint purge

Allow guest to bypass the Guest portal

Account Expiration Notification

Send account expiration notification days before account expires

View messages in:

Email

Use customization from:

Messages: Copy text from:

Send test email to me at:

Configure SMTP server at: Administration > Systems > Settings > SMTP server

SMS

Messages: Copy text from:

(160 character limit per message)*Over 160 characters requires multiple messages.*

Send test SMS to me at:

Configure SMS service provider at: Administration > Systems > Settings > SMS Gateway

These sponsor groups can create this guest type:

Sponsor Groups:

På den här sidan kan konfigurering göras som kommer begränsa gästkontot på olika sätt t.ex. vilka dagar det kan skapas och hur länge ett konto gäller.

Längs ner vid "Sponsor Groups" läggs de Sponsor groups som ska kunna skapa den här typen av gästkonto.

Slutsats experiment 2

Det här experimentet har bevisat det påstående att olika besöksmottagare kan ha rättigheter att skapa olika typer av konton för gästerna. Att planera nya sponsorgrupper kan vara en svår uppgift, det gäller att ha en tydlig strategi på hur dessa ska se ut och vilka som ska tillhöra de olika grupperna.

Experiment 3

Det här experimentet går ut på att stödja referens [30] i det här arbetet.

Dessa steg ska leda fram till att visa att konton som skapats i gästaccess-servern behövs tas bort från servern då annars kontot bara blir inaktivt när det gått ut men fortfarande finns kvar i databasen på servern.

För att kunna göra det här experimentet behövs: En gästaccess-server (ISE används i detta experiment), En PC samt ett gästkonto som är inaktivt och redo att tas bort.

Både ISE och PC ska vara konfigurerade med IP-adresser samt nåbara från respektive enhet.

Steg 1)

Öppna Webbläsaren på PC och används IP-adressen för ISE so URL.

Steg 2)

Logga in med giltigt användarnamn.

Steg 3)

För att hantera konton gå in på portalen "Manage Accounts" via: Guest Access -> Manage Accounts

Steg 4)

Här syns kontot som har status "Expired". Möjligheten att förlänga och ge kontot status "Active" finns fortfarande därför finns kontot fortfarande kvar i ISE databasen.

Create Accounts **Manage Accounts (1)** Pending Accounts (0) Notices (0)

Edit Resend Extend Suspend Delete Reset Password Reinstate Refresh

User...	State	First Na...	Last Name	Email A...	Phone N...	Group Tag	Location	Sponsor	Guest T...	Expirati...	Time Left
<input type="checkbox"/> mkallur	Expired	Marcus	Kallur	test@1net...	0761112222		CET	markal	Guest-DefaultEightH	2015-05-12 11:05	0D 00H 00M

[Help](#)

Steg 5)

För att ta bort kontot: Markera kontot som ska tas bort i rutan till vänster om användarnamnet -> Delete -> OK

Create Accounts **Manage Accounts (1)** Pending Accounts (0) Notices (0)

Edit Resend Ext... Refresh

User...	State	First Na...	Last Name	Email A...	Phone N...	Group Tag	Location	Sponsor	Guest T...	Expirati...	Time Left
<input checked="" type="checkbox"/> mkallur	Expired	Marcus	Kallur	test@1net...	0761112222		CET	markal	Guest-DefaultEightH	2015-05-12 11:05	0D 00H 00M

[Help](#)

Slutsats experiment 3

Det här experimentet har lett fram till att efter att ett konto gått ut i giltighetstid så tas det inte automatiskt bort från gästaccess-servern. Utan en behörig person måste logga in i enheten och manuellt ta bort det inaktiverade kontot.

Experiment 4

Det här experimentet ska visa hur en uppsättning kan göras av metoden "Självregistrering" som både kan notifiera gästen med kontotuppgifterna via SMS och Epost.

Det som behövs för detta experiment är de material som beskrivits i "1.4 Material" för självregistrering (ISE används som gästaccess-server).

Förutsättningarna som behövs för att det här experimentet ska fungera är att alla enheter är konfigurerade med IP-adresser samt att enheterna kan nå varandra.

Steg 1)

Logga in på ISE genom att skriva in dess IP-adress som URL i en webbläsare.

