

Gäste W-LAN

Hotspot-Lösung für T-Systems Bremen

Dokumentation der betrieblichen Projektarbeit



Ausbildungsberuf: Fachinformatiker Systemintegration

Durchführungszeitraum: 22.03 – 21.04.2006

Verfasser: Stephan Springer

Prüfung: Sommer 2006

Prüfungsnummer: 1755

Inhaltsverzeichnis

Einleitung	2
1. Projektplanung.....	2
1.1 Projektumfeld	2
1.2 Projektdefinition	2
1.3 Ist-Zustand	3
1.4 Besprechung mit dem Administrator	3
1.5 Sicherheitskonzept	4
1.6 Soll-Konzept	5
2. Projektstart	6
2.1 Ablauf / Zeitplanung	6
2.2 Material / Software	6
2.3 Angebotsvergleich.....	7
2.4 Bestellung.....	7
2.5 Kosten-Analyse	7
3. Projektdurchführung	8
3.1 Netzwerkaufbau / Anpassung	8
3.2 Software Installation	10
3.3 Software Konfiguration	10
3.4 Programmierung.....	11
3.5 Inbetriebnahme/ Funktionstest	12
4. Projektabschluss	14
4.1 Anwenderbroschüre	14
4.2 Betriebsdokumentationen.....	14
4.3 Einweisung der Teams.....	15
4.4 Übergabe des W-LANs	15
4.5 Fazit.....	15
Anlagenverzeichnis	16

Einleitung

Dieses Projekt ist entstanden, da der Leiter der Abteilung ICTS neben dem W-LAN-Netz für Mitarbeiter, ein Netz haben wollte, das einfach und unkompliziert anzuwenden ist. Angesprochen werden sollen vor allem die Menschen, die geschäftlich zu Besuch bei T-Systems sind. Dieses Projekt habe ich als Abschlussprojekt für meine Ausbildung, die ich seit 2003 bei der Deutschen Telekom AG zum Fachinformatiker Systemintegration absolviere, durchgeführt.

Aus Gründen der Sicherheit und des Datenschutzes wurden firmeninterne und geschäftsrelevante Daten, wie z.B. Passwörter, E-Mail Adressen und Benutzernamen nicht erwähnt oder unkenntlich gemacht. Wörter die fett gekennzeichnet sind, werden im Glossar erläutert.

1. Projektplanung

1.1 Projektumfeld

Die T-Systems Enterprise Services GmbH beschäftigt am Standort Bremen 300 Mitarbeiter und gehört dem Konzern der Deutschen Telekom AG an.

Die Aufgabe der Standorte Bremen und Hamburg ist die Entwicklung und Betreuung von Softwarelösungen, hauptsächlich für interne Kunden. Ein Beispiel hierfür ist, die Leitungsüberwachung der T-Com. Seit 2004 bin ich im Rahmen meiner Berufsausbildung in der Abteilung ICTS¹ beschäftigt. Zur Abteilung gehören zwei Disponenten und ein Leiter. Ferner ein Server-Team, welches für die zentralen Server-Dienste nebst Netzwerk zuständig ist, und ein Arbeitsplatz-Serviceteam, das die Anwender und deren PC-Equipment betreut. Neben mir werden hier vier weitere Auszubildende beschäftigt.

1.2 Projektdefinition

Ziel dieses Projektes ist es, Kunden, Gästen und freien Mitarbeitern einen Internetzugang per W-LAN zur Verfügung zu stellen.

Mittels dieser W-LAN-Verbindung könnten die Benutzer, z.B. einen VPN-Tunnel zum eigenen Firmennetzwerk aufbauen. Dieses Verfahren wäre ähnlich dem eines Hotspots, z.B. auf Bahnhöfen, in Hotels und auf Flughäfen. In diesem Fall wäre die Verfügbarkeit des W-LAN-Netzes nur an ausgewählten Punkten, wie z.B. Konferenz- und Präsentationsräume, gewährleistet.

Der Zugang per Kabel soll hingegen permanent verfügbar sein. Für diesen gibt es zwei Anwendungsfälle. Zum einen haben nicht alle Gäste einen W-LAN-fähigen Laptop, zum anderen ist W-LAN fehleranfälliger und langsamer als kabelgebundenes LAN. Für freie Mitarbeiter, die länger bei uns eingesetzt sind, stellt ein normales LAN-Kabel daher die bessere Alternative dar.

Die Umsetzung soll mittels eines Linux-Server-Systems realisiert werden, wofür die Software „Chillispot“ zum Einsatz kommt. Da unsere Abteilung schon in früheren Kundenprojekten gute Erfahrungen mit der Software sammeln konnte, bot sich ein Einsatz auch in diesem Projekt an.

¹ Information and Communication Technologie Service, Supportgruppe der T-Systems

1.2.1 Beschreibung „Chillispot“

„Chillispot“ ist eine klassische Hotspot-Software, die den Zugriff auf eine Internet- / Netzwerkverbindung steuert. Nach Anmeldung des Benutzers am Access Point, bekommt dieser von der „Chillispot“ Software per dynamischer Zuweisung eine IP-Adresse. Die Authentifizierung startet mittels einem vorgeschaltetem Webinterfaces bei Aufruf einer beliebigen Internetseite. Nach Eingabe von Benutzername und Passwort auf der Anmeldeseite, werden diese Daten an einen Radius-Server weitergeleitet. Sind die Anmeldedaten in Ordnung, schaltet die Software die interne Firewall für die Client-IP-Adresse frei. Die Software wird unter **GPL**-Lizenz vertrieben und ständig von den Entwicklern erweitert.



Abbildung 1: Chillispot Logo

1.3 Ist-Zustand

Am Standort Bremen existiert für T-Systems-Mitarbeiter neben dem vorhandenen Firmennetzwerk ein W-LAN-Netz. 29 Access Points der Firma Nortel, die den **IEEE**-Standard 802.11a, 802.11b und **802.3af** unterstützen, sorgen für flächen-deckende Verfügbarkeit des Funknetzes. Für die Authentifizierung der Clients wurde ein **Radius**-Server auf einem Linux-Server-System eingerichtet. Das Verschlüsselungs-verfahren **WPA / TKIP** wird angewandt, um die sichere Kommunikation zwischen den Clients und den Access Points zu gewährleisten.

Das Firmennetzwerk besteht aus einem zentralen Router, an dem Switches angeschlossen sind, die per VLAN auf weitere 16 Subnetze verweisen. Für W-LAN, **DMZ**, **VPN**, **VoIP**-Telefonanlage und Netzmanagement wurden weitere **VLAN**-Netze eingerichtet. (Netzplan [Anhang A](#)).

Dies ermöglicht die Verteilung der Access Points auf den ganzen Standort, als auch die Integration aller Komponenten in einem Subnetz.

Sowohl der DMZ, als auch dem VPN-Server steht eine 2-MBit-Leitung zur Verfügung, welche sich über mehrere IP-Adressenbereiche erstreckt. Als Internet-anbindung des Firmennetzwerks dient ein DSL 6000 Business-Anschluss mit einem Proxy-System, der getrennt vom Konzern-Intranet arbeitet (Netzplan siehe [Anhang A](#)). Für Kunden, freie Mitarbeiter und Gäste gibt es zahlreiche ISDN-Anschlüsse, die eine Verbindung ins Internet ermöglichen. Ein Zugang zum Firmennetzwerk ist für Nicht-Mitarbeiter der Deutschen Telekom AG nicht erlaubt.

1.4 Besprechung mit dem Administrator

1.4.1 Vorbereitung

Für das Gespräch mit dem Systemadministrator, Herrn Robert M. Albrecht, wurde überlegt, welche offenen Fragen noch zu klären sind, damit das Projekt erfolgreich abgeschlossen werden kann. Folgende Fragen sind dabei entstanden:

- Wie viele Zugangspunkte soll es geben?
- Muss neue Hardware für das Projekt beschafft werden?
- Muss ein Verschlüsselungsverfahren für die Kommunikation zwischen Client und Access Points eingerichtet werden?

- Wie sollen die Zugangskennungen für die Benutzer aussehen?
- Wie oft sollen Zugangsdaten gewechselt werden?
- Wie bekommt der Kunde die Daten für die Benutzung?
- VLAN oder eigenes Netzwerk?
- Welche Internetanbindung soll benutzt werden?
- Soll eine Abrechnung der entstehenden Kosten gemacht werden?
- Integration des Servers im vorhandenen Netz?

1.4.2 Besprechung

In der Besprechung ergab sich, dass für das Projekt nur ein Server beschafft werden soll. Die Access Points, für die vier Konferenz- und Präsentationsräume und einen Raum in der Abteilung ICTS, sind noch vom Projekt „Campus W-LAN“ übrig.

Auf den Einsatz von WEP oder WPA sollte verzichtet werden, um die Benutzung für den Kunden möglichst einfach zu gestalten, zumal unsere Kunden im Normalfall ohnehin eine VPN-Lösung benutzen, um sich mit ihrem Firmennetzwerk zu verbinden. Dieses wurde von der Unternehmenssicherheit aber untersagt, so dass WEP eingesetzt werden musste. WPA schied aus, da viele Laptops diese Verfahren noch nicht unterstützen.

Bei den Zugangskennungen und dessen Verteilung hatte Herr Albrecht schon konkrete Vorstellungen. Es sollte einen Benutzernamen und eine vierstellige PIN-Nummer, ähnlich wie bei einer EC-Karte geben. Für Kunden und Gäste, an die die Zugangsdaten ausgegeben werden, soll der Benutzername einen Teil des Abteilungsnamen enthalten, von der sie betreut werden. Die Daten sollten wöchentlich mit einer neuen PIN-Nummer an die Sekretariate via E-Mail versandt werden. Diese haben dann die Aufgabe, für ihre Abteilung, die Kennungen an Kunden und Gäste zu verteilen

Bei der Integration des neuen Netzes in die vorhandene Netzwerkstruktur, soll wie, z.B. bei der DMZ, ein eigenes VLAN auf den Netzwerkkomponenten eingerichtet werden. Herr Albrecht möchte gern, dass die 2-MBit-Leitung-Synchron für das Projekt mitbenutzt wird, wo der Server auch direkt angeschlossen wird. Des Weiteren möchte der Systemadministrator eine Übersicht über erfolgreiche und fehlerhafte Login-Versuche haben, die die Benutzer in einem Monat verursachen, es sollen keine Benutzeraktivitäten mitprotokolliert werden. Außerdem soll das schlichte Design des Webinterfaces noch ansprechender gestaltet werden.

Die laufenden Kosten, die durch die Benutzung der W-LAN entstehen, werden nach Aussage von Herrn Albrecht als Gemeinkosten auf den gesamten Standort umgelegt. (2.5 Kosten-Analyse)

1.5 Sicherheitskonzept

1.5.1 W-LAN

WEP arbeitet mit einer Verschlüsselungslänge von 64 und 128 Bit. Ein 128 Bit-Schlüssel sollte für dieses Projekt ausreichend sein, denn desto mehr Zeichen eingegeben werden, umso höher ist die Fehleranfälligkeit. Als so genannter **Pre-Shared Key** wird ein 13 Zeichen langer **ASCII-Code** erstellt. Der Schlüssel sollte möglichst einfach sein, damit die Benutzung unkompliziert ist. Da WEP-Verschlüsselung schon in allen W-LAN-Geräten implementiert sind, sollte aus Gründen der Kompatibilität nichts gegen den Einsatz dieses Verschlüsselungsverfahrens sprechen.

1.5.2 Server

Der zentrale Linux-Server verfügt über eine permanente Verbindung ins Internet, und ist hierüber auch erreichbar. Um zu verhindern, dass der Server **kompromittiert** wird, bringt die Software „Chillispot“ fertige **IP-TABLEs**-Skripte mit. Die Firewall auf dem Linux-System ist nur über den Port 22 zum Internet hin offen, damit hierüber der Server über **SSH** zu administrieren ist. Das SSH-Protokoll ermöglicht eine sichere, authentifizierte und verschlüsselte Verbindung zwischen zwei Rechnern, über ein unsicheres Netzwerk. Es gibt mehrere Möglichkeiten, um sich am Server einzuloggen. Der Standard ist die Angabe von Benutzername und Passwort. Diese Authentifizierungsmethode bietet Angreifern Gelegenheiten, wie z.B. eine **Brute-Force-Methode** anzuwenden. Um diese Sicherheitslücke zu eliminieren, konfiguriert man den SSH-Dienst auf dem Server dementsprechend, so dass nur noch ein Public-Key-Verfahren zugelassen wird. Dieses Verfahren bietet die Sicherheit auf der einen Seite mittels eines Public-Keys, und auf der anderen Seite die eines Private-Keys. Der Public-Key wird lokal im Home-Verzeichnis des jeweils zugelassenen Benutzers abgelegt. Der Private-Key wird während des Logins mit dem Benutzernamen abgefragt. Um den Root-User besonders zu schützen, sollte das direkte Einloggen unterbunden werden, dies kann man auch in der Konfiguration des SSH-Dienstes einstellen. Unser Haus setzt die Software Tripwire ein, die auch auf diesem System installiert wird, um die Systemintegrität auf Linux-Systemen zu überwachen.

