



Avdelning för datavetenskap

Adnan Baktirovic

Utveckling av hotspotsystem

Hotspot system development

Datavetenskap
C-uppsats 15hp

Datum/Termin: 070118
Handledare: Thijs Holleboom
Examinator: Martin Blom
Lönummer: C2008-02

Utveckling av hotspotsystem

Adnan Baktirovic

Denna rapport är skriven som en del av det arbete som krävs för att erhålla en kandidatexamen i datavetenskap. Allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och inget material är inkluderat som tidigare använts för erhållande av annan examen.

Adnan Baktirovic

Handledare: Thijs Holleboom

Examinator: Martin Blom

Sammanfattning

Detta examensarbete är gjort på uppdrag av Fiber Optik Valley. Huvuduppdraget i projektet var att skapa ett fungerande betalningssystem för en hotspot och att utveckla företagets webbsida. Hotspotsystemet som baserades på en gratis tjänst från Public IP, är tänkt att kunna fungera delvis autonomt utan ägarens ingripande. Företagets webbsida skapades i en Flex2-utvecklingsmiljö och produkten blev en Adobe Flash-applikation. För att få ett dynamiskt och konfigurerbart system skapades även en kontrollpanel till webbsidan åt företagets webbadministratörer, så att innehållet på sidan ska kunna förändras utan att behöva kompilera om koden. Kontrollpanelen säkrades också med en inloggningsprocess.

Som underliggande motor och som ersättning för brister i Flash-funktionaliteten, användes Simple PHP-tjänster mellan Flash-applikationen och PHP-skripten på servern. Betalningssystemet utvecklades med hjälp av PHP, MySQL och JavaScript. I systemet ingår PayPal's IPN-tjänster för penningtransaktioner och validering av transaktioner. En självständig AMP-server, Apache2, MySQL och PHP5.0, lades till hotspotsystemet för att minska behovet av att ha en webbsida på ett externt webbhotell.

Hotspot system development

Abstract

This graduation work was done as a assignment from Fiber Optic City company based in Hudiksvall Sweden. The base assignment was to create an automated payment system for a Hotspot network and a company web page. The hotspot system should work as a standalone service. The company has already a working free-of-charge service that is offered to its customers and is based on Public IP system.

The company webpage was done with the help of a development suite called Flex2 and the result was an Adobe Flash application. To increase webpage dynamics a second page was developed for the company to have the ability to change and configure the main company webpage. An authentication service was deployed to configuration page to increase its security. As an engine and a substitute for lack of functionality and security in Adobe Flash simplePHP web service was used to connect Flash with a PHP script on its server.

The payment system was developed with the help of PHP, MySQL and JavaScript. The system uses Paypal IPN service for money transaction and transaction validation

A standalone web server with Apache2, PHP 5.0 and MySQL was deployed to the hotspot system to reduce the need of having an authentication system on a commercial Internet based web hotel.

*Albert Einstein, when asked to describe radio,
replied:*

*"You see, wire telegraph is a kind of a very, very long
cat. You pull his tail in New York and his head is
meowing in Los Angeles. Do you understand this? And
radio operates exactly the same way: you send signals
here, they receive them there. The only difference is
that there is no cat."*

Innehåll

1	Inledning	1
1.1	Syfte	1
2	Bakgrund	1
2.1	Hotspot.....	2
2.2	Trådlös kommunikation.....	3
2.3	IEEE standard	4
2.3.1	IEEE 802.11	5
2.3.2	IEEE 802.11a	6
2.3.3	IEEE 802.11b.....	7
2.3.4	IEEE 802.11g.....	7
3	Existerande system.....	9
3.1	Public IP-tjänsten.....	9
3.1.1	ZoneCD.....	10
3.1.2	Public IP's kontrollserver.....	14
3.2	Webbutveckling	15
3.2.1	HTML	15
3.2.2	XML.....	17
3.2.3	PHP	18
3.2.4	JavaScript.....	19
3.2.5	Flex2 och ActionScript 3.0	20
3.2.6	CSS	22
3.3	Serverapplikationer.....	22
3.3.1	Apache	23
3.3.2	MySQL	23
3.3.3	DDClient	24
3.4	PayPal	24
3.4.1	Betallänkar	25
3.4.2	Instant Payment Notification (IPN).....	25
3.4.3	Payment Data Transfer (PDT)	25
3.4.4	SOAP-webbtjänster (APIs).....	26
3.4.5	Express Checkout."PayPal-plånbok"	27
3.5	Säkerheten.....	28
3.5.1	Iptables.....	28
3.5.2	WEP	29
3.5.3	WPA.....	30
3.5.4	WPA2.....	31
3.5.5	VPN	31
3.5.6	SSL.....	33
4	Beskrivning av konstruktionslösning	34
4.1	Public IP's kontrollserverinställningar	34
4.2	ZoneCD-konfiguration	35
4.3	Apache, MySQL och PHP	35

4.4	Webbdesign	36
4.4.1	Företagets webbsida	36
4.4.2	Administratörens kontrollpanel	37
4.4.3	Användarnas webbsidor	37
4.5	Den trådlösa säkerheten	38
5	Användargränssnitt	39
5.1	Företagets webbsida	39
5.1.1	Nyheter/News	40
5.1.2	Om oss/About us	41
5.1.3	Hjälp/Help	42
5.1.4	Beställ/Order	43
5.2	Administratörens webbsida	44
5.2.1	Administratörspanelen	45
5.2.2	Layout	46
5.2.3	Om oss	47
5.2.4	Användare	48
5.2.5	Faq	50
5.2.6	Nyheter	51
5.3	Användarnas webbsidor	53
5.3.1	Inloggningswebbsida	53
6	Implementering	55
6.1	Förberedning	55
6.2	Hårdvaran	56
6.2.1	Inställningar för accesspunkten	56
6.3	Apache, PHP och MySQL på flashminnet	56
6.3.1	Apache	57
6.3.2	Skapa ett SSL-certifikat	59
6.3.3	MySQL-konfiguration	60
6.3.4	PHP5-konfiguration	60
6.4	Webbdesign och webbprogrammering för hotspoten	61
6.4.1	Kundinloggning	61
6.4.2	Registreringsfilerna	64
6.5	Webbdesign och webbprogrammering för företagets webbsida	65
6.5.1	Katalogen /xml-textuell databas	65
6.5.2	Katalogen /bin-företagets Flash-webbsida	66
6.5.3	Katalogen /admin-administratörens kontrollpanel	67
6.5.4	MXML- och ActionScript-tjänster	68
7	Resultat	72
8	Slutsats	73
	Referenser	75
	Akronym	76
A	ZoneCD-automatiserade skript	77
A.1	Zonecd-unpack.sh	77
A.2	cleanup.sh	78

A.3	init.sh	79
B	Funktionslista med beskrivningar	80
B.1	login.php	80
B.2	ipn_user.php.....	81
C	MySQL-tabeller (SQL-syntax)	86
C.1	users	86
C.2	ipn_users	87

Figurförteckning

Figur 1 Hotspots	2
Figur 2 Vanlig radiosändare	4
Figur 3 802.11a, 802.11b och 802.11g kan användas samtidigt i ett nätverk.....	6
Figur 4 ZoneCD tillhör Debian-familjen.	10
Figur 5 Förslag på en hotspotkonfiguration	13
Figur 6 Strikt kodad "Hello World" I HTML	16
Figur 7 Enkel "Hello World" i SGML.....	17
Figur 8 "Hello World" i XML	18
Figur 9 "Hello World" i PHP	19
Figur 10 "Hello World"-popup med JavaScript.....	20
Figur 11 "Hello World" som Flash-animation med MXML och ActionScript	22
Figur 12 PayPal's SOAP-tjänster	27
Figur 13 Enkel WEP-kryptering	30
Figur 14 Ett OpenVPN-nätverk	33
Figur 15 Autentiseringsprocess för en kund	37
Figur 16 Företagets webbsida	39
Figur 17 Företagets webbsida med tillståndet "Nyheter/News"	41
Figur 18 Tillståndet "Om oss/About us" på företagets webbsida	42
Figur 19 Tillståndet "Hjälp/Hel" på företagets webbsida	43
Figur 20 Tillståndet "Beställ/Order" på företagets webbsida	44
Figur 21 Inloggningsrutan till administratörens kontrollpanel	45
Figur 22 Ändringar av webbsidans layout från administratörens panel	47
Figur 23 "Om oss" på administratörens panel	48
Figur 24 Dialogruta som bekräftar att en användare har tagits bort	49
Figur 25 Lista över hotspotanvändarna på administratörens panel.....	49
Figur 26 "Faq" på administratörens panel	51
Figur 27 "Nyheter" på administratörens panel.....	52
Figur 28 Användarens inloggningsformulär	53
Figur 29 Användarens registreringsformulär	54
Figur 30 Ett exempel på en serverkonfigurationsfil för Apache2.....	58
Figur 31 Exempel på ett apache2-ssl-certifikat.....	59
Figur 32 Konfigurationsfilen /etc/mysql/my.cnf för MySQL.....	60

Figur 33 Konfigurationsvariabler som ska ställas in för login.php.....	63
Figur 34 Ett exempel på en MXML-http-tjänst	70
Figur 35 Ett exempel på en ActionScript-http-tjänst	70

Tabellförteckning

Tabell 1 Kanalindelning för IEEE 802.11g.....	8
---	---

1 Inledning

Fiber Optic Valley¹ är en arena för utveckling och test av bredbandsteknik och tjänster baserade på fiberoptisk spjutspetskompetens. Med utbredningen av den trådlösa tekniken bland den allmänna befolkningen skapades behovet för trådlösa LAN², hotspotsystem, som kan erbjuda åtkomsten till Internet på allmänna platser till potentiella kunder. Fiber Optic Valley har redan en gratistjänst, som sköts manuellt av systemadministratören genom ett webbaserat gränssnitt. För att erbjuda ett flexibelt system för betalning till sina användare, med den Internettjänst de erbjuder, beslöt sig Fiber Optik Valley för att använda PayPal-tjänster³.

1.1 Syfte

Syftet med följande projekt är att skapa ett fungerande hotspotsystem för privat bruk eller ett mindre företag. Arbetet kommer att innefatta allt som ingår i en fungerande lågkostnadshotspot med: företagets välkomstwebbsida, en inloggningshemsida för kunder som ersätter standardinloggningssidan från Public IP och ett betalningssystem. Systemet ska vara helt automatiserat och hemsidan ska vara snyggt designad.

2 Bakgrund

Följande kapitel kommer att beskriva de olika tekniker och benämningar som idag används för att överföra data trådlöst på en allmän plats eller i hemmet. Inledningsvis förklaras begreppet hotspot och dess användningsområden och laglighet inom det svenska rättssystemet. Vidare beskrivs i korthet hur trådlös överföring i allmänhet fungerar från en

¹ <http://www.fiberopticvalley.se/>

² LAN Akronym för *Local Area Network* och ett begrepp inom datakommunikation.

³ PayPal Ett företag som specialiserat sig på Internetbetalningar: <https://www.paypal.com/>

sändare till en mottagare. Avslutningsvis tas de olika IEEE⁴-standarderna upp som används för trådlös dataöverföring och som utnyttjas i en hotspot, deras för- och nackdelar samt hur de fungerar.

2.1 Hotspot



Figur 1 Hotspots

En hotspot är ett aktivt publikt område som erbjuder höghastighets-Internet. Allmänheten kan koppla upp sig enbart med hjälp av ett trådlöst nätverkskort. Tekniken kan erbjudas gratis för alla, men kan också begränsas till ett antal trådlösa användare som är gäster på ett café eller ett hotell. Ägaren till en hotspot kan även välja att ta betalt för tjänsten. Men som ett tredje alternativ, kan man som användare koppla upp sig mot någon annans hotspot, om man själv

⁴ **IEEE** *Institute of Electrical and Electronics Engineers* är en sammanslutning på över 360 000 tekniker från cirka 175 länder varav 1664 (2006-04-15) finns i Sverige. <http://www.ieee.se>

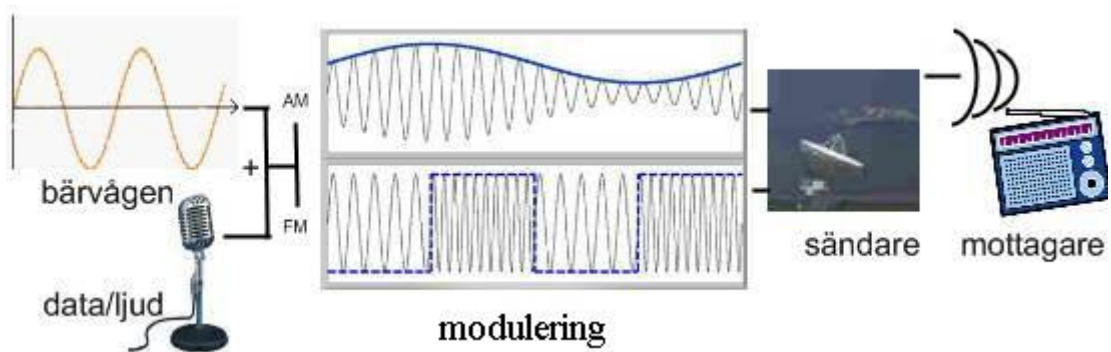
erbjuder en gratis hotspotuppkoppling. Några olika platser och miljöer med en hotspot kan ses i figur 1.

Den svenska lagen, närmare bestämt Post & Telestyrelsen, som hanterar frågor som berör tele, IT och post, säger att man som Internetanvändare skall följa de lagar i kontraktet som Internetleverantören satt upp. Står det att man inte får sända vidare anslutningen, är det alltså olagligt att dela ut denna. Tar man däremot betalt för tjänsten hamnar man i ett område där man måste anmäla sig som operatör. Detta innebär i sin tur särskilda lagar och nya kostnader som man har att ta hänsyn till.

2.2 Trådlös kommunikation

Inom den trådlösa kommunikationen använder man sig av elektromagnetiska vågor, för att överföra information från en punkt till en annan, utan att förlita sig på en fysisk anslutning. Några exempel på elektromagnetiska vågor är röntgenstrålning, synligt ljus och radiovågor. I ett trådlöst nätverk används antenner för att omvandla en elektrisk informationssignal till radiovågor, men även motsatsen, för att avkoda en signal från dessa vågor. Radiovågorna fungerar här som bärare av informationen som ska sändas och kallas därför bärvågen. Den data som skall överföras överlagras (läggs på) på bärvågen och extraheras (rensas ut) när den når mottagarantennen. Informationen som ska sändas ligger på så sätt inbäddad i bärvågen. Inom radiotekniken säger man att bärvågen är modulerad, se figur 2.

En bärvåg är i sitt omodulerade skick, en konstant (odämpad) våg. När data väl modulerat bärvågen, kommer utseendet att ha ändrats, till en ny och modulerad bärvåg. För alla de olika sätt som finns att modulera en bärvåg på, är de två absolut vanligaste sätten amplitudmodulering (AM) och frekvensmodulering (FM). När data läggs på i AM ändras amplituden (avståndet mellan vågens jämviktsläge och vågtopp) för bärvågen. I FM ändras istället frekvensen hos bärvågen, dvs. antal svängningar per tidsenhet för densamma.



Figur 2 Vanlig radiosändare

För ett typiskt trådlöst nätverk ansluter man en sändare/mottagare, även kallad basstation eller accesspunkt, till Internet via en vanlig nätverkskabel, se figur 3. Accesspunkten tar sedan emot, buffrar och sänder data, mellan den trådlösa utrustningen och det trådburna nätverket.

En enstaka accesspunkt kan förse en mindre grupp användare och har ett täckningsområde på mellan 30-50 meter inomhus (beroende på väggarnas tjocklek och material). Användaren får tillgång till det trådlösa nätverket genom ett trådlöst nätverkskort, som finns både för bärbara, stationära och portabla handdatorer. De trådlösa nätverken är oberoende av operativsystemet som används i mottagarstationen och i användarens dator, och kan således användas i såväl Windows, UNIX och Mac-miljö.

2.3 IEEE standard

IEEE är en standardiseringsorganisation som har ett antal arbetsgrupper, som jobbar med utvecklingen av öppna standarder för trådlös kommunikation. IEEE har utvecklat flera specifika standarder för olika ändamål. Dessa är tillgängliga för alla att använda och implementera.

Specifikationskraven för varje standard anger de bästa möjliga resultaten för den aktuella standarden. Exempelvis är IEEE 802.11b, även känd som Wi-Fi, en standard designad för trådlös kommunikation på kort avstånd. Även om den kan användas för andra typer av kommunikation, så är den inte optimerad för dessa tjänster, och kommer därför inte att utnyttja alla resurser eller få samma prestanda som i kommunikation på kort avstånd. IEEE 802.16 standarden eller Wireless MAN (eng. Metropolitan Area Networks), som den också

kallas, är avsedd främst för kommunikation på långt avstånd, från en punk via flera accesspunkter (bryggor) till slutpunkten. Inom denna standard överförs data på det fysiska skiktet i nätverket, och från en Mac-adress⁵ till en annan Mac-adress.

År 2002 introducerades en ny standard för trådlös kommunikation på långt avstånd, som var avsedd för stora städer. Den betecknades IEEE 802.20 och var tänkt som en ersättare för IEEE 802.16. Nyheterna för standarden var ett bättre utnyttjande av de lägre frekvenserna i det radiovågspektra den verkade inom, IP-baserad kommunikation och dessutom, tillämpningar av en teknik som möjliggjorde trådlös kommunikation för mobil utrustning, med en maxhastighet på 250 km/h.

2.3.1 IEEE 802.11

Som de flesta standarder har IEEE 802.11 genomgått många förändringar och förbättringar. Till en början kunde man överföra information med en hastighet på 1 Mbps genom en 900 MHz kanal. Idag är denna hastighet uppe i 54 Mbps och med en bandbredd från 2400 MHz till 5600 MHz. Bandbredden är uppdelad i ett antal kanaler som överlappar varandra. Man kan använda två kanaler som inte ligger för nära varandra, för att förhindra interferens mellan bär vågorna i två närbelägna nätverk. [23] För IEEE 802.11g används 13 kanaler (se tabell 1 sid. 7). Väljs kanal 1 och kanal 11 för två accesspunkter som ligger nära varandra, undviks störningar dem emellan.

IEEE 802.11 standarden är oberoende av den data som skickas över den. Den används mest för TCP/IP⁶ -protokoll, men kan också hantera andra protokoll som AppleTalk⁷ eller NetBEUI⁸. [4] Alla produkter som följer standarden begränsar sin radiofrekvens och sin utstrålningseffekt från sändaren. Standarden använder sig också av CSMA/CA (eng. Carrier Sense Multiple Access/Collision Avoidance) som accessmetod, för att flera användare skall kunna sända information i det trådlösa nätverket.

CSMA används när en basstation märker att en kanal är upptagen, då avvaktar den ett slumpmässigt antal minuter innan den kontrollerar kanalstatusen igen. Användare som

⁵ **Mac-adress** Hårdvaruadressen till nätverkskortet som är unikt för varje kort som tillverkas. Exempel: xx:xx:xx:xx:xx:xx, där x kan anta värden mellan 0-F i det hexadecimala systemet.

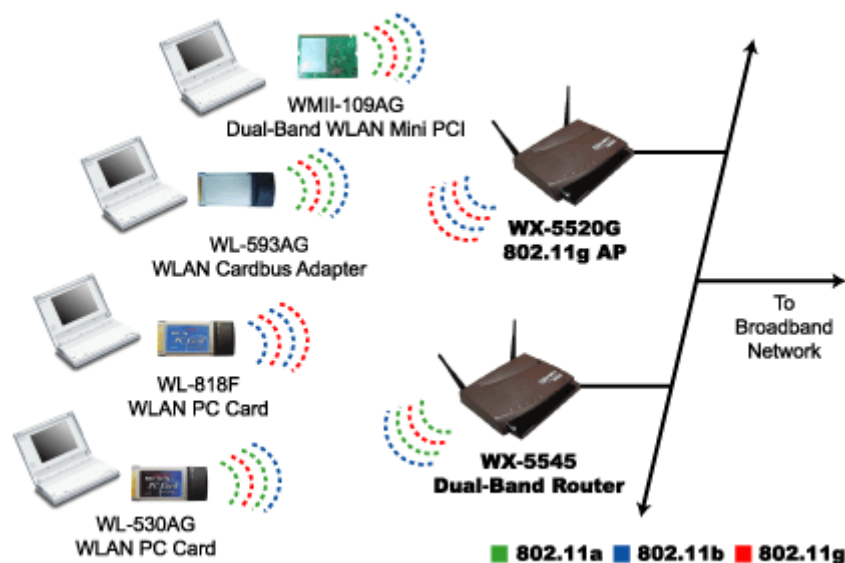
⁶ **TCP/IP** Står för *Transmission Control Protocol/Internet Protocol* och är en arkitektur för datakommunikation över nätverket.

⁷ **AppleTalk** En uppsättning av nätverksprotokoll och ett nätverksfilsystem utvecklat av Apple Computer.

⁸ **NetBEUI** Ett gammalt nätverksprotokoll som används för kommunikation mellan datorer som använder sig av operativsystemet Microsoft Windows.

befinner sig på långt avstånd från basstationen kan se att den finns, men kommer inte åt den då CA-systemet stoppar deras tillträde. Detta beror på att systemet redan är upptaget och blockerat av alla de användare som befinner sig närmare basstationen. Med sitt kortare avstånd utväxlas deras data snabbare med stationen och de får på så vis förtur framför de användare som sitter längre bort. Radiosignalstyrkan minskar med distansen och dataöverföringskanalen täpps till av informationspaketen från de närmaste användarna, som kan sända snabbare. För att avhjälpa dessa resursfördelningsproblem har tillverkarna skapat en typ av väntekö i sina accesspunkter. Väntekön faller inte under någon standard och är oftast en hårdvarulösning.

IEEE 802.11 kan antingen implementeras som Ad-hoc-modell eller infrastruktursmodell. Ad-hoc-modellen används då slutanvändaren inte är uppkopplad mot en accesspunkt, utan skickar data direkt från en dator till en annan. I infrastruktursmodellen används vanligtvis accesspunkten som router, genom vilken all trafik går för att skapa ett trådlöst nätverk.



Figur 3 802.11a, 802.11b och 802.11g kan användas samtidigt i ett nätverk

2.3.2 IEEE 802.11a

Standarden IEEE 802.11a introducerades 1999 och använder sig av digital frekvensmodulering, med frekvenser på mellan 5,150 GHz och 5,825 GHz. Grundprincipen för digital frekvensmodulering bygger på en delning av hög-hastighetsdataströmmar i ett antal

låg-hastighetsdataströmmar, som sedan skickas samtidigt på en lägre frekvens, även benämnda som lågfrekventa bär vågor. [16]

IEEE 802.11a-standarden var från början designad för en frekvens som inte skulle störas av valiga hushållsapparater, såsom mikrovågsugnar eller trådlösa telefoner. Kanalerna i standarden överlappar inte varandra, utan är istället uppdelade i 12 stycken separata och 20 MHz breda frekvensband. Den största och rent teoretiskt möjliga dataöverföringshastigheten för standarden är 54 Mbps. Andra möjliga hastigheter är 6, 9, 12, 18, 24, 36 och 48 Mbps. Av dessa är 6,12 och 24 Mbps obligatoriska för alla produkter. [23]

2.3.3 IEEE 802.11b

Standarden IEEE 802.11b introducerades 1999 och implementerades först av Apple⁹ i deras AirPort-komponenter, som också ingick i deras datorer. Standarden är kompatibel med äldre versioner av IEEE 802.11. Frekvensbandet som ligger mellan 2.400 GHz och 2.487 GHz, är uppdelat i 14 stycken 5 MHz breda kanaler, som överlappar varandra. Designen för IEEE 802.11b tillåter accesspunkter i ett och samma område att sända i dessa kanaler, trots att de delvis täcker varandra. Men eftersom frekvensbandet ligger i den del av radiofrekvensspektrumet som kallas för UHF (Ultra High Frequency), kommer den i kontakt med frekvenser som i en del länder redan är upptagna för andra ändamål. En betydande del av UHF-bandet används exempelvis för television och mobiltelefoni. Somliga kanaler för standarden är därför förbjudna i en del länder. Exempelvis är kanalerna 12, 13 och 14 förbjudna i USA.

