Projektdokumentation

zur Abschlussprüfung zum

Fachinformatiker/Systemintegration

Integration einer Wireless LAN Infrastruktur in ein vorhandenes Netzwerk unter Einbindung eines Radius – Servers

erstellt von:

Björn Weßler

Parkallee 281

28213 Bremen

Prüfungsnummer: 2035

Ausbildungsbetrieb:

Deutsche Telekom AG

Utbremer Str. 90

28217 Bremen

Inhaltsverzeichnis

1. Einleitung

1.1 Vorwort

Zur Zeit absolviere ich bei der Deutschen Telekom eine Ausbildung zum IT-Fachinformatiker/Systemintegration. Ich habe die Ausbildung im September 2002 begonnen und seitdem in unterschiedlichen Abteilungen der Deutschen Telekom gearbeitet.

1.2 Projektumfeld

Seit Mai 2004 bin ich bei der T-Systems International GmbH eingesetzt und arbeite beim Information and Comunication Technologie Service (ICTS). Die Abteilung ICTS unterteilt sich in zwei Gruppen, dem Arbeitsplatzteam und dem Serverteam. Das Arbeitsplatzteam unterstützt die Mitarbeiter bei Hard- und Software-Problemen sowie bei Neubeschaffungen. Das Serverteam kümmert sich um die Administration der Server und des Haus-Netzes.

1.3 Projektauftrag

In diesem Projekt sollen die Konferenzräume der T-Systems International GmbH zusätzlich zum Haus - LAN mit Wireless-LAN* (WLAN) ausgestattet werden. Um das Wireless-LAN so sicher wie möglich zu machen, müssen deswegen verschiedene Sicherheitsfeatures genutzt werden. Hierunter fällt die Verschlüsselung der zu übertragenden Daten sowie ein Radius*-Server der zur Authentifizierung dient. Der Projektverantwortliche Robert M. Albrecht übergab mir dieses Projekt zur Durchführung.

1.4 Datenschutz

Aus Gründen der Sicherheit und des Datenschutzes habe ich firmeninterne und geschäftsrelevante Daten wie z.B Bezugspreise, Benutzernamen, Passwörter oder Kundennummern nicht erwähnt oder unkenntlich gemacht.

2. Projektanalyse

2.1 Ist – Analyse

Die Vernetzung der Konferenzräume wird durch LAN-Dosen in den entsprechenden Räumen realisiert. Da diese im Anforderungsfall erst noch gepatcht werden müssen, wird jedes Mal eine Betriebskraft benötigt, die dieses erledigt. Bei Konferenzen werden jedoch hauptsächlich Laptops eingesetzt, von denen die meisten sogar die WLAN-Technik schon unterstützen. Des Weiteren werden alle neu bestellten Laptops immer mit der WLAN-Technologie ausgestattet.

2.2 Soll - Konzept

Aufgrund der hohen Anzahl von Besprechungen, die pro Woche stattfinden, und dem Umstand, dass alle neu beschafften Laptops in unserem Unternehmen WLAN unterstützen, sollen die Konferenzräume mit Wireless-LAN ausgestattet werden. Das WLAN soll, genau wie das Hausnetz, das Internet, das Intranet der Deutschen Telekom sowie das Netzwerk der T-Systems bereitstellen.
Um dieses jedoch realisieren zu können, müssen ausreichend Access Points aufgebaut werden, damit eine bestmögliche Abdeckung der Konferenzräume erreicht wird.
Aufgrund der Tatsache, dass ein Wireless-LAN sich aber nicht nur auf einen Raum beschränkt, muss man es ausreichend gegen Angriffe absichern. Bei diesem Projekt soll das WLAN mit einer WPA*-Verschlüsselung abgesichert werden und dazu soll ein Radius-Server die Benutzeranmeldung und Authentifizierung übernehmen.
Um sicherzugehen, dass das Wireless LAN gegen Angriffe von Außen ausreichend geschützt ist, folgen zu einem späteren Zeitpunkt noch Sicherheitstests.
Der Vorteil der Umsetzung dieses Projektes besteht darin, dass die User ihren Laptop einfach in den Konferenzraum mitnehmen und sich dann dort mit dem Wireless LAN verbinden können. Dadurch wird vor Besprechungen keine Betriebskraft mehr zum Patchen der LAN-Dosen benötigt und sie kann andere Tätigkeiten ausführen.

3. Informationsphase

Nachdem mir das Projekt übergeben wurde, habe ich mich zu Anfang ca. 3 Stunden über die wichtigsten Inhalte des Projektes informiert. Darunter fallen Wireless LAN, die räumlichen Gegebenheiten der Konferenzräume sowie die unterschiedlichen Möglichkeiten eines Radius-Servers.