Steg 2)

Konfigurera en SMTP-server så att Epost kan skickas till gästen: Administration -> System -> Settings -> SMTP Server. Skriv in IP-adressen för SMTP-Servern t.ex. *192.168.2.100*

Steg 3)

Konfigurera en SMS-Gateway: Administration -> System -> Settings -> SMS Gateways -> Add.

The screenshot shows the configuration page for an SMS Gateway Provider. The title is "SMS Gateway Provider List > Global Default". The main heading is "SMS Gateway Provider". The configuration fields are as follows:

- SMS Gateway Provider Name: * **Global Default**
- Select Provider Interface Type:
 - SMS Email Gateway
 - SMS HTTP API
- SMS Gateway Provider Domain: (ex: mms.smsprovider.com)
- Provider account address: (optional field used as FROM address of email. ex: myaccount@smsprovider.com)
- SMTP API destination address: (optional field used as TO address of email. ex: sms@smsprovider.com)
- SMTP API body template: (optional, for API requiring email body template format.)
- Break up long message into multiple parts (140 byte chunks)

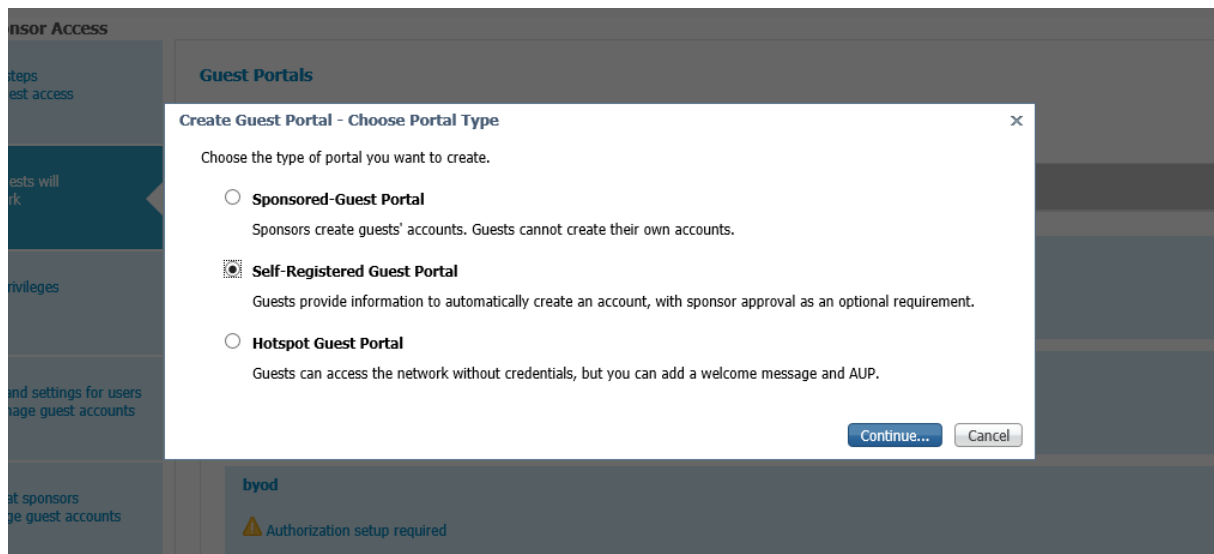
At the bottom, there are "Save" and "Reset" buttons.

Notis: Den här SMS Gatewayen använder sig av en SMTP-Server som sedan skickar vidare uppgifterna till en SMS Gateway. Det som står i "SMTP-API body template:" är olika variabler som skickas med till SMTP-servern från ISEn. Variabeln \$mobilenumber\$ är gästens mobilnummer som den angivits och

\$message\$ är det meddelande gästen kommer få som SMS med sina uppgifter. SMTP-servern fungerar på så sätt att den plockar ut mobilnumret som står inom mobb- -mobb och flyttar upp det istället för "mobbhere" i "SMTP API destination address:".

Steg 4)

Skapa en ny "Self-Registered Guest Portal" genom att gå via: Guest Access -> Configure -> Guest Portals -> Create -> Self-Registered Guest Portal



Steg 3)

Sedan är det bara att konfigurera portalen som företaget vill ha den. Under "Self-Registration Page Setting" kan vilka uppgifter som företaget vill att gästen ska lämna konfigureras samt vilket typ av konto gästen ska få tillgång till.

Beroende på hur företaget vill ha det så kan konfigureringen se annorlunda ut. Men för att SMS och Epost ska fungera så måste "Email address" och "Phone number" vara med. Sen Måste även rätt SMS Gateway vara med för att SMS ska fungera.