2.3.4 IEEE 802.11g

IEEE 802.11g är en standard som är kompatibel med IEEE 802.11b-försedda enheter. Precis som IEEE 802.11a använder den digital frekvensmodulering och har liksom denna en maximal överföringshastighet på 54 Mbps. Den stora skillnaden mellan IEEE 802.11g och IEEE 802.11a är istället bandbredden. [23] Frekvensbandet för standarden ligger mellan 2.400 GHz och 2.500 GHz och är uppdelat i 13 kanaler, med 25 MHz bredd (se tabell 1).

⁹ <http://www.apple.com/se/>

Kanal	Frekvens	Frekvensintervall
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

Tabell 1 Kanalindelning för IEEE 802.11g

3 Existerande system

I föregående kapitel beskrevs de tekniker som ligger till grund för en trådlös datakommunikation. Kapitlet som följer, har istället till ämne att förklara de tekniker som kan användas för att skapa en dynamisk och professionell hemsida. Med dynamisk hemsida menas en automatiserad hemsida, som kan kommunicera med betalningssystemserverar, skicka meddelanden till supporten och ta hand om kunduppgifter. Den mjukvara som kan läggas till operativsystemet och Public IP¹⁰-tjänsten kommer också att tas up.

För det här arbetet valdes av företaget ett operativsystem som har minimala hårdvarokrav. Det heter ZoneCD. Den speciella fördelen med ZoneCD är att man kan styra funktionaliteten och säkerheten för operativsystemet, genom att själv välja vilka program som ska läggas till på CD-skivan. ZoneCD är bland annat baserad på Debian och Morphix, som båda är Linuxdistributioner med en öppen källkod. Inledningsvis ges i kapitlet en kortare presentation av dessa Linuxdistributioner, för dem som önskar skapa sin egen Live-CD Linuxdistribution, och således röja undan behovet av Public IP's kontrollserver.

För dagens olika betalningssystemlösningar på Internet är PayPal en självklarhet. PayPal har utvecklat ett antal tjänster för olika behov och dessa tas alla upp under avsnittet PayPal. Säkerheten innefattar dels trådlösa säkerhetslösningar som finns inbyggda i routern, nämligen som WEP och WPA, dels VPN och Iptables som kan installeras och konfigureras i operativsystemet.

3.1 Public IP-tjänsten

Public IP erbjuder en tjänst som ger möjligheten för exempelvis kaféägare, små och stora företag samt vanliga användare, att bygga upp ett eget hotspotsystem eller en trådlös accesspunkt. Som ägare till en hotspot, kan man genom att använda tjänsten från Public IP kontrollera vem som får koppla upp sig mot nätverket och vilka rättigheter dessa användare får.

Dagens routrar och accesspunkter är alla utrustade med en inbyggd trådlös säkerhet, i form av WPA eller WEP. För att öka säkerheten för sin hotspot kan kunden ges en fast IP-

¹⁰ <http://www.publicip.net/>

adress genom routern, som kan inaktiveras genom servern, för att tidsbegränsa Internetanvändningen. All sådan typ av trafik kontroll för en hotspot kan naturligtvis skötas rent manuellt, men att göra så för en hotspot i ett mindre företag är inte att tänka på. Orsaken till detta är att:

- Kunden kan inte registrera sig utan administratörens ingripande.
- Routern blockerar inte åtkomsten genom WAN porten. Administratören behöver sålunda vara på plats 24 timmar om dygnet för att upprätthålla säkerheten.
- De flesta routrar har ingen informationsfiltrering. Tillfälliga användare har därför öppen uppkoppling mot Internet och möjligheten att ladda ner olagligt material
- Routrar har ingen inbyggd webbtrafikgränskontroll eller fördelning av resurserna bland användarna.

Det finns andra kommersiella lösningar som erbjuder hotspotlösningar, men inget komplett system kan jämföras med Public IP's funktionalitet, öppenhet för förändring och pris. Public IP erbjuder en gratiskontroll av hotspotssystemet, samt en GNU/Linux¹¹-baserad LiveCD¹² som heter ZoneCD, med många inbyggda program. [1]

3.1.1 ZoneCD

ZoneCD är baserad på en Morphix Live-CD. Morphix är en deriverad version av den populära Debian-baserade Live-CD-distributionen Knoppix (se figur 4). [1]



Figur 4 ZoneCD tillhör Debian-familjen.

¹¹ **GNU/Linux** eller alternativt bara **Linux** Ett fritt operativsystem som består av programmen från GNU-projektet med Linux som kärna. Linux är ett framstående exempel på vad utveckling av fri programvara och öppen källkod kan åstadkomma.

¹² **LiveCD** Ett operativsystem som kan köras direkt från CD-skivan utan att installeras.

3.1.1.1 Debian

Debian som påbörjades i augusti 1993 av Ian Murdoch, var en distribution som skulle göras öppen i GNU-anda. Debian fick sitt namn efter grundarens dåvarande och nuvarande flickvän Debra, samt efter Ian, grundaren själv. Debian är en uppsättning av grundläggande program och verktyg som gör datorer körbara, ett s.k. operativsystem. Hjärtat i Debian-systemet är själva Linuxkärnan samt systemverktygen. Ett av de viktigaste verktygen är DPKG (DebianPacKaGes), som används för installation samt borttagning och rensning av Debian-paket. I aktuella Debiandistributioner används verktygen libapt, dselect och den grafiska applikationen Synaptic för pakethantering, medan DPKG används för att behålla beroendegrafens konsistens för installerade paket. Detta gör att installation av extra program är lätt att göra. Allt som krävs är att skriva kommandodelen `apt-get install`, följt av programnamnet, för att installera önskat program. [2,3]

3.1.1.2 Knoppix

Knoppix som är en kompilation av Debian-paket på en CD, känner igen och stödjer de flesta hårdvarukomponenter och perifer utrustning. Knoppix är också en Live-CD, vilket innebär att operativsystemet inte behöver installeras på en hårddisk för att kunna köras. Knoppix använder sig istället av det primära minnet för att skapa ett temporärt filsystem, som behåller den nödvändiga informationen för olika enheter, systemet och användarens filer. [4]

3.1.1.3 Morphix

Morphix är skapat som ett modulärt ramverk, med ett antal moduler för olika ändamål. Upplägget gör det enkelt att skapa och skräddarsy en Live-CD. Baserad på Debian och Knoppix, är det huvudsakliga ändamålet med Morphix att vara lätt att använda samt att installera och dessutom, tack vare Debian och pakethanteraren apt, lätt att uppdatera.

Som en hybrid mellan Debian och Knoppix är Morphix lika användbar som en vanlig Live-CD, men också lika pålitlig och lätt att installera på en hårddisk som Debian. Den innehåller vissa icke-fria drivrutiner (såsom `nvidia-drivrutinen`), vilka kan väljas vid systemstart, men som även kan slås av för att helt stämma överens med Debians filosofi.

Förutom det specialskrivna installationsprogrammet i öppen källkod, jobbar folket bakom Morphix även aktivt med att skapa ett antal extra verktyg och program, för att göra Morphix ännu mer användbart för nya användare. Dessa verktyg licensieras under GPL¹³.

Den enklaste versionen av Morphix består av en uppstartsekvens (bassekvens) och en huvudsekvens. Dessa sekvenser finns också i ZoneCD. De olika modulerna för Morphix och deras uppgifter:

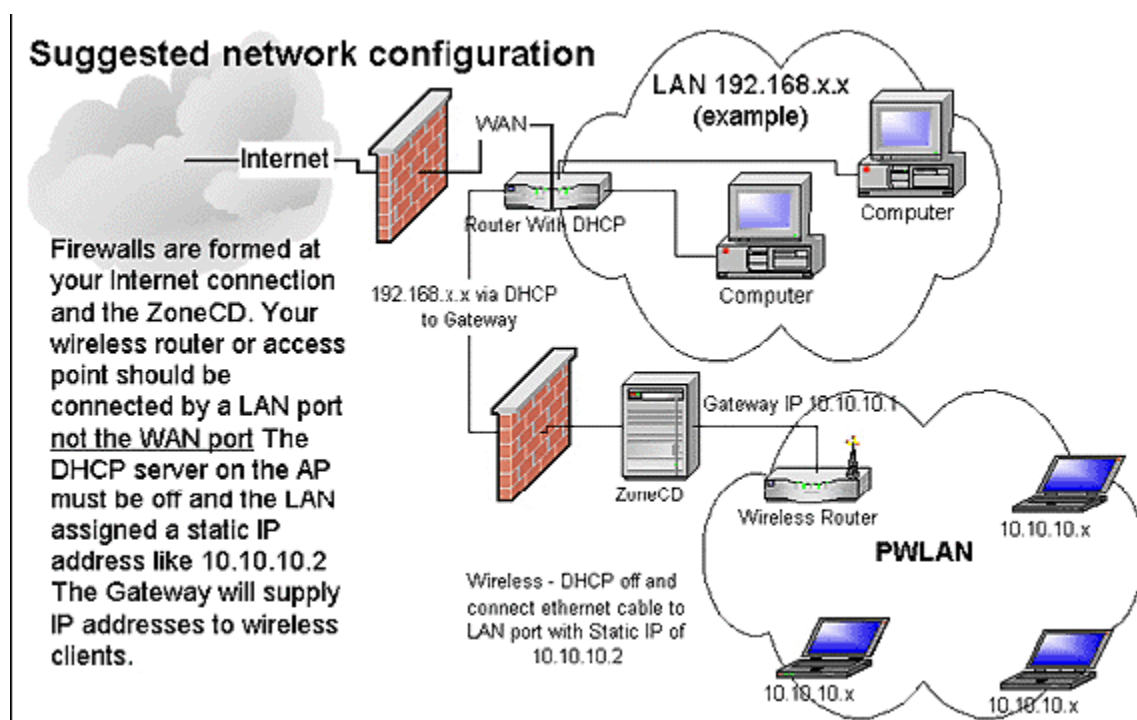
- **MorphixBase** utgör tillsammans med `isolinux` eller `boot.img` grundsystemet, som tillhandahåller en systemuppstart och laddar `lkm` (loadable kernel/linux modules) som motsvarar drivrutinerna i Windows, samt utför en hårdvarudetektering och ansluter (mountar) huvudmodulen (MainModule). Base är alltså den modul som används för att extrahera både MiniModules och MainModules.
- **MiniModules** är byggblocken som tillåter anpassning av egenskaperna för en specifik huvudmodul eller för alla huvudmodulerna som helhet. MiniModules ligger komprimerade i ISO9660-filsystemet.
- **MainModules** utformar CD:n för specifika uppgifter och skapar användarmiljöerna för en Morphix CD-skiva. Skaparen bestämmer själv vilka program som ska ingå i en MainModule på CD-skivan och vilken skrivbordsmiljö den ska användas för. En extraherad MainModule utgör ett karakteristiskt Linuxsystem, med katalogerna arrangerade i en typisk Debian-struktur. [5]

¹³ **GPL** En upphovsrättslicens för fri programvara.

3.1.1.4 ZoneCD, en Live-CD

Tjänsten Public IP tillhandahåller fungerar som hårdvaran mellan den trådlösa routern och Internetanslutningen. Hårdvaran är en PC med en ZoneCD. Minimumkraven för ZoneCD är en PC med:

- 386-kompatibel processor samt ett moderkort
- 128 MB RAM
- 2 Ethernet-nätverkskort
- En floppy eller ett flashminne
- CD-rom läsare
- Trådlös router med DHCP¹⁴ avstängd
- Trådburen Internetuppkoppling



Figur 5 Förslag på en hotspotkonfiguration

Figur 5 är en illustration av en nätverkskonfiguration för anslutning mot WLAN. I exemplet ses en anslutning för ett existerande LAN. Brandväggen mellan det lokala nätverket och

¹⁴ **DHCP** Ett nätverksprotokoll som tilldelar IP-adresser automatiskt till datorerna i ett LAN.

WLAN är ett förkonfigurerat Linux Iptables-system, som är den inbyggda brandväggen i ZoneCD.

ZoneCD kan självklart fungera med en direktanslutning till Internet, utan LAN. Men den låga kostnaden och funktionaliteten för dagens modem och routrar till LAN, gör det emellertid lönsamt och resurseffektivt att lägga till en router mellan ZoneCD och Internet. Dessutom blir det lättare att bygga på och expandera nätverket senare. [1]

3.1.2 Public IP's kontrollserver

Public IP erbjuder ett kostnadsfritt master-konto. En master är den mall, efter vilken ett företag lägger till en eller flera subnätverk (s.k. zoner) i sitt hotspotsystem. Konfigurationen av en master erbjuder full kontroll över nätverket och är vad Public IP's tjänst handlar om. När man väl skapat ett konto och bekräftat sin e-postadress kan man logga in och utforma sitt konto. Resterande inställningar görs i en guidad konfigurationsprocess på Public IP's webbsida, där varje inställning är förklarad i guiden.

Vid uppstarten skickar ZoneCD en begäran om inställningar till Public IP's kontrollserver. Funktionaliteten beror på vilken typ av ZoneCD-konfiguration man valt, det öppna eller det stängda läget. I det öppna läget behöver man redigera inställningarna med hjälp av en textredigerare och har inget behov av en kontrollserver. [1]

Lista över funktionaliteten:

Öppna läget:

- Omredigering till hemsidan.
- Självstiliserad välkomstsida.
- Innehållsfiltrering (vuxet innehåll, mp3, filmer mm.).
- Konfiguration av brandväggen.
- Danaguardians konfigurationsfiler sparas på ett flashminne eller på en floppydisk.

Stängda läget:

- Verifiering av användare samt registrering och inloggning.
- Omredigering till hemsidan.
- Bandbreddshantering.
- Tidsbegränsad Internetåtkomst per dag för olika användare.
- Nedladdningsbegränsningar per dag för olika användare.
- Öppnings- och stängningstid för hotspoten.
- Blockering av Mac-adresser.
- Uppdelning av användare i användarklasser.
- Konfiguration av brandväggen för varje användarklass.
- Inbyggd innehållsfiltrering.
- E-postsystem för att skicka loggar till administratören (fungerade inte under testet av systemet).
- Blockering av trafiken mellan olika användare.
- Självstilerad välkomstsida.
- Egna termer för användning och regler.
- Användningsstatistik.
- Stöd för olika språk på inloggningssidan (dock ej svenska).
- Användarrapportering och möjlighet till statistikexportering.
- Danaguardians konfigurationsfiler sparas på ett flashminne eller en floppydisk.

3.2 Webbutveckling

3.2.1 HTML

Den tjänst som först och främst förknippas med Internet är World Wide Web (www). Redan från sin tillblivelse har www använt sig av HTML (HyperText Markup Language), som är ett sidbeskrivningsspråk för att beskriva hur dokument på en webbsida ska se ut, såsom innehållet på en hemsida. Hemsidan kan innehålla dokument i form av bilder, text, ljud, animationer, formulär, länkar mm. HTML ska vara:

- Öppen, väl dokumenterad och offentlig.
- Fritt för alla att använda.
- Plattformsoberoende.

Under sin utvecklingsgång har HTML ändrats från ett strukturspråk till ett layoutpresentationsspråk¹⁵. Olika tillverkare av webbläsare har sin egen uppfattning om hur HTML ska representeras och webbsidor kan därför se olika ut beroende på vilken webbläsare man använder. På grund av detta har man försökt skapa en standard för HTML-kod, som döpts till XHTML. XHTML är HTML omdefinierad i form av en XML-applikation (se 3.2.2). XHTML kan kodas strikt (se figur 6) eller tillåtande. [24] Den strikta formen av XHTML tillåter inte överlappande HTML-taggar, uteslutna taggar eller webbramar. [8]



```
<!DOCTYPE HTML PUBLIC "-//W3C/DTD HTML 4.01//EN
"http://www.w3.org/TR/htm14/strict.dtd">
<html>
  <head>
    <title>Exempel</title>
  </head>
  <body>
    <p>Hello World</p>
    <br />
  </body>
</html>
```

Figur 6 Strikt kodad "Hello World" i HTML

¹⁵ **Layout** Den grafiska formgivningen med text och bild på en yta.

3.2.2 XML

Den officiella arbetsgruppen för XML beskriver sitt språk så här:

XML står för eXtensible Markup Language och är en delmängd av SGML. Målet med språket är att göra det möjligt att erbjuda, ta emot och bearbeta generisk SGML på Internet på samma sätt som det idag är möjligt att arbeta med HTML. XML har utformats så att det ska vara lätt att implementera och fungera ihop med både SGML och HTML.



```
!DOCTYPE exempel[
<!ELEMENT helloworld (author,text,reference)>
<!ELEMENT author (#PCDATA)>
<!ELEMENT text (#PCDATA)>
<!ELEMENT reference EMPTY>
<helloworld><author> Adnan Baktirovic </author>
<text>Hello World</text>
</helloworld>
]]>
```

Figur 7 Enkel "Hello World" i SGML

SGML (Standard Generalized Markup Language) är urmodern till alla markeringsspråk. Språket är utvecklat av IBM, främst som ett metaspråk som kan läsas både av datorer och av människor i plan text (se figur 7). XML består enbart av grundläggande syntax som används för att beskriva ett objekt (se figur 8). Varje element i en XML-fil kan vara egna fördefinierade element. XML-filer kan också behandlas av användaren på tre olika sätt:

- **Länkade stilmallar:** Precis som för HTML kan CSS användas för att bestämma hur data i en XML-fil ska representeras.

- **Databindningar:** Inbäddad XML-kod i en HTML-fil kan användas för att organisera och strukturera information, eller datamängder som t.ex. tabelldata.
- **XMLDOM-skript:** En teknik som konverterar en XML-fil till en dokumentobjektmodell, med hjälp av Java, JavaScript och PHP mm. Med DOM¹⁶-funktionerna kan man hämta, skapa, ändra eller radera elementen och attributen i ett objekt. [11]



```

<?xml version="1.0" encoding="UTF-8"?>
<xml>
  <webpage id="1" language="english">
    <date><![CDATA[13th November 2007 03:02:18 PM]]></date>
    <head><![CDATA[Hello World exemple]]></head>
    <text><![CDATA[Hello World]]> </text>
  </webpage>
</xml>

```

Figur 8 "Hello World" i XML

3.2.3 PHP

Ursprungsversionen av PHP skapades av Rasmus Lerdorf 1994 och är ett modernt skriptspråk som tolkas på serversidan. Vanliga programmeringsspråk kompileras till maskinkod först innan de körs, men ett skriptspråk tolkas direkt vid körning. [9] All källkod till PHP är också öppen och distribueras fritt på Internet till alla privatpersoner och företag, att ladda ner och använda. I och med den öppna källkoden har webbutvecklarna i sin tur sluppit oroa sig för diverse licenser, vilket medfört att PHP-tekniken blivit väldigt populär. [9,10]

¹⁶ **DOM** *Document Object Model* är ett plattform- och språkoberoende gränssnitt för åtkomst och dynamisk uppdatering av ett dokument innehåll, struktur och formatering.

Framgången för PHP beror också mycket på att språket har stöd för flertalet vanliga program och programmeringsbibliotek. Det är exempelvis väldigt enkelt att koppla upp databaser till PHP och sedan kommunicera med dessa, genom olika funktioner som finns inbyggda i språket. Det krävs heller ingen speciell kunskap för att använda funktionerna, eftersom de är så skickligt utformade. [9] Enkelheten i denna användning framgår av exemplet i figur 9. Med lanseringen av version 5.0 av PHP kom ytterligare funktioner för bland annat hantering av XML-filer, så kallade DOM-dokument.



```
k?php
$a = "Hello";
$a .= " ";
$a .= "World";

echo $a;

?>
```

Figur 9 "Hello World" i PHP

3.2.4 JavaScript

JavaScript är ett objektorienterat skriptspråk utvecklat av Netscape och används mest i HTML-dokument för att öka en webbsidas dynamik (se figur 10). Skriptspråket påminner också ganska mycket om Sun Microsystems programspråk Java, som förutom namnet har en liknande syntax och struktur, men där slutar likheterna. Java används främst till självständiga Java-applikationer och HTML-inbäddad JavaApplets. Koden måste också först kompileras om till maskinberoende bytekod, som därefter exekveras av Java Virtuall Machine © på datorn som programmet körs.

JavaScript-koden som bäddas in i ett HTML-dokument, är helt synlig för de användare som laddar ner dokumentet. Skriptet implementeras också samtidigt som sidan laddas. HTML-koden som JavaScript laddas ner med, tolkas av JavaScript som ett DOM-dokument med HTML-taggar som element. Med JavaScript kan man ändra innehållet på en HTML-sida, kontrollera ifyllda fält i ett formulär och öppna nya fönster mm. [8]



```
<HTML>
<HEAD><TITLE>Hello World With JavaScript</TITLE> </HEAD>
<BODY>
  <FORM Name="Form1" ACTION="">
    <INPUT TYPE=BUTTON VALUE="Click me" NAME="BtnHello"
      OnClick="Hello()">
  </FORM>
  <SCRIPT LANGUAGE="JavaScript">
  <!-- function Hello (){
      alert("Hello World!")
    }
  //--> <SCRIPT>
</BODY>
</HTML>
```

Figur 10 "Hello World"-popup med JavaScript

3.2.5 Flex2 och ActionScript 3.0

Under sitt projekts utveckling har Adobe¹⁷ Labs släppt en gratisversion av Adobe Flex2 SDK, ett ramverk för Rich Internet Applications (RIA). Med Flex2 SDK, som bygger på Adobe Flash, kan snygga och skalbara tillämpningar skapas på de flesta plattformar. Flex2 SDK består av ett antal olika delar:

- ActionScript 3.0 (en variant av JavaScript).
- MXML, markeringsspråk som beskriver ett gränssnitt (en XML dialekt, se figur 8)

¹⁷ Adobe <http://adobe.com/> Ett företag beläget i San Jose, Kalifornien USA, som utvecklar programvara för grafik (ritprogram, bildbehandlingsprogram mm.) samt sidbeskrivningsspråken PostScript och PDF.

- Ett komponentbibliotek
- Dokumentation
- IDE (Flex Builder, baserad på Eclipse)
- Flex Dataservices Server
- Kompilator
- Diagramkomponent

Flex2-applikationerna placeras ut som kompilerad bytekod, som är exekverbar av Flashspelaren. Flashspelaren är installerad på över 97 % av alla Internetanslutna PC-datorer och utgör en konsekvent miljö för alla webbläsare, såsom IE, Opera och FireFox, på olika operativsystem. Flashspelaren har också en unik kombination av funktioner som utvecklaren i sina applikationer kan använda sig av, bland annat tolkning av olika markeringspråk (XML, MXML m.fl.), kraftfull grafisk API, en animationsmotor, samt en integrerad ljud- och videodekoder.

Klientdelen av Flex2-applikationerna är distribuerad som binära filer. Utvecklaren placerar ut filerna på webbservern på samma sätt som med vanliga HTML-filer. När filerna efterfrågas av webbläsaren, laddas dessa ner och bytekoden exekveras av Flashspelaren. Under exekveringstiden kan applikationen sedan begära externa resurser eller data genom nätverket, med vanliga http-anrop eller genom webbtjänster som SOAP. Flexklienten som är oberoende av de skriptspråk som används på servern för kommunikation, kan kombinera tjänster med olika skriptspråk, såsom PHP, ASP och JavaScript m.fl.

Precis som HTML är MXML ett markeringspråk, som beskriver layouten, kontexten och funktionaliteten. Skillnaden är att MXML är en deklarerbar abstraktion för klientlogiken och för bindningar mellan användaren, klienten och dess innehåll. [12]



Figur 11 "Hello World" som Flash-animation med MXML och ActionScript

3.2.6 CSS

CSS (Cascading Style Sheets) är ett webbdesignspråk, som beskriver presentationsstilen för ett DOM-dokument, såsom typsnitt, textstorlek och färg mm. Språket används oftast för att snygga till en HTML-sida. En referenslänk till CSS bäddas in i HTML-dokumentet, och vid nerladdningen av webbsidan hämtas både HTML-sidan och den tillhörande stilmallen.

3.3 Serverapplikationer

Den svenska benämningen för server är värddator. Egentligen är servern, om man ser till funktionen, att betrakta som mjukvara och inte hårdvara. En server kan, som namnet anger, "serva" med olika uppgifter. I datasammanhang är servern det system som betjänar andra system, s.k. klienter, oftast över ett större nätverk. Filservern, webbservern, databasservern, e-

postservrar av olika slag och DNS¹⁸, är några av de vanliga tjänster på Internet som behöver en värddator.