*im Glossar erklärt

4. Planungsphase

4.1 Auswahl der Access Points

Da in unserem Unternehmen schon Laptops mit unterschiedlichen WLAN - Standards vorhanden sind, sollten auch mehrere Standards bei unserem WLAN angeboten werden. Hinzu kommt, dass man besonders auf die Verschlüsselungsmechanismen achten muss. Ein weiterer Punkt, der zu beachten ist, ist der Preis der Access Points* (AP), da nicht nur ein AP sondern mehrere beschafft werden müssen. Des Weiteren sollte man auf zusätzliche Funktionen der AP´s achten, die unter Umständen Vorteile mit sich bringen können.
Durch die Informationsphase habe ich mehrere Hersteller herausgefiltert, die solche WLAN-Access-Points anbieten. Damit man die AP´s besser vergleichen kann, wird eine Nutzwertanalyse durchgeführt, um zu verdeutlichen, welcher AP sich für das Projekt am besten eignet.
In die nähere Auswahl kommen Access Points von Linksys, D-Link und Nortel Networks.

Rang	Kriterien	Gewichtung
1	Unterstützte Standards	35
2	Verschlüsselungsmechanismen	30
3	Preis	25
4	Zusätzliche Funktionen	10

Tabelle 1: Auswahlkriterien der Access-Points

		Linksys WAP55AG			D-Link DWL-2000AP+			Nortel Networks DR4001B55		
Kriterien	G		W	G*W		W	G*W		W	G*W
Unterstützte Standards	35	IEEE 802.11a & 802.11g	9	315	IEEE 802.11b/b+ & 802.11g	6	210	IEEE 802.11a & 802.11b	8	280
Verschlüsselungs-mechanismen	30	64/128/256-bit WEP	6	180	64/128/256-bit WEP ; WPA durch Software Upgrade	9	270	64/128-bit WEP ; WPA	8	240
Preis	25	ca 95€	4	100	ca 65€	6	150	ca 50€	8	200
Zusätzliche Funktionen	10		0	0		0	0	Power over Ethernet	6	60
Nutzwert				595			630			780

Tabelle 2: Nutzwertanalyse der Access-Points

*im Glossar erklärt

Aus der Nutzwertanalyse haben sich folgende Ergebnisse ableiten lassen: Der Access Point von Nortel Networks hat uns am meisten überzeugt, da er durch die Unterstützung der Standards 802.11* a & b alle Erweiterungsmöglichkeiten offen lässt (fast alle 802.11g Clients sind abwärtskompatibel zu 802.11b, was umgekehrt nicht so ist). Darüber hinaus beherrscht er die WPA-Verschlüsselung, ist im unteren Preissegment angegliedert und bringt auch noch die Option „Power over Ethernet“* mit sich, welche bei uns ebenfalls genutzt werden kann. Dadurch wird kein zusätzliches Netzteil benötigt und man ist flexibler bei dem Aufbau der AP´s, da keine Stromversorgung in der Nähe sein muss.

4.2 Auswahl des Radius-Servers

Durch die Informationsphase konnte ich mir schon einen Überblick über die verschiedenen Möglichkeiten, wie man einen Radius-Server aufbaut, verschaffen. Da es Radius-Server auf Windows- sowie auf Linux-Basis gibt und das Projekt über ein nicht sehr hohes Budget verfügt, kann man die Windows-Variante ausschließen, da hohe Lizenzkosten anfallen würden. Dies kommt zustande, weil ein Windows Server nur max. 50 Clients (Client=Access-Point) verwalten kann. Wenn mehr Access-Points verwendet werden sollen, muss ein Windows Advanced Server beschafft werden, der ca. 4000€ kosten würde. Diese Kosten fallen bei Linux nicht an, da es Distributionen* gibt, die frei erhältlich sind. Aus diesem Grund entschied ich mich für RedHat 9.0, da man es frei aus dem Internet herunterladen kann und es bei uns auch schon im Unternehmen eingesetzt wird.

4.3 Leistung des Radius-Servers

Durch die Entscheidung, den Radius-Server auf Linux-Basis zu realisieren, wird nun entsprechende Hardware benötigt. Damit man einen Überblick bekommt, was für ein Hardwarebedarf von Nöten ist, müssen die Systemanforderungen von Linux ermittelt werden.