Företaget kan även här välja ifall de vill att gästen ska komma till en viss URL efter att registreringen lyckats.

Self-Registration Page Settings

Assign self-registered guests to guest type:

Configure guest types at:
[Guest Access > Configure > Guest Type](#)

Account valid for: Maximum: 5 DAYS

Require a registration code for self registration:

Fields to include	Required
<input checked="" type="checkbox"/> User name	<input type="checkbox"/>
<input checked="" type="checkbox"/> First name	<input type="checkbox"/>
<input checked="" type="checkbox"/> Last name	<input type="checkbox"/>
<input checked="" type="checkbox"/> Email address	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Phone number	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Company	<input type="checkbox"/>
<input checked="" type="checkbox"/> Location	<input checked="" type="checkbox"/>

Guests can choose from these locations to set their time zone:

Guests see the locations list only if multiple locations are specified.
Configure guest locations at:
[Guest Access > Settings > Guest Locations and SSIDs](#)

SMS Service Provider

Guests can choose from these SMS providers:

Test
 MK
 Global Default
 T-Mobile
 ATT

Guest see providers list only if multiple are selected
Configure SMS providers at:
[Administration > System > Settings > SMS Gateway](#)

Person being visited

Reason for visit

Configure custom fields at:
[Guest Access > Settings > Custom Fields](#)

Include an AUP

Require acceptance

Only allow guests with an email address from:

Ex. example1.com, example2.com

Do not allow guests with an email address from:

Ex. example1.com, example2.com

Require self-registered guests to be approved
[Guest Access > Settings > Guest Email Settings](#)

Email approval request to:

Enter a comma-separated list of email addresses

After registration submission, direct guest to

Self-Registration Success page
 Login page with instructions about how to obtain login credentials
 URL:

Send credential notification automatically using:

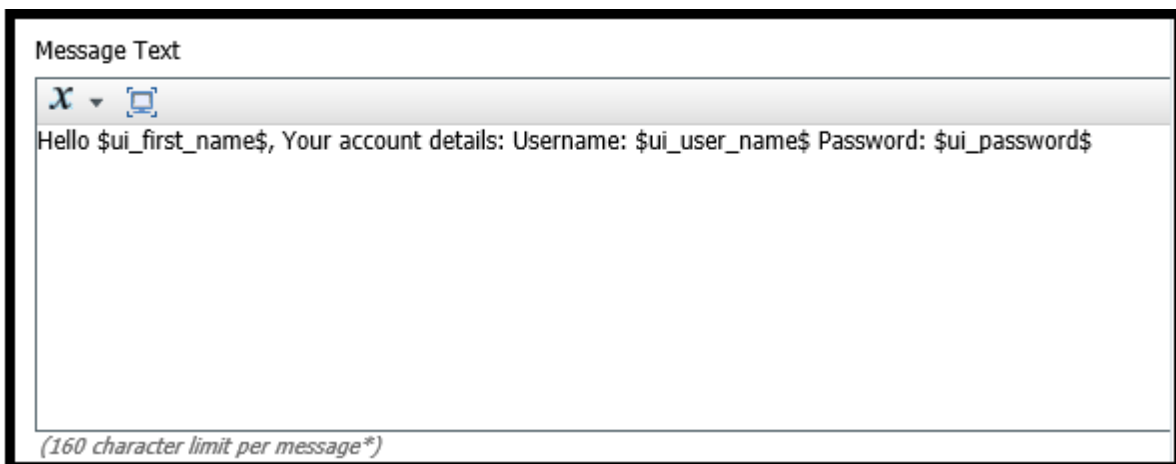
Email
 SMS

Steg 4)

Gå sedan till "Portal Page Customization" för att konfigurera portalen mer så att den passar företaget bättre.

Här kan egna loggor läggas till samt skriva om den defaulta texten som redan står så att det passar företaget bättre.

Under "Notifications" skapas den text som ska skickas till gästen efter registrering. Här används olika variabler för att skicka med rätt uppgifter som t.ex. \$ui_password\$ för användarens lösenord.