3.3.1 Apache

Apache är en fri webbserver, som just nu är uppe i version 2.2. Den är världens populäraste webbserver och används enligt Netcraft¹⁹ i 40 miljoner domäner på Internet. Inställningarna för Apache skiljer sig beroende på versionen man använder och vilket system webbservern installeras på. För att hantera externa objekt och bibliotek använder sig Apache av s.k. moduler.

För Apache finns ett namnbaserat virtuellt värdsystem och ett IP-baserat värdsystem. Det namnbaserade virtuella värdsystemet tillåter att en enda server är värd för flera domäner. Faktum är att användarna inte märker av att de är på samma fysiska server. Konfigurationen tillåter också användning av flera alias för samma virtuella server. Intranät- och Internetanvändare kommer alltså åt samma webbsida från olika IP-adresser och fysiska vägar, men innehållet på webbsidan blir det samma. [6] Det IP-baserade virtuella värdsystemet tillåter istället att servern använder olika IP-adresser för varje virtuell domän, till skillnad från det namnbaserade virtuella värdsystemet, som ger multipla virtuella domäner för samma IP-adress. [6]

3.3.2 MySQL

MySQL är ett SQL²⁰-databashanteringssystem (SQL är ett frågespråk), som sponsras och utvecklades av det svenska bolaget MySQL AB²¹ i Uppsala. Systemet används idag på fler än fyra miljoner webbsidor och är därmed den populäraste databashanteraren i hela världen. [29]

En databas är en strukturerad mängd data som *modellerar en del av världen* och som är persistent, dvs. som inte försvinner när man avslutar programmet eller stänger av datorn. Varje databas används för att lagra data och databasstrukturen är definierad med hjälp av tabeller och relationer mellan dessa tabeller. [29]

¹⁸ **DNS** *Domain Name System* är det system på Internet som översätter domännamn (t.ex. susning.nu) till IP-adresser (t.ex. 193.15.191.196).

¹⁹ <http://news.netcraft.com/>

²⁰ **SQL** *Structured Query Language* är ett språk som används för att skapa, modifiera och manipulera data samt hämta information från databaser.

²¹ <http://www.mysql.com>

Inom datasammanhang skiljer man på betydelsen av data och information. Med information avser man innebörden i data, som förutsätter en mottagare med förmågan att tolka och bearbeta data. Exempelvis är talet ”23” som sådant, bara är en typografisk representation, och ett exempel på data. Information, dvs. innebörd och innehåll, får vi först om vi förslagsvis vet att det är den 23:dje dagen i månaden idag och att lönen kommer snart. Data är alltså en representation medan information är dess mening.

3.3.3 DDClient

DDclient är en Perl-baserad klient som uppdaterar dynamiska DNS-adresser, för användare av gratis DNS-nätverktjänster, bland annat DynDNS²². Klienten kan även hämta en WAN-IP-adress på ett antal olika sätt. Då DDclient också är en *daemon* behöver den inte heller några speciella inställningar, utan bara sina konfigurationsfiler. [7]

3.4 PayPal

PayPal är ett företag med ett internationellt system för onlinebetalningar och har omkring 20 miljoner anslutna kunder. Som registrerad kund och med ett anslutet kreditkort till systemet, kan man skicka eller ta emot pengar från andra anslutna privatpersoner och företag. Som kund betalar man heller inget extra för att använda de olika tjänsterna och den höga säkerheten PayPal erbjuder. [13]

Från att ha varit ett företag som främst förmedlat betalningar mellan köpare och säljare på auktionssajten eBay, växte PayPal upp till ett standardiserat och säkert pengatransaktionssystem på Internet. År 2002 köpte eBay upp PayPal för 1,5 miljarder dollar och under sin expansion har man skapat flera alternativa sätt för säker betalning över Internet. [14]

²² <https://www.dyndns.com>

3.4.1 Betallänkar

Betallänkar (eng. Buy now button) är PayPal's äldsta teknik, som skapades för eBay's auktioner och används än idag på grund av sin enkelhet. Allt en säljare behöver göra för att börja ta betalt av sina kunder för de varor han erbjuder på sin hemsida, är att applicera PayPal's betallänkar. När kunden klickar på betallänken skickas hon till PayPal. Härifrån kan kunden logga in på sitt existerande PayPal-konto eller skapa ett nytt, ifall hon inte redan har ett. Därefter kan pengarna och ett meddelande skickas till säljaren. Men i ett ickeautomatiserat system måste säljaren bekräfta pengatransaktionen, för att ta emot pengarna. [13,14]

3.4.2 Instant Payment Notification (IPN)

Om ett företag vill få lite större kontroll och automatisering av betalningstjänsten som PayPal erbjuder, kan de använda sig av IPN-tjänsten. För IPN krävs en skriptspråk-algoritm på företagets server, för att kunna ta emot meddelanden från PayPal efter att en transaktion genomförts, och för att kunna svara med en http-begäran. För att använda IPN-tjänsten krävs också ett företagskonto på PayPal, med bekräftad e-postadress och bekräftat betalkort.

Notifikationstiden för en transaktion är oftast 10 sekunder, men kan ibland dröja ett par minuter. Med transaktionen får företaget de uppgifter kunden har skickat med sin beställning från betallänken, samt en säkerhetskod, överföringsstatusen och en eventuell orsak till transaktionens fördröjning, om sådan förekommer. Företaget kan sedan använda koden och uppgifterna, för att validera transaktionen asynkront (utan kundens ingripande) mot PayPal. [14]

3.4.3 Payment Data Transfer (PDT)

En annan av de klassiska PayPal-tjänsterna, där ett skriptspråk är användbart, är PDT-tjänsten. Efter att kunden beställt sina varor eller tjänster länkas hon till PayPal. De data som sedan skickas av kunden genom betallänken, är av samma slag som för IPN-tjänsten, men det finns vissa skillnader mellan de båda tjänsterna.

PDT:

1. Kräver att automatisk länkning till företagets hemsida är påslagen.
2. Efter att kunden genomfört sin pengatransaktion på PayPal, skickas PDT-data som en GET-förfrågan till företaget.
3. Företagets server tar sedan emot dessa data och svara med metoden POST, som innehåller inkommen PDT-data med transaktionsidentifikation och värden, verifierad i en `cmd=notify-synch`.
4. PayPal skickar därefter en bekräftelse med antingen SUCCESS (lyckad transaktion) eller FAIL (icke lyckad transaktion) på denna transaktionsidentifikation.

IPN:

1. Kräver ingen automatisk länkning.
2. När kunden är klar med sin pengatransaktion på PayPal, skickas IPN-data med metoden POST asynkront från PayPal.
3. Företagets server tar sedan emot dessa data och svarar med metoden POST, som innehåller inkommen IPN-data med transaktionsidentifikation och värden, verifierad i en `cmd=notify-synch`.
4. PayPal skickar därefter en bekräftelse med antingen VERIFIED (giltig data) eller INVALID (ogiltig data) på denna transaktionsidentifikation.

3.4.4 SOAP-webbtjänster (APIs)

SOAP är ett XML-baserat protokoll som används för utbyte av information i decentraliserade och distribuerade miljöer. År 2004 levererade PayPal ett par kärnfunktioner till systemutvecklare, med lanseringen av den första SOAP-webbtjänsten. Genom denna SOAP-webbtjänst kan en mängd extra funktioner läggas till på en webbsida (se figur 12). Som de flesta webbtjänster fungerar PayPal's SOAP API i ett begära/svara -format på en SSL-anslutning. [14]

Webbtjänst	Beskrivning
TransactionSearch	Sök efter en transaktion
GetTransactionDetails	Detaljerad info om en transaktion
RefundTransaction	Begär återbetalning
MassPay	Betala till flera samtidigt
DoDirectPayment	Behandla en kortbetalning direkt
DoAuthorization	Tillåt en kreditkortsbetalning
DoReauthorization	Tillåt igen kreditkortsbetalning
DoCapture	Info om tidigare tillåtna kreditkort
DoVoid	Töm tidigare tillåtna transaktioner
SetExpressCheckout	Skapa Express-Checkout-transaktioner
GetExpressCheckoutDetails	Info om en Express-Checkout-transaktion
DoExpressCheckoutPayment	Färdigställ en Express-Checkout-transaktion

Figur 12 PayPal's SOAP-tjänster

3.4.5 Express Checkout."PayPal-plånbok"

Express Checkout är en API-baserad betaltjänst, som tillåter större kontroll över företagets betalningsprocess. När kunden vill betala för sina varor eller tjänster på företagets webbsida, omdirigeras hon först till PayPal, genom att klicka på en länknapp. Härifrån kan hon sedan logga in på sitt PayPal-konto. Efter lyckad inloggning, omdirigeras hon tillbaka genom en annan länknapp till företagets betalningssida, där den egentliga pengatransaktionen sker. Genom denna länknapp skickas bl.a. kundens adressuppgifter och PayPal-kontonummer till företaget. PayPal kallar processen för "hämtning av Internet-plånbok". Transaktionen går snabbt och kunden kan med denna enkla treknappsklickprocess betala för varan. [14]

3.5 Säkerheten

3.5.1 Iptables

I samband med utsläppet av Linux-kärnan 2.4 introducerades Iptables för att kontrollera brandväggsfunktionerna. Iptables är numera en standardkomponent av kärnan i de flesta Linux-distributioner och hanteras som en kärnmodul. När ett nät-paket anländer till nätverkskortet behandlas det på olika sätt, beroende på destinationsport och adress. En rad av brandvägsregler som är av samma typ kallas för en kedja (chain) och de behandlas i tur och ordning som länkarna i en kedja. Som en grundregel för Iptables finns det tre typer av kedjor. [2]

- INPUT: Inkommande paket till systemet berörs av de regler som är satta här. Inputkedjan har regler för den destinationsadress som finns i de inkommande paketen. Får paketen inte access, kommer de heller inte att upptäckas av processerna i systemet.
- OUTPUT: En kedja av regler som bestämmer vilka paket som får lämna systemet.
- FORWARD: Reglerna för den här kedjan berör transiterade paket, som har skickats från ett nätverksgränssnitt till ett annat. Reglerna används till nätverksöversättning av de olika systemen i ett nätverk, som försöker komma åt ett annat nätverk.

Exempel på Iptables:

```
iptables -I OUTPUT -p tcp -d 10.10.10.0/24 -s 10.10.10.1 -j  
ACCEPT Program -I (kedja) -p (protokoll) -d (destinationsadress)  
-s (källadress) -j (regel)
```

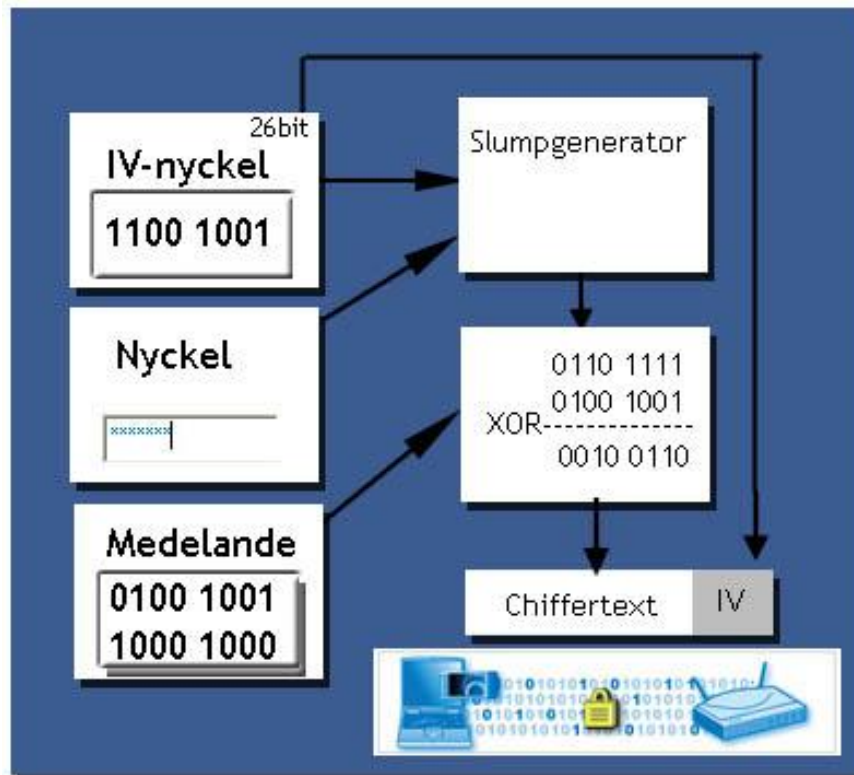
3.5.2 WEP

Wired Equivalent Privacy (WEP) var tänkt främst som ett skydd för det trådburna nätverket. Konceptet skulle skydda mot obehörigt tillträde och avlyssningar. WEP implementerades senare i IEEE 802.11-standarden. [19]

För att skydda data använder sig WEP av en krypteringsnyckel som ligger utanför protokollet. Nyckeln anges av nätverksadministratören och tilldelas behöriga användare. Krypteringsnyckeln har även en viss livslängd och måste bytas ut efter ett tag. [19] WEP's trådlösa sessioner kan konfigureras på flera sätt:

- Ingen kryptering
- 40-bit-kryptering
- 64-bit-kryptering
- 128-bit-kryptering

I en 64-bit-kryptering används en 40-bitars-nyckel, som sammanfogas med en 24-bitars initieringsvektor för att skapa en RC4-trafiknyckel. RC4 (Rivest Cipher 4) är en dataströmskryptering som använder samma nyckel för kryptering och dekryptering. En vanlig textsträng som krypteras kommer alltid att ha samma värde. Därför tillämpar WEP en teknik, som producerar en unik nyckel för varje skickat paket med hjälp av en initieringsvektor (IV). Initieringsvektorn består av en 3 byte lång sträng som förnyas för varje paket och producerar ett unikt krypterat datapaket (se figur 13). Man behöver inte heller begränsa sig till en WEP-krypteringsnyckel, med fördel kan man använda flera nycklar samtidigt för att få en bättre säkerhet. [18]



Figur 13 Enkel WEP-kryptering

3.5.3 WPA

På grund av den bristande säkerheten i WEP-tekniken skapades ett nytt säkerhetsprotokoll, som kallas IEEE 802.11i. Protokollet använder sig av en autentiseringsteknik med ett starkt krypteringsschema, som tilldelar de nycklar som byts ut över tiden under varje datatransaktion.

Inloggningen till ett trådlöst WPA-nätverk sker genom autentisering mot en accesspunkt. Accesspunkten agerar som en mellanhandsserver som tar emot användarens inloggningsuppgifter, packar om dem och skickar dem vidare till en autentiseringsserver. Om uppgifterna med ett korrekt givet lösenord stämmer, får accesspunkten instruktioner att ge användaren tillträde till den skyddade nätverksinfrastrukturen. Efter lyckad autentisering upphör accesspunkten med att ompaketera paketen från användaren. Istället genereras en temporär och hemlig nyckel för sessionen genom en överenskommelse mellan autentiseringsservern och användaren. [19]

3.5.3.1 PSK och TKIP

PSK (PreShared Key) är som namnet antyder en nyckel som är utdelad på förhand. Nätverksadministratören matar in nyckeln manuellt i en accesspunkt och tilldelar därefter nyckeln till behöriga klienter i nätverket. PSK fungerar efter samma princip som WEP, men använder till skillnad från WEP istället en nyckel som består av minst åtta tecken. Nyckeln är bara avsedd för autentiseringen och vid lyckad inloggning startar en WPA-session med TKIP.

TKIP (Temporal Key Integrity Protocol) är ett protokoll som erbjuder sammanfogning av temporära sessionsnycklar, men har även längre initieringsvektorer än WEP-protokollet. TKIP inkluderar också en integritetskontroll, som förhindrar att data som skickats ändras under den trådlösa dataöverföringen. [19] De temporära nycklar som sammanfogas och används i TKIP, skapar 500 triljoner möjliga värden för en sessionsnyckel. Både data och initieringsvektorer krypteras innan de sänds iväg och tekniken i TKIP förhindrar också att samma nyckel slumpas fram två gånger, under en och samma session. [20]

3.5.4 WPA2

WPA användes som en temporär lösning för att täppa till de säkerhetsluckor som fanns i WEP, innan slutversionen av IEEE 802.11i släpptes. I efterföljaren WPA2 ersatte man TKIP med en teknik kallad AES (Advanced Encryption Standard). AES är ett symmetriskt blockkrypto skapat för att hantera krypteringsnycklar med längderna 128, 192 och 256 bit. Varje paket som krypteras genomgår ett antal krypteringsiterationer, med substitution och permutation av bitar i paketet. Antalet iterationer beror på krypteringsnyckelns längd. Denna avancerade krypteringsteknik är fortfarande obrytbar och bara tiden kan utvisa om den kommer att hålla i framtiden också. [20]

3.5.5 VPN

VPN (Virtual Private Network) är definierad som en temporär fysisk väg eller tunnel, som skapas över ett strukturerat och publikt nätverk. VPN-standarden är inte definierad för att användas över något speciellt OSI-modellager och den har inga speciella säkerhetskrav. [24]

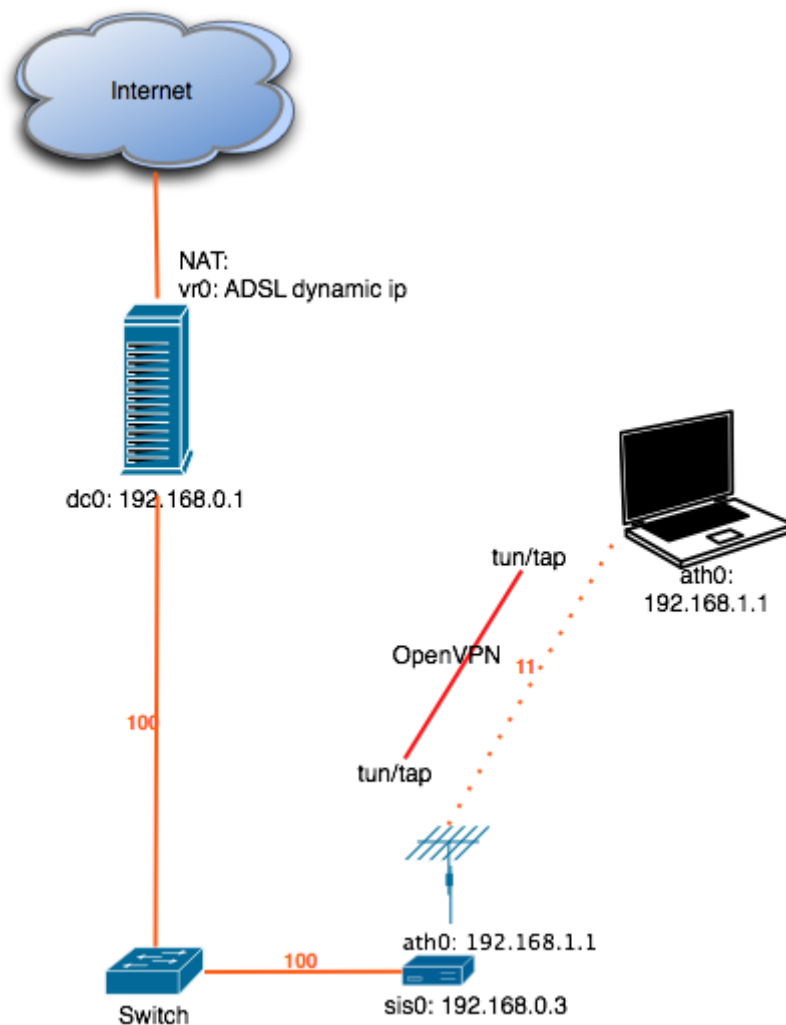
Men de flesta implementeringarna av VPN använder sig av nätverkslagret eller datalänkslagret. [25]

För det trådlösa nätverket som tillämpar IEEE 802.x delas OSI-modellagret upp i två extra undergrupper, nämligen MAC (Media Access Control) och LLC (Logical Link Control). [27] LLC används dels för att ompaketera data som ska sändas, dels för att lägga till destinationsadressen samt källadressen till paketet, och för hantering av flödeskontrollen. [26] Man kan också kategorisera VPN efter tjänsten den utför. Tjänsten kan vara en fjärråtkomst eller plats-till-plats VPN. Fjärråtkomsten kan erbjuda en en-till-en förbindelse men även en en-till-många förbindelse. Plats-till-plats VPN används istället då man vill förbinda många med många. IKEA i Kiruna och IKEA i Malmö kan exempelvis skapa en sådan VPN för sina dataavdelningar. [25]

Man kan implementera VPN antingen genom hårdvaran eller mjukvaran. En av de mest kända VPN mjukvarulösningarna för Internet är SSL (kapitel 3.8.6). Dagens accesspunkter som använder sig av hårdvarulösningar för VPN har blivit allt billigare och lättare att installera och konfigurera. Men själva installationen av ett VPN-nätverk garanterar ingen säkerhet, utan förståelse för konfigurationen som anpassar systemet.

3.5.5.1 OpenVPN

De flesta regler som sätts för en VPN anges av tillverkaren och de programmerare som har skapat mjukvaran. Ett exempel är en gratis paketslösning för VPN, som heter OpenVPN. OpenVPN är kompatibel med de vanligaste operativsystemen och kostar ingenting. Den använder sig av en enda port för nätverkskommunikation, antingen TCP eller UDP. I figur 14 ges en tänkbar OpenVPN-konfiguration över datalänkslagret. Istället för att skicka datapaketet direkt genom nätverkskortet (i Linux heter detta oftast `/dev/eth0`), så skapar OpenVPN en extra enhet som heter `/dev/tap` och som används som en tunnelgenväg för kommunikationen. [27]



Figur 14 Ett OpenVPN-nätverk

3.5.6 SSL

SSL (Secure Socket Layer) skyddar webbttrafikdata genom att kryptera innehållet i de datapaket som överförs. Varje domän kräver ett eget SSL-certifikat som innehåller en publik och en privat nyckel. Den publika nyckeln används för att kryptera informationen som sänds iväg och den privata nyckeln dekrypterar sedan denna information hos mottagaren. När en webbläsare söker tillträde till en webbsida som finns på en SSL-autentiserad domän, inleds en handskakningsprocess mellan servern och klienten. Klienten måste här ta emot en unik sessionsnyckel innan den får tillträde till webbfiler. [15]

4 Beskrivning av konstruktionslösning

Att anordna en hotspot är ett omfattande projekt som kräver hårdvaruimplementering, ett användargränssnitt för kunder, verktyg för kundadministration och serveradministration, samt sammankoppling av de olika elementen. För att ge en bättre översikt har följande kapitel delats in i fyra delar. I första delen, kapitel 4.1, beskrivs i korthet konfigurationen av Public IP's kontrollserver. Här redogörs kort för de funktionalitetsinställningar som nämndes i kapitel 3.1.2. Andra delen av kapitlet, ZoneCD-konfiguration, är en alternativ lösning för en hotspot som saknar webbsida och utrymme på ett Internetwebbhotell. Denna del innehåller också en tänkbar lösning för MySQL och Apache. I tredje delkapitlet, kapitel 4.3, förs en diskussion om för- och nackdelar med de verktyg och språk som användes för att skapa webbsidorna. I slutet av kapitlet beskrivs den trådlösa säkerheten som valdes för projektet (valet är överraskande).

4.1 Public IP's kontrollserverinställningar

Public IP's kontrollserver är nödvändig då NoCat som finns på ZoneCD är gjord av Public IP's programmerare. Inställningarna för NoCat är bundna till de SOAP-tjänster som finns på CD:n. Dessa SOAP-tjänster hämtar regelbundet nya inställningar från kontrollservern och skriver över grundinställningarna för NoCat. Public IP's NoCat är inte förklarad eller dokumenterad och Public IP erbjuder också ett antal funktioner som inte finns med i originalet av NoCat-programmet.

Zontypen som valdes på Public IP's kontrollserver är en privatzon (eng. private zone). Anledningen till att använda den här typen av zon är främst säkerheten. En privatzon tillåter inte inloggning av användare som samtidigt är inloggade eller registrerade på en annan zon, vilket är fallet för andra zontyper. Dessutom finns det heller inga tidsbegränsade användare för andra typer av zoner. Detta kan medföra en potentiell fara, om exempelvis kontrollservern hos Public IP inte kan nå den egna inloggningssidan. Då kommer en standardinloggningsruta att visas för kunderna och utan tidsbegränsningar kan dessa användare logga in utan att betala.