Empfohlene Systemvoraussetzungen von RedHat 9.0 mit grafischer Oberfläche	
Prozessor	400 MHz
Speicher	256 MB
Festplatte	1,1 GB

Tabelle3: Systemvoraussetzung von RedHat 9.0

*im Glossar erklärt

4.4 Anzahl und Positionierung der Access Points

Um die Anzahl der Access Points herauszufinden, benötigte ich einen Raumplan, in dem alle Konferenzräume eingezeichnet sind. Diesen Raumplan konnte ich mir von dem Solution Managment besorgen. Durch die Räumpläne habe ich herausgefunden, dass wir über insgesamt fünf Konferenzräume verfügen, wovon sich ein Raum in der ersten Etage und die restlichen vier Räume in der zweiten Etage befinden. Damit das Unternehmen für mögliche Erweiterungen gerüstet ist, sollen zusätzlich fünf weitere Access Points zu denen, die für das Projekt benötigt sind, beschafft werden.
Die genaue Positionierung der Access Points wird erst zu einem späteren Zeitpunkt erledigt werden, da zunächst die gegebene Reichweite zu testen ist. Dies folgt in der Testphase.

5. Beschaffungsphase

5.1 Beschaffung der Access Points

Durch die Ergebnisse der Nutzwertanalyse ist die Entscheidung zugunsten des Access Points von Nortel Networks gefallen. Durch die vorherigen Recherchen kommen wir auf eine Anzahl von zehn benötigten Access Points. Damit die AP´s bestellt werden können, muss ich meine Auswahl an den Einkauf melden.

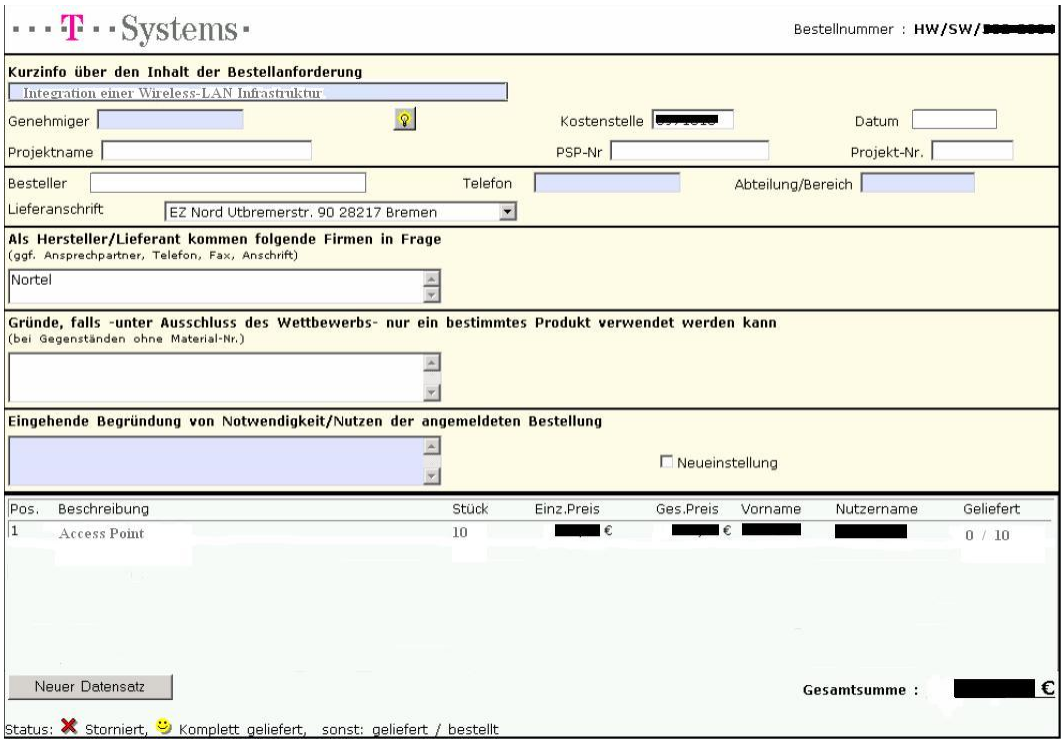


Abbildung 1: Screenshot von der Bestellung der Access-Points

*im Glossar erklärt

5.2 Beschaffung des Radius-Servers

Aufgrund der geringen Hardwareanforderungen von Linux wird kein neuer Server benötigt, sondern es kann ein älterer PC aus dem Lager der T-Systems International Bremen GmbH genutzt werden.