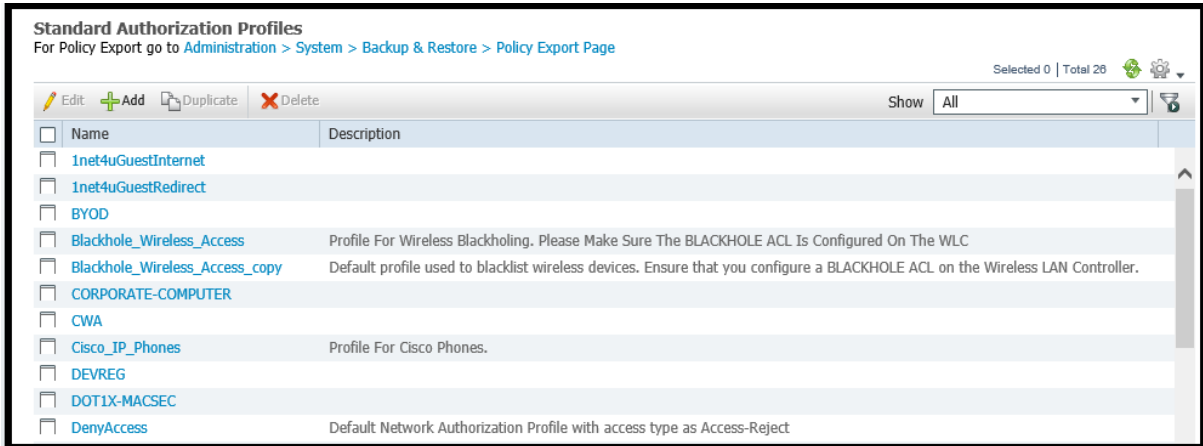
Notis: Detta är för SMS och är det som byts ut istället för \$message\$ som konfigurerades under SMS Gateway i steg 3. Det går att testa att skicka ett SMS/Epost via vardera flikar under "Notifications -> Settings"

Steg 5)

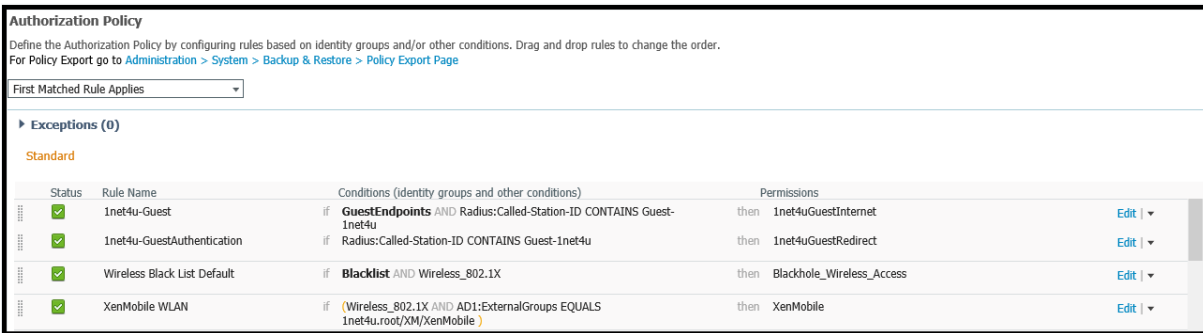
Efter att portalen konfigurerats som företaget vill ha den är det dags att skapa olika authorization profiles och policys.

Notis: Detta görs på exakt samma sätt som i "Experiment 1" steg 4-13. Skapa exakt samma ACLer som beskrivits i "Experiment 1".

Skapa två "Authorization Profiles" *1net4uGuestInternet* och *1net4uGuestRedirect* med den konfiguration beskrivet i "Experiment 1" steg 11-12.



Skapa två "Authorization policys" *1net4u-Guest* och *1net4u-GuestAuthentication*.