4.2 ZoneCD-konfiguration

Efter att ha fått en viss vägledning av företaget och efter att själv ha testat ett flertal olika lösningar för en ZoneCD-konfiguration, blev överenskommelsen att spara företagets hemsida på ZoneCD och användaruppgifterna på en databas med hjälp av Apache och MySQL. Versionen av ZoneCD som företaget redan använde till sitt trådlösa nätverk behålldes. Ägare av ett hotspotsystem har möjligheten att själv välja, om de vill ha sin webbsida och MySQL på ett flashminne eller på ett Internetwebbhotell, genom att ändra inställningarna för uppstartskriptet `init.sh`.

Funktioner på ZoneCD som företaget valde att ta bort:

- **Floppy:** Det är svårt att hitta en bra anledning till att ha en floppy som lagringsmedia, då denna lagringsform idag är föråldrad. I undersökningen av Public IP's forummedlemmar framkom också att, flertalet användare haft problem med att skriva till och läsa från sin floppydisk, efter ett antal omstarter av systemet.
- **Open mode:** Om ZoneCD-konfigurationen inte kan hämtas från Internet, kommer ZoneCD att startas om automatiskt tills dess att Public IP är nåbara igen.

Funktioner som företaget valde att lägga till:

- Möjligheten att ha en http-server med SSL på CD:n
- En databas i form av MySQL på CD:n
- PHP5-stöd (nya funktioner för att bearbeta XML finns i PHP5)
- DynDNS-uppdateringssupport för en FQDN²³
- Fjärråtkomst för serveradministratörer

4.3 Apache, MySQL och PHP (LAMP)

LAMP-lösningen är en självklarhet när man talar om webbaserade autentiseringstjänster. Det som talar för LAMP är att det är lätt att installera från APT, lätt att konfigurera och att programmen är gratis. PHP5 är den PHP-version som valdes till systemet.

²³ **FQDN** *Fully Qualified Domain Name* är en DNS-term som beskriver en värd och sökvägen till denna. Ex: www.google.com

Apache implementerades från ZoneCD som en namnbaserad server. Administratören kan själv välja om han vill använda denna server. Servern kommer enbart att fungera med SSL-protokollet.

MySQL kommunicerar med två databaser som lagrar information för de användare som använder hotspoten och innehåller de autentiseringsprotokoll, som tillåter administratörer att logga in. Första databasen, `users`, innehåller två tabeller. Den ena, tabellen `users`, innehåller Public IP's variabler för registrerade användare och behövs för korrekt inloggning, samt för att bokföra den betalda tiden som en användare beställer. Den andra tabellen, `paypal_data`, innehåller användarens transaktionsdata för PayPal. En relationsnyckel²⁰ som finns mellan tabellerna `users` och `paypal_data`, kopplar ihop informationen som är listad för en specifik användare. Relationsnyckeln förbinder kolumnen `ID` i tabellen `users` med `custom` i tabellen `paypal_data`.

4.4 Webbdesign

4.4.1 Företagets webbsida

Flash valdes som designspråk till företagets webbsida. Säkerheten i Flash är dock bristfällig, eftersom det går att dekompilera de binära Flash-filerna till källkod och därmed få fram den skyddade informationen.

Men Flash ger en dynamisk webbsida och användes för att skapa en snygg layout, samt för att läsa de konfigurationsfiler som visas för användarna. All dynamik som PHP, ASP och Java klarar av, klarar också Flash av genom ett par extra finesser. En Flashsida ser också lika dan ut med olika webbläsare, såsom Opera, IE, Fire Fox mm.

CSS ersattes av XML-konfigurationsfiler. I och med att PHP bearbetar XML-filer så snabbt kan man ändra elementen på sidan, såsom bakgrund, text mm. Detta ger administratören ett större antal konfigurationsmöjligheter.

4.4.2 Administratörens kontrollpanel

En Flash-inloggningswebbsida med understöd av PHP skapades för administratören. Den validering av inloggningsuppgifter som görs av administratören omfattar kommunikation mellan Flash och ett PHP-skript, som validerar uppgifterna mot en MySQL-databas. Varje ändringsanrop av exempelvis XML-filer kräver administratörens namn och lösenord. Bearbetning och validering av data som skickas från kontrollpanelen implementerades med ett PHP-skript.

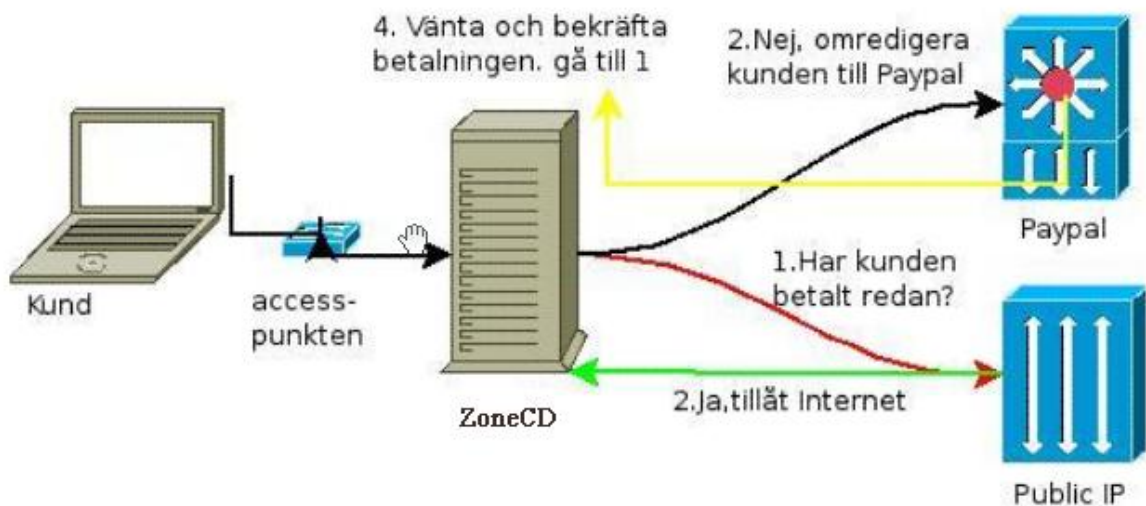
Bearbetningen sker i form av:

- Funktioner mot Cross-site-scripting.
- Funktioner mot MySQL-injektion.

Dessutom innehåller PHP-skriptet funktioner för:

- Bakgrundsredigering, redigering av företagsnamn, användaröversikt och en nyhetspanel.

4.4.3 Användarnas webbsidor



Figur 15 Autentiseringsprocess för en kund

Användarnas inloggningswebbsida skapades i PHP. Sidan hämtar data som skickas från Public IP-kontrollservern (Mac-adressen, token, timeout) och lagrar informationen i företagets databas efter inloggningsvalideringen. För de användare som inte redan har ett

konto finns ett registreringsformulär. All inkommande data säkerhetskontrolleras också och behandlas av samma typ av säkerhetsrutiner som hanterar administratörens inloggningsdata.

Dubbla användarnamn tillåts inte i databasen. Användarnamnet måste också vara av e-posttyp, eftersom databasen hos Public IP bara godtar en typ av användarnamn. Efter att användaren har loggat in får hon en länk till PayPal där hon kan betala för tjänsten. När tjänsten är betald, valideras kontouppgifter och betalningsuppgifter mot PayPal av företagets server (se figur 15). Stämmer uppgifterna får användaren automatiskt tillträde till Internet. All trafik som IPN och Public IP genererar göms för användaren och skickas genom ett PHP-skript.

4.5 Den trådlösa säkerheten

Eftersom kunden ansluts till det trådlösa nätverket och PayPal för att betala för tjänsten, behöver inte WPA eller nyckelskyddat WEP tillämpas. Nätverket är öppet, men kan skyddas genom VPN i hårdvaran. Webbtrafiken från webbservern, som sköter inloggningen, autentiseringen och betalningen mot PayPal, krypteras med SSL.

5 Användargränssnitt

Följande kapitel kommer att beskriva företagets webbsida, administratörens webbsida, samt användarens inloggningssida och registreringssida. Inledningsvis tas den implementerade funktionaliteten upp och designbeskrivningen av företagets webbsida. I kapitel 5.2 beskrivs sedan administratörens inloggningsprocess och den kontrollpanel med vars hjälp han kan förändra innehållet på företagets webbsida. Avslutningsvis, i kapitel 5.3, beskrivs layouten som användaren möter vid uppkoppling mot hotspotsystemet.

5.1 Företagets webbsida



Figur 16 Företagets webbsida

Då Fiber Optic Valley ville ha samma CSS på sin webbsida som de hade på huvudsidan, valdes samma bakgrundsfärger men med lite modernare stil. Målet har varit att kunden ska mötas av en professionellt designad webbsida vid inloggningen.

Figur 16 visar företagets webbsida som är sammanställd av tre paneler. Den övre panelen är en språkpanel, där man har möjlighet att växla språket på sidan från engelska till svenska. Den andra panelen är själva huvudpanelen, där kunden kan få information om företaget, få hjälp och beställa tjänster. Panelen längst ner på webbsidan innehåller företagets namn, faxnummer, E-post och besöksadress.

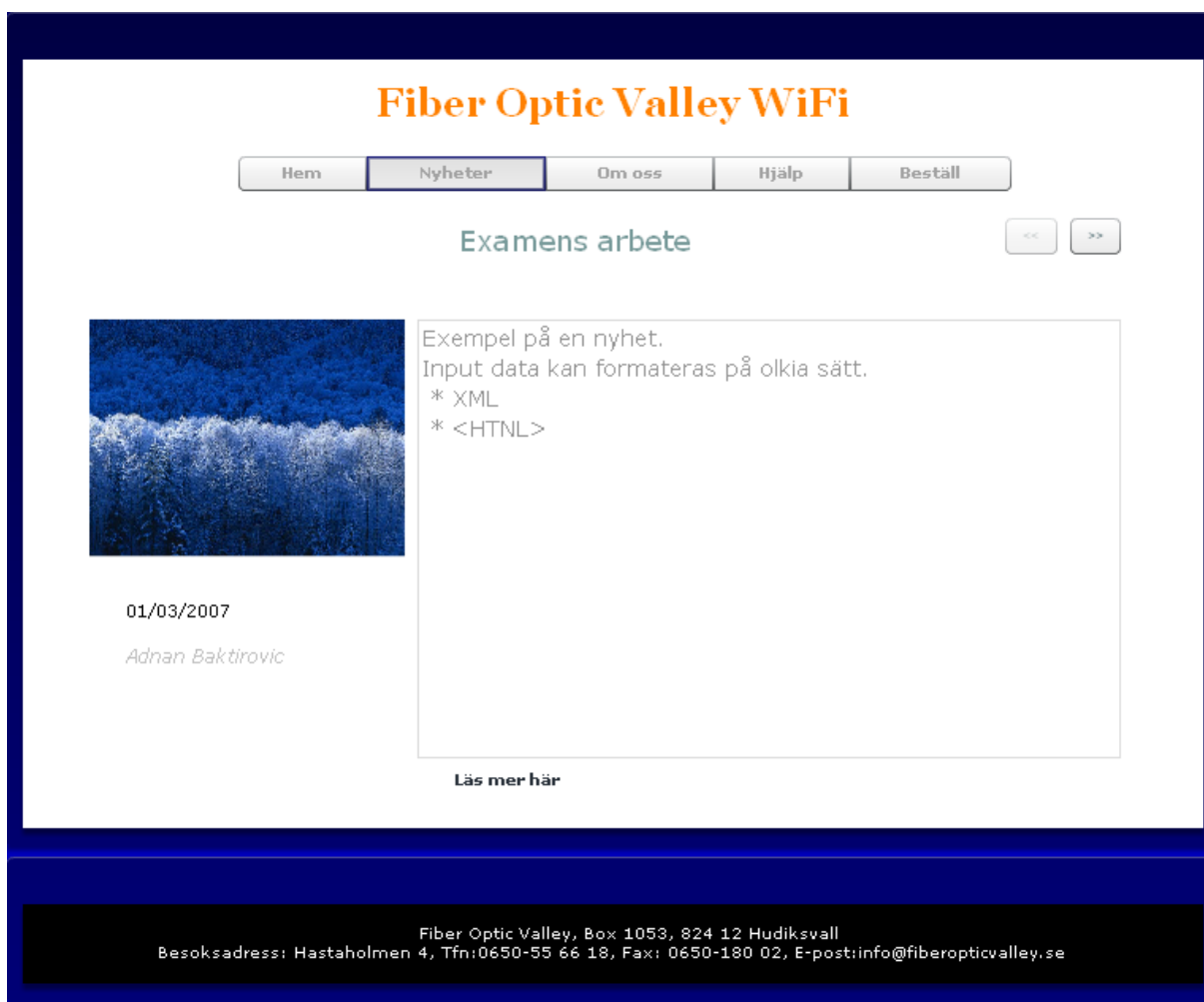
När kunden besöker företagets webbsida kan hon navigera med hjälp av menyn på huvudpanelen. På Flash-sidor som denna använder man sig inte av hemsidor som länkar, utan istället av tillstånd som förändrar sidans innehåll. Följande vanligt förekommande knappar och tillstånd finner man på företagets webbsida:

- **Hem/Home:** Tillståndet innehåller en Flash-animation som presenterar vad företaget står för. En introduktion till webbsidan.
- **Nyheter/News:** Här kan man läsa om företagets nyheter. Nyhetssidan har ett antal tillstånd, ett för varje nyhet som har lagts in. Användaren kan navigera mellan nya och äldre nyheter med hjälp av två blädder-knappar i nyhetstillståndet.
- **Om oss/About us:** Tillståndet innehåller lite historia om företaget, men även annan information som kan vara av intresse för exempelvis intresserade investerare.
- **Hjälp/Help:** Här kan användaren hitta de vanligaste frågorna om företaget och deras tjänster. När man klickar på en fråga visas ett textfält med svaret på frågan.
- **Beställ/Order:** Tillståndet innehåller ett beställningsformulär och lite information om företagets produkter. Man kan också använda tillståndet för att skicka E-post till företaget.

5.1.1 Nyheter/News

Ett nyhetstillstånd är alltid disponerat på ett typiskt och bestämt sätt: Bilden, skribentens namn och datumet har sin plats i den vänstra delen av tillståndsfönstret och själva nyhetstexten finner man i den högra delen. Ett nyhetstillstånd kan också användas för publiceringstillstånd, en extern fil för nedladdning kan då läggas som länk i det länkfält man finner strax under nyhetsfältet (se figur 17). Användaren kan bläddra igenom nyheterna i

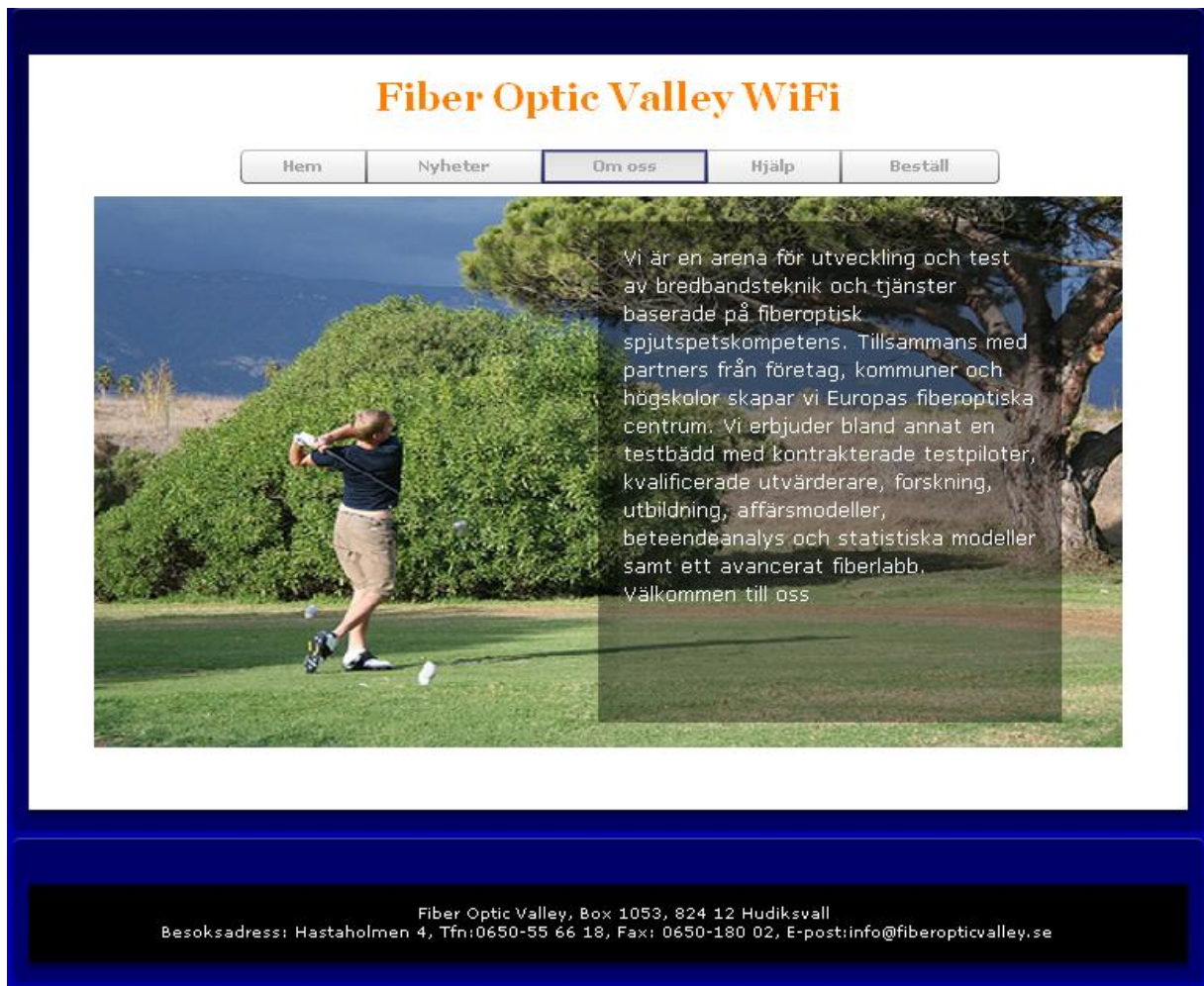
tillståndet med hjälp av knapparna ”<<” och ”>>”. En av de båda knapparna blir automatiskt inaktiv om man befinner sig på den första eller sista delen i nyhetskedjan.



Figur 17 Företagets webbsida med tillståndet ”Nyheter/News”

5.1.2 Om oss/About us

Tillståndet ger information om företaget, aktörerna bakom företaget och dess historia (se figur 18). Texten presenteras här i en textruta som också har en rullningslist till höger i tillståndet, om hela texten inte får plats i textrutan.

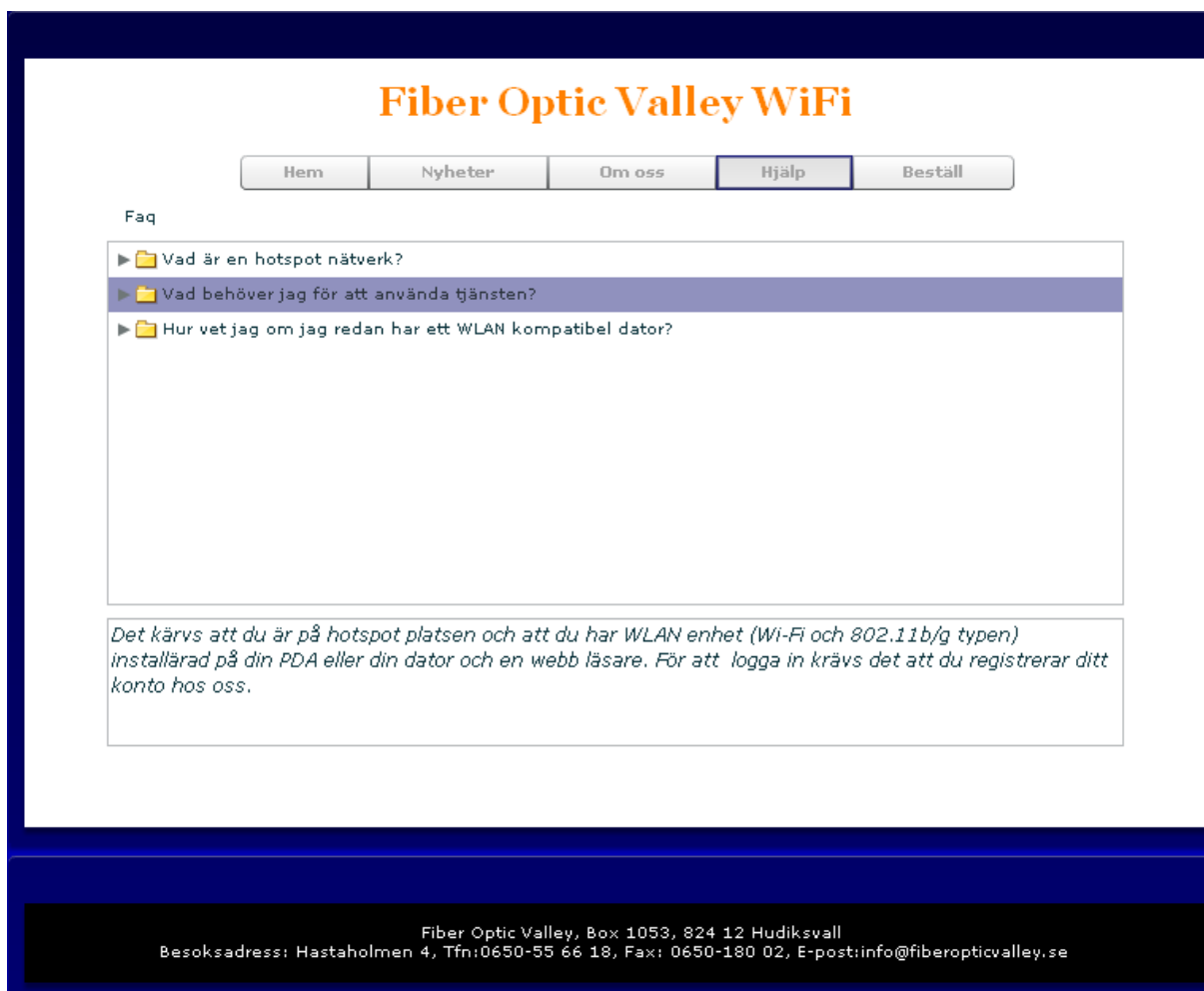


Figur 18 Tillståndet "Om oss/About us" på företagets webbsida

5.1.3 Hjälp/Help

FAQ (Frequently Asked Questions) är termen som används av supporten för de frågor som återkommer ofta. Kunderna får snabbare hjälp genom FAQ:n där de själv kan söka svaren på sina frågor, istället för att skriva till supporten och invänta ett e-postsvar.