Technische Daten des Radius-Servers

- Intel Pentium III 700MHz Prozessor
- Chipsatz: Intel 440BX Chipsatz
- 256MB PC-100 SDRAM
- 10GB Festplatte
- Grafikkarte: VGA Matrox MAG-GA200A 8MB AGP
- Soundkarte:Creative SB128 PCI Soundkarte
- 3,5“ Diskettenlaufwerk
- 48x CD-Rom Laufwerk
- Steckkartenplätze: 1 x AGP, 3 x PCI, 3 x RAM
- Anschlüsse: 2 x USB, 2 x PS/2, 2 x seriell, parallel, Monitor, Sound Eingang, Sound Ausgang, Mikrofonanschluss
- Bauform: Midi-Tower ATX Design
- Netzteil: 200W

Abbildung 2: Radius-Server

6. Installation und Konfiguration

6.1 Installation des Betriebssystems

Da die Wahl des Betriebssystems auf Linux gefallen ist, werden als erstes die Installations-CD´s benötigt, die bei uns im Unternehmen bereits vorhanden sind. Dann kann mit der Installation begonnen werden.
Nachdem das Betriebsystem vollständig installiert ist, müssen die Netzwerkeinstellungen vorgenommen werden.
Zusätzlich muss noch Software hinzugefügt werden. Einmal die Radius-Server-Software sowie eine SSL*-Unterstützung für die Erzeugung von Zertifikaten und Schlüsseln. Falls diese Software noch nicht vorhanden ist, kann sie frei aus dem Internet herunter geladen werden. Die Quellen dafür sind www.freeradius.org und www.openssl.org.
Da diese Software schon im Vorfeld beschafft wurde, kann gleich mit der Installation begonnen werden.

6.2 Installation von openssl

Um openssl zu installieren sollte man ein neues Verzeichnis mit dem nachfolgenden Befehl anlegen:

```
mkdir -p /usr/test/openssl
```

Der Name des Verzeichnisses lautet jetzt openssl. Dort muss nun die im Vorfeld geladene openssl-Installationsdatei einfügt und dann entpackt werden.

```
gunzip openssl-0.9.7f.tar.gz
```

```
tar xvf openssl-0.9.7f.tar
```

Wenn das Entpacken erfolgreich war, sollte sich ein neues Verzeichnis mit dem Namen openssl-0.9.7f in dem zuvor angelegten Ordner befinden. Man wechselt in das neu angelegte Verzeichnis und gibt dann den Installationspfad an.

```
./config shared --prefix=/usr/local/openssl
```

Jetzt muss openssl noch kompiliert und installiert werden.

```
make
```

```
make install
```

Damit ist die Installation von openssl abgeschlossen.

6.3 Installation von Freeradius

Anschließend ist es nötig, Freeradius zu installieren. Hierzu beginnt man wie bei der vorherigen Installation und legt ein neues Verzeichnis an.

```
mkdir -p /usr/test/Freeradius
```

Auch hier wird die Installationsdatei in das neue Verzeichnis eingefügt und muss ebenso noch entpackt werden.

```
gunzip freeradius-1.0.2.tar.gz
```

```
tar xvf freeradius-1.0.2.tar
```

Jetzt sollte sich auch hier ein neues Verzeichnis mit dem Namen freeradius-1.0.2 befinden. Man wechselt in das neu angelegte Verzeichnis und teilt dem Freeradius mit, wo er openssl findet und dass openssl verwendet werden soll. Des Weiteren muss man ebenfalls wieder den Installationspfad angeben.

```
./configure --with-openssl-includes=/usr/local/openssl/include \
--with-openssl-libraries=/usr/local/openssl/lib \
--prefix=/usr/local/radius
```

Zum Schluss ist auch Freeradius zu kompilieren und installieren:

*im Glossar erklärt

```
Make
```

```
make install
```

6.4 Konfiguration des Radius-Servers in Verbindung mit openssl

Da in unserem Unternehmen PEAP* genutzt werden soll, müssen Zertifikate erstellt werden. Um diese zu erstellen, nutzen wir das CA.all Script*, das im Freeradius schon enthalten ist. CA.all nutzt Informationen, die aus der Konfigurationsdatei von openssl kommen. Um einen reibungslosen Ablauf zu gewährleisten, muss diese Konfigurationsdatei (openssl.cnf) zuerst mit Voreinstellungen für dieses Projekt versehen werden. Hier ein Auszug aus der erwähnten Datei:

```
[ req_distinguished_name ]
countryName                     = DE
countryName_default             = DE
countryName_min                 = 2
countryName_max                 = 2

stateOrProvinceName             = Bremen
stateOrProvinceName_default     = Bremen

localityName                    = Bremen

0.organizationName              = T-Systems International Bremen
0.organizationName_default      = T-Systems International Bremen

organizationalUnitName          = Entwicklungszentrum Nord
organizationalUnitName_default  = Entwicklungszentrum Nord

commonName                      = ITC-Service
commonName_default              = ITC-Service
commonName_max                  = 64

emailAddress                    = ts.eznordxxxxxxxxx
emailAddress_default            = ts.eznordxxxxxxxxx
emailAddress_max                = 64

[ req_attributes ]
challengePassword               = xxxxxxxxxxx
challengePassword               = xxxxxxxxxxx
challengePassword_min           = 4
challengePassword_max           = 20

unstructuredName                = T-Systems
```