Bezüglich der Ausfallsicherheit wurden keine Anforderungen gestellt. Somit wird auch keine **USV**, **Raid-System** oder Doppelung des Servers benötigt.

1.5.3 Anwendung

Die „Chillispot“ Software benutzt für die Eingabe und Übermittlung der Zugangsdaten einen Webserver. Seitens der Kommunikation zwischen Client und Webserver akzeptiert die Software nur eine verschlüsselte Verbindung via **SSL**. Aus Sicherheitsgründen sollte die Anwendung nicht täglich und rund um die Uhr laufen, sondern nur zu den Arbeitszeiten der Mitarbeiter. Dies verhindert, z.B. nächtliche, über längere Zeiträume, unbemerkte Angriffe.

1.6 Soll-Konzept

Auf der Basis des Sicherheitskonzeptes ergaben sich bei der Besprechung mit Herrn Albrecht noch folgende Aufgaben, wie z.B. das Ergänzen von fehlenden Funktionen. Hierzu zählen: Verschicken von E-Mails, Erstellen der Zugangsdaten und Log-Auswertung. Diese Aufgaben sind in einem Pflichtenheft zusammengestellt, welches im [Anhang B](#) zu finden ist.

Aus Zeitgründen musste das Erstellen des Webinterfaces an einen Mitauszubildenden abgegeben werden. Er wird sich lediglich um die Überarbeitung des Webinterface Layouts kümmern, umso intensiver kann die Arbeit auf den Kern des Projektes konzentriert werden. Am Ende soll das Gäste W-LAN so aufgebaut sein, wie es im Netzplan (*Abbildung 2, Seite 6*) dargestellt ist.

1.6.1 Vorstellung des Soll-Konzeptes

Das ausgearbeitete Soll-Konzept wurde Herrn Albrecht vorgestellt. Er war damit zufrieden und stimmt dem Konzept zu.

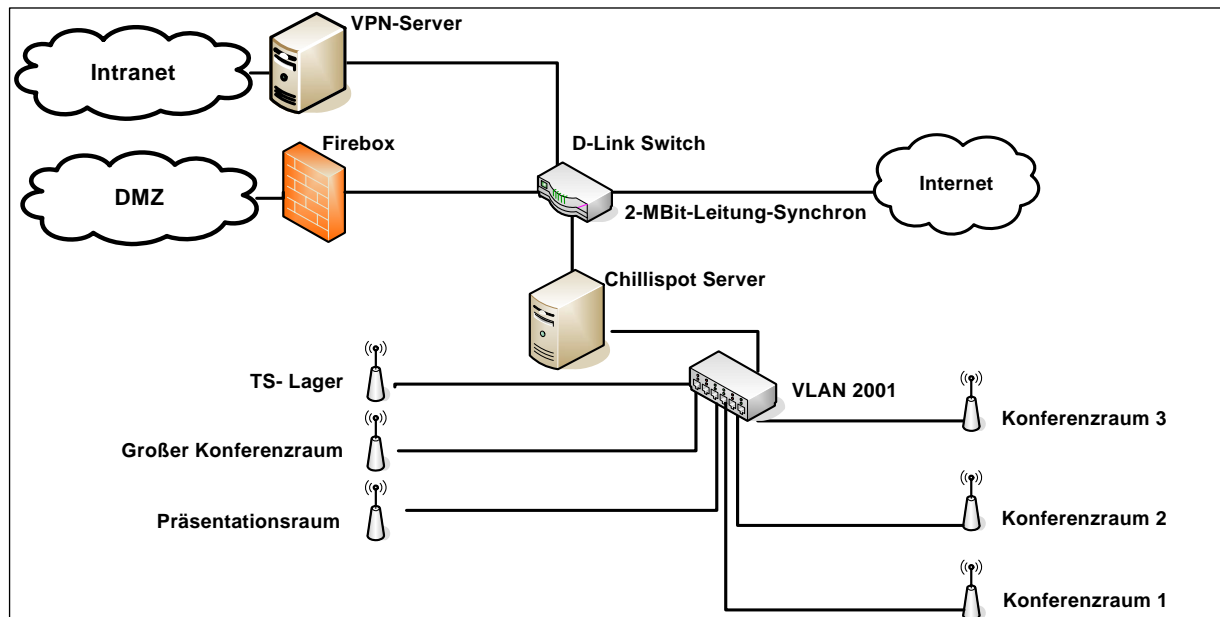


Abbildung 2: Netzplan Gäste W-LAN

2. Projektstart

2.1 Ablauf / Zeitplanung

Die Chronologie wurde mit Hilfe des Programms „MS Project“ erstellt. Dort wurden alle Arbeitsschritte und Zeitfaktoren zusammengefasst, gegliedert und in die richtige Abfolge gebracht. Es wurden insgesamt drei Meilensteine für das Projekt definiert. Geplant waren 35 Stunden, auf mehrere Tage verteilt, da auch noch Lieferzeiten und andere Tätigkeiten berücksichtigt werden mussten. (Projektplan im [Anhang C](#))

2.2 Material / Software

Die „Chillispot“ Software setzt ein Linux-Betriebssystem voraus. Unser Haus verwendet hier immer „Redhat Enterprise“ in der aktuellen Version. Diese Version stellt alle, die vom „Chillispot“ vorausgesetzten Softwarepakete zur Verfügung. Für das Betriebssystem gibt es einen Lizenzvertrag, der es ermöglicht, mehrere Server mit diesem Betriebssystem auszustatten.

Die Software „Chillispot“ kann kostenlos, von der Webseite der Entwickler, bezogen werden, da sie unter **GPL**-Lizenz vertrieben wird. Es entstehen keine weiteren Kosten für die Anschaffung von Software.

Es werden noch insgesamt 16 Patchkabel benötigt, um die Access Points in den Räumen zu verkabeln, und im Patchschrank an die Switches anzuschließen. Vier Kabel werden für den Server benötigt. Dieses Material muss nicht extra bestellt werden, da diese Kleinmaterialien immer vorrätig sind.

2.3 Angebotsvergleich

Es wurden drei Angebote von Firmen eingeholt, die Server-Systeme vertreiben, um zu überprüfen, ob für die Serverhardware, die standardmäßig für alle Server beschafft wird, seit längerem, das Preis-Leistungs-Verhältnis stimmt.

Im Standort sind 90 % der **x86-Server** von der Firma Fujitsu-Siemens im Betrieb. Um die Hardware zu überwachen, wird die Anwendung „ServerView“ eingesetzt.

Da zum Betreiben der „Chillispot“ Software keine besonderen Anforderungen notwendig sind, kommt ein **1HE-19-Zoll-Server** in Betracht. Diese werden in großer Stückzahl für nicht kritische Aufgaben eingesetzt. Ein 3-Jahres-Wartungsvertrag soll bei allen angebotenen Servern dabei sein.

Selbst die kleinsten Server-Systeme haben heute schon CPUs, jenseits der 2 GHz, und ausreichend große Festplatten. Allerdings sind zwei Netzwerkkarten für das Projekt erforderlich, was jedoch auch nichts außergewöhnliches ist.

Es wurden bei den Firmen Fujitsu-Siemens, SUN Microsystems und Maxdata Angebote eingeholt.

Anforderung	Fujitsu-Siemens	Sun Microsystems	Maxdata
Bezeichnung	RX100 S3	Sun Fire X2100	Platinum 820R
CPU	P4 630 / 3 GHz	AMD Opteron 164 / 2 GHz	P4 E / 3 GHz
Arbeitspeicher	512	512	512
Festplatte	80	80	80
CD / DVD	JA / JA	JA / JA	JA / JA
Netzwerkkarten	2x 10/100/1000 MB	2x 10/100/1000 MB	2x 10/100/1000 MB
Wartungsvertrag	3 Jahre	3 Jahre	3 Jahre
Preis inkl. Mwst.	851,15 €	1384,94 €	1281,80 €

Tabelle 1: Angebotsvergleich

Alle Angebote wurden über den zentralen Einkauf angefordert, damit die Firmen interne Rabatte, sofern sie welche anbieten, bei jedem Angebot mit einkalkulieren können. ([Anhang D](#))

Das Angebot von Siemens bietet immer noch das beste Preis-Leistungs-Verhältnis. Daher sprach aus wirtschaftlicher und technischer Sicht nichts dagegen, dieses Angebot weiterhin anzunehmen.

2.4 Bestellung

Alle Bestellungen, die die Abteilung ICTS tätigt, müssen über eine Bestell-Software vorgenommen werden. Auf diese Anwendung haben nur unsere beiden Disponenten Zugriff, sie regeln im Team alle anfallenden Bestellungen. Das Angebot von der Firma Siemens wird an die Disponenten weitergeleitet, welche eine Bestätigung der Bestellung zurücksenden.

2.5 Kosten-Analyse

Um einschätzen zu können, was das ganze Projekt der Abteilung ICTS kostet, werden die einmaligen Kosten, sowie die monatlichen Kosten, die entstehen können, betrachtet. Alle Kosten, die in unserer Abteilung anfallen, werden entweder direkt einer Kostenstelle im Standort zugeordnet oder auf alle Kostenstellen als Gemeinkosten umgelegt

Einmalige Projektkosten

Bezeichnung	Anzahl	Einzelpreis	Gesamtpreis
Access Point	6 x	62,50 €	375,00 €
Server	1 x	851,15 €	851,15 €
Patchkabel	16 x	3 €	48,00 €
Arbeitszeit*	45 x	75 €/h	3375,00 €
Einmalige Gesamtkosten			4649,15 €

Tabelle 2: Einmalige Projektkosten

*Die Arbeitszeit errechnet sich aus meinen 35 Stunden und 10 Stunden die der Kollege benötigt hat, um das Webinterface zu ändern.

Monatliche Betriebskosten

Bezeichnung	Anzahl	Einzelpreis	Gesamtpreis
Strom pro Server	1 x	13,60 €	13,60 €
Kühlung pro Server	1 x	19,50 €	19,50 €
Internetanschluss 1/6	1 x	114,06 €	114,06 €
Traffic 2 GB Volumen (geschätzt)	2000 x	0,03 €/MB	60,00 €
Support Kosten / Arbeitszeit (geschätzt)	2 x	75 €/h	150,00 €
Betriebskosten			357,16€

Tabelle 3: Monatliche Betriebskosten

Der Internetanschluss wird zum größten Teil für die DMZ benutzt, daher werden die monatlichen Kosten aufgeteilt. Die DMZ = 4/6, VPN-Server und Gäste W-LAN je 1/6. Die Supportkosten sind zunächst geschätzte Werte, da zurzeit noch keine Informationen vorhanden sind, wie viel technische Unterstützung notwendig sein wird. Zurzeit ist noch nicht bekannt, wie intensiv das Gäste W-LAN von den Kunden genutzt wird. Aus diesem Grunde wird das Datenvolumen eines Normal-DSL-Kunden (2 GB pro Monat) als Basis genutzt.

3. Projektdurchführung

3.1 Netzwerkaufbau / Anpassung

3.1.1 IP-Adressen / Namensgebung

Die „Chillispot“ Software arbeitet für das interne Netz mit privaten Class C-Adressen. Wegen der Benutzerfreundlichkeit bekommen alle Access Points eine statische IP-Adresse zugewiesen. Die 217.6.255.x-Adressen gehören zu den IP-Adressen, die zu den 2-MBit-Internetanschluss gehören. Dies kann unter <http://www.ripe.net/> eingesehen werden.

Bezeichnung	IP Adresse
Server eth0	217.6.255.44
Server eth1	192.168.182.1
DHCP Adresse Pool	192.168.182.2 – 192.168.182.199
Access Points	192.168.182.200 – 192.168.182.254

Tabelle 4: IP-Adressen für das Gäste-W-LAN

3.1.2 Einrichtung der Ports und des VLANs

Als erstes mussten die Standorte der Access Points und des Servers bestimmt werden, um die dafür nötige Patchdose zu ermitteln.

Da die Geräte **PoE** unterstützen, musste nicht darauf geachtet werden, ob eine Steckdose vorhanden ist. Den Strom bekommen sie durch den Nortel Baystack 460-24T Switch, die Geräte unterstützen auch PoE. Das Einrichten der VLAN pro Port musste auf den beteiligten Switch und den zentralen Router eingerichtet werden. Wichtig dabei ist, dass nicht nur die Ports, wo die Access Points dranhängen, in das VLAN kamen, sondern auch die Up-Link-Ports von den Switchen.

Die Switches konnten komfortabel über eine Managementsoftware (*Abbildung 3*) konfiguriert werden. Das neue VLAN bekommt den Namen: VLAN2001.