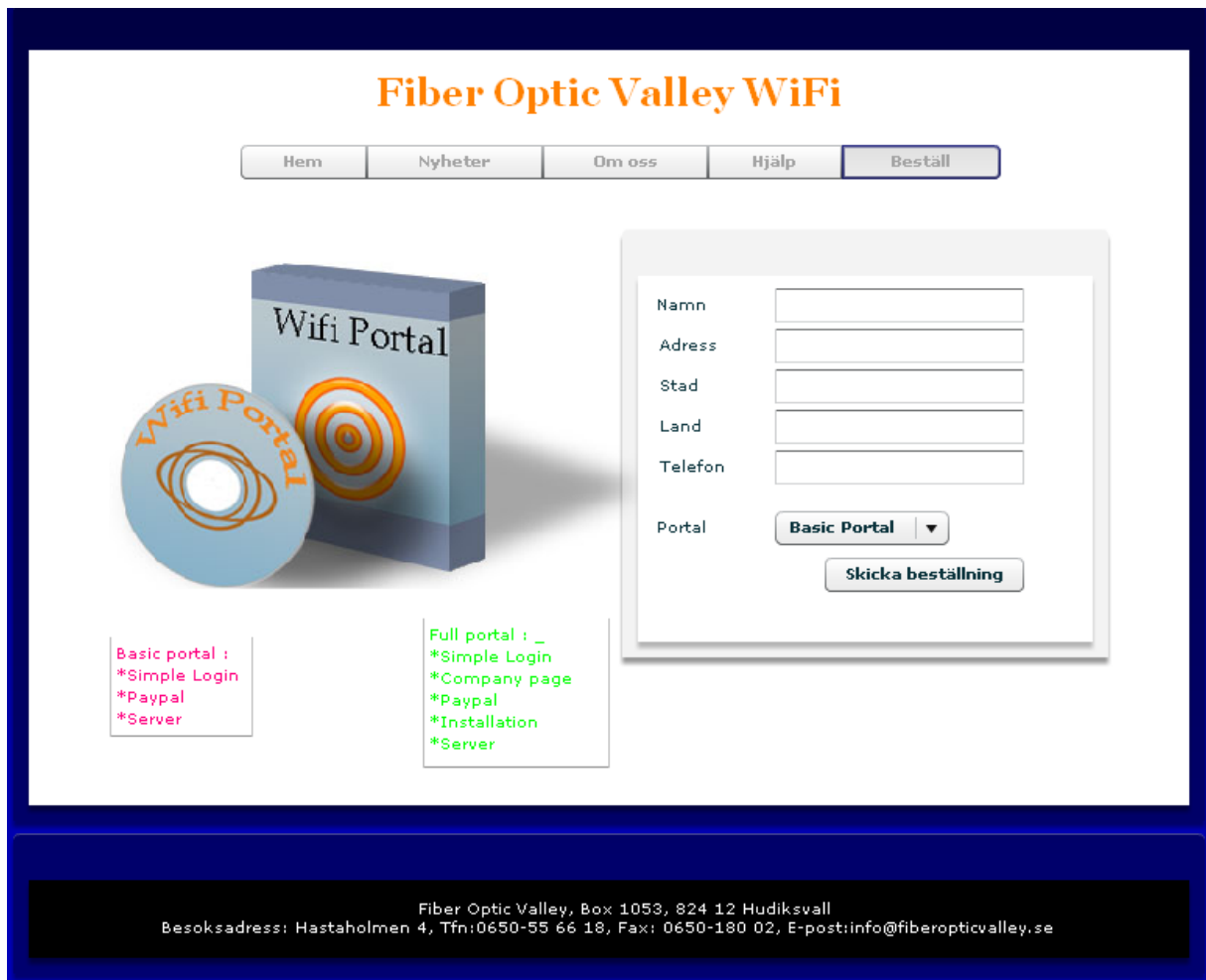
FAQ:n på webbsidan är ordnad i ett klickbart katalogträd, som kunden själv kan navigera i (se figur 19). FAQ-frågorna finns förutom på svenska också på engelska, men behöver inte vara desamma. Om kunden inte hittar ett svar på sin fråga på svenska, kan hon byta språk i den övre panelen och se om hon istället finner svaret på engelska. Det är upp till supporten på företaget att formulera svaren som de själv vill.



Figur 19 Tillståndet "Hjälp/Hel" på företagets webbsida

5.1.4 Beställ/Order

Önskar kunden beställa en produkt kan detta göras i tillståndet Beställ/Order. I figur 20 ses en bild på en hotspotprodukt med tillhörande information, samt ett formulär som ska fyllas i innan ordern skickas iväg. Om samtliga fält i formuläret inte fylls i kommer en varningsruta upp, som talar om för kunden att en del av fälten inte är ifyllda. Texten i varningsrutan finns både på engelska och svenska.

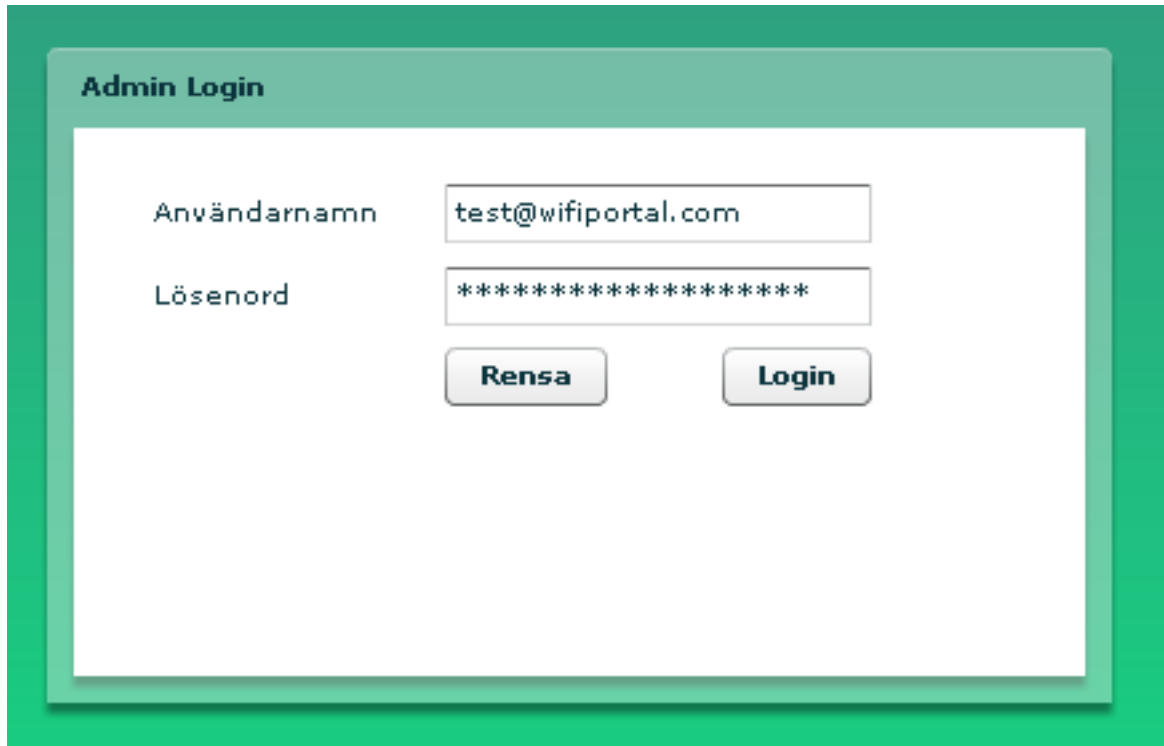


Figur 20 Tillståndet "Beställ/Order" på företagets webbsida

5.2 Administratörens webbsida

För att göra det enkelt för administratören på företaget att ändra webbsidans utseende, utan att behöva kompilera om alla filer på sidan, så skapades en administratörswebbsida. Administratörswebbsidan finns bara på svenska och har en inloggningspanel, så att bara administratören får tillträde till redigeringsverktygen på kontrollpanelen. Inloggningspanelen har två inmatningsfält, en för användarnamnet och en för lösenordet. För att skydda administratörens inmatning döljs detta lösenord i lösenordsfältet med stjärntecken (se figur 21). När inmatningen är klar klickar administratören på knappen "Login" för att validera uppgifterna eller på knappen "rensa" för att rensa fälten. Stämmer uppgifterna får

administratören tillgång till kontrollpanelen, där administrationsverktygen till företagets webbsida finns. Är uppgifterna felaktiga visas istället en röd text som meddelar detta.



The image shows a screenshot of a web-based login form titled "Admin Login". The form is set against a light green background. It contains two input fields: "Användarnamn" (Username) with the text "test@wifiportal.com" and "Lösenord" (Password) with masked characters "*****". Below the input fields are two buttons: "Rensa" (Clear) and "Login".

Figur 21 Inloggningsrutan till administratörens kontrollpanel

5.2.1 Administratörspanelen

På kontrollpanelen finner man information om företagets webbsida, versionen, samt en meny med de olika tillstånden.

Administratörspanelens olika tillstånd:

- **Info:** Ett tillstånd med en kort beskrivning av administratörspanelens olika funktioner samt aktuellt versionsnummer av panelen.
- **Layout:** Här kan administratören ändra bakgrundsfärgerna, panelfärgen och titeln på företagets webbsida.

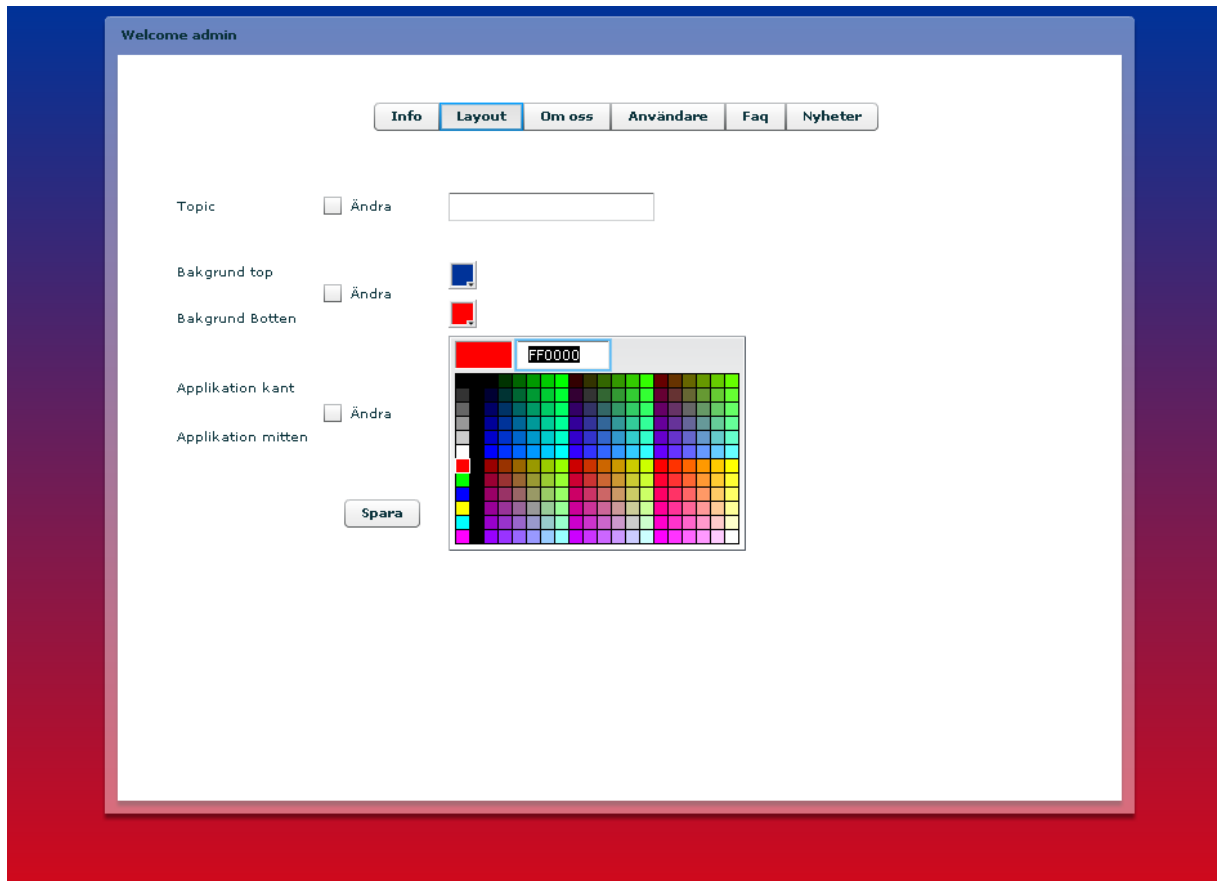
- **Om oss:** Här har administratören möjligheten att ändra texten i tillståndet ”Om oss/About us” på företagets webbsida samt besöksadressen, telefonnumret och E-postadressen dit beställningar skickas.
- **Användare:** Tillståndet presenterar hotspotens alla användare. Administratören kan välja att ta bort en användare eller ändra en användares lösenord i databasen `users`.
- **Faq:** Tillståndet ger administratören möjligheten, att lägga till eller ta bort de frågor och svar som finns under Faq-menyn på företagets webbsida.
- **Nyheter:** Ett tillstånd som används för att lägga till eller ta bort en nyhet.

5.2.2 Layout

Under tillståndet Layout ändras webbsidans utseende hos företaget (se figur 22). Här kan administratören ändra bakgrundsfärgerna, panelfärgen eller företagets namn. För att ändra på färger används en färgväljare som rymmer olika RGB²⁴-värden. Man kan också välja en färg direkt från en färgkarta. När färgen valts får administratören upp en layoutförhandsgranskning för webbsidan. Färger för en Flashsida, som i detta fall, sparas som ett talpar för färgkombinationen man valt. För att ändringen ska verkställas måste man bekräfta valet genom att kryssa i rutan ”ändra”, som finns till vänster om färgkartan. Samma sak gäller för att bekräfta ändringen av en ”Topic” (företagets namn). För att spara ändringen klickar man på knappen ”Spara”. Efter ett antal sekunder kommer en ruta fram, som talar om för administratören om värdena har sparats.

Färgändringar som görs på företagets webbsida kommer också att påverka utseendet för administratörens panel temporärt, men gäller inte vid nästa inloggning, utan bara tills administratören stänger ner sin sida. I figur 23 kan man se att färgändringen som gjordes på företagets webbsida, inte har påverkat färgen för administratörspanelen efter omstart av systemet.

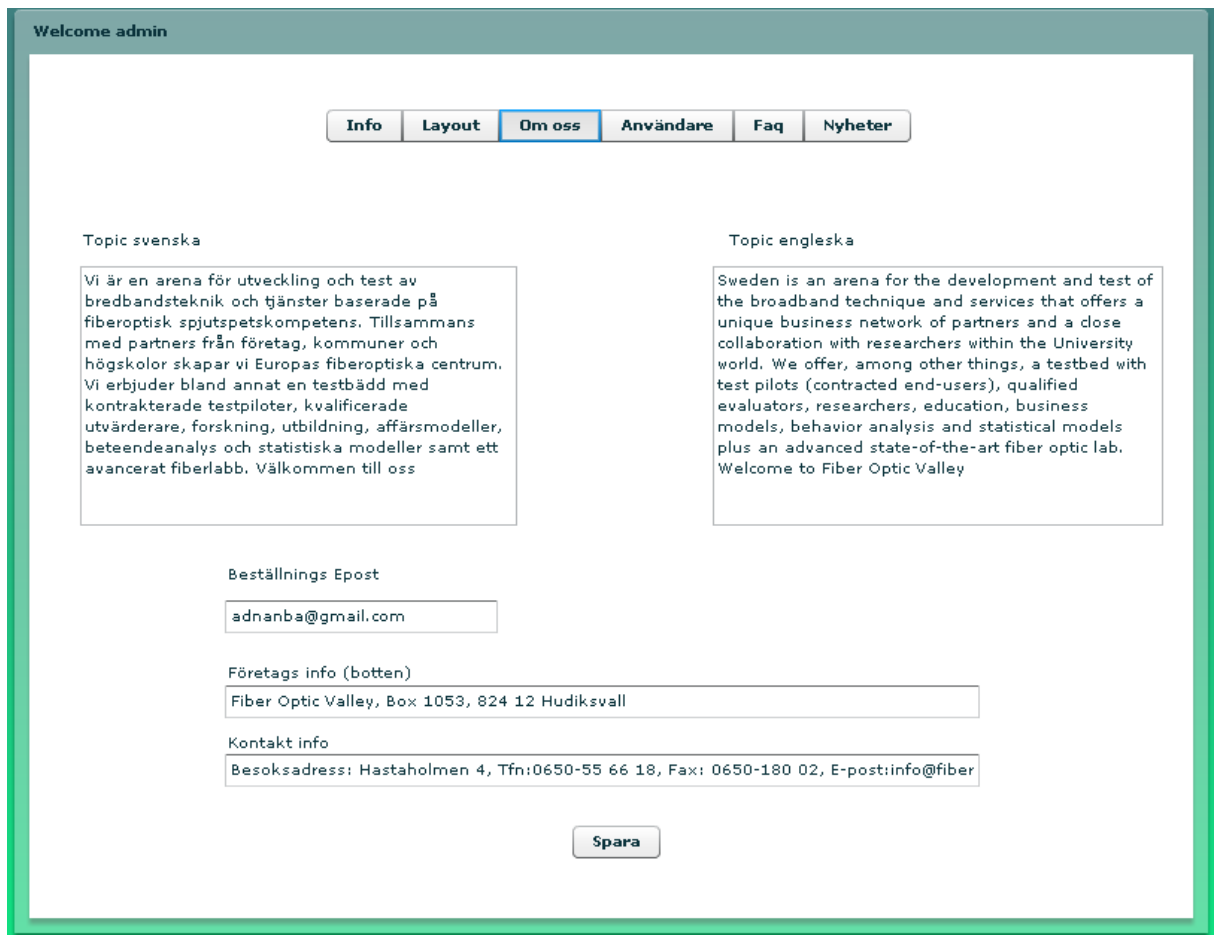
²⁴ **RGB** En akronym för färgerna rött, grönt och blått som används som grundfärger i en additiv färgblandning.



Figur 22 Ändringar av webbsidans layout från administratörens panel

5.2.3 Om oss

I figur 23 ses de ändringar som administratören kan göra för informationen i tillståndet "Om oss/About us" på företagets webbsida och även fälten inunder, med ändringar för e-postadressen till orderbeställning och informationen, som finns i bottenpanelen på webbsidan. För att spara värdena i ändringen trycker administratören på knappen "Spara". Efter några sekunder kommer då en ruta fram som bekräftar om värdena har sparats.



Figur 23 "Om oss" på administratörens panel

5.2.4 Användare

I tillståndet Användare presenteras en lista över alla hotspotanvändarna (se figur 25). Den ordning efter vilken användarna presenteras i listan bestäms av ID-numret för användaren, om inget annat väljs. Vill administratören istället ordna användarna i en stigande eller fallande ordning efter annan kolumn, klickar han bara på kolumnnamnet. Väljs kolumnen "Förnamn", ordnas användarna i bokstavsordning efter sitt förnamn.

Under användarlistan i tillståndet Användare finns också två knappar för att ta bort en användare eller ändra ett lösenord. Efter att ha markerat en användare i listan, kan administratören ta bort en användare genom att klicka på knappen "Ta bort användaren". En dialogruta kommer då fram där ändringen måste bekräftas. Bekräftas borttagningen, kommer systemet att försöka ta bort användaren från Public IP's databas och även från företagets egen databas. Efter någon sekund kommer sedan en ny dialogruta fram, som meddelar resultatet av

ändringen (se figur 24). Ska lösenordet för en användare ändras, markerar administratören en användare i listan och klickar istället på knappen ”Ändra lösenordet”. En dialogruta med två lösenordsfält kommer då fram. Administratören matar här in det nya lösenordet i båda fälten och klickar sedan på knappen ”OK” för att bekräfta ändringen.



Figur 24 Dialogruta som bekräftar att en användare har tagits bort

A screenshot of an administrative panel. At the top left, it says "Welcome admin". Below that is a navigation bar with buttons for "Info", "Layout", "Om oss", "Användare", "Faq", and "Nyheter". The "Användare" button is highlighted. Below the navigation bar is a table with the following columns: "User ID", "Förman", "Eftersmann", "Postadress", "Stad", "Land", "Telefon", and "Epost". The first row of data shows: "5", "Adnan", "Baktirovic", "Våglägndsg. 4", "Stockholm", "Sverige", "234432432", and "adnanba@gm.". Below the table are two buttons: "Ändra lösenordet" and "Ta bort användaren".

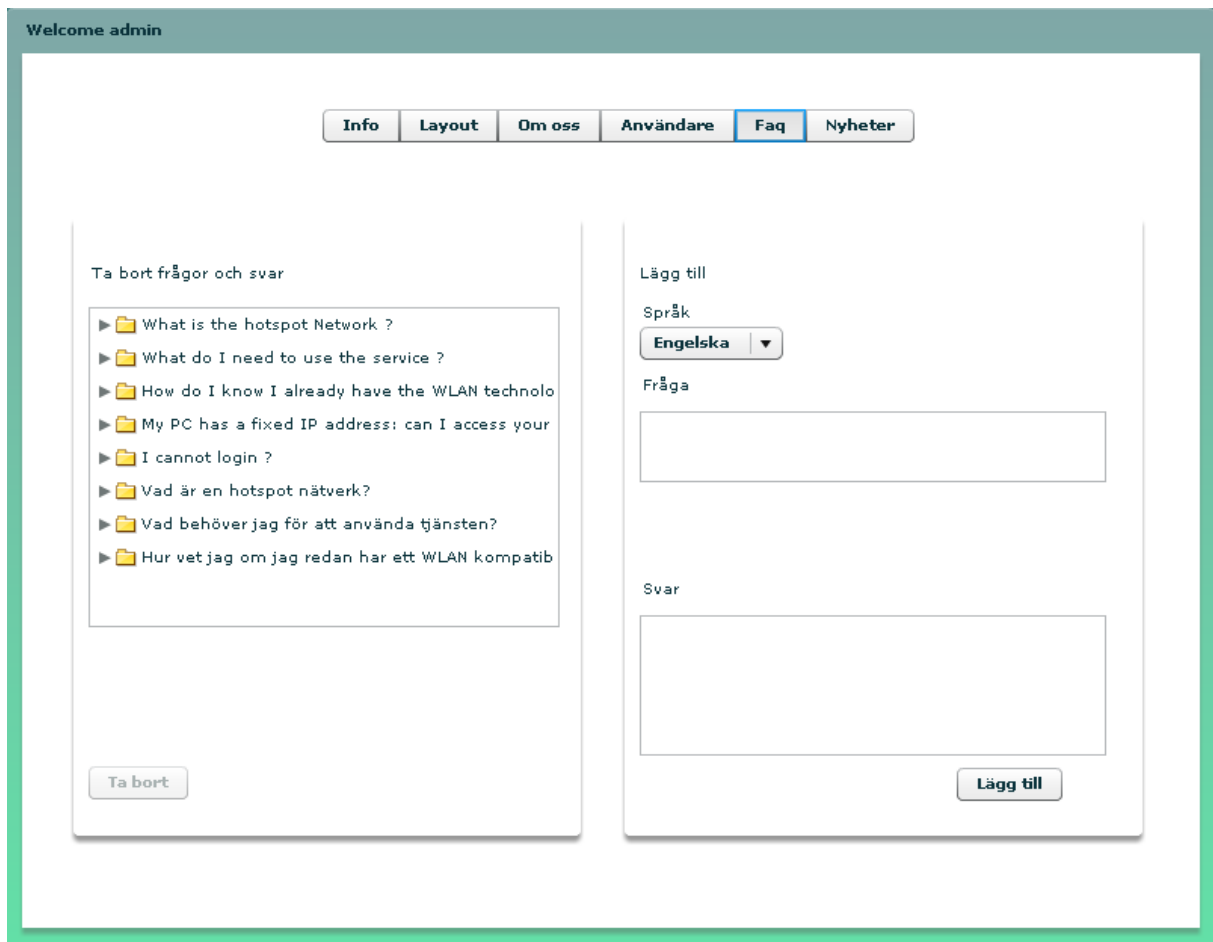
User ID	Förman	Eftersmann	Postadress	Stad	Land	Telefon	Epost
5	Adnan	Baktirovic	Våglägndsg. 4	Stockholm	Sverige	234432432	adnanba@gm.

Figur 25 Lista över hotspotanvändarna på administratörens panel

5.2.5 Faq

Tillståndet Faq på administratörens panel är till för att sköta företagets FAQ-frågor. I tillståndet finns två paneler, ”Ta bort frågor och svar” samt ”Lägg till”. I figur 26 kan man se hur dessa båda paneler är disponerade. För att ta bort ett FAQ-element, måste administratören först markera en fråga ur panelen ”Ta bort frågor och svar” och sedan klicka på knappen ”ta bort”, i panelens botten. Då en nod kan expanderas från katalogträdet i panelen, går det i praktiken också att markera ett svar i noden. Men försöker administratören att ta bort ett FAQ-element, genom att markera ett svar, kommer en dialogruta fram som meddelar administratören att istället markera en fråga.

För att lägga till ett FAQ-element måste först ett språk för frågan väljas, därefter skrivs frågan och svaret in i respektive textfält. Texten till frågan kan vara på maximalt 250 tecken. När administratören klickat på knappen ”Lägg till”, kommer en dialogruta fram som meddelar om värdena har sparats.