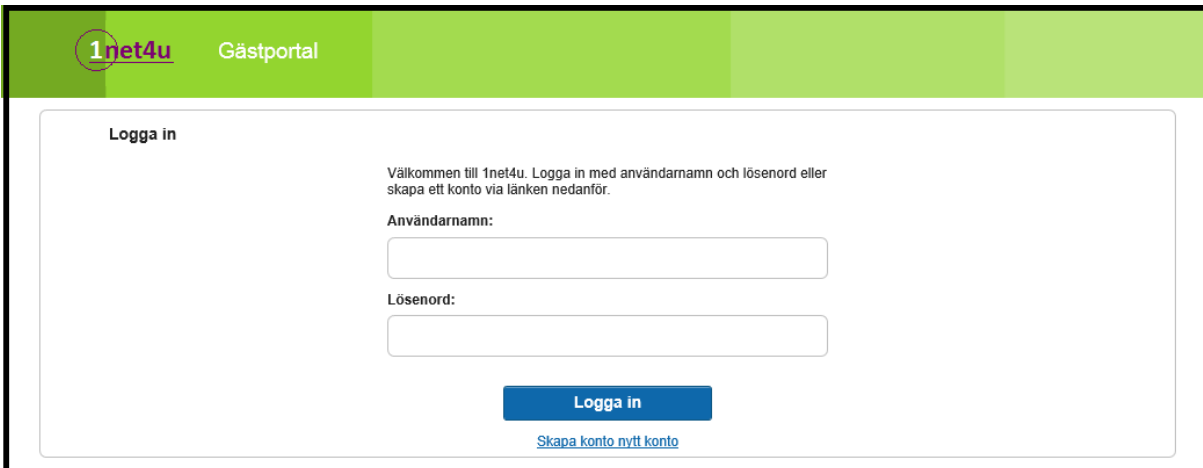


Notis: Se till att det ligger i rätt ordning och har den följande konfigurationen.

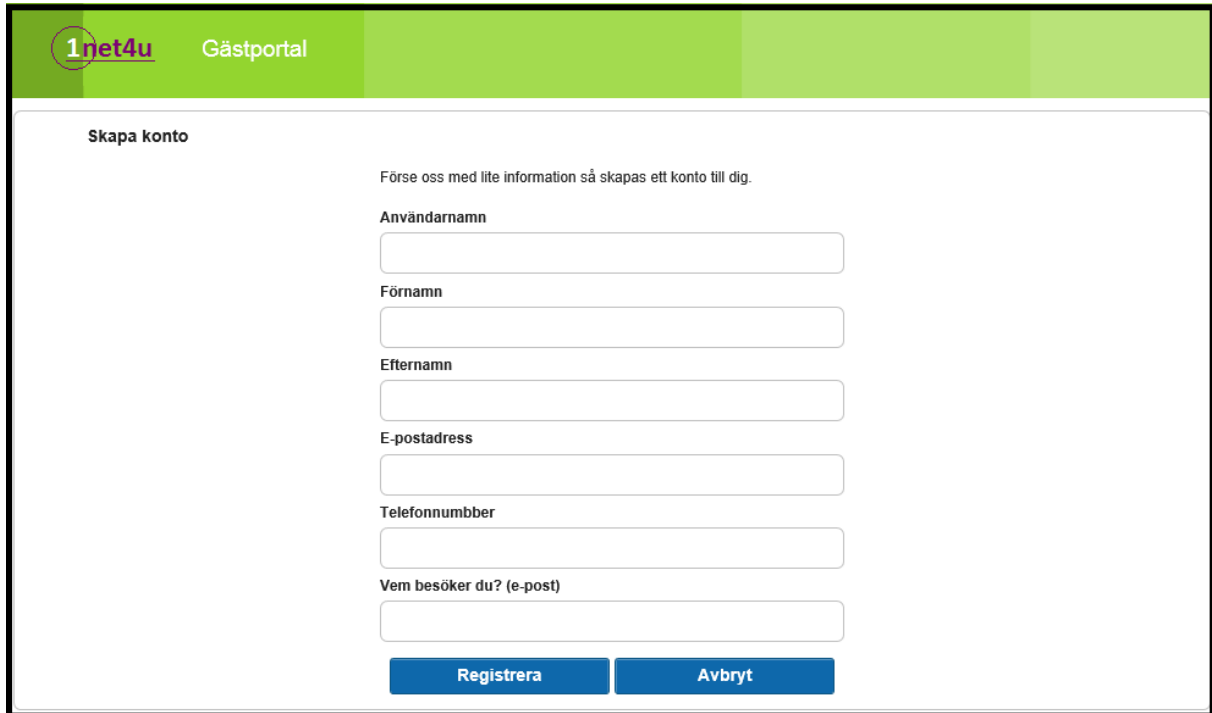
Steg 6)

Testa portalen genom att gå in på portalens konfiguration: Guest Access -> Configure -> Guest Portals -> *din portal* -> Portal test URL

Beroende på hur portalen är konfigurerad att se ut kan den skilja sig från nedanstående bilder.