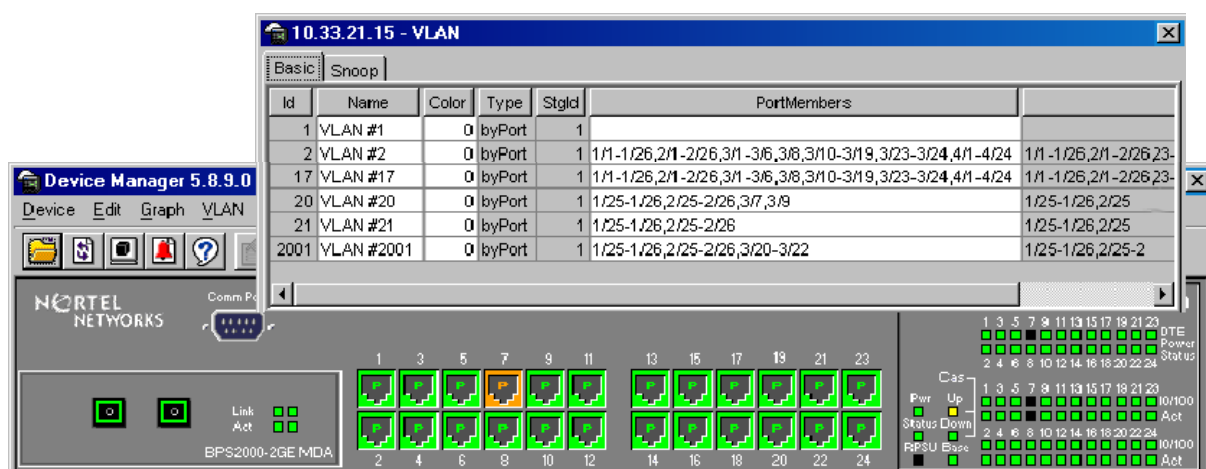


Abbildung 3: Nortel-Switch Manager – VLAN bei einem BayStack 460-24T

3.1.3 Konfigurieren der Access Point

Die Access Points wurden über ein Browser-Menü konfiguriert. Zuerst wurde das Standard-Passwort durch ein eigenes ersetzt. Alle bekamen eine feste IP, die gleiche SSID und den gleichen WEP-Key. Jedem Access Point konnte noch eine Standort-Information eingegeben werden, z.B. Konferenzräume 3. Nähere Informationen dazu sind in der Installationsanleitung. ([Anhang E](#))

3.1.4 Hardware Installation

Nach dem Erhalt der Server durch den Lieferanten wurde die Bestellung auf Vollständig- und Richtigkeit überprüft. Die bestellte Ware entsprach der Bestellung.

Das Einbauen in das Siemens Rack verlief reibungslos. Das eine Interface „eth1“ wurde mit Switch-Port verbunden, an dem das „VLAN 2001“ eingerichtet ist. Das zweite Interface „eth0“ wurde mit dem Switch (D-Link) verbunden, welches die Internetleitung zur Verfügung stellt. (siehe dazu Netzplan im [Anhang A](#) und *Abbildung 2, Seite 6*)

Das Aufstellen der Access Points verlief ohne Probleme, da sie nicht aufwendig an einer Wand oder ähnliches montiert werden mussten.

3.2 Software Installation

Bei der Installation des Betriebssystems wurde der Apache Webserver und der Radius-Server mitinstalliert. Die Konfiguration des Interface „eth0“, mit der IP-Adresse 217.6.255.44, wurde während der Installation getätigt. Mehr Information dazu in der Installationsanleitung ([Anhang E](#)). Die Installation der Software „Chillispot“ wurde direkt aus dem Internet vorgenommen.

```
rpm -i http://www.chillispot.org/download/chillispot-1.0.i386.rpm
```

Die Installation war damit vollständig abgeschlossen.

3.3 Software Konfiguration

Anhand der leicht verständlichen Konfigurationsanleitung, die bei der „Chillispot“ Software dabei war, konnte diese sehr gut umgesetzt werden. Beschrieben wurde, wie der Radius-Server konfiguriert wird und welche Einstellungen am System vorgenommen werden mussten.

Als nächsten Schritt mussten alle Programme so im System integriert werden, dass sie bei einem Neustart des Systems wieder zur Verfügung stehen. Diese wurde unter anderem mit dem Programm „ntsysv“ (*Abbildung 4*) konfiguriert. Die benötigten Dienste wurden hier nur ausgewählt und standen dann beim nächsten Neustart zur Verfügung.

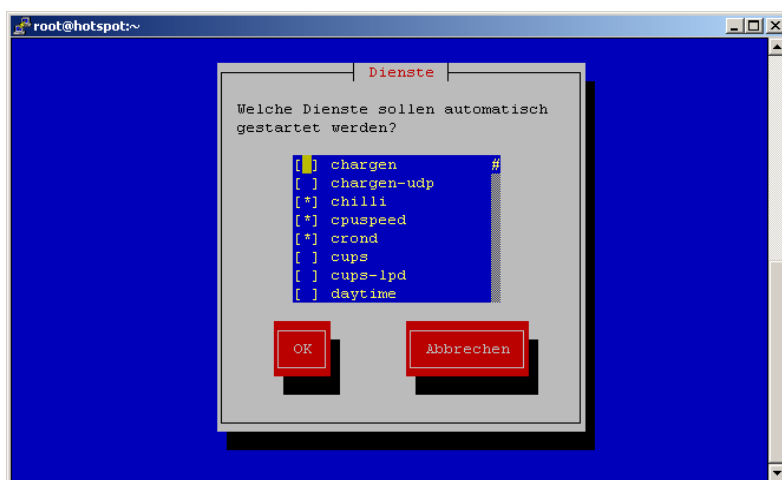


Abbildung 4: ntsysv, setzt Dienste in den Autostart

Da die Anmeldung nur zu einer bestimmten Zeit möglich sein soll, also nicht rund um die Uhr, stellt man den Dienst „Chillispot“ mit Hilfe von „Cronjob“ ab und am nächsten Tag wieder an. Das regelmäßige Versenden der neuen Zugangsdaten wird später auch so realisiert. (*Abbildung 5*)

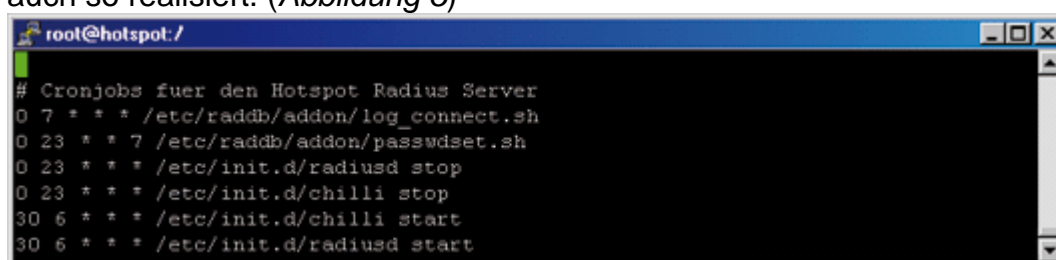


Abbildung 5: Auszug aus dem Crontab Tabelle vom Hotspot-Server

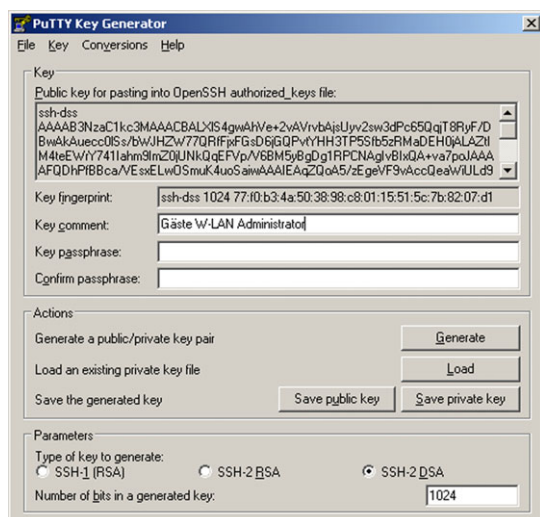


Abbildung 6: Putty Key Generator

Im nächsten Schritt musste der Mail-Dienst eingerichtet werden, z.B. Sendmail, damit die E-Mails vom System verschickt werden können. Der Mitauszubildende übergab das neue Layout des Web-interfaces, welches dann das Standard-Layout ersetzt hat. Als nächstes musste noch der SSH-Dienst mit Public- und Private-Key konfiguriert werden. Dafür wurde zunächst mit dem Programm „Putty Key Generator“ (Abbildung 6) das Schlüsselpaar erstellt. Als Parameter wurde „SSH-2 DSA“ mit einer Schlüssellänge von 1024 Bit ausgewählt. Optional kann ein Passwort für den „Private-Key“ vergeben werden. Der Public-Key wurde auf das

Linux-System unter „/home/Benutzer/.ssh/authorized_keys“ abgelegt. In der Datei „/etc/ssh/sshd_config“ wurde noch die Parameter für das Verbot der Passwordeingabe, das Unterbinden des „root-login“ und das der Authentifizierungsmethode mittels Key konfiguriert.

3.4 Programmierung

Für das Projekt wurden noch zwei Shell-Skripte und zwei Programme geschrieben. Das eine Programm generiert eine vierstellige PIN-Nummer und berechnet einen Datum-Zeitraum. Das zweite Programm war eigentlich nicht geplant, da erst angenommen wurde, dass man das Datum auslesen kann und dann die Variabel um sieben erhöht. Dies führte zu einem Problem, weil es dann auch Monate mit 34 Tage und mehr gab, und das Jahr 13 Monate hatte.

3.4.1 Planung

Passwortsript

Das Skript musste dafür sorgen, dass der Radius-Server neue Anmeldedaten bekommt und dass die Benutzer sie per Mail erhalten. In der Mail sollen die Zugangsdaten stehen, sowie der Zeitraum, von wann bis wann die Daten gültig sind. Damit unsere ICTS-Hotline für Notfälle oder Störungen alle PIN-Nummern hat, soll es eine gesamte Liste aller Benutzernamen und PIN-Nummern geben, die dann auch versendet wird.

Der PIN-Generator sollte per Zufallsprinzip die PIN generieren und sie dann ausgeben; dies konnte im Shell-Skript weiterverarbeitet werden. Auf eine Überprüfung der PIN-Nummer, bezüglich der Gleichheit wurde verzichtet, da dieses nur ein Teil der Zugangskennung ist, und die Wahrscheinlichkeit gering, dass die gleichen Zahlen mehrmals vorkommen.

Für den Zeitraum vom Datum wurde ein Programm so programmiert, dass der jeweilige aktuelle Monat, die exakte Anzahl der Tage hat, die kalendarisch vorgegeben sind. Auch ein Schaltjahr musste beachtet werden. Die Ausgabe wird so ausgelegt, dass es gleich in das Shell-Skript übernommen werden konnte.

Log-Auswertung

Der Radius-Server protokolliert seine Anfragen in eine Log-Datei. Das Skript muss nun aus dieser Datei die fehlerhaften und erfolgreichen Logins auslesen und diese Information per E-Mail verschicken.

3.4.2 Umsetzung

Linux hat alle Tools um die Anforderungen von den Skripten umzusetzen. Die beiden Programme konnten in Programmiersprache „C“ geschrieben werden. Dazu benötigte man nur einen ganz normalen Editor. Das Kompilieren der Programme unter Linux verlief ohne Probleme.

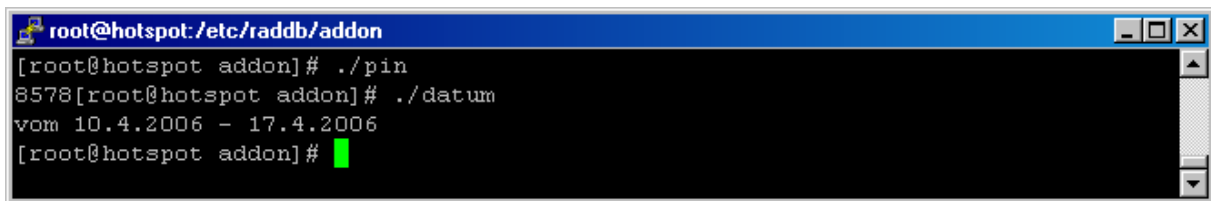
Der Code der Programme und der Skripts befinden sich im [Anhang F](#).

3.4.3 Test

Damit man die Shell-Skripte, die Programme und Linux ausführen darf, müssen die Rechte der Skripte noch geändert werden. Dies wurde in Linux mit dem Befehl „*chmod*“ realisiert:

```
chmod 755 pin datum
```

Bei den Tests der beiden Programme ergab sich folgende Ausgabe (*Abbildung 7*):

A screenshot of a terminal window with a blue title bar that reads 'root@hotspot:/etc/raddb/addon'. The terminal shows the following commands and output: '[root@hotspot addon]# ./pin' followed by '8578', '[root@hotspot addon]# ./datum' followed by 'vom 10.4.2006 - 17.4.2006', and finally '[root@hotspot addon]# ' with a green cursor. The terminal has standard window controls on the right side.

```
root@hotspot:/etc/raddb/addon
[root@hotspot addon]# ./pin
8578
[root@hotspot addon]# ./datum
vom 10.4.2006 - 17.4.2006
[root@hotspot addon]#
```

Abbildung 7: Programmausgabe von „pin“ und „datum“

Beim Testen der beiden Skripte, mussten wenige kleine Fehler behoben werden, damit beim Testdurchlauf nicht jedes Mal die Sekretariate eine Mail bekommen, wurden diese deaktiviert. Beispiele zu der Log-Auswertung, zu den E-Mails die zum Sekretariat versendet werden und der PIN-Liste, befinden sich im [Anhang G](#).