Figur 26 "Faq" på administratörens panel

5.2.6 Nyheter

Tillståndet Nyheter är liksom tillståndet Faq uppdelat på två paneler, en för borttagning av nyheter och en annan för tillägg av nyheter. En borttagning av en nyhet fungerar utifrån samma princip som borttagningen av ett FAQ-element. Att lägga till en nyhet är en ganska enkel process. I högra delen av nyhetstillståndet, "Lägg till en nyhet" (se figur 27), finns sju fält som skall fyllas i innan nyheten kan läggas till:

- Nyhetsämnet på svenska
- Nyhetsämnet på engelska
- Datum (Med en datumväljare som datumet väljs ur)
- Skribentens namn
- Länk (ej obligatorisk)

- Nyhetstexten på svenska
- Nyhetstexten på engelska

Det finns även ett åttonde fält i panelen, ett bildfält, som fylls i automatiskt då administratören väljer att ladda ner en bild till nyheten. När nyheten är klar att läggas till på servern, klickar administratören på knappen ”Spara”. En överföringsprocess startas då med en panel som visar överföringsförloppet av informationen, texten och bilden, till servern. Är administratören inte nöjd med nyheten, kan han istället klicka på knappen ”Rensa” i panelens botten, för att ta bort texten i fälten och bilden.

Det som användaren först möter på sin inloggningswebbsida är inloggningsformuläret, med en engelsk flagga uppe i det vänstra hörnet. Med ett klick på flaggan ändras texten på sidan från svenska till engelska.

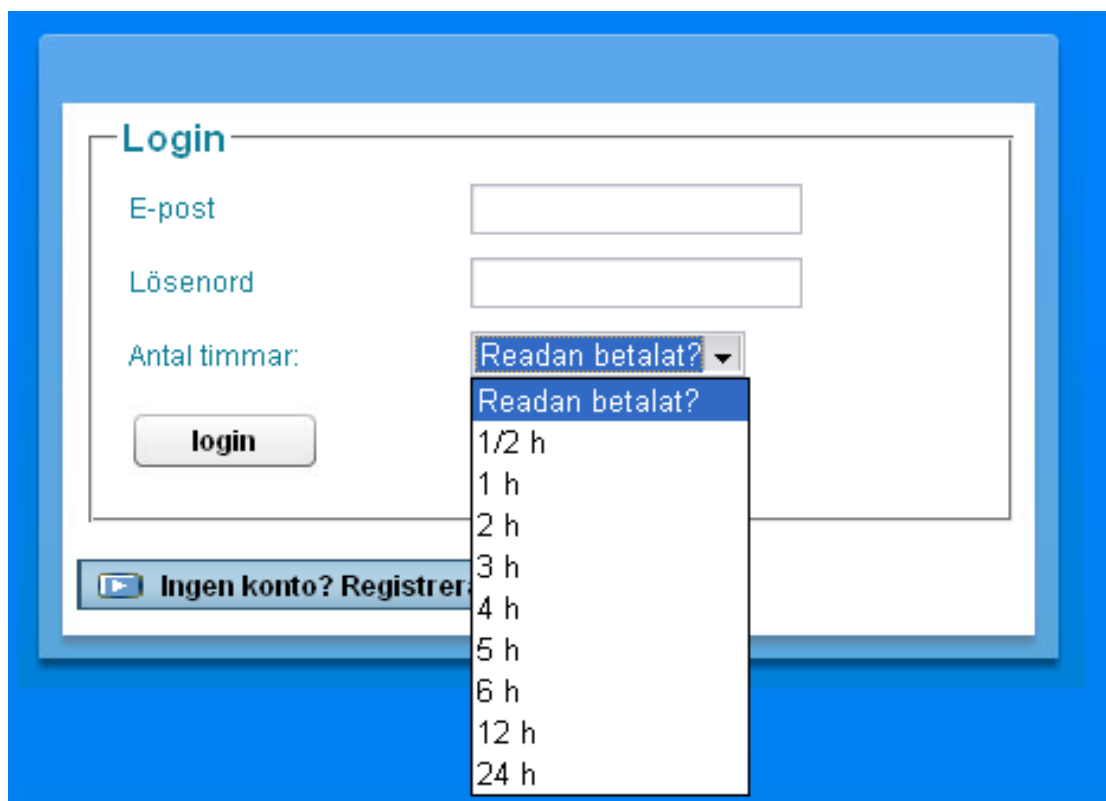
Figur 27 ”Nyheter” på administratörens panel

5.3 Användarnas webbsidor

5.3.1 Inloggningswebbsida

På inloggningsformuläret kan användaren välja antalet timmar hon önskar köpa för tillgång till Internet på hotspoten, registrera sig eller låta servern kontrollera eventuell återstående tid från ett tidigare köp (se figur 28).

När användaren valt sitt köp av tid, skriver hon in sina inloggningsuppgifter i e-post- och lösenordsfältet och klickar sedan på knappen "Login". Vid lyckad inloggning kommer hon då direkt vidare till PayPal, där hon kan betala för den beställda tiden. Om användaren istället valt alternativet "Redan betalt" vid inloggningen, får hon automatiskt direkt tillträde till Internet på hotspoten eller eventuellt ett felmeddelande.



The image shows a login form with the following elements:

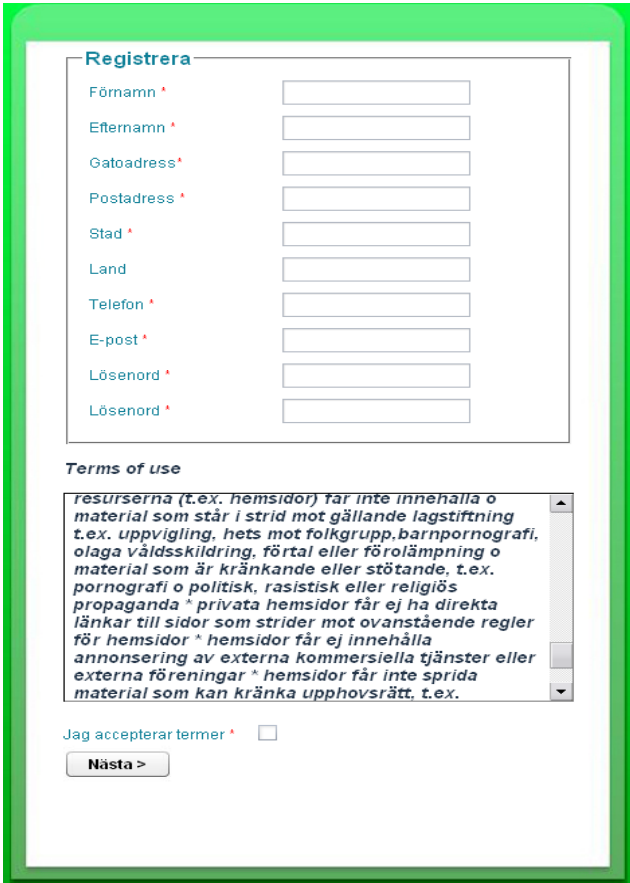
- Title:** Login
- Fields:** E-post, Lösenord, and a dropdown menu for "Antal timmar:".
- Dropdown Menu:** Open, showing options: "Redan betalat?", "1/2 h", "1 h", "2 h", "3 h", "4 h", "5 h", "6 h", "12 h", and "24 h".
- Buttons:** A "login" button and a "Ingen konto? Registrera dig" link.

Figur 28 Användarens inloggningsformulär

5.3.2 Registreringswebbsidan

Användarnas registreringswebbsida finns både på engelska och på svenska. Önskar användaren skifta språk, klickar hon bara på ikonerna med flaggan. De fält som är obligatoriska att fylla i på registreringsformuläret är markerade med en röd stjärna (en asterisk *, se figur 29). Dessa fält fylls i med strängar om 2-25 tecken. För att registreringen sedan ska genomföras, måste användaren också markera boxen ”Jag accepterar de här termerna”, som finns längst ner på registreringsformuläret.

Är registreringsformuläret korrekt ifyllt kommer användaren vidare till inloggningswebbsidan för hotspoten. Skulle istället någon eller några av uppgifterna på registreringsformuläret vara fel, visas ett kontrollmeddelande för användaren som upplyser om detta. I kontrollen ingår även eventuell förekomst av dubbla e-postadresser i databasen.



The image shows a registration form titled "Registrera" with a green border. It contains the following elements:

- A list of input fields, each with a red asterisk indicating it is mandatory:
 - Förnamn *
 - Efternamn *
 - Gatoadress *
 - Postadress *
 - Stad *
 - Land
 - Telefon *
 - E-post *
 - Lösenord *
 - Lösenord *
- A section titled "Terms of use" containing a scrollable text area with the following text:

resurserna (t.ex. hemsidor) får inte innehålla o material som står i strid mot gällande lagstiftning t.ex. uppvigling, hets mot folkgrupp, barnpornografi, olaga våldsskildring, förtal eller förolämpning o material som är kränkande eller stötande, t.ex. pornografi o politisk, rasistisk eller religiös propaganda * privata hemsidor får ej ha direkta länkar till sidor som strider mot ovanstående regler för hemsidor * hemsidor får ej innehålla annonsering av externa kommersiella tjänster eller externa föreningar * hemsidor får inte sprida material som kan kränka upphovsrätt, t.ex.
- A checkbox labeled "Jag accepterar termer *" which is currently unchecked.
- A button labeled "Nästa >" at the bottom.

Figur 29 Användarens registreringsformulär

6 Implementering

I kapitlet som följer kommer implementeringen av de olika projektdelarna att beskrivas. Inledningsvis redovisas för de inställningar som gjordes före utformningen av ZoneCD. Konfigurationen av hårdvaran för hotspotsystemet beskrivs i kapitel 6.2. Vidare skildras hur man lägger till en LAMP-lösning på en Live-CD-skiva, i kapitel 6.3. De skript som krävs vid utformningen av ZoneCD återges i bilaga B. Avslutningsvis tas de olika skripten upp, som är motorn för de olika webbsidorna och som även sköter logiken för dessa. För att göra texten i rapporten mer överskådlig, har pseudokod²⁵ använts för funktioner och logik i källkoden. Men för att visa hur Flex2 fungerar ges även något exempel på riktig kod.

6.1 Förberedning

Innan ZoneCD kan utformas måste ett konto registreras hos Public IP. Vill man utforma sin ZoneCD för Apache, PHP och MySQL måste man även registrera ett konto hos DynDNS. DynDNS-tjänsten skall ställas in så att:

- Värnamnet (eng. hostname) som refererar till hotspotinloggningsservern, väljs till `dinadress.dyndns.org`.
- `dinadress1.dyndns.org = 10.10.10.1`

De webbsidor som ska tillåtas för kunderna, måste listas och läggas till på kontrollservern hos Public IP innan de kan besökas: `dinadress.dyndns.org`, `dinadress1.dyndns.org`, `paypal.com`, `paypalobjects.com`, `www.paypalobjects.com` och `developer.paypal.com`. Detta är nödvändigt då kontrollservern på Public IP inte kan tyda IP-adresser, utan bara kan tolka FQDN. I annat fall kommer anslutningen till kundernas inloggningssida och returwebbsidan (sidan som visas efter att betalningen på PayPal är gjord) inte att tillåtas av NoCat, på grund av att `10.10.10.1` inte finns med i kontrollserverns register. Även om man istället har sin kundinloggningssida på ett webbhotell och inte på ZoneCD, måste adressen läggas till på kontrollservern hos Public IP.

²⁵ **Pseudokod** Ett icke-programmeringsspråk som beskriver algoritmer med en blandning av programspråk och vanlig skriven text.

6.2 Hårdvaran

Som ZoneCD-testserver användes en dator med en 1.5 GHz processor, 512 MB Ramminne, DVD-/CD-läsare och ett USB-flashminne. Datorn var även utrustad med två nätverkskort. Systemet anslöts till Internet genom en valig nätverkskabel. Det går även att använda en VMware-workstation²⁶ som testplattform. I VMware-workstation använder man istället två bryggade nätverkskort.

6.2.1 Inställningar för accesspunkten

En trådlös router fungerar utmärkt som en accesspunkt för en mindre WLAN-konfiguration. Det som behöver ställas in i routern är:

- Den öppna WEP-konfigurationen, utan nyckel eller alternativt helt utan säkerhet.
- DNS-tjänsten som finns inbyggd i routern måste stängas av.
- Routers IP-adress ställs in som en statisk IP-adress: 10.10.10.2

I en modern router görs ovanstående inställningar genom att koppla upp sig via routers LAN-port mot webbinterfacet. Man skriver in adressen <http://192.168.0.1> i webbläsaren eller den adress som anges i routermanualen. För att de nya inställningarna ska gälla krävs sedan en omstart av routern.

6.3 Apache, PHP och MySQL på flashminnet

För att en webbserver ska fungera ihop med ett flashminne, behöver den utrymme för temporära filer samt lagring av data. Flashminnet måste formateras med en FAT32-sda1-partition på maximalt 20 MB samt en Linux-sda2-partition för serverns filsystem. För LAMP-lösningen behövs följande kataloger på flashminnet:

²⁶ VMware Tillhandahåller virtuella maskiner för att köra nya instanser av operativsystemen. <http://www.vmware.com>

- `/var/www`-katalogen för webbsidor
- `/ssl`-katalogen för SSL-certifikat
- `/var/run/mysqld`-katalogen för MySQL PID och socket filer (MySQL-process-filer)
- `/var/lib/mysql`-katalogen för MySQL-loggfiler
- `/var/lib/mysql/mysql`-katalogen för MySQL-databaser
- `/var/lib/php5.0`-katalogen för PHP-sessionsfiler²⁷

När formateringen av flashminnet är klar och efter att ha skapat katalogerna till LAMP, kan man utforma sin ZoneCD och installera de program man själv väljer. För att genomföra utformningen behövs en HD-avbildning av ZoneCD, som skapas med hjälp av automatiserade skript (se bilaga B). För att använda dessa skript krävs en Debian-baserad Linux-distribution och programmet `cloop-utils` (i projektet användes version 1.0). `Cloop-utils` är den typ av verktyg som används för att komprimera och dekomprimera en Live-CD. Då `Cloop-utils`-programmen vare sig är bakåtkompatibla eller framåtkompatibla, kan en ZoneCD som är komprimerad med exempelvis `cloop-utils 1.0`, inte dekomprimeras på ett system med en nyare eller äldre version av programmet.

6.3.1 Apache

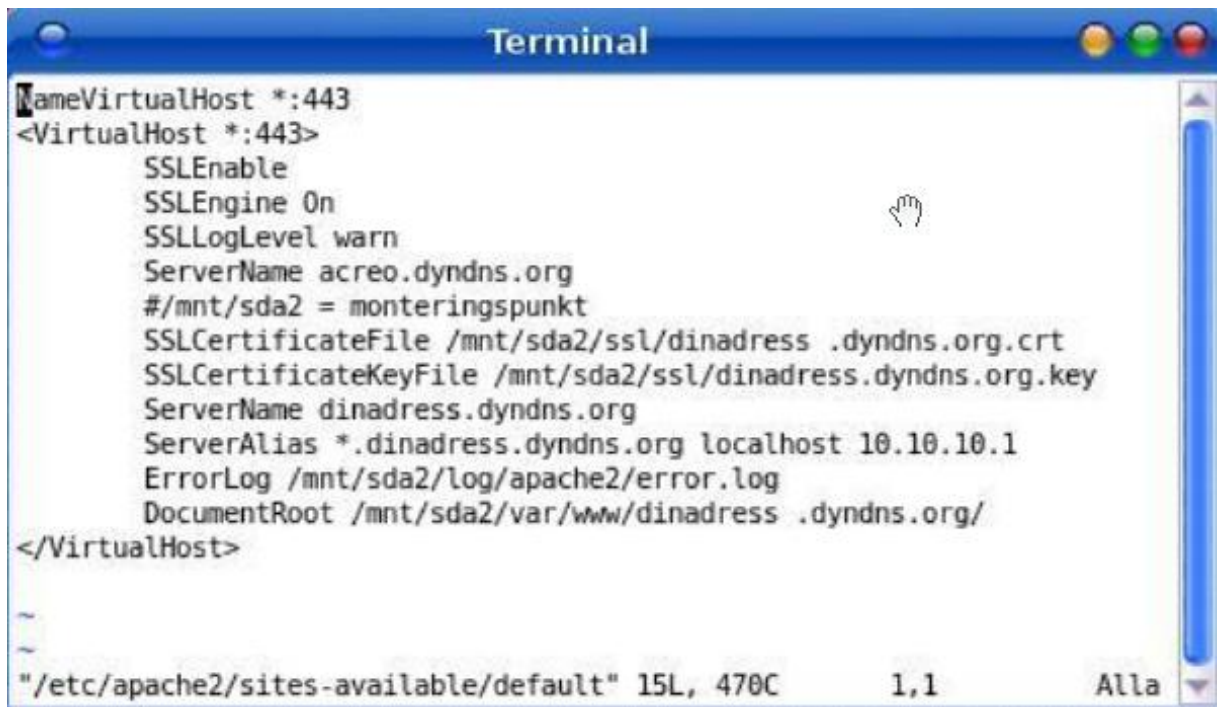
Eftersom ZoneCD kan dekomprimeras i en grafisk arbetsmiljö kan man använda verktygen som finns på värdoperativsystemet, för att redigera konfigurationsfilerna på CD:n. Att redigera dessa filer kräver administratörsrättigheter.

För att ställa in Apache2 att fungera med SSL-protokollet, måste en del av Apache2-konfigurationsfilerna redigeras som finns i katalogen `/etc/apache2`. Filen `ports.conf` innehåller inställningarna för de portar Apache2 lyssnar på och `Listen 443` är inställningen för SSL-porten. Apache2-versionen har också två kataloger för virtuella servrar. Den ena är `sites-available` och den andra är `sites-enabled`. Katalogen `sites-available` innehåller konfigurationsfilerna (för ett hotspot-konfigurationsexempel, se figur 30) i ren textform, medan `sites-enabled` är katalogen som innehåller länkarna till filerna i `sites-available`. Efter att ha redigerat filerna i `sites-available` ska dessa länkas till

²⁷ **Session** En temporär identifikations-cookie som håller reda på en webbplatsbesökare med hjälp av en unik `SESSION-ID`. Sessionen gäller tills besökaren stänger ner sin webbläsare.

katalogen `sites-enabled`, som är den katalog Apache2 läser in de virtuella serverinställningarna från vid uppstart. De virtuella serverinställningarna länkas med Linux-kommandot `ln`. Ett exempel på detta är:

```
ln -s /etc/apache2/sites-available/default
/etc/apache2/sites-enabled/default
```

A screenshot of a terminal window titled "Terminal". The window displays the contents of an Apache2 virtual host configuration file. The configuration is enclosed in XML-like tags: `<NameVirtualHost *:443>` and `</VirtualHost>`. Inside, various settings are listed, including `SSLEnable`, `SSLEngine On`, `SSLLogLevel warn`, `ServerName acreo.dyndns.org`, a comment `#/mnt/sda2 = monteringspunkt`, `SSLCertificateFile /mnt/sda2/ssl/dinadress.dyndns.org.crt`, `SSLCertificateKeyFile /mnt/sda2/ssl/dinadress.dyndns.org.key`, `ServerName dinadress.dyndns.org`, `ServerAlias *.dinadress.dyndns.org localhost 10.10.10.1`, `ErrorLog /mnt/sda2/log/apache2/error.log`, and `DocumentRoot /mnt/sda2/var/www/dinadress.dyndns.org/`. At the bottom of the terminal, a status bar shows the file path `"/etc/apache2/sites-available/default"`, its size `15L, 470C`, and other details like `1,1` and `Alla`.

Figur 30 Ett exempel på en serverkonfigurationsfil för Apache2

Apache2-serverkonfigurationsfilen i figur 30 sammanfattar inställningarna för hotspoten.

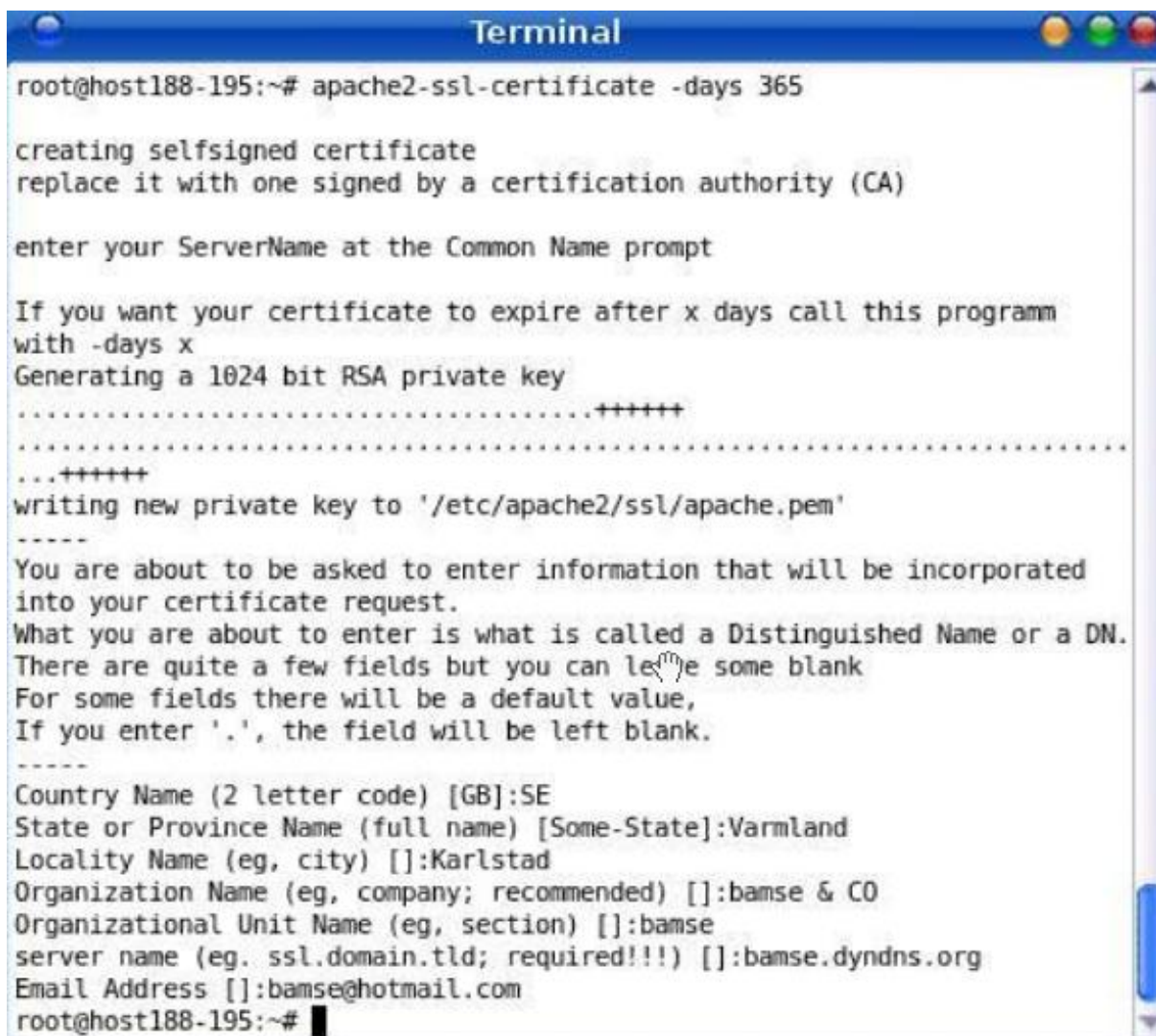
Kort förklaring av variablerna i filen:

- **NameVirtualHost *:443** talar om för Apache2 att all inkommande begäran till port 443 ska skickas till hotspotens virtuella server.
- **ServerAlias *.dinadress.dyndns.org 10.10.10.1**: För att servern ska kunna expediera hotspot-användarna talar man om vilka alias-adresser den ska nås från.
- **DocumentRoot /mnt/monteringspunkt/var/www/**: DocumentRoot är webbplatsens baskälla och den katalog där alla webbfiler placeras som den virtuella servern behöver.
- **SSLEnable**, **SSLEngine On** och **SSLLogLevel warn** är de variabler som talar om att SSL-anslutningen gäller.

- `SSLCertificateFile`, `SSLCertificateKeyFile`: Alla SSL-certifikat ligger lagrade här.