Tryck på "Skapa konto nytt konto"



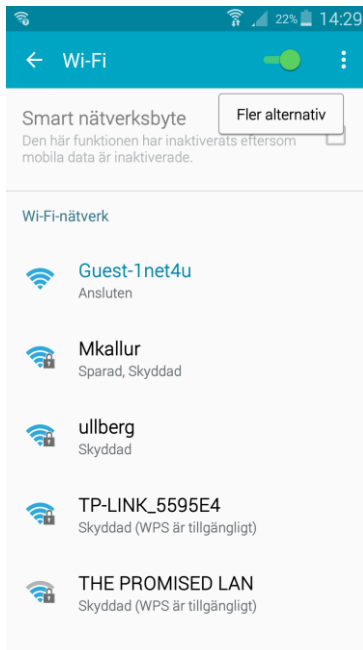
The screenshot shows a web page for creating a new account. At the top, there is a green header with the logo '1net4u' and the text 'Gästportal'. Below the header, the page title is 'Skapa konto'. A message reads: 'Förse oss med lite information så skapas ett konto till dig.' The registration form consists of several input fields: 'Användarnamn', 'Förnamn', 'Efternamn', 'E-postadress', 'Telefonnummer', and 'Vem besöker du? (e-post)'. At the bottom of the form, there are two blue buttons: 'Registrera' and 'Avbryt'.

Bevis att det fungerar

Detta bevis är utfört på en Samsung Galaxy S5.

Steg 1)

Anslut till SSID



Steg 2)

Öppna Webbläsare (om det inte sker automatiskt)

1net4u Gästportal

Logga in

Välkommen till 1net4u. Logga in med användarnamn och lösenord eller skapa ett konto via länken nedanför.

Användarnamn:

Lösenord:

Logga in

[Skapa konto nytt konto](#)

Steg 3)

Fyll i den information som begärts

1net4u Gästportal

Skapa konto

Förse oss med lite information så skapas ett konto till dig.

Användarnamn

Förnamn

Efternamn

E-postadress

Telefonnummer

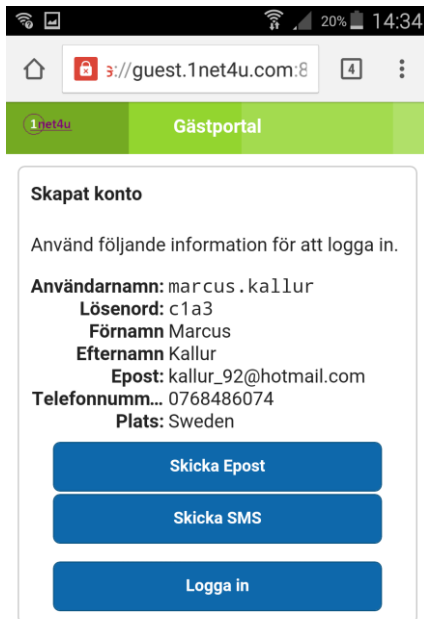
Vem besöker du? (e-post)

Registrera

Avbryt

Steg 4)

Ditt konto skapas och skickas till den angivna Epost och telefonnumret.



1net4u Gästportal

Skapat konto

Använd följande information för att logga in.

Användarnamn: marcus.kallur
Lösenord: c1a3
Förnamn: Marcus
Efternamn: Kallur
Epost: kallur_92@hotmail.com
Telefonnumm...: 0768486074
Plats: Sweden

Skicka Epost

Skicka SMS

Logga in

Steg 5)

Logga in



1net4u Gästportal

Logga in

Välkommen till 1net4u. Logga in med användarnamn och lösenord eller skapa ett konto via länken nedanför.

Användarnamn:

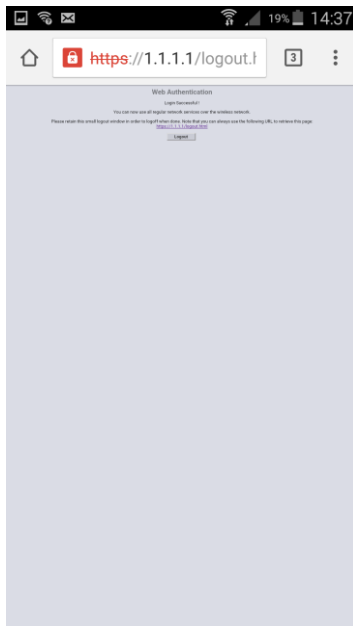
Lösenord:

Logga in

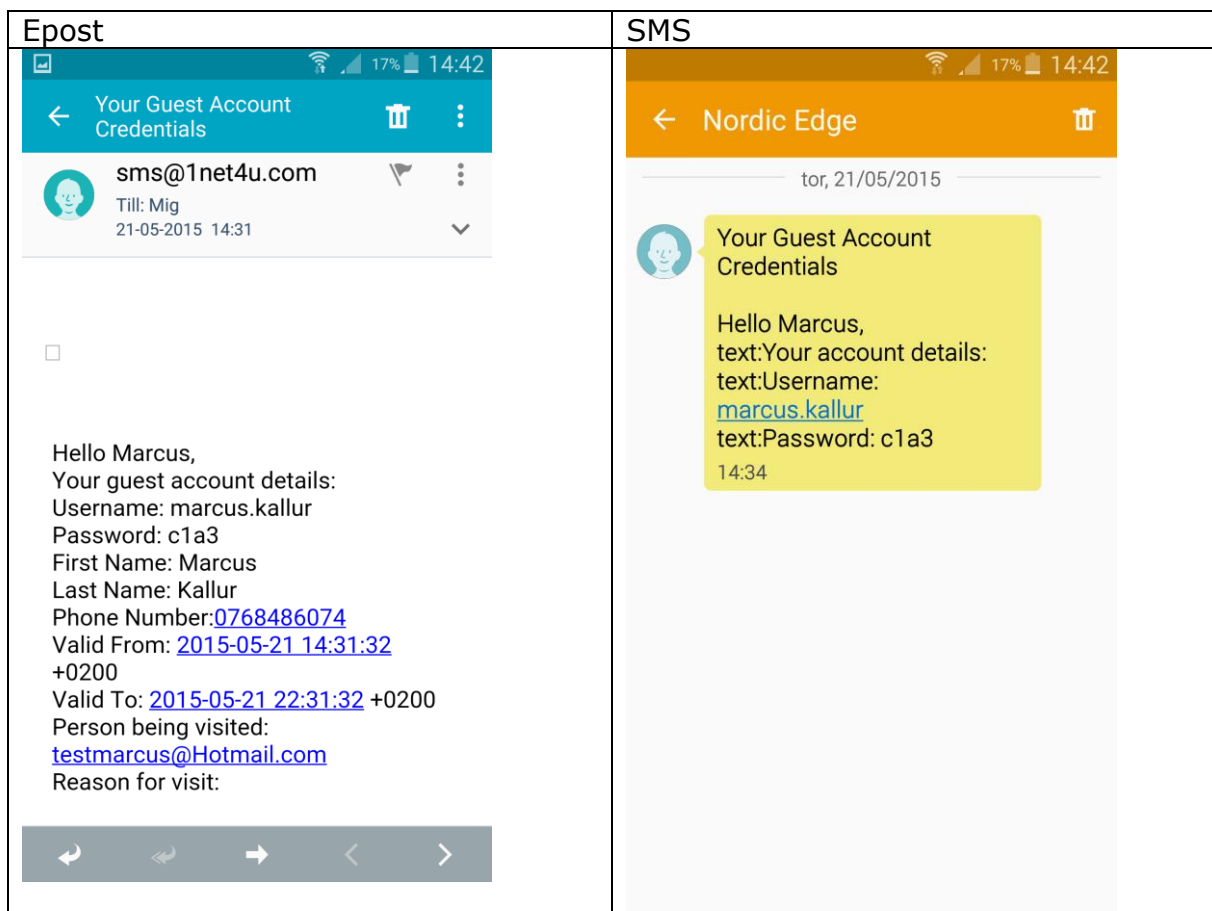
[Skapa konto nytt konto](#)

Steg 6)

Acceptera eventuella policys och sedan är det klart



Så här ser kan Epost och SMS ut som gästen får skickad till sig.



Slutsats experiment 4

Som beskrivits i inledningen till experimentet har det här experimentet gått ut på att visa hur en självregistreringsportal konfigureras på en Cisco ISE. Då det finns väldigt många sätt att konfigurera en portal på och bestämma vilken typ utan information som ska anges av gästen vid registrering har experimentet bara visat lite snabbt om vad som kan göras. Konfigurering av både portal och SMS gateway kommer inte vara exakt likadana på olika företag då de kräver olika saker av en portal. Beviset styrker även att konfigurationen som gjord fungerar.