3.5 Inbetriebnahme/ Funktionstest

Während der Inbetriebnahme und Testphase mussten folgende Punkte getestet werden:

- Das Hochfahren der Dienste nach einem Neustart
- E-Mail-Versand
- Anmeldung an den Access Points
- Anmeldung am Hotspot
- Zugangsmöglichkeit per Kabel
- Passwort-Skript
- Logauswertung-Skript
- SSH-Verbindung
- Webinterface (siehe Abbildungen 9 und 10)

Beim Testen des Verbindungsaufbaus passierten intern mehrere Schritte, die anhand des Ablaufplanes verdeutlicht werden sollen (*Abbildung 8*).

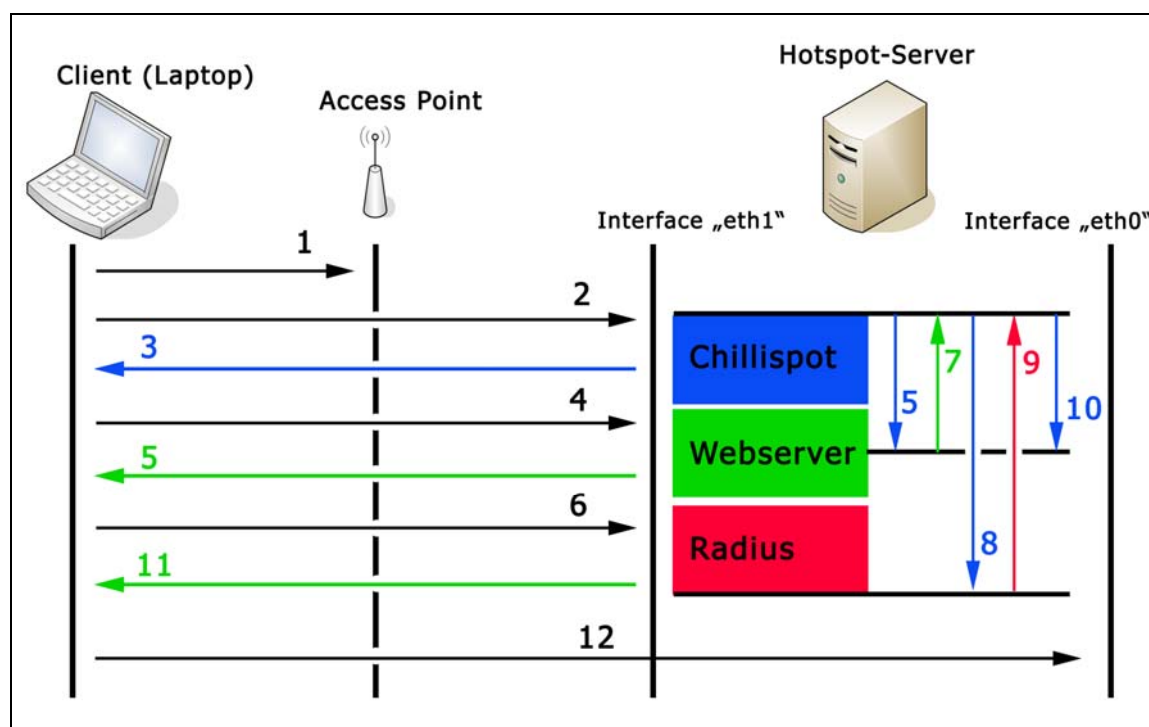


Abbildung 8: Anmeldevorgang im Gäste W-LAN

1. Client meldet sich beim Access Point mit WEP-Schlüssel an.
2. Danach sendet er eine Anfrage für eine IP-Adresse per **Broadcast** ins Netzwerk.
3. Der Server mit dem „Chillispot“ Dienst antwortet mit einer IP-Adresse.
4. Als nächsten Schritt muss der Client eine Internetseite öffnen, er sendet seine Anfrage an das **Gateway**.
5. Der Chillispot Dienst erkennt die Anfrage und speichert diese zwischen. Der Webserver wird von dem „Chillispot“ Dienst angewiesen, dem Client das Anmeldeformular (*Abbildung 9, Seite 14*) zu übermitteln, welches mittels eines „**CGI**“ Skript realisiert ist.
6. Wurden die Anmeldedaten eingegeben, übermittelt der Client die Anmeldedaten an den Webserver.
7. Das Skript wiederum, übermitteln die Daten dann an den „Chillispot“ Dienst.
8. Dieser leitet die Daten für die Authentifizierung an den „Radius“ Dienst weiter.
9. Der „Radius“ Dienst prüft die Daten und sendet sein Ergebnis wieder zurück.
10. Nun entscheidet der „Chillispot“ Dienst anhand der Daten, vom „Radius“ Dienst, und leitet seine Entscheidung an das „CGI“ Skript.
11. Das Skript liefert entweder das Logout Fenster (*Abbildung 10, Seite 14*) und die Internetseite, die der Client am Anfang angefragt hat, aus, oder die Anmeldeseite mit einer Fehlermeldung (Login Fehlerhaft).
12. Wenn das Login erfolgreich war, hat der „Chillispot“ Dienst die Client IP-Adresse freigeschaltet und leitet (routet) nun alle Datenpakete vom Client weiter an das zweite Interface.

Beim Logout wird eine Meldung an das „CGI“ Skript gesendet, welche dann beim „Chillispot“ Dienst die Sperrung der IP-Adresse veranlasst.



Abbildung 9: Anmeldeformular



Abbildung 10: Nach erfolgreichen Login

Bei dem Test „Zugangsmöglichkeit per Kabel“ wurde anstelle eines Access Points ein Laptop mit dem Port verbunden. Alle Tests, die mit Clients zutun haben, wurden mit drei verschiedenen Laptop-Modellen getestet. Unterschiedliche Anwendungen, wie z.B. E-Mail und VPN-Client wurden ausprobiert. Alle Tests konnten erfolgreich abgeschlossen werden. Um spätere Neuinstallationen zu erleichtern, wurden die Skripts, die Programme und das neue Webinterface zu einem Add-On zusammengefasst.

4. Projektabschluss

4.1 Anwenderbroschüre

Schritt für Schritt wird anhand eines Beispiels erklärt, wie man vorzugehen hat, um eine Verbindung zum Gäste W-LAN aufzubauen. Da es viele unterschiedliche Geräte gibt, ist es schwer den richtigen Mittelweg zu finden. Letztendlich wurde sich für eine W-LAN-Karte entschieden, um daran das Beispiel gut erklären zu können. Die Broschüre befindet sich im [Anhang H](#).

4.2 Betriebsdokumentationen

In der Abteilung ICTS werden die meisten Dokumentationen schon in digitaler Form abgelegt. Möglich wird dieses durch zwei Anwendungen: Software „PHD¹“ und „GS Tool²“. Das Programm „PHD“ wird verwendet, um Hardware zu inventarisieren; man kann dort z.B. Seriennummern, Standorte und Produktbezeichnungen eingeben. Für technische Feinheiten und Konzepte wird das Programm „GS Tool“ benutzt, welches vom Bundesamt für Sicherheit in der Informationstechnik vertrieben wird. Dort werden alle Sicherheitskonzepte und wichtige Informationen für die Systeme abgelegt.

Für das Linux-Server-System und dem Access Point wurde eine Installationsanweisung angefertigt, die für eine eventuelle Neuinstallation zu benutzen ist.

¹ Produktions Help Desk

² Grundschutz Tool <http://www.bsi.de/gstool/index.htm>

4.3 Einweisung der Teams

Bei der Einweisung waren die Administratoren vom Server-Team anwesend, so wie zwei Leute aus dem Arbeitsplatz-Serviceteam. Das Server-Team wurde speziell in die Hardware, wie Access Point und den Server eingewiesen, die andere Gruppe hingegen, sollte den Support beim Benutzer gewährleisten.

4.4 Übergabe des W-LANs

Die Übergabe erfolgt an den Hauptverantwortlichen, Herrn Albrecht. Dieser möchte im Anschluss an das Projekt eine vierwöchige Testphase beginnen, in der Testbenutzern das System zum Ausprobieren angeboten werden soll. Anschließend werden die Nutzer gebeten einen Fragebogen auszufüllen, in dem sie Verbesserungsvorschläge und aufgetretene Fehler dokumentieren und beschreiben können.

4.5 Fazit

Während der Projektdurchführung stellte sich heraus, dass der Zeitaufwand für einige Punkte anders eingeschätzt war. Vor allem bei dem Projektabschnitt „Programmieren“ wurde für einige Dinge länger gebraucht als erwartet. Die Berechnung des Datum-Zeitraumes war schon etwas komplexer als vorher angenommen. Weniger Zeit wurde für die Erstellung des PIN-Generators und der Konfiguration der Software benötigt. Am Ende ergaben sich lediglich minimale Veränderungen bei der Zeitplanung.

Ansonsten verlief das Projekt ohne größere Komplikationen und es konnten alle Punkte die im Pflichtenheft aufgeführt waren, erreicht werden. Die Entscheidung, die „Chillispot“ Software zu nutzen, hat sich als richtig herausgestellt. Die Software lässt sich leicht konfigurieren und ist einfach in der Handhabung.

Ich hätte noch gerne eine Benutzerverwaltung mit Hilfe von PHP eingerichtet, so dass man die Benutzer und Verteiler komfortabler einrichten kann. Dieses war im Rahmen des Projektes jedoch nicht mehr realisierbar und wird eventuell später umgesetzt werden.

Das Projekt hat sehr viel Spaß gemacht. Ich habe viel durch dieses Projekt gelernt und bin schon gespannt wie die Testphase verläuft, und wie das W-LAN-Netz bei den Benutzern ankommt.

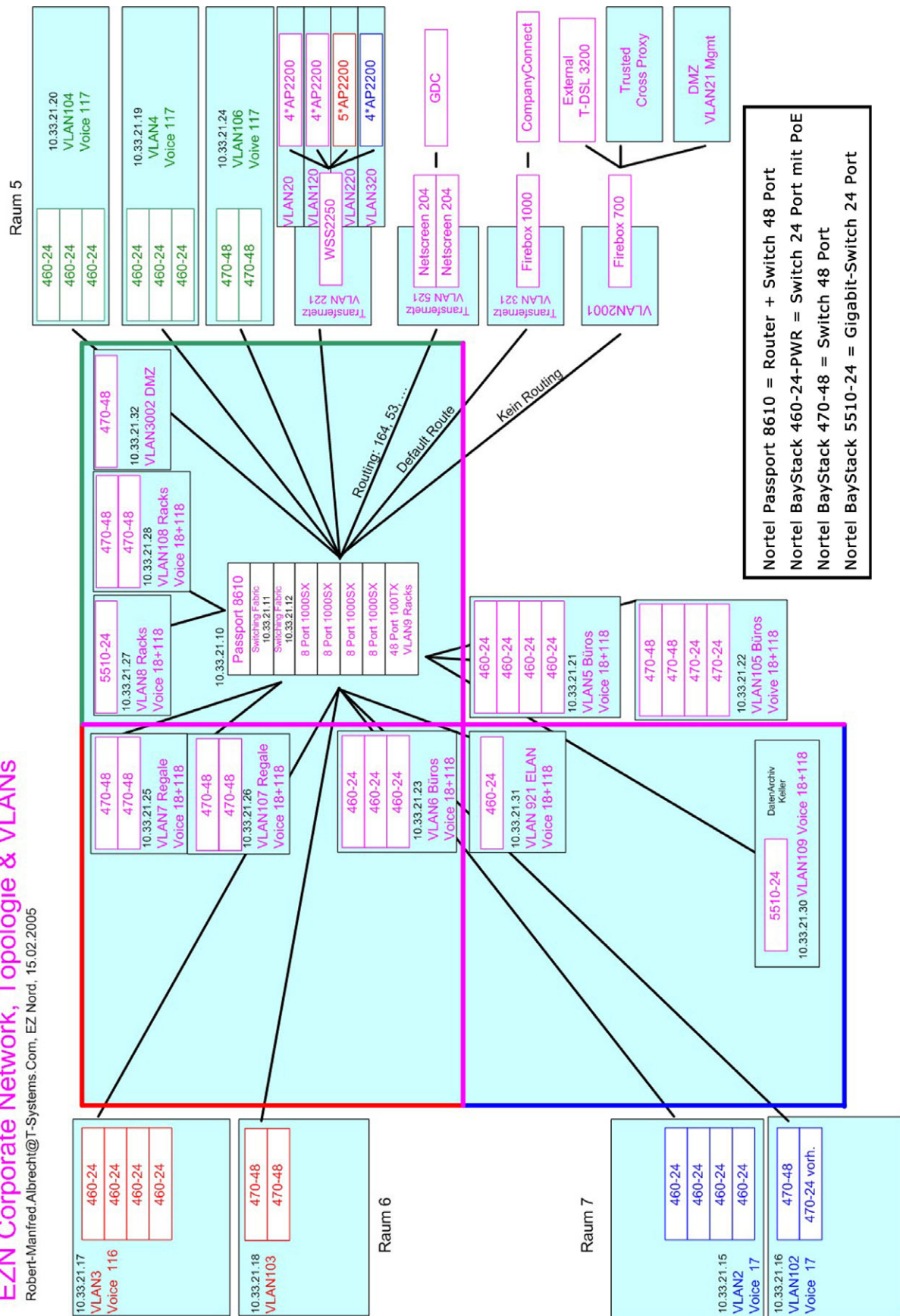
Anlagenverzeichnis

Anhang A : Netzplan	17
Anhang B : Pflichtenheft	18
Anhang C : Projektplan	19
Anhang D : Angebote	20
Anhang E : Gäste W-LAN Server Installation	25
Anhang F : Programm Code & Shell-Skripte	29
Anhang G : E-Mail, PIN-Liste und Logauswertung	32
Anhang H : Anwenderbroschüre	34
Anhang I : Glossar	35
Anhang J : Literatur-, Abbildung- und Tabellenverzeichnis	36
Anhang K : Eidesstattliche Erklärung	37