6.3.2 Skapa ett SSL-certifikat

Apache2 innehåller ett OpenSSL-hölje som heter `apache2-ssl-certificate`. Certifikatet tillåter administratören att skapa ett SSL-certifikat genom att svara på ett par frågor i kommandotolken. Funktionen kräver administratörsrättigheter.



```
Terminal
root@host188-195:~# apache2-ssl-certificate -days 365

creating selfsigned certificate
replace it with one signed by a certification authority (CA)

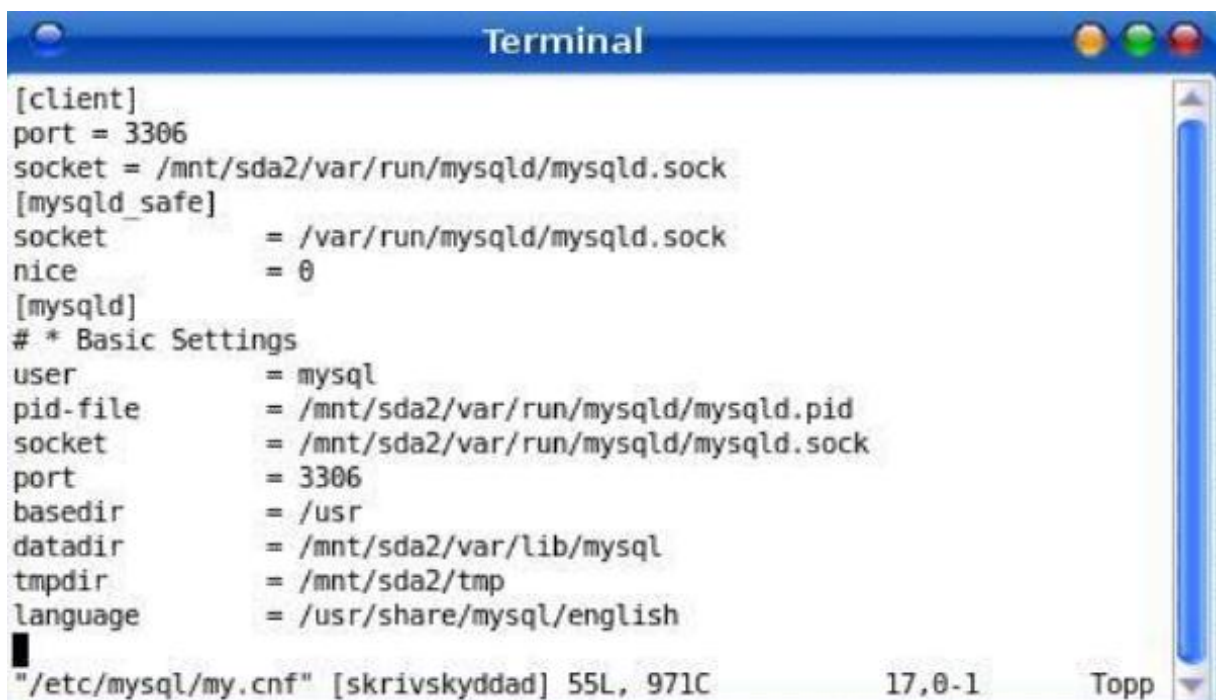
enter your ServerName at the Common Name prompt

If you want your certificate to expire after x days call this programm
with -days x
Generating a 1024 bit RSA private key
.....++++++
.....
...++++++
writing new private key to '/etc/apache2/ssl/apache.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:SE
State or Province Name (full name) [Some-State]:Varmland
Locality Name (eg, city) []:Karlstad
Organization Name (eg, company; recommended) []:bamse & CO
Organizational Unit Name (eg, section) []:bamse
server name (eg. ssl.domain.tld; required!!!) []:bamse.dyndns.org
Email Address []:bamse@hotmail.com
root@host188-195:~# █
```

Figur 31 Exempel på ett `apache2-ssl-certifikat`

6.3.3 MySQL-konfiguration

Det krävs inte så mycket arbete och kunskap för att få en portabel MySQL-databas. Det enda som ska ändras för MySQL är variablerna `pid-file`, `socket`, `datadir` och `tmpdir` som alla finns i filen `/etc/mysql/my.cnf` (se figur 32). Filen `socket` används för kommunikationen mellan databasanvändarna och MySQL, medan databaserna med tabeller och rättigheter finns i mappen `datadir`.



```
Terminal
[client]
port = 3306
socket = /mnt/sda2/var/run/mysqld/mysqld.sock
[mysqld_safe]
socket      = /var/run/mysqld/mysqld.sock
nice        = 0
[mysqld]
# * Basic Settings
user        = mysql
pid-file    = /mnt/sda2/var/run/mysqld/mysqld.pid
socket      = /mnt/sda2/var/run/mysqld/mysqld.sock
port        = 3306
basedir     = /usr
datadir     = /mnt/sda2/var/lib/mysql
tmpdir      = /mnt/sda2/tmp
language    = /usr/share/mysql/english
"/etc/mysql/my.cnf" [skrivskyddad] 55L, 971C      17,0-1      Topp
```

Figur 32 Konfigurationsfilen `/etc/mysql/my.cnf` för MySQL

6.3.4 PHP5-konfiguration

Då variabelvärdena för MySQL kräver en dynamisk miljö måste dessa peka på en plats på flashminnet.

PHP-konfigurationsfilen finns i mappen `/etc/php5/apache2/` och heter `php.ini`. De ändringar som måste göras i konfigurationsfilen är följande:

- `file_uploads = On` Då webbsidorna har bilder som laddas upp till servern måste variabeln vara på (eng. On).

- `upload_tmp_dir = /monteringspunkt/var/www/tmp` Inställningen medger att PHP gör en felkontroll för de filer som ska laddas upp till katalogen på servern, innan de skickas.
- `upload_max_filesize = 2M` Begränsar filstorleken för de filer som laddas upp till servern.
- `session.save_path = /monteringspunkt/var/lib/php5` Alla sessionsfiler sparas här. En `cronjob5`-tjänst (schemalagd aktivitet) rensar efterhand mappen på gamla sessionsfiler för att spara plats.

6.4 Webbdesign och webbprogrammering för hotspoten

Följande del har till ämne att beskriva de filer och procedurer i hotspotens webbinterface, som utgör systemet för användarens inloggning, registrering och PayPal-tjänster. I kapitel 6.4.1 beskrivs inloggningsprocessen för registrerade kunder, vad som sker i PHP-algoritmen när kunden gör en beställning, samt säkerheten och felhanteringen. Avslutningsvis behandlas registreringsprocessen i kapitel 6.4.2.

All kunddata kontrolleras med PHP och sparas i MySQL-databasen. Databasstrukturen återfinns i bilaga D och samtliga funktioner som beskrivs i kapitlet finns inkluderade i bilaga C.

6.4.1 Kundinloggning

De PHP-skriptfiler som är verksamma under kundens inloggningsprocess och som finns i mappen `/login/` är:

-  `login.php`
-  `ipn_reciver.php`
-  `ipn_user.php`
-  `login.css`
-  `paypal/`

När en användare besöker företagets inloggningswebbsida startar skriptet `login.php` funktionen `session_start()`, för att servern ska kunna skilja på olika användare. Av

`session_start` tilldelas användaren en unik nyckel (strängen `SSID` visas vanligtvis inte av webbläsaren, ex. `ssid=X123BASD123`). För att servern ska hålla reda på språket användaren har under sessionen, då hon besöker företagets nätverk, tilldelar `login.php` användaren även en sessionsvariabel kallad `language`, som kan ha värdet "svenska" eller "engelska". Vanligtvis är de här variablerna bara giltiga under en bestämd tid eller tills dess användaren stänger ner sin webbläsare. Vid lyckad inloggning tilldelas ytterligare en sessionsvariabel, variabeln `email`, för autentisering av användaren när hon återvänder till inloggningswebbsidan, efter att ha besökt PayPal. Om användaren redan har betalt men av någon orsak råkar stänga ner sin webbläsare, kan hon logga in igen med alternativet "redan betalt" på inloggningsformuläret, för att återställa sina sessionsvariabler.

HTML- och CSS-delen av skriptet `login.php` sköter en viktig utseendefiness på användarnas inloggningssida. När en användare besöker inloggningssidan hämtas sidan automatiskt från företaget, av Public IP's server, som lägger in sin egen kod. För att gömma denna kod för användaren utnyttjar företaget därför ett `div`-element, som skapar en illusion av ett XML-dokument inuti HTML-koden och tilldelar `div`-elementet ett CSS-stilvärde, "visibility:hidden;". XML-elementet som alstras får då värdet: `<div id="1" style="visibilty:hidden;"> ZONE_ELEMENT</div>`. All kod från Public IP göms på så sätt i XML-elementets `ZONE_ELEMENT` och tas därför bort från layouten på inloggningssidan.

Till största del utgörs skriptet `login.php` av de funktioner som sköter inloggningen och valideringen av de uppgifter användaren matar in. Men innan skriptet kan användas måste en del definitionsvariabler ställas in (se figur 33). För att se en lista över funktionerna och deras användning, se bilaga C.



```
define ("PUBLICIPKEY","YOUR_KEY"); ## /zonecd/zone.key
define ("ZONEADMIN","ZON_NAMN");
define ("ZONEPASSWORD","ZON_LÖSENORDET");
define ("MERCHANTEMAIL","DIN_PAYPAL_EPOST");
define ("PAYPAL_URL","https://www.sandbox.paypal.com/cgi-bin/webscr"); /
define ("YOURIPN_URL","http://DINSIDA.dyndns.org/login/ipnreciver.php");
define ("RETURN_URL","http://DINSIDA.dyndns.org/login/login.php");
define ("CANCEL_URL","http://DINSIDA.dyndns.org/login/cancel.php");
define ("TAX","30"); ## taxerings värde
define ("PRISPERSECOND","0.05"); ## pris för en sekund
define ("DBHOST","DB_HOST");
define ("DBNAME","DB_NAMN");
define ("DBUSER","DB_ANVÄNDARE");
define ("DBTABLE_USERS","users");
define ("DBTABLE_PAYPAL","ipn_users");
define ("DBPASS","LÖSENORDET");
#####
```

Figur 33 Konfigurationsvariabler som ska ställas in för login.php

Då användaren loggar in från inloggningssidan anropas klassobjektet `ipn_user`, som finns i PHP-skriptet `ipn_user.php`. Detta klassobjekt har till funktion att bevara användarens inloggningsuppgifter samt transaktionsuppgifterna från PayPal. Dessa transaktionsuppgifter (den beställda tiden, priset mm.) samt användarens uppgifter från tabellen `DBTABLE_USERS`, sparas i tabellen `DBTABLE_PAYPAL` på företagets server. När användarens betalning på PayPal är genomförd, skickas dessa uppgifter från tabellen `DBTABLE_PAYPAL` automatiskt till PayPal för validering. Men i denna validering, som sker i två steg, skickas först en transaktionsbekräftelse till företagets server från PayPal, därefter skickas företagets svar, en IPN-bekräftelse genom en `fsocket` som valideras mot PayPal. Den dubbla valideringens andra del, som är en automatisk och explicit kommunikation mellan PayPal och företagets server, är användaren ovetande om.

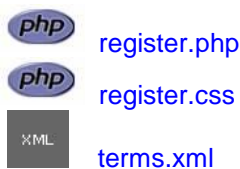
Klassen `ipn_user` innehåller även funktioner som imiterar en webbläsare och som registrerar en temporär användare på kontrollservern hos Public IP. För att imitera en webbläsare med ett PHP-skript, spåras `SSID`-variabeln som skickas från Public IP, efter att den temporära användaren loggats in på Public IP's inloggningssida. För att den temporära inloggningen ska lyckas, ansluter sig inloggningsfunktionen genom en `fsocket` till kontrollservern på Public IP, med användarens inloggningsuppgifter samt ett falsk knappvärde, som representerar användarens tryck på knappen "Log in". Därefter läggs den

temporära användarens giltighetstid för kontot in på kontrollservern, som motsvarar den betalda tiden.

6.4.2 Registreringsfilerna

Katalogen `/paypal` innehåller alla transaktionsloggar för användaren. Här sparas all transaktionsdata i filer efter det datum de mottagits av servern.

De filer som är verksamma under registreringsprocessen är:



`register.php` är en skriptfil som bara kan nås med registreringslänken på `login.php`-sidan. För att skriptfilen ska kunna utföra registreringslogiken, krävs ett antal `$_POST`-värden från kontrollservern, såsom `mac`, `token`, `timeout` mm. Varje inmatningsvärde vid registreringen kontrolleras med hjälp av PHP:s inbyggda funktioner för längdkontroll och kontroll av ogiltiga tecken. Skriptfilen gör även en kontroll av dubbla e-postadresser i MySQL-databasen. Efter användarens registrering sparas MAC, IP och alla andra värden i databasen `DATABASE_USERS`.

`register.css` som är en kopia av `login.css`, skapas för att ägaren av hotspoten ska få en bättre översikt över layoutinställningarna på registreringswebbsidan.

`terms.xml` innehåller bara två element, `<svenska>` och `<engelska>`. För att redigera data i de här elementen, använder man sig av en textredigerare som klarar av UTF-8-formatet. Filen `terms.xml` skapas i XML-format, då formatet kan läsas som vanlig skriven text och lätt kan redigeras med hjälp av en textredigerare. Termerna med villkoren för användningen av hotspoten bestämmer ägaren själv.

6.5 Webbdesign och webbprogrammering för företagets webbsida

Följande kapitel har till ämne att beskriva tre huvudkataloger, xml-, bin- och admin-katalogen, som finns på företagets webbsida. Avsikten med uppdelningen på tre huvudkataloger, är att öka säkerheten och få en bättre översikt över alla filerna. Filerna i xml- och bin-katalogen använder sig av en http-anslutning, medan den tredje katalogen /admin, innehåller data som skyddas med SLL-anslutning. Apache2 kräver att filerna på servern delas upp i olika kataloger, då varje katalog endast kan ha en http-anslutning eller en SLL-anslutning.

När en användare besöker en webbsida som innehåller Flex2-Flash-applikationer, sänder webbläsaren en begäran till webbservern, om den HTML-källkod som krävs för att läsa sidan. När källkoden därefter anger för webbläsaren vilken Flash-applikation som krävs för webbsidan, tas denna emot från webbservern. Härifrån tar sedan Flash-applikationen över den fortsatta HTML-kommunikationen med webbservern. Hur denna kommunikation går till beskrivs i sista kapitlet.

6.5.1 Katalogen /xml-textuell databas



All information som finns på företagets webbsida och som går att ändra finns i xml-katalogen. XML-filerna är konfigurerade att innehålla layoutinställningarna samt informationstexten till webbsidan. Filerna indelas också efter tillståndet de bestämmer på webbsidan. För att ändra data i XML-filerna används administratörens kontrollpanel eller en vanlig textredigerare.

Poängen med att ha företagets information i XML-filer, är att den data de innehåller går att redigera i plan text och att filerna inte behöver någon dataintegritet, på så vis belastas inte databasen. Xml-filer på företagets server som representerar ett tillstånd:

- about.xml-filen innehåller den information om företaget som visas i tillståndet ”Om oss/About us”.
- faq.xml-filen rymmer faq-element av typen `<fråga type="språk">svar </fråga>`. Elementen kan tas bort och nya kan läggas till från administratörens kontrollpanel.
- news.xml-filen innehåller nyhetselementen, rankade efter tiden de lades in.
- style.xml-filen innehåller bakgrundfärgerna till företagets webbsida samt företagets namn. Elementen ändras i tillståndet ”Layout” från administratörens kontrollpanel.

6.5.2 Katalogen /bin-företagets Flash-webbsida



[Wifiportal.swf](#)



[Wifiportal.html](#)



[Images](#)

[Wifiportal.swf](#) är en Flash-animation på webbsidan som presenterar företaget för användaren. Funktionerna i filen `Wifiportal.swf` läser data från XML-filer, som sedan presenteras. ActionScript som ingår i filen, har inbyggda funktioner för tolkning av externa XML-filer. Det som krävs för tolkningen är en `creationComplete`-funktion i `<application>`-taggen, som finns i MXML-källkodsfilen för applikationen. Efter att webbsidan laddats ner, talar värdet `creationComplete=downloadRestInfo()` om för Flash-applikationen, att börja nerladdningen av XML-filer och övrig data som hör till sidan. En liknande algoritm som den ovan kan ses i figur 35.

[Wifiportal.html](#) är en enkel webbsida som har `Wifiportal.swf` inbäddad i kroppen (`<body>`). Webbsidan innehåller en JavaScript-funktion, som kontrollerar om användarens webbläsare uppfyller kraven för presentation av Flash-applikationer. Om så inte är fallet, uppmanas användaren att installera Macromedias flashspelare.

[Images](#)-katalogen innehåller alla bilder som finns på företagets webbsida. Katalogen används också som förvaringsplats för bilder till nyheter.

6.5.3 Katalogen /admin-administratörens kontrollpanel



[checklogin.php](#)

[admin.html](#)

[admin.swf](#)

Filen `checklogin.php` är själva motorn för `admin.swf` (administratörens kontrollpanel). I `checklogin.php` finns alla de funktioner som ändrar och uppdaterar informationen i företagets XML-filer. Filen innehåller även funktioner för validering av administratörens inloggningsuppgifter och funktioner för att ta bort en användare från databasen eller ändra en användares lösenord.

För att aktivera filen `checklogin.php` uppger administratören sitt namn och lösenord. Vill administratören använda sig av funktionerna i filen, anger han en `cmd`-variabel och tillhörande argument, som krävs för uppgiften som ska utföras. Valideringen av den data som skickas mellan `checklogin.php` och `admin.swf` finns i både Flash- och PHP-filen. Beskrivning av iterationsproceduren i `checklogin.php`:

Validering av administratörens inloggningsuppgifter:

```
if( isset($_POST['username']) AND isset($_POST['password'])){\
```

Om det är administratörens uppgifter, ...:

```
if(admin){
```

... utför `cmd`-variabeln som administratören angett!:

```
switch($_POST['cmd'])
```

- `case 'aboutusedit'` Om `cmd`-variabeln är lika med strängen "aboutusedit", förväntar sig funktionen ett argument i form av en XML-sträng, som ska sparas i filen `aboutus.xml`.

- **case 'listusers'** Är `cmd`-variabeln lika med "listusers", kommer funktionen att lista en XML-sträng med användarna och deras uppgifter.
- **case 'removefaq'** Ifall `cmd`-variabeln är lika med "removefaq", förväntar sig funktionen ett talvärde från variabeln `$_POST["id"]`, för att ta bort ett faq-element i `faq.xml`.
- **case 'addfaq'** Är `cmd`-variabeln lika med "addfaq", förväntar sig funktionen en XML-sträng (ett faq-element) som ska sparas i filen `faq.xml`.
- **case 'removenews'** Om `cmd`-variabeln är lika med "removenews", förväntar sig funktionen ett talvärde från variabeln `$_POST["id"]`, för att ta bort ett nyhetselement i `news.xml`.

Filen `admin.swf` är en bytekod-applikation, som skapades med hjälp av Flex2 och ActionScript. För att skapa en kommunikation mellan Flash och PHP, användes de funktioner som finns inbyggda i Flash och som står förklarade i Flex2-utvecklingsmiljöns hjälpavsnitt.

När en webbläsare laddar ner en webbsida som innehåller en Flash-applikation, kommer läsaren att kontrollera om filen redan finns i webb-cachen. Om webb-cachen redan innehåller Flash-applikationen, kontrollerar flashspelaren inte om det finns nyare versioner av externa filer till applikationen på webbsidan, och hämtar därför istället filerna från webb-cachen. För att kunna uppdatera företagets webbsida för användare som redan besökt sidan tidigare, används därför ett trick som heter cachebuster. Cachebuster producerar ett unikt `$_POST`-värde varje gång en Flash-applikation startas och lurar på så sätt flashspelaren att hämta de nya externa filerna från webbservern. Ett exempel på en cachebuster för nyhetsfilen på företagets webbsida:

```
var XML_URL:String = new String( "/xml/news.xml?cachebuster=" +
new Date().getTime());
```

6.5.4 MXML- och ActionScript-tjänster

I en Flex2-utvecklingsmiljö kan man använda sig av både MXML- och ActionScript-tjänster. Men ibland är det svårt att skilja mellan dessa båda tjänsters implementation, då en del av tjänsternas bibliotek med funktioner liknar varandra och detta kan ibland medföra både problem och oönskade resultat. Ett exempel, är en http-tjänst som används för att

kommunicera med SOAP eller simplePHP²⁸ För denna tjänst kan två funktioner användas, en från respektive tjänst och bibliotek. Den ena av de båda funktionerna, från biblioteket `mx.rpc.http.HTTPService`, kan emellertid bara användas och definieras med ActionScript-tjänsten, medan funktionen från biblioteket `mx.rpc.http.mxml.HTTPService`, bara kan användas med MXML-tjänsten.

Trots den möjliga förväxlingen mellan olika bibliotek för MXML- och ActionScript-tjänsten, används båda dessa tjänster i Flash-filer på företagets webbsida. Tjänsterna kompletterar varandra i ändamål. ActionScript-tjänsten behöver mer kod, men i gengäld är fel i koden lätta att upptäcka och koden är även lätt att utöka, vilket gör koden lätt att konfigurera. För MXML-tjänsten gäller istället att koden är lätt att implementera, men att funktionaliteten är begränsad.

I figur 34 beskrivs en enkel MXML-http-funktion, som används till att hämta information om användarna från filen `checklogin.php`. Informationen listas i tabellen under tillståndet Användare på administratörens kontrollpanel (se figur 25). Varje tabellelement i Flash kräver en datatillhandahållare, exempelvis i form av `HTTPService` eller en XML-fil. När funktionen i exemplet i figur 34 så är genomförd, innehåller funktionen en XML-sträng, som senare kan hämtas av tabellen med hjälp av dess lyssnare.

²⁸ **SimplePHP** En typ av kommunikation med vanliga textutskrifter för PHP-skripten. Skripten returnerar ett svar till funktionen som efterfrågade tjänsten, i form av en webbsida. PHP skriver ut `true` på webbsidan som läses som en sträng av Flash och som därefter kan tolkas som ett boolskt värde.



```
1. <mx:HTTPService id="userRequestDB"  
url="checklogin.php" useProxy="false"  
method="POST">  
2. <mx:request xmlns="">  
3. <username>{this.adminusername}</username>  
4. <password>{this.adminpassword}</password>  
5. <cmd>{this.listusers}</cmd>  
6. </mx:request>  
7. </mx:HTTPService>
```

Figur 34 Ett exempel på en MXML-http-tjänst



```
1. DBconnect=new HTTPService();  
2. DBconnect.url=("checklogin.php");  
3. DBconnect.useProxy=false;  
4. DBconnect.method="POST";  
5. DBconnect.request.username=adminusername;  
6. DBconnect.request.password=adminpassword;  
7. DBconnect.request.cmd="listusers";  
8. DBconnect.addEventListener(ResultEvent.RESULT,addFaqQuestionOk);  
9. DBconnect.addEventListener(FaultEvent.FAULT,addFaqQuestionError);  
10. DBconnect.send();
```

Figur 35 Ett exempel på en ActionScript-http-tjänst

Koden i exemplet i figur 35 motsvarar samma funktion som är kodad i figur 34, men är skriven i ActionScript. För att starta en kommunikation med andra skript, rad 1 i exemplet,

initieras en ny instans av en http-tjänst. På rad 2 anges vilket skript funktionen ska kommunicera med. Rad 4-7 anger vidare, de utgående \$_POST-variablerna till skriptet på rad 2. På rad 8 läggs en lyssnare till för tjänsten av typen "händelse", `ResultEvent.RESULT`, som anropas då skriptet utfört kommandot och skickat tillbaka värdena till funktionen. För att behandla returvärdena från skriptet vid utfört kommando, anropas sedan en funktion som heter `addFaqQuestionOk`. Rad 9 i koden fungerar efter samma princip som deklarationen på rad 8, fast här används istället en lyssnare för felhantering. Den ovan beskrivna proceduren är grunden för de flesta funktioner som styr både webbsidan på företaget och administratörens kontrollpanel.