Anhang A

EZN Corporate Network, Topologie & VLANs

Robert-Manfred.Albrecht@T-Systems.Com, EZ Nord, 15.02.2005



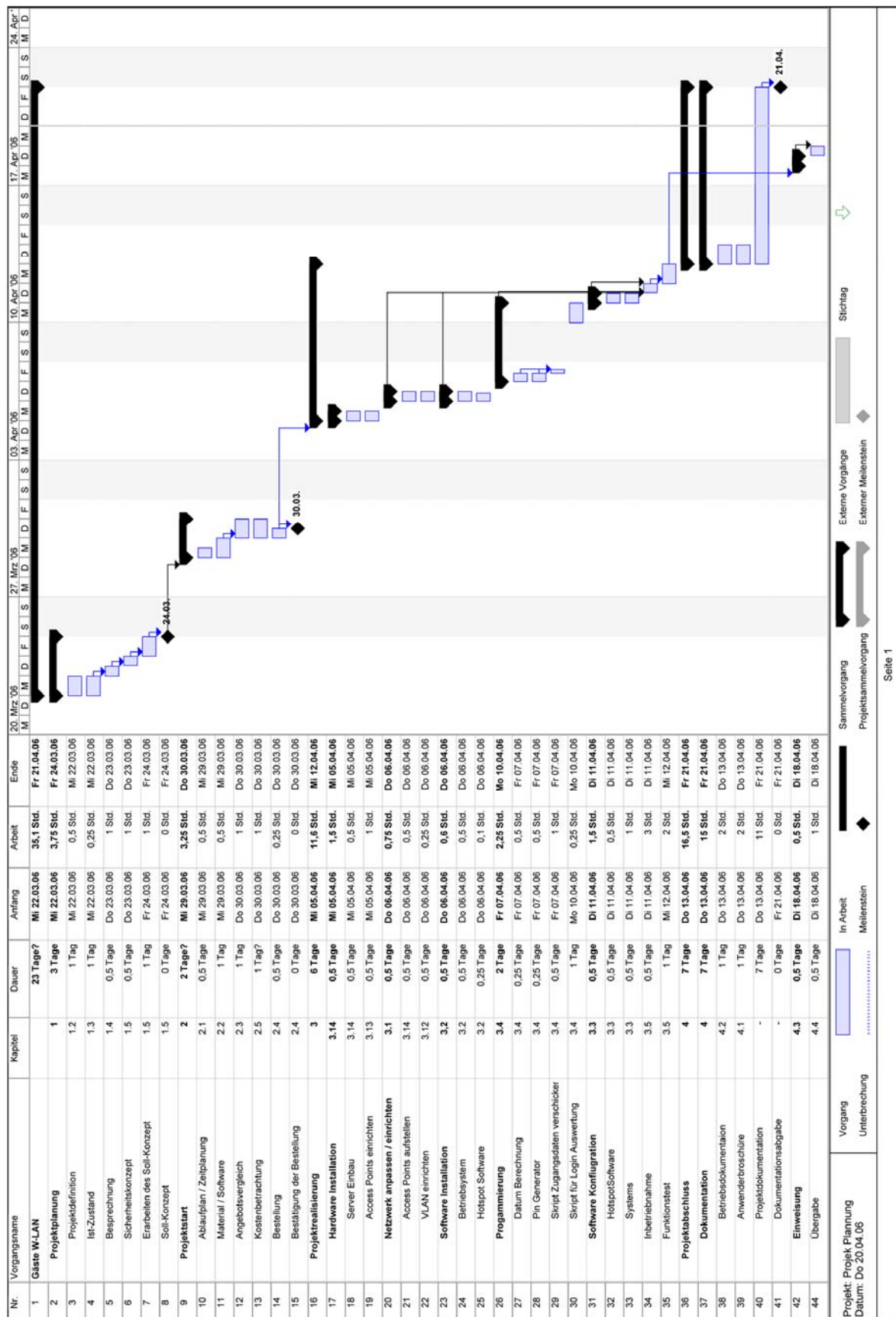
Anhang B

Pflichtenheft – Projekt Gäste W-LAN

Beschreibung	Anforderung	Zusatz
Hardware	Beschaffung Server	Angebotsvergleich/ Bestellung
	Installation Server in Rack	Serverraum
	Aufbau / Konfiguration AP	Konferenzräume Präsentationsraum Abteilung ICTS
	Einrichten VLAN	Netzkomponenten
Software	Betriebssystem Installation	
	Anwendungssoftware	Chillispot
	Konfiguration System/ Anwendung	Sendmail, SSH
Programmieren	PIN-Nummer Generator	„C“ Programm
	Datum-Zeitraum Berechnung	„C“ Programm
	Verteilersskript Zugangsdaten	Shell-Skript
	Auswertungsskript	Shell-Skript
Testen / Qualitätskontrolle	Linux-Server-System	
	Access Points	WEP
	An- und Abmelden	Webinterface
	Anwendersoftware	E-Mail, VPN
Dokumentation / Einweisung	Betriebsdokumentation	PHD, GS-Tool
	Anwenderbroschüre	
	Installationsanleitung	Server, AP
	Einweisung des Teams	

Anhang C

Projektplan



Anhang D

Angebot per E-Mail von Fujitsu-Siemens

Pos.	Produktnr.	Anz.	Bezeichnung	Listenpreis	Rabatt	Kaufpreis	Summe(Netto)
1	S26361-K968-V311	1	PY RX100S3/ P4 630/512M	1.095,00	50,00	547,50	547,50
2	S26361-F3123-E1	1	CD-RW \ DVD ATAPI slimline	105,00	25,00	78,75	78,75
3	S26361-F3218-E80	1	HD SATA 3Gb/s 80GB 7.2k hot plug 3.5"	95,00	50,00	47,50	47,50
4	S26361-F3199-E2	1	Option hot-plug Festplatten RX100S3	55,00	25,00	41,25	41,25
5	S26361-E395-E1	1	PCI-X riser für RX100 S3	25,00	25,00	18,75	18,75
6	W0	1	Standard Garantie 36 Monate ohne festgelegte Wiederherstellzeit (0,%)	-	0,00	-	-
	Summe						733,75

Sehr geehrte [REDACTED],
anbei die Preisübersicht für o.g. Angebot.

HINWEIS: - Die drei Systeme sind fast gleich. RX100S3 mit AMD Prozessor können wir nicht anbieten. Im Angebot Alternativ RX220.

Bei Rückfragen oder Bestellungen bitte immer die Angebotsnummer angeben.

Angebotsanfragen bitte an: abrufbox@fujitsu-siemens.com

Vorbehaltsklausel:

FSC ist nicht verpflichtet Lieferungen und andere Verpflichtungen aus einem Angebot, Vertrag oder einer Auftragsbestätigung durchzuführen, falls FSC hieran durch geltende Exportvorschriften der Bundesrepublik Deutschland, der EU, der USA oder anderer Länder gehindert ist."

Diese Konditionen haben nur für Eigenbedarf Gültigkeit. Basieren auf dem derzeit gültigen X86-Rahmenvertrag.

Aufträge bitte direkt an unser Logistikfax 089/3222-329 2299 (Achtung neu !!) senden.

Mit freundlichen Grüßen

[REDACTED]

Fujitsu Siemens Computers GmbH

Rathausplatz 3-7
61348 Bad Homburg

Telefon: 06172-188 6003
Telefax: 06172-188 9722

e-Mail: [REDACTED]@fujitsu-siemens.com



ANGEBOT

Sun Microsystems GmbH -- Sonnenallee 1 -- D-85551 Kirchheim-Heimstetten

T-Systems Enterprise Services GmbH

Witteststr. 30H
13509 Berlin
GERMANY

Angebotsnummer: T-DE-145786-A

Angebotsdatum: 28.03.06

Angebotsgültigkeit: 30 Tage

Lieferzeit:

**Ihr
Ansprechpartner:**

Sun Microsystems GmbH
SunCenter Quotes - vt
Sonnenallee 1
85551 Kirchheim-Heimstetten
Tel/Fax: 0800 - 10 10 147 /
06103 - 752299

**Bitte bei Bestellung stets die
Angebotsnummer angeben**

Preise im Überblick

Pos.	Beschreibung	Gesamt-Nettopreis
1	Sun Fire X2100	1.193,91 EUR
Gesamtsumme netto		1.193,91 EUR
MwSt. 16%		191,03 EUR
Endsumme:		1.384,94 EUR

Eine detaillierte Aufstellung aller Komponenten finden Sie auf den Folgeseiten.

BITTE SENDEN SIE IHRE BESTELLUNG AN DIE FAX-NR. 06103/752-299.
Es gelten die vertraglich vereinbarten Bedingungen des OSYS III Rahmenvertrages Nr. 9000123592 0004 R.
Dieses Angebot wurde elektronisch erstellt und versandt. Es ist deshalb ohne handschriftliche Unterschrift gültig.

Amtsgericht München: HRB 76513
Geschäftsführer:
WEEE-Reg.-Nr.: DE 20803943
Bankverbindung: HypoVereinsbank München, Konto 31 625 009, BLZ 700 202 700

Angebots-Nr: T-DE-145786-A

Sun Microsystems GmbH

Seite 1 von 2



Aufstellung im Detail

Pos.	Modell	Anz.	Beschreibung	Nettopreis
Sun Fire X2100 bestehend aus: Position 1				1.193,91 EUR
Eigenbedarfskonditionen (VEU/Outsourcing)				
1		1	Configuration: A75-LYB1-N-512-AL8	1.193,91 EUR
1.1	A75-LYB1-N-512-AL8	1	Sun Fire X2100 x64 Server: 1x AMD Opteron Modell 146 Prozessor (2.0 GHz/1 MB), 1x 512 MB unbuffered ECC PC3200 DDR-400 Speicher, keine Festplatte, ohne DVD, 2x 10/100/1000 Ethernet Anschlüsse, 6x USB 2.0 Anschlüsse, 1x PCI-Express x8 Slot, ohne Stromkabel (geo-spezifische X-Option zu bestellen). Standardkonfiguration.	
			Einzel-Listenpreis: 654,23 EUR Rabatt: 5.00%	621,51 EUR
1.2	X8082A	1	DVD-ROM Laufwerk für Sun Fire X2100 x64 Server.	
			Einzel-Listenpreis: 83,67 EUR Rabatt: 5.00%	79,48 EUR
1.3	X8029A	1	Slide Rail Kit für Sun Fire X2100, X4100 und X4200 x64 Server. Passt nur in Sun Rack 900-38, Sun Rack 1000-38, Sun Rack 1000-42, oder Racks mit interner Tiefe (Pfosten zu Pfosten) von 27".	
			Einzel-Listenpreis: 132,10 EUR Rabatt: 5.00%	125,50 EUR
1.4	X312L	1	Netzkabel mit Schuko-Stecker Einmal kostenlos bei Systembestellung - kontinentaleuropäisches Netzkabel mit Schuko-Stecker	
			Einzel-Listenpreis: 0 Rabatt:	0
1.5	X8079A	1	80 GB interne serielle ATA (SATA) Festplatte für Sun Fire X2100 Server.	
			Einzel-Listenpreis: 132,10 EUR Rabatt: 5.00%	125,50 EUR
1.6	W9D-A75-24-3H	1	Sun Fire X2100 Server upgrade to 3 years of 7x24 hardware only support.	
			Einzel-Listenpreis: 432,00 EUR Rabatt: 44.00%	241,92 EUR

made with

StarOffice™
 sun.com/staroffice

 Dieses Dokument wurde mit StarOffice erzeugt -- ein Softwareprodukt von Sun Microsystems
 Lesen Sie mehr unter www.sun.de/staroffice

MAXDATA

MAXDATA Computer GmbH & Co. KG · Elbestraße 12-16
45768 Marl · Tel. (02365) 952-0 · Fax (02365) 952-2005

Firma
T-Systems Enterprise Services GmbH
Ges.- Nr. 8454
Postfach 1545
88244 Weingarten

Versandanschrift

Firma
T-Systems Enterprise Services GmbH
Ges.- Nr. 8454
Postfach 1545
88244 Weingarten

Angebot

Nummer/Datum
425450442 / 28.03.2006
Bestellnummer/Datum
[REDACTED]
Kundennummer
160931
Gültigkeitszeitraum
28.03.2006 bis 11.04.2006
Sachbearbeiter:
[REDACTED]
Betreuer:
Telekom

Bedingungen

Zahlungsbedingung: 31 Tage ohne Abzug
Versandbedingung : Paketd. frei Haus
Lieferbedingungen: EXW (Ab Werk) Würselen

Angebot freibleibend

Pos	Material	Bezeichnung	Einzel-VK	Währung	Menge	Gesamt-VK EUR
100	105593	MAXDATA PLATINUM Server Konfiguration				
		Nettopreis	966,00	EUR	1 ST	966,00
		MPL Standard-Server / NAS				
		System			Standard-Server	
		Standcase/19"-Rack			PLATINUM 820R	
		Netzteil			19 Zoll-Rack	
		Mainboard			PSU 1 x 400W	
		Onboard-Komponenten			Intel SE7210TP1	
		Produkttyp			Dual Intel PRO/100+/1000 Serv.	
		Projekt			Server Entry	
		Produktstandort			kein Projekt	
		Service 1. Jahr			Deutschland	
		Service 2. Jahr			Onsite NED	
		Service 3. Jahr			Return To Base	
		Betriebssystem Downgradeoption			Return To Base	
		Betriebssystem			kein Downgrade	
		Systemname			DR-DOS 7.0 UK Preload OEM	
		1. CPU			MAXDATA PLATINUM 820R	
		1. Speichermodul			Pentium 4E 3,0GHz 1M 800 HT	
		1. HDD (/ Combo-Drive)			DDR400 512MB ECC	
		Optisches Laufwerk			HDD 80GB ST3808110AS, SATA-II	
		1. Controller			Slim Line DVD Teac DV-28E-QM3	
		Tastatur			Onboard-Controller	
		Maus			Cherry K/B G83-6199 black DE	
					MS Wheel Mouse Optical black	
		Zur Position gehört diese Unterposition				
	105103	MAXDATA Service-Konfig. (Direktbuchung)				
		Nettopreis	139,00	EUR	1 ST	139,00

Es gelten ausschließlich unsere Allgemeinen Verkaufs-, Liefer- und Zahlungsbedingungen

Gesellschaftssitz
Marl, HR A 2783
AG Gelsenkirchen
www.maxdata.com
St-Nr. 359/5762/0281
EAR DE 13494190

Komplementärin
MAXDATA
Verwaltungs-GmbH
Gesellschaftssitz Marl
HR B 3654, AG Gelsenkirchen

Geschäftsführung
Dirk Quell

Dresdner Bank AG Essen
BLZ 360 800 80, Konto 0428770800
IBAN DE72 3608 0080 0428 7708 00
S.W.I.F.T. Code DRES DE FF 360
UST-ID-Nr/VAT Reg.No.DE812700054

MAXDATA

T-Systems Enterprise Services GmbH Beleg-Nr./Datum Seite
 88244 Weingarten 425450442 / 28.03.2006 2

Pos	Material	Bezeichnung	Einzel-VK	Währung	Menge	Gesamt-VK EUR
	Projekt			kein Projekt		
	Produktstandort			Deutschland		
	Produktgruppe			Server		
	Produkttyp			Server Entry		
	Service 1. Jahr			Onsite NED		
	Service 2. Jahr			Onsite NED		
	Service 3. Jahr			Onsite NED		
Summe Positionen						1.105,00
Mehrwertsteuer						176,80
Endbetrag						1.281,80

Es gelten ausschließlich unsere Allgemeinen Verkaufs-, Liefer- und Zahlungsbedingungen

Gesellschaftssitz Marl, HR A 2783 AG Gelsenkirchen www.maxdata.com St-Nr. 359/5762/0281 EAR DE 13494190	Komplementärin MAXDATA Verwaltungs-GmbH Gesellschaftssitz Marl HR B 3654, AG Gelsenkirchen	Geschäftsführung Dirk Quell	Dresdner Bank AG Essen BLZ 360 800 80, Konto 0428770800 IBAN DE72 3608 0080 0428 7708 00 S.W.I.F.T. Code DRES DE FF 360 USt-ID-Nr/VAT Reg.No.DE812700054
--	--	--------------------------------	--

Anhang E

Gäste W-LAN Server Installation

Als erstes muss eine Linux-Version installiert werden, bei der man das Paket „Server“ auswählt.

1. Bei den Netzwerkeinstellungen sind folgende Punkte zu beachten:

- „eth0“ ist für die Internetanbindung
 - IP : 217.6.255.44
 - Mask : 255.255.255.224
 - Gateway : 217.6.255.1
 - DNS 1 : 217.237.149.161
 - DNS 2 : 217.237.150.225

DNS Server kann man nachschauen unter:

<http://www.atelier89.de/users/dirk/t-o/>

- „eth1“ ist für die W-LAN-Anbindung und muss unkonfiguriert bleiben, da „Chillispot“ Software die Konfiguration selbst übernimmt.
- Der Hostname ist : *Hotspot.ez-nord.de*

2. Bei dem Aktivieren der Firewall muss nichts Weiteres eingestellt werden.

3. Bei der Paketauswahl müssen folgende Pakete zusätzlich ausgewählt werden:

- „Server Configuration Tools“
- „Webserver“ wichtig mit SSL-Unterstützung
- unter „Netzwerk Server“ den Freeradius auswählen
- Administration Tools

4. Installieren der „Chillispot“ Software aus dem Internet:

```
rpm -i http://www.chillispot.org/download/chillispot-1.0.i386.rpm
```

5. In der /etc/chilli.conf müssen noch einige Einstellungen vorgenommen werden:

- radiusserver1 127.0.0.1
- radiusserver2 127.0.0.1
- radiussecret testing123 muss aktiv sein
- uamserver https://192.168.182.1/cgi-bin/hotspotlogin.cgi
- uamsecret ht2eb8ej6s4et3rg1ulp

6. An der Firewall müssen folgende Einstellungen vorgenommen werden:

- /etc/init.d/iptables stop
- /usr/share/doc/chillispot-1.0/firewall.iptables
- /etc/init.d/iptables save
- in der /etc/sysctl.conf muss noch net.ipv4.ip_forward = 0 auf 1 gestellt werden.

7. Als Nächstes muss das Gäste-W-LAN-Add-On für den Radius-Server installiert und konfiguriert werden. Hierfür legt man unter „/etc/raddb/“ das Verzeichnis „addon“ an.

8. Um Daten auf den Server zu bekommen, nehmen wir das Programm WinSCP3. Das ist ein SSH Client, der Daten übermittelt. Die Datei „Gäste-W-LAN Addon v1.0.tar“ wird in das „Addon-Verzeichnis“ kopiert.
9. Mit dem Befehle „tar -xvf Gaeste-W-LAN Addon v1.0.tar“ wird die Datei ausgepackt und mit „rm -f Gaeste-W-LAN Addon v1.0.tar“ löscht man die Datei.
10. Der Inhalt vom Verzeichnis „/addon/www“ muss ins Dokumenten-Root vom Webserver kopiert werden „/var/www/“.
11. Nun muss man in den Dateien log_connect.sh und passwdset.sh noch die Verzeichnisse anpassen.
12. In der „crontab“ müssen jetzt die Skripte angelegt werden:
 - 0 7 * * * /etc/raddb/addon/login_connect.sh
 - 0 23 * * 7 /etc/raddb/addon/passwdset.sh
 - 0 23 * * * /etc/init.d/radiusd stop
 - 0 23 * * * /etc/init.d/chilli stop
 - 30 6 * * * /etc/init.d/radiusd start
 - 30 6 * * * /etc/init.d/chilli start

Ab 23 Uhr soll sich der Radius-Server runterfahren und um 6.30 Uhr wieder starten. Die Passwörter sollen jeden Sonntag um 23 Uhr neu gesetzt werden. Der Login-Bericht wird jeden Tag um 7 Uhr an den Administrator geschickt.

Einrichtung Access Points

Die Anleitung basiert auf einem neuen Access Point, wo keine Einstellungen verändert sind. Kommt ein vorkonfiguriertes Gerät zum Einsatz, muss dieses auf Werkseinstellungen zurückgesetzt werden.

Die auf der Abbildung dargestellten Einstellungen müssen den jeweiligen Geräten noch angepasst werden. Unter dem Punkt „Administration“ ändert man das Standardpasswort; sofern es eine neue Firmware gibt, muss sie an diesem Punkt eingespielt werden.

Danach folgt man der Reihenfolge der Abbildung 1-5.