7 Resultat

Det i rapporten avhandlade hotspotprojektet utfördes åt företaget Fiber Optic Valley, som är beläget i Hudiksvall. Projektet har varit både lärorikt och givande. Den omfattande uppgiften, med alla olika delar som ingår i hotspoten och all webbprogrammering och webbdesign till företagets hemsida, har i mån av tidsbrist dock inte kunnat färdigställas fullt ut. I nuläget fungerar emellertid betalningssystemet med PayPal samt registreringen för kunderna och även funktionerna till de flesta tillstånden på administratörens kontrollpanel. Enkelheten i de olika webbsidornas konfiguration, har under projektets gång varit ett mål som har prioriterats och som uppnåtts.

Till de brister som återstår att lösas kan den bugg nämnas, som finns i tillståndet ”Nyheter” på administratörens kontrollpanel och som tillåter gamla bilder vara kvar efter att ett nyhetselement tagits bort. Programfelet gör att utrymmet på servern successivt tas upp och därför belastar systemet. En ökande utrymmesbrist påverkar på sikt inte bara möjligheten att lägga till andra nyhetsdata, utan även säkerheten, i form av platsbrist för PHP-sessionsfiler till inloggningssystemet. På grund av tidsbristen har inte heller ett fullständigt systemtest kunnat utföras, med belastning samt säkerhetsluckor, för alla ingående delar sammankopplade i hotspoten. En marknadsundersökning i Hudiksvall, där företaget tänkt bedriva sin marknadsprodukt, är ett annat åliggande som inte genomförts.

Ett huvudmål för hotspotprojektet har varit budgetmålet, att hålla kostnaden för hotspotens hårdvara samt underhållskostnaderna på en låg och acceptabel nivå. Budgetmålet har uppfyllts till fullo, mycket tack vare den billiga hårdvarolösningen, där flashminnet och operativsystemet varit gratis. Genom automatiserad informationsuppdatering till företagets alla webbsidor, har även underhållskostnaderna kunnat hållas låga.

8 Slutsats

För informationen som legat till grund för rapporten, har rikligt med litteratur om den bakomliggande tekniken och säkerheten för en hotspot funnits att tillgå. Men litteratur angående själva tjänsten har varit svår att hitta. Att arbeta med ett område som har en möjlig utvecklingspotential och som är så pass nytt, har varit både en inspiration och en utmaning.

Public IP's hotspottjänster erbjuder ett stadigt system till alla ägare av ett hotspotsystem. Tjänsten som användes till det mindre hotspotsystemet hos Fiber Optic Valley, var lätt att konfigurera och är Public IP's gratislösning. Nackdelen med gratisversionen är emellertid att man saknar full kompatibilitet för de nyaste systemen, med säkerhetslösningar till trådlösa nätverk. Man får heller ingen personlig support, utan erbjuds istället ett diskussionsforum där man själv får söka sina svar. De flesta problem jag haft har jag därför tvingats försöka lösa på egen hand. För att få tillgång till alla systemförbättringar, med kompatibilitet för nya säkerhetslösningar, program för betalningssystemet med mera, får man vända sig till Public IP's systerprojekt, som är en kommersiell lösning. I systerprojektet ingår alla dessa förbättringar samt en personlig support.

Public IP tillåter inte någon inloggning från webbsidor som ligger på andra servrar. Användarens inloggning måste ske direkt via Public IP's kontrollserver. Detta innebär en nackdel om man väljer Public IP's gratislösning, där någon kontroll inte ingår. Användaren som har kännedom om PHP-skripting kan då lätt slinka igenom systemet, utan att ha betalt för tjänsten, genom att använda sig av kodinjektion. Lösningen, för vilken tid saknades, är att implementera företagets inloggningssida med JavaScript och SOAP, för att etablera en kommunikation med företagets server. Med implementerad JavaScript kan användaren omdirigeras till PayPal. Vidare kan en SOAP-funktion styra vad som visas för användaren, beroende på om hon betalt eller inte. Inloggningssidans kommunikation med den egna servern kan också inrättas med hjälp av SOAP.

Det Linux-baserade operativsystemet till hotspoten var en stor ekonomisk fördel och har även varit lätt att omforma och modifiera. En stor fördel med *open source* är traditionen med användare som samlas och delar med sig av sina erfarenheter, samt bistår varandra med eventuella skriptförbättringar, som är tillgängliga för alla att implementera.

Flex2 och PHP fungerade bra ihop på alla företagets webbsidor. Flex2-utvecklingsmiljön är fortfarande i utvecklingsstadiet, med många olika standarder som kan tillämpas för samma uppgift. I Flex2 saknas emellertid ett funktionsbibliotek för kryptering, en grundläggande funktion som ingår i många andra programspråk. För att få upp en säker kommunikation över

nätverket med Flex2, får man därför förlita sig på andra skriptspråk som ligger på samma server. Men Flex2 var en självklar vinnare, vad gäller layoutmöjligheterna och lättheten att skapa en webbsida i en grafisk miljö.

Med mer tid för fininställningen av hotspotsystemet och med bättre support från företaget, hade antagligen resultatet delvis kunnat bli annorlunda. Eftersom jag inte har funnit liknande arbeten om hotspotsystem, anser jag att materialet i rapporten ändå delvis kan vara av intresse. Kanske för ett mindre företag, café eller dylikt, som funderat på att starta en hotspot och som vill få en viss uppfattning om uppgiftens omfång.

Referenser

- [1] Scott Tully, Gary N McKinnedy, Jim Shope, *PublicIp Wireless WiFi Hotspot Control Server*, 2006 . (<http://www.ewcllc.net/files/PublicIP-System-Doc.pdf>)
- [2] Linus Walleij, *Att använda Linux och Gnu*, 2006
- [3] <http://www.debian.org/intro/about> , 2006-10-16
- [4] <http://www.debian.org/misc/children-distros.sv.html> , 2006-10-16
- [5] <http://www.morphix.org/wiki/index.php> 2006-12-3
- [6] <http://www.debian-administration.org/articles/18> 2006-12-3
- [7] <http://ddclient.sourceforge.net/> 2006-12-4
- [8] Pär Hagberg, Alexander Hällström, *Kom igång med webbutvecklingen*, 2002
- [9] Viktor Jonsson, *Webbprogrammering med PHP*, 2001
- [10] W.Jason Gilmore *Beginning PHP 5 and MySQL From Novice to Professional*,2004
- [11] Michael J. Young ,*XML steg för steg 2:A UPPLAGAN*, 2002
- [12] <http://www.adobe.com/products/flex/productinfo/datasheet/>, 2006-12-05
- [13] <https://www.paypal.com/cgi-bin/webscr?cmd=p/pdn/paypal-solutions-outside>, 2006-12-07
- [14] <http://devzone.zend.com/node/view/id/12>, 2006-12-07
- [15] http://en.wikipedia.org/wiki/Secure_Sockets_Layer, 2006-12-10
- [16] Prasad Neel ,*IEEE 802.11 WLANs and IP Networking : Security, QoS, and Mobility*
- [17] *Wireless Networks for Dummies -Lewis, Barry-2005*
- [18] http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy, 2006-12-12
- [19] Dean Tamara , *Network+ 2005 In Depth - -2005*
- [20] Gaskin James, *Broadband Bible (Desktop Edition) -2004*
- [21] http://en.wikipedia.org/wiki/IEEE_802.20, 2006-12-15
- [22] http://en.wikipedia.org/wiki/IEEE_802.16, 2006-12-15
- [23] Ron Olexa,*Impletmenting 802.11, 802,16 and 802.20 Wireless Netowrks* ,2004
- [24] <http://www.w3.org/TR/xhtml1> 2007-01-9/
- [25] Held, Gilbert ,*Virtual Private Networking : A Construction, Operation and Utilization Guide*, 2005
- [26] http://en.wikipedia.org/wiki/IEEE_802.2 2007-1-05
- [27] <http://en.wikipedia.org/wiki/Vpn> 2007-1-05
- [28] <http://en.wikipedia.org/wiki/Openvpn> 2007-1-05
- [29] <http://www.databasteknik.se/webbkursen/databaser/index.html> 2007-1-06

Akronym

API - Application Programming Interface

APT - Advanced Packaging Tool

CD - Compact Disc

CSS - Cascading Style Sheets

DOM - Document Object Model

DPKG - Debian package management system

FAQ - Frequently Asked Questions

FQDN - Fully Qualified Domain Name

GNU - Gnu Not UNIX

GPL- General Public License

HTML- HyperText Markup Language

IEEE- Institute of Electrical and Electronics Engineers

IPN -Instant Payment Notification

LAMP - Linux Apache PHP MySQL

LLC - Logical Link Control

MAC - Media Access Control

Mbps - Mega bits per second

MHz - Mega Herz

MySQL- My Structured Query Language

PSK- Pre Shared Key

RC4 - Rivest Cipher 4

RGB - Red Green Blue

SGML- Standard Generalized Markup Language

SOAP - Simple Object Access Protocol

SQL- Structured Query Language

SSL- Secure Sockets Layer

TKIP -Tempral Key Integrity Protocol

WEP - Wired Equivalent Privacy

WIFI - Wireless Ethernet Compatibility Alliance

WLAN - Wireless Local Area Network

WPA- Wi-Fi Protected Access

XML- Extensible Markup Language

A ZoneCD-automatiserade skript

A.1 Zonecd-unpack.sh

```
#!/bin/bash
#OBS adminstrator?
#this is for remastering zonecd
# Av Adnan Baktirovic
#
if [ "$UID" -ne "0" ]
then
echo "This script must be run as root"
exit 1
fi
if [ -f $1 ]; then
mkdir /mnt/zonecd
killall mysqld
mount -o loop $1 /mnt/zonecd
echo "kopierar zonecd cd till my_cd \n"
cp -Rp /mnt/zonecd /my_cd
echo "avmonterar zonecd \n"
umount /mnt/zonecd
echo "extraherar zonecd mode till temp.iso \n"
extract_compressed_fs /my_cd/mainmod/publicip.mod > ./temp.iso
echo "monterar temp.iso \n"
mount -o loop temp.iso /mnt/zonecd
echo "extraherar mainmode till my_mod \n"
cp -Rp /mnt/zonecd /my_mod
rm -rf /my_mod/.rr_moved
echo "avmonterar \n"
umount /mnt/zonecd
echo "backar up filer \n"
cp /etc/fstab /etc/fstab.backup
cp /my_mod/etc/fstab /my_mod/etc/fstab.backup
cp /my_mod/etc/resolv.conf /my_mod/etc/resolv.conf.backup
cp /my_mod/etc/hosts /my_mod/etc/hosts.backup
cp /etc/resolv.conf /my_mod/etc/resolv.conf
cp /etc/hosts /my_mod/etc/hosts
mount --bind /etc/fstab /my_mod/etc/fstab
mount --bind /etc/mtab /my_mod/etc/mtab
rm -rf /my_mod/.rr*
echo "deb http://ftp.se.debian.org/debian/ stable main non-free
contrib" >
/my_mod/etc/apt/sources.list
echo "deb http://people.debian.org/~dexter php5 sarge" >>
/my_mod/etc/apt/sources.list
echo "loggar in i zonecd du e nu root"
echo "mount /proc" > /my_mod/apt.sh
echo "apt-get update" >> /my_mod/apt.sh
echo "sudo apt-get install php5.0-session php5 libapache2-mod-php5
php5-MySQL php5-
curl php5-gd MySQL-server apache2 apache2-common" >> /my_mod/apt.sh
echo "skriv: sh apt.sh"
chroot /my_mod
```

```
mount /proc
apt-get update
fi
exit 0
```

A.2 cleanup.sh

```
#!/bin/bash
#OBS needs root account
#this is for remastering zonecd
#no sudo use sudo -i to root prompt
#add your network interface as arg 2
if [ "$UID" -ne "0" ]
then
echo "This script must be run as root"
exit 1
fi
if [ -f $1 ]; then
echo "inget kör bara";
#cp /etc/fstab.backup /etc/fstab
cp /my_mod/etc/fstab.backup /my_mod/etc/fstab
cp /my_mod/etc/resolv.conf.backup /my_mod/etc/resolv.conf
cp /my_mod/etc/hosts.backup /my_mod/etc/hosts
cp /my_mod/etc/resolv.conf /my_mod/etc/resolv.conf
cp /my_mod/etc/hosts /my_mod/etc/hosts
cd /
mkisofs -R -U -V "ZoneCD" -P "ZoneCD" -hide-rr-moved -cache-inodes -
no-bak -pad
my_mod | nice -5 create_compressed_fs - 65536 >
my_cd/mainmod/publicip.mod
mkisofs -r -J -b base/boot.img -c base/boot.cat -o publicip.iso
my_cd
rm temp.iso
#rm -rf my_mod
#rm -rf my_cd
fi
exit 0
```


A.3 init.sh

```
#!/bin/sh
#
PUB=`host 'ssl.publicip.net' | cut -d: -f2 | awk '{ print $3}'`
IP=`ifconfig eth0 | grep 'inet addr:' | grep -v '127.0.0.1' | cut -d:
-f2 | awk '{ print $1}'`
echo "10.10.10.1 acreol.dyndns.org" >> /etc/hosts
echo "$IP" "acreo.dyndns.org" >> /etc/hosts
/usr/local/sbin/iptables -I INPUT -p tcp -d 10.10.10.1 --dport 80 -i
eth1 -s 10.10.10.0/24 -j
ACCEPT
/usr/local/sbin/iptables -I INPUT -p tcp -d $IP --dport 80 -i eth0 -
s $PUB -j ACCEPT
/usr/local/sbin/iptables -I INPUT -p tcp -d 10.10.10.1 --dport 443 -
i eth1 -s 10.10.10.0/24 -j
ACCEPT
/usr/local/sbin/iptables -I INPUT -p tcp -d $IP --dport 443 -i eth0
-s $PUB -j ACCEPT
/usr/local/sbin/iptables -I OUTPUT -p tcp -d 10.10.10.0/24 -s
10.10.10.1 -j ACCEPT
/usr/local/sbin/iptables -I OUTPUT -p tcp -d $PUB -s $IP -j ACCEPT
/usr/local/sbin/iptables -I OUTPUT -p tcp -d 10.10.10.0/24 -s
10.10.10.1 -j ACCEPT
/usr/local/sbin/iptables -I OUTPUT -p tcp -d $PUB -s $IP -j ACCEPT
mkdir /mnt/MySQL
mount /dev/sda2 /mnt/MySQL
chmod 755 /mnt/MySQL/*/*/*/*
chmod 755 /mnt/MySQL/*/*/*
chmod 755 /mnt/MySQL/*/*
chmod 755 /mnt/MySQL/*
echo "starting apache"
apache2ctl start &
echo "starting MySQL"
mysqld &
sleep 1
```

B Funktionslista med beskrivningar

B.1 login.php

```
##
# Funktionen tar emot en sträng och rensar den från HTML-
# taggar och annan kod som kan skada databasens integritet.
# @access: public
# @In-parametrar:
#     $value(string): En sträng som ska sparas i databasen.
# @Retur:
#     (string): En stäng inom apostroftecken.
##
quote_smart($value)

##
# Denna funktion kontrollerar post-värdena vid användarens
# inloggning.
# @Access: public
# @In-parametrar:
# @Retur:
#     (boolean) [true,false]: Returvärdet anger om användarens E-
#     post och lösenord matchade inloggningsuppgifterna i
#     databasen.
##
check_login()

##
# Funktionen visar ett inloggningsformulär.
# @Access: public
# @In-parametrar:
# @Retur:
##
show_login_form()

##
# Man kontrollerar om en användares betalda tid fortfarande
# är giltig.
# @Access: public
# @In-parametrar:
#     $email(string): Användarens E-postadress.
# @Retur:
#     (boolean) [true,false]: Om användaren har tid kvar
#     returneras true (sant).
##
CustomerHasPayed($email)
```

```

##
# Eftersom IPN-tjänsten anländer några sekunder efter användaren,
# visas en progressbar som informerar
# användaren om att bekräftelseprocessen är på väg.
# @Access: public
# @In-parametrar:
# @Retur:
##
progressbar()

##
# Vid transaktionsfel informeras användaren om att ett
# tekniskt fel inträffat. En knapp finns också, som låter
# användaren kontrollera transaktionen igen.
# @Access: public
# @In-parametrar:
#     $msg(string): Felmeddelande som man vill visa.
# @Retur:
##
show_wait_form($msg)

```

B.2 ipn_user.php

```

##
# Funktionen är en konstruktör för klassen ipn_user.
# @Access: public
# @In-parametrar:
#     $email (string): Användarens e-postadress.
# @Retur:
##
__construct($email)

##
# Funktionen är en destruktör för klassen ipn_user.
# @Access: public
# @In-parametrar:
# @Retur:
##
__destruct()

```

```

##
# I funktionen valideras e-postformatet.
# @Access: private
# @In-parametrar:
#     $email_value(string): Användarens e-postadress i form av
#                             en sträng.
# @Retur:
#     (boolean) [true,false]: Bekräftar om strängen i
#     $email_value är av e-postformat.
##
valid_email($email_value)

##
# Här kan man lägga till tiden användaren beställde i klassen
# ipn_user.
# @Access: public
# @In-parametrar:
#     $duration(int): Användarens beställda tid angiven i
#     sekunder.
# @Retur:
##
set_amount_time($duration)

##
# Funktionen tar emot en sträng och rensar den från HTML-
# taggar och annan kod som kan skada databasens integritet.
# @Access: private
# @In-parametrar:
#     $value(string): En sträng som ska sparas i databasen.
# @Retur:
#     (String): En stäng inom apostroftecken.
##
quote_smart($value)

##
# I funktionen hämtas information för användaren från
# databastabellen DBTABLE_USERS.
# @Access: private
# @In-parametrar:
# @Retur:
#     (array): Användarens information returneras som en array
##
db_get_user()

```

```

##
# Funktionen bör användas innan användaren länkas till
# Paypal. Funktionen sparar transaktionsinformationen i
# databastabellen DBTABLE_PAYPAL för senare validering. OBS!:
# funktionen rensar användarens tidigare transaktionsinformation
# från DBTABLE_PAYPAL.
# @Access: public
# @In-parametrar:
# @Retur:
#     (boolean)[true,false]: Om informationen sparats i
#     databasen returneras sant (TRUE), annars falskt(FALSE)
##
pre_setup_paypal_user()

##
# Kontrollfunktionen används för att beräkna tiden användaren får
# utifrån summan han betalt på Paypal.
# @Access: private
# @In-parametrar:
#     $amount(int): Summan användaren har betalat.
# @Retur:
#     (int): Tiden användaren har betalt, angiven i sekunder.
##
get_time_from_ammount($amount)

##
# Funktionen beräknar priset användaren ska betala.
# @Access: private
# @In-parametrar:
#     $time(int): Tiden angiven i sekunder.
# @Retur:
#     (float): Summan användaren ska betala.
##
getgrossvalue($time)

##
# Funktionen används för att hämta användarens
# transaktionsinformation från databasen DBTABLE_PAYPAL.
# @Access: private
# @In-parametrar:
# @Retur:
#     (array): En array med användarens transaktionsinformation.
##
get_PDT_info()

```

```

##
# Funktionen tar bort användaren från PublicIP System's databas.
# @Access:private
# @In-parametrar:
# @Retur:
#     (boolean) [true,false]: Returvärde bekräftar om användaren
#     har tagits bort från PublicIP System.
##
publicip_remote_remove_user()

##
# Funktionen används för att registrera en ny hotspot-användare
# på PublicIP.
# @Access: private
# @In-parametrar:
#     $email(string): Användarens e-postadress.
#     $pass(string): Användarens lösenord.
#     $name(string): Användarens namn.
#     $status(int) [0,1]: Användarens kontostatus.
#         0: Aktiverar inte kontot.
#         1: Aktiverar kontot.
#     $expire(string): Kontots giltighetstid.
#     $class(int) [0,1,2,3]: Typ av användare
#         3: Administratör
#         2: Privilegierad användare
#         1: Användare med färre restriktioner
#         0: Användare med skyddat konto
# @Retur:
#     (boolean) [true,false]: Värdet bekräftar om användaren har
#     registrerats.
##
publicip_remote_register_user($email,$pass,$name,$status,$expire,$
class)

##
# Funktionen används som en emulerad webbläsare för fjärråtkomst
# till en webbserver på port 80.
# @Access: private
# @In-parametrar:
#     $host(string): Webbserverns Internetadress (FQDN).
#     $service_url(string): Webbsidans sökväg på webbservern
#         (ex. /login/login.php)
#     $post_parm(string): Post-värden som skickas till
#         servern.
# @Retur:
#     (string): HTML-kod returnerad som en sträng.
##
port80_remote_access($host,$service_url,$post_param)

```

```
##
# Funktionen validerar IPN-data som skickats från Paypal.
# @Access: public
# @In-parametrar:
#     $POST_VARS(array): En IPN-bekräftelse som en array
#                       som innehåller $_POST-värden.
# @Retur:
#     (boolean)[true,false]: Returvärdet bekräftar om IPN-
#                             parametern är giltig.
##
ipn_service_accept($POST_VARS)
```

C MySQL-tabeller (SQL-syntax)

C.1 users

```
CREATE TABLE `users` (  
  `uid` bigint(20) NOT NULL auto_increment,  
  `email` varchar(30) NOT NULL default '',  
  `password` varchar(45) NOT NULL default '',  
  `timeexpire` timestamp(14) NOT NULL,  
  `class` enum('0','1','2','3') NOT NULL default '0',  
  `paid` enum('N','Y') NOT NULL default 'N',  
  `firstname` varchar(30) NOT NULL default '',  
  `lastname` varchar(30) NOT NULL default '',  
  `city` varchar(20) NOT NULL default '',  
  `postaddress` varchar(30) NOT NULL default '',  
  `mac` varchar(40) NOT NULL default '',  
  `country` varchar(20) NOT NULL default '',  
  `telephone` varchar(20) NOT NULL default '',  
  `lastorderdtime` timestamp(14) NOT NULL default '0000000000000000',  
  `token` varchar(40) NOT NULL default '',  
  `remote` varchar(20) NOT NULL default '',  
  `gateway` varchar(20) NOT NULL default '',  
  `timeout` varchar(20) NOT NULL default '',  
  `host` varchar(20) NOT NULL default '',  
  `path` varchar(20) NOT NULL default '',  
  `street` varchar(24) NOT NULL default '',  
  PRIMARY KEY (`uid`),  
  UNIQUE KEY `email` (`email`)  
) TYPE=MyISAM COMMENT='Store user paid y/n information'  
AUTO_INCREMENT=0 ;
```


C.2 ipn_users

```
CREATE TABLE `ipn_users` (  
  `custom` int(10) unsigned NOT NULL default '0',  
  `receiver_email` varchar(60) default NULL,  
  `item_name` varchar(100) default NULL,  
  `item_number` varchar(10) default NULL,  
  `quantity` varchar(6) default NULL,  
  `payment_status` set('Completed','Pending','Failed','Denied')  
default NULL,  
  `pending_reason`  
set('echeck','intl','verify','address','upgrade','unilateral','other'  
' ),  
  `payment_date` timestamp(14) NOT NULL,  
  `gross` varchar(20) default NULL,  
  `mc_fee` varchar(20) default NULL,  
  `tax` varchar(20) default NULL,  
  `currency_code` char(3) NOT NULL default '',  
  `txn_id` varchar(20) default NULL,  
  `txn_type`  
set('web_accept','cart','send_money','subscr_signup','subscr_cancel'  
, 'subscr_failed','subscr_payment','subscr_eot') default NULL,  
  `first_name` varchar(30) default NULL,  
  `last_name` varchar(40) default NULL,  
  `address_street` varchar(50) default NULL,  
  `address_city` varchar(30) default NULL,  
  `address_state` varchar(30) default NULL,  
  `address_zip` varchar(20) default NULL,  
  `address_country` varchar(30) default NULL,  
  `address_status` set('confirmed','unconfirmed') default NULL,  
  `payer_email` varchar(60) default NULL,  
  `payer_status` varchar(10) default NULL,  
  `payment_type` varchar(10) default NULL,  
  `notify_version` varchar(10) default NULL,  
  `verify_sign` varchar(10) default NULL,  
  `referrer_id` varchar(10) default NULL,  
  `id` varchar(10) default NULL,
```

```
`amount` varchar(30) NOT NULL default '',
`business` varchar(30) NOT NULL default '',
`address_country_code` char(3) default NULL,
`address_name` varchar(30) default NULL,
`test_ipn` char(1) default NULL,
`residence_country` varchar(30) default NULL,
`shipping` varchar(5) default NULL,
`payment_gross` varchar(10) default NULL,
PRIMARY KEY (`custom`)
) TYPE=MyISAM;
```