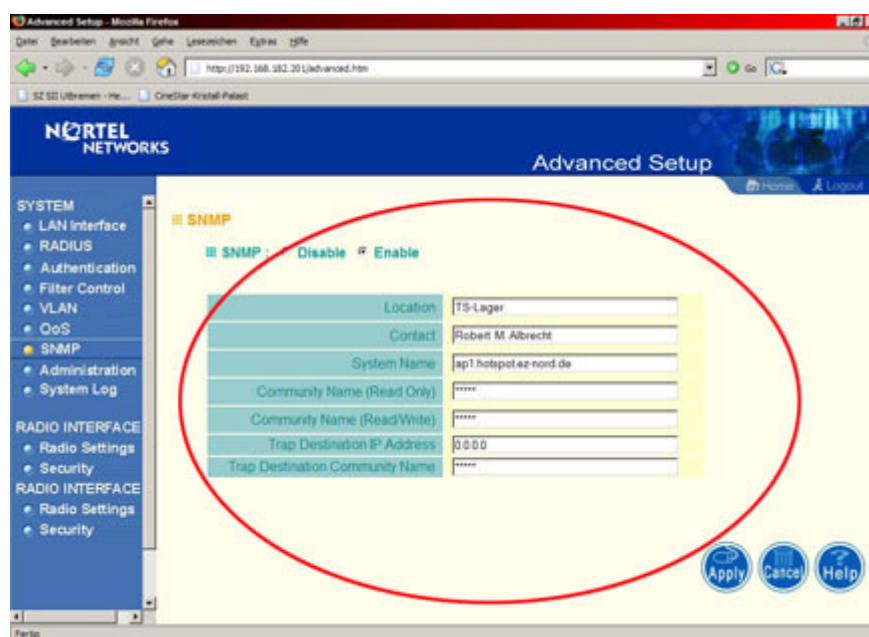


Abbildung 1: SNMP Einstellungen

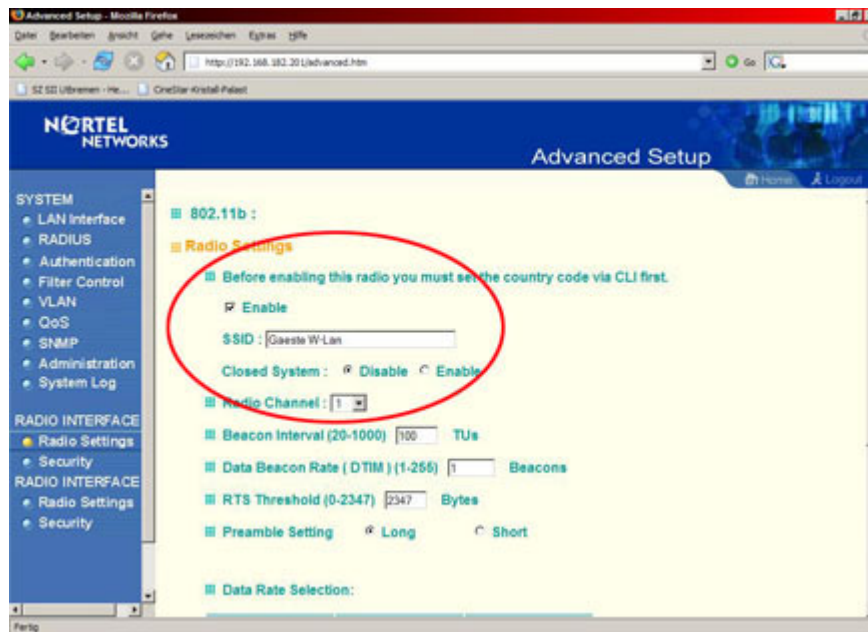


Abbildung 2: Interface B – Radio Settings

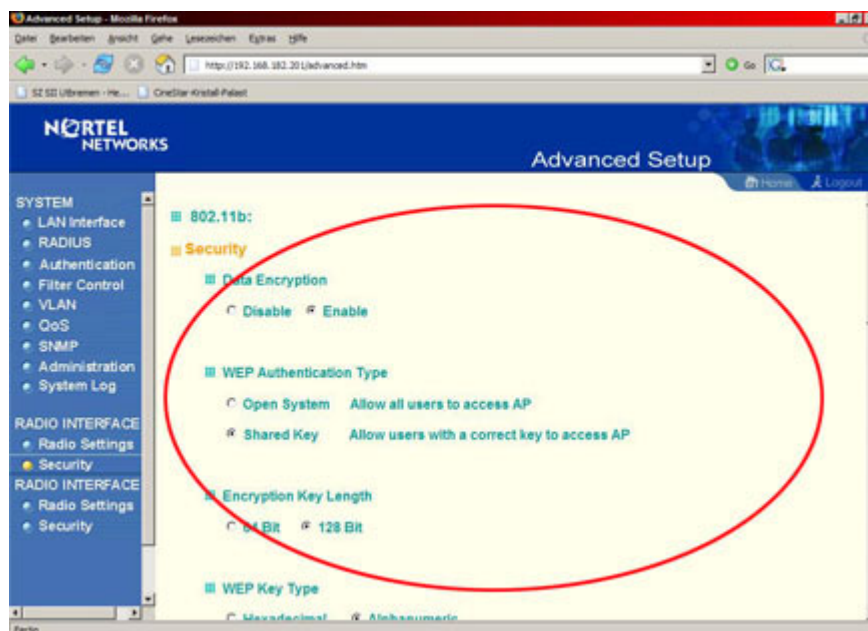


Abbildung 3: Security Einstellung Interface B Ausschnitt 1

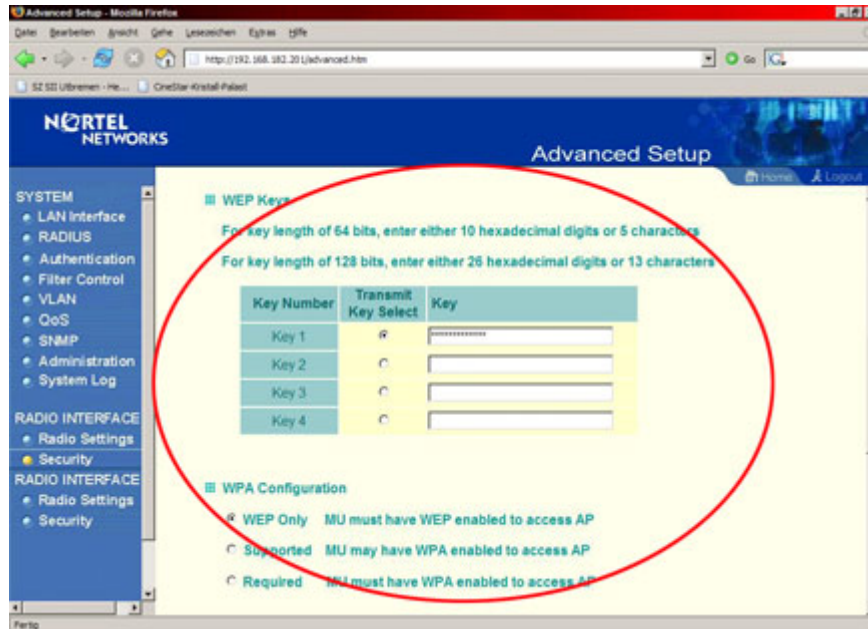


Abbildung 4: Security Einstellung Interface B Ausschnitt 2

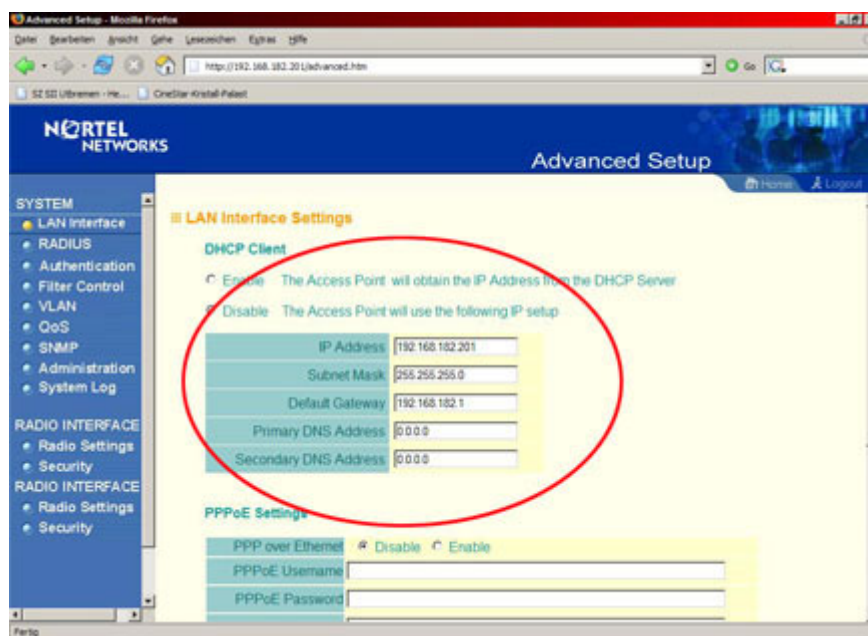


Abbildung 5: System – LAN Interface Einstellungen

Anhang F

```
/bin/mail -s"Loginliste vom Hotspot" $mailto < $radiusmail
rm -f $radiusmail > /dev/null
```

Shell-Skript: log_connect.sh

```
#!/bin/bash
#
# Skript fuer automatische Erzeugung von Pin
# Nummern und zur Weiterleitung an Personen
# per E-Mail
#
# Ersteller : Stephan Springer
# Version : 1.0
# Datum : 20.03.2006
# E-mail : Stephan.Springer@telekom.de *
#
# T-Systems Enterprise NITS GmbH
#
# Userliste fuer das Gaeste W-LAN
#
# Hier koennen einfach weitere User angelegt werden user[xxx]
# die eMail Adresse muss weiter unten eingetragen werden,
# dabei muss der Index bei beiden gleich sein.
#

user[1]=" "
user[2]=" "
user[3]=" "
user[4]=" "
user[5]=" "
user[6]=" "
user[7]=" "
user[8]=" "
user[9]=" "
user[10]=" "
user[11]=" "
user[12]=" "

# Adminpasswort
Adminpwd=" "

# Mail Adressen für PIN Nummer Liste
mail[88]="-c [REDACTED]@telekom.de [REDACTED]@t-systems.com"
```

```
#!/bin/sh
#
# Ein Skript fuer die Login-Auswertung beim
# Radius-Server vom hotspot.ez-nord.de
#
# Ersteller : Stephan Springer
# Version : v.1.0
# eMail : Stephan.Springer@telekom.de
#
# T-Systems Enterprise GmbH
#
# Verzeichnisse
Radiuslog="/var/log/radius/radius.log"
Radiusmail="/etc/raddb/addon/radiusmail"
#
# Suchstrings
LogOkNr=`grep -c OK $Radiuslog`
LogFehlerNr=`grep -c incorrect $Radiuslog`
LogGnNr=`grep -c Login $Radiuslog`
#
# eMail, an wen der Report geschickt werden soll
mailto="-c [REDACTED]@telekom.de -c [REDACTED]@t-systems.com"
#
# Ausgabeteil
echo "===== " >> $Radiusmail
echo " T-Systems Enterprise GmbH Hotspot EzNord" >> $Radiusmail
echo "===== " >> $Radiusmail
echo "Login Gesamt : $LogGnNr" >> $Radiusmail
echo "Login Erfolgreich : $LogOkNr" >> $Radiusmail
echo "Login Fehlerhaft : $LogFehlerNr" >> $Radiusmail
echo " " >> $Radiusmail
echo " " >> $Radiusmail
echo "Erfolgreiche Logins" >> $Radiusmail
echo "===== " >> $Radiusmail
echo " " >> $Radiusmail
grep OK $Radiuslog >> $Radiusmail
echo " " >> $Radiusmail
echo " " >> $Radiusmail
echo "Fehlgeschlagene Logins" >> $Radiusmail
echo "===== " >> $Radiusmail
echo " " >> $Radiusmail
grep incorrect $Radiuslog >> $Radiusmail
```

```

# eMailliste fuer das Gaeste W-LAN
#
# Die Empfänger der Benutzernamen und Passwoertern muessen hier
# eingetragen werden user[x] gleich email an mail[x] der Index
# muss
# bei beiden gleich sein.

mail[1]="[REDACTED]@telekom.de"
mail[2]="[REDACTED]@telekom.de"
mail[3]="[REDACTED]@telekom.de"
mail[4]="[REDACTED]@telekom.de"
mail[5]="[REDACTED]@telekom.de"
mail[6]="[REDACTED]@telekom.de"
mail[7]="[REDACTED]@telekom.de"
mail[8]="[REDACTED]@telekom.de"
mail[9]="[REDACTED]@telekom.de"
mail[10]="[REDACTED]@t-systems.com"
mail[11]="[REDACTED]@t-systems.com"
mail[12]="[REDACTED]@t-systems.com"

#
# Hier koennen noch weitere Kommandos fuer den Radius-Server
# angegeben und das Aussehen des Datums veraendert werden.
#

Date=`/bin/date +%d. %B.%Y`~
Kommando1="Auth-Type :=Local, User-Password =="
Kommando2="Session-Timeout=60"
fuell=""

#
# Benoetigte Dateinamen und Pfade

#
addon="/etc/raddb/addon"
mails="$addon/mail"
tsmail="$addon/tsmail"
pin="$addon/pin"
userslist="/etc/raddb/users"
anhang="$addon/anhang.txt"
radiusd="/etc/init.d"
datum="$addon/datum";

#
# Hauptskript

#
# Wenn man Benutzer zum Verteiler hinzufuegen moechte, um
# dann muss man in der for Schleife den Index erhoehen, um
# die Anzahl der Neueintraege anzupassen

```

```

rm -f $userslist >> /dev/null
echo "Hallo," >> $tsmail
echo " " >> $tsmail
echo "Hier die Passwortliste ab dem $Datum" >> $tsmail
echo " " >> $tsmail
echo "Benutzername      Passwort" >> $tsmail
echo "-----" >> $tsmail

# For Schleife "for in 1 2 3 4 5 x x x"
for i in 1 2 3 4 5 6 7 8 9 10 11 12
do
    Pswd=`$pin`
    Datum=`$datum`
    echo "${user[$i]} $Kommando1"$Pswd\" >> $userslist
    echo "$Kommando2" >> $userslist
    echo "Sehr geehrter W-LAN Nutzer," >> $mails
    echo "die Zugangsdaten fuer das Gaeste WLAN $Datum sind:" >> $mails
    echo " " >> $mails
    echo "Benutzer: ${user[$i]}" >> $mails
    echo "Pin : $Pswd">> $mails
    cat $anhang >> $mails

# Mailoptionen

/bin/mail -s"Die aktuelle PIN fuer das Gaeste WLAN $Datum ist :
$Pswd" ${mail[$i]} < $mails
rm -f $mails >> /dev/null
lng=`echo "${user[$i]}"|wc --chars`
fill=`echo "${fuell}"|cut -c ${lng}`~
echo "${user[$i]}$fill| $Pswd" >> $tsmail
done
echo "administrator $Kommando1"$Adminpwd\" >> $userslist

# Mailoptionen fuer ICTS-Liste

echo " " >> $tsmail
cat $anhang >> $tsmail
/bin/mail -s"Die aktuelle Pinliste fuer das Gaeste W-LAN $Datum
" ${mail[88]} < $tsmail
rm -f $tsmail >> /dev/null

```

Shell-Skript : passwdset.sh

```
//
// Dieses C Programm generiert
// vierstellige Pinnummern.
//
// Autor : Stephan Springer
// Version: 1.0
// Datum : 22.10.2004
// eMail : Stephan.Springer@telekom.de
// Datei : Pin.cpp
//
// T-Systems Enterprise GmbH

#include <iostream>
#include <math.h>
#include <time.h>

int main()
{
    int zahl;
    bool fertig=true;
    srand((unsigned) time(NULL));
    while(fertig)
    {
        for(int xy=0;xy<99999999;xy++)
        {
            zahl = rand();
            zahl = zahl % 9999+1000;
            if(zahl<9999) fertig=false;
        }

        cout << zahl;
        return 0;
    }
}
```

Pin.cpp

```
// Dieses C Programm erzeugt eine Datumspanne
// vom xx.xx.2006 - xx.xx.2006
//
// Autor : Stephan Springer
// Version: 1.0
// Datum : 22.10.2004
// eMail : Stephan.Springer@telekom.de
// Datei : Pin.cpp
//
// T-Systems Enterprise GmbH

#include <iostream>
```

```
#include <time.h>

int main() {

    time t Zeitstempel;
    tm *nun;
    Zeitstempel = time(0);
    nun = localtime(&Zeitstempel);

    int arrTageImMonat[12] = { 31, 28, 31, 30, 31, 30, 31, 31, 30,
    31, 30, 31 };

    int Tag=nun->tm mday;
    int Monat=nun->tm mon+1;
    int Jahr=nun->tm year+1900;

    std::cout << "vom " << Tag << " " << Monat << " " << Jahr;
    for(int i=0;i<7;++i)
    {
        if(Tag<arrTageImMonat[Monat-1]) Tag++;
        // Wenn die Anzahl der Tage groesser ist, als die zulaessige Zahl
        // der Tage im Monat, liegt ein Monatswechsel vor.
        else {
            if (Monat==12)
            {
                Jahr++;
                Monat=1;
                Tag=1;
            }
            else {Monat++;Tag=1;}
        }
    }

    std::cout << " - " << Tag << " " << Monat << " " << Jahr <<
    std::endl;
    return 0;
}

datum.cpp
```


Anhang G

E-Mail für die Zugangsdaten

Sehr geehrter W-LAN Nutzer,
die Zugangsdaten fuer das Gaeste W-LAN 10.4.2006 - 17.4.2006 sind:

Benutzername: Test-User
Pin : 8765

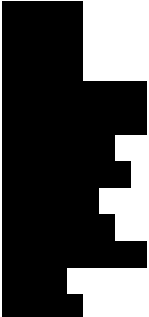
Diese ist eine automatische generierte E-Mail. Antworten auf diese E-Mail werden nicht verarbeitet. Bei Fragen und Problemen wenden Sie sich bitte an den Servicedesk unter -277.

Mit freundlichen Gruessen
Ihr ICT-Service des SSC NITS

T-Systems
Systems Integration
ICT Service, SSC NITS
Industry Business Unit Telco
T-Systems Enterprise GmbH
Hausadresse: Utbremer Straße 90, 28217 Bremen
Postanschrift: Postfach 15 01 93, 28091 Bremen
Telefon: + 49 421 3799-277
Telefax: + 49 421 3799-279
E-Mail: 277@t-systems.com

E-Mail für die Pinliste

Hier die Passwortliste ab dem 10.4.2006 - 17.4.2006

Benutzername	Passwort
Test-User	8765
	6534
	5678
	6734
	4563
	2387
	5612
	3412
	2343
	9876
	8089
	4789
	4711

E-Mail – Log-Auswertung

```
=====
      T-Systems Nova GmbH Hotspot EzNord
=====
Login Gesamt      : 3
Login Erfolgreich : 2
Login Fehlerhaft  : 1
```


```
=====
Erfolgreiche Logins
=====
```

```
Mon Apr 18 10:45:01 2006 : Auth: Login OK: [REDACTED/REDACTED] (from
client localhost port 2 cli 0020d803afba)
Mon Apr 18 12:36:34 2006 : Auth: Login OK: [Test-User/8765] (from client
localhost port 8 cli 000e353c75b7)
```

```
=====
Fehlgeschlangene Logins
=====
```

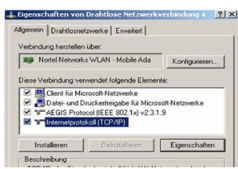
```
Mon Apr 18 10:44:48 2006 : Auth: Login incorrect: [Test-User/1112] (from
client localhost port 2 cli 0020d803afba)
```

Anhang H

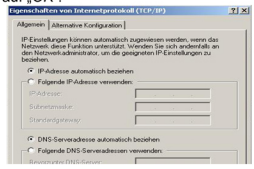


Die Konfiguration

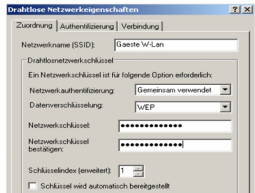
1. Klicken Sie auf „Start“.
2. Gehen Sie in die „Systemsteuerung“.
3. Wählen Sie „Netzwerkverbindung“.
4. Markieren Sie Ihre „Drahtlose Netzwerkverbindung“ und klicken Sie mit der rechten Maustaste. Wählen Sie „Eigenschaften“ aus dem Menü.
5. „Internetprotokoll (TCP/IP)“ auswählen und auf „Eigenschaften“ klicken.



6. Markieren Sie „IP-Adresse automatisch beziehen“ und „DNS Server Adresse automatisch beziehen“¹ und um die Einstellungen abzuschließen klicken Sie auf „OK“.



7. Klicken Sie jetzt auf dem Reiter „Drahtlosnetzwerke“.
8. Wählen Sie jetzt „Hinzufügen“ aus.
9. Bitte geben Sie unter Netzwerkname (SSID) folgendes ein : Gäste W-Lan
10. Der Haken bei „Schlüssel wird automatisch bereitgestellt“ darf nicht gesetzt sein.
11. Unter „Netzwerkauthentifizierung“ muss „Gemeinsam verwendet“ ausgewählt werden.
12. Bitte tragen Sie unter dem Punkt „Netzwerkschlüssel“ folgenden Schlüssel ein: XXXXXXXXXX und bestätigen Sie das in der nächsten Zeile noch einmal.
13. Zum Abschließen klicken Sie auf „OK“



Jetzt haben Sie eine Verbindung zum Gäste W-LAN

Bitte wenden ...

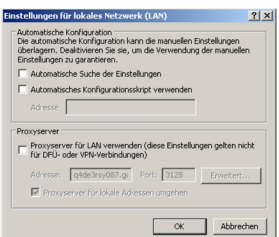
¹ Notieren Sie Ihre eigenen Einstellung

Vorderseite Anwenderbroschüre

Einrichten des Internet Explorers (nur für Windows)

1. Öffnen Sie Ihren Browser und gehen Sie auf „Extras“.
2. Wählen Sie „Internetoptionen“ und Registerkarte „Verbindungen“.
3. Unter „LAN-Einstellungen“ klicken Sie auf den Button „Einstellung“.
4. Stellen Sie sicher, dass folgende Felder nicht ausgewählt sind :
 - „Automatische Suche der Einstellungen“
 - „Automatisches Konfigurationskript“
 - „Proxyserver für LAN verwenden“.


Klicken Sie zum Abschluss auf OK.




Anmeldevorgang beim Gäste W-LAN

1. Um eine Internetverbindung nutzen zu können, müssen Sie einmal den Browser öffnen und eine Internet Adresse aufrufen z.B. www.t-systems.de
2. Jetzt werden Sie aufgefordert eine sichere Verbindung zuzulassen. Klicken Sie dazu auf „Ja“ um das Zertifikat anzunehmen.
3. Bei „Benutzername“ und „Passwort“ tragen Sie die Daten ein, die Sie vom örtlichen Sekretariat erhalten haben.

Klicken Sie „Login“ um sich ins Gäste W-Lan anzumelden.



Nun hat sich bei Ihnen das „Logout Fenster“ geöffnet. **Dieses Fenster darf bei der Benutzung des Gäste W-LAN's nicht geschlossen werden**, da es sonst zu Problemen beim Ausloggen kommen kann.



Zum Ausloggen klicken Sie bitte auf „Logout“. Jetzt sehen Sie den Anmeldebildschirm wieder.

Bei Problemen wenden sie sich bitte bei der **ICTS Hotline** des SSC NITS unter:

Tel : 0421 / 3799-277

Wir stehen Ihnen

Mo – Fr von 8 – 16 Uhr

zur Verfügung

Version 1.0
Datum : 13.04.2006

Rückseite Anwenderbroschüre

Anhang I

Glossar

Begriff:	Erklärung:
1-HE	Höheneinheit, bei 19-Zoll-Server rechnet man die Höhe in dieser Einheit
802.11af	Ist die Norm von IEEE für Power over Ethernet
ASCII	American Standard Code for Information Interchange, für jedes Zeichen gibt es einen Zahlencode, der es ermöglicht zwischen verschiedenen Systemen Text auszutauschen.
Broadcast	Rundruf im Computernetzwerk. Alle Teilnehmer bekommen die Nachricht
Brute-Force-Methode	Methode der rohen Gewalt ist eine Fachbegriff für eine Lösungsmethode aus dem Bereich der Informatik, sieh beruht auf Ausprobieren aller Varianten.
CGI	Common Gateway Interface, ist eine Standard im Web für Datenaustausch zwischen einem Webserver und Programmen.
Cronjob (Cron)	ist eine Jobsteuerung von Unix bzw. Linux
DMZ	demilitarized zone, darunter versteht man ein „Grenznetzwerk“, das zwischen ein zuschützendes Netz und ein unsicheres Netz geschaltet wird.
Gateway	Bezeichnet man im Netzwerk die Adresse wo alle Anfragen hingeleitet werden, die nicht zum eigenem Netz gehören.
GPL	General Public License, alternatives Vertriebskonzept, das im weitesten Sinne mit „Shareware“ vergleichbar ist.
IEEE	Institute of Electric and Electronic Engineers, 1963 gegründet Institut zur Festlegung von Normen im Netzwerkbereich.
IP-TABEL	Ist eine Firewall unter Linux
Kompromittiert	ist, wenn ein System Daten manipulieren könnte und wenn der Adminis-trator des Systems keine Kontrolle über die korrekte Funktionsweise mehr hat.
PoE	Power over Ethernet, bezeichnet eine Technologie, mit der netzwerk-fähige Geräte über das 8-adrige Ethernet-Kabel mit Strom versorgt werden können.
Pre-Shared-Key	so wird der Schlüssel bezeichnet den man z.B. bei WEP-Verschlüsselung einträgt, um Zugang zum W-LAN zu bekommen.
RADIUS	Remote Authentication Dial-In User Service, ist ein Client-Server-Protokoll, das zur Authentifizierung von Benutzern bei der Einwahl in ein Computernetzwerk dient.
SSH	Secure shell ist ein Netzwerkprotokoll, mit dessen Hilfe man sich z.B. über das Internet auf einen entfernten Computer einloggen und dort Programme ausführen kann.
SSID	Service Set Identifier auch Network Name genannt .Es dient zur Kenzeichnung eines Funknetzwerkes, was auf IEEE 802.11 basiert.
SSL	Secure Sockets Layer ist ein Verschlüsselungsprotokoll für Daten-übertragung im Internet.
TKIP	Temporal Key Integrity Protocol ist Teil des Standards von IEEE 802.11i und wird zur Verschlüsselung der Daten im W-LAN verwendet.
USV	unterbrechungsfreie Stromversorgung
VLAN	Virtual Local Area Network ist ein virtuelles lokales Netzwerk innerhalb eines physikalischen Netzwerkes
VoIP	Voice over IP ist das Telefonieren über ein Computernetzwerk auf der Grundlage des Internetprotokolls (IP).
VPN	Virtuelles Privates Netzwerk ist ein Computernetz, das zum Transport privater Daten im öffentlichen Netz z.B. Internet genutzt.wird.
WEP	Wired Equivalent Privacy ist ein ehemalige Standard-Verschlüsselungs-algorithmus für W-LAN. Es soll sowohl den Zugang regeln, als auch die Integriät der Daten sicherstellen.
WPA	Wi-Fi Protected Access ist eine Verschlüsselungsmethode für W-LAN. Nachfolger von WEP das als unsicher gilt.
X86	bezeichnet den Befehlssatz einer von der Firma Intel entwickelten Mikroprozessor-Architektur

Anhang J

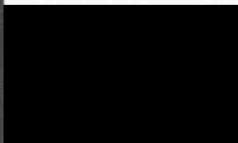
Literaturverzeichnis

Buchnachweise
Kai Fuhrberg, Dirk Häger , Stefan Wolf, Internet-Sicherheit – Browser, Firewall und Verschlüsselung. Carl Hanser Verlag München Wien 2001
H. J. Petersen, C. Rathgeber, K. Richter: IT – Handbuch, Westermann Schulbuchverlag GmbH, Braunschweig, 4 Auflage 2005
Daniel J. Barrett, Linux Kurz & Gut, O'Reilly - 1 Auflage Köln 2005
Webnachweise
Arnold Willemer, 2005: Zeitfunktionen in C++ http://www.willemer.de/informatik/cpp/timelib.htm
ChilliSpot - Open Source Wireless LAN Access Point Controller. Spice up your HotSpot with Chilli http://www.chillispot.org/
Wikimedia Foundation Inc, http://de.wikipedia.org/
ARCHmatic - Alfons Oebbeke: http://www.glossar.de/

Abbildung- und Tabellenverzeichnis

Abbildung 1 : Chillispot Logo.....	3
Abbildung 2 : Netzplan Gäste W-LAN.....	6
Abbildung 3 : Nortel-Switch Manager – VLAN bei einem BayStack 460-24T.....	9
Abbildung 4 : ntsysv, setzt Dienste in den Autostart	10
Abbildung 5 : Auszug aus dem Crontab Tabelle vom Hotspot-Server	10
Abbildung 6 : Putty Key Generator.....	11
Abbildung 7 : Programmausgabe von „pin“ und „datum“	12
Abbildung 8 : Anmeldevorgang im Gäste W-LAN	13
Abbildung 9 : Anmeldeformular.....	14
Abbildung 10: Nach erfolgreichen Login	14
 Tabelle 1 : Angebotsvergleich	 7
Tabelle 2 : Einmalige Gesamtkosten.....	8
Tabelle 3 : Monatliche Betriebskosten	8
Tabelle 4 : IP-Adressen für das Gäste-W-LAN.....	8

Anhang K

Handelskammer Bremen Abschlussprüfung: Sommer 2006 im Ausbildungsberuf: Fachinformatiker - Systemintegration		
<u>Prüfungsteilnehmer:</u> 	<u>Ausbildungsbetrieb:</u> Deutsche Telekom AG Telekom Training Berufsbildung Bremen Utbremer Str. 90 28217 Bremen	
<u>Prüfungs-Nr.: 1755</u> erhalten Sie mit der Einladung zur schriftlichen Prüfung		
Projektbezeichnung Gäste W-LAN – Hotspotlösung im T-Systems Standort Bremen		
Bestätigung des Ausbildungsbetriebes Wir bestätigen, dass der/die Auszubildende das oben bezeichnete Projekt einschließlich der Dokumentation im Zeitraum vom 22.03.2006 bis 21.04.2006 selbständig ausgeführt hat.		
Projektverantwortliche/er in Ausbildungsbetrieb Albrecht, Robert M. 0421/3799-712		
Name	Telefon	Unterschrift 
Ausbildungsverantwortliche/er im Ausbildungsbetrieb Gottwald, Peter 0421/3005400		
Name	Telefon	Unterschrift 
Eidesstattliche Erklärung: Ich versichere, dass ich das Projekt und die dazugehörige Dokumentation selbständig erstellt und dass ich bei der Erstellung weder vollständig noch teilweise Passagen aus anderen betrieblichen Aufträgen bzw. Dokumentationen übernommen habe, die bei der prüfenden oder einer anderen Kammer eingereicht wurden.		
Bremen, den 18.04.2006		
Ort und Datum		Unterschrift des Prüflings
HK HB 01/06		