Abbildung 3: Ausschnitt aus der Datei openssl.cnf

*im Glossar erklärt

Nun wird das CA.all Script angepasst, damit es die geänderten Daten der openssl.cnf übernimmt und die Zertifikate erstellt. In diesem Script ist zu beachten, dass der Pfad für openssl richtig angegeben wird.

```
SSL=/usr/local/openssl/ssl

export PATH=${SSL}/bin/:${SSL}/ssl/misc:${PATH}

export LD_LIBRARY_PATH=${SSL}/lib


echo "newreq.pem" | /usr/local/openssl/ssl/misc/CA.pl -newca
```

Abbildung 4: Ausschnitt aus dem Skript CA.all

Des Weiteren müssen noch ein paar Dateien angepasst werden. Es handelt sich hierbei um die Dateien clients.conf, users, und eap.conf, die sich im Verzeichnis /etc/raddb befinden.

Clients.conf

In dieser Datei wird der Radius-Server angegeben sowie der Netzbereich in dem sich die Access Points befinden.

```
client 10.xx.xx.xx {
      secret        = testxxxxx
      shortname     = q4dxxxxxx
}
client 10.xx.xx.xx/24 {
      secret        = wlanxxxxx
      shortname     = EZNxxxxxx
}
```

Abbildung 5: Ausschnitt aus der Datei clients.conf

Users

In dieser Datei werden die Nutzer angelegt. Sie werden alle nach dem folgenden Prinzip eingetragen.

```
"MaxMustermann" User-Password == "Test1234"
```

Abbildung 6: Ausschnitt aus der Datei users

eap.conf

In dieser Datei muss der eap-Standardtyp auf peap gesetzt werden.

```
eap {
            default_eap_type = peap
            }
```

Abbildung 7: Ausschnitt aus der Datei eap.conf: Einstellung auf peap

*im Glossar erklärt

Weiterhin muss die peap – Sektion der Datei eap.conf noch geändert werden.

```
peap {
        default_eap_type = mschapv2
    }
```

Abbildung 8: Ausschnitt aus der Datei eap.conf: Einstellung auf mschapv2

Zusätzlich müssen in dieser Datei weitere Anweisungen abgeändert werden. Dazu wird ein neues Verzeichnis benötigt, welches vorher anzulegen ist. In dieses Verzeichnis müssen dann die Zertifikate cert-srv.pem und root.pem kopiert werden. Außerdem ist das Anlegen zwei Dateien erforderlich: dh und random. Diese Dateien werden mit einem kleinen Trick erstellt: Man wechselt in das Verzeichnis usr/test/certs und gibt dort „date > dh“ und „date > random“ in der Konsole ein, so werden die Dateien erstellt.

```
mkdir -p /usr/test/certs
```

```
tls {
        private_key_password = Airxxxxxx
        private_key_file =  usr/test/certs/cert-srv.pem

        certificate_file = usr/test/certs/cert-srv.pem

        CA_file = usr/test /certs/root.pem

        dh_file = usr/test /certs/dh
        random_file = usr/test /certs/random
```

Abbildung 9: Ausschnitt aus der Datei eap.conf: Passwort und Pfadangaben

Zum Schluss muss noch ein kleines Script im Verzeichnis /usr/local/radius/sbin geschrieben werden, welches die Zuordnung der richtigen Pfade übernimmt und den Radius-Server startet.

```
#!/bin/sh -x
LD_LIBRARY_PATH=/usr/local/openssl/lib
LD_PRELOAD=/usr/local/openssl/lib/libcrypto.so
export LD_LIBRARY_PATH LD_PRELOAD
/usr/local/radius/sbin/radiusd $@
```

Abbildung 8: Script für die Zuordnung der Pfade und starten des Radius-Servers

*im Glossar erklärt

6.5 Konfiguration der Access Points

Um die Access Points das erste Mal zu konfigurieren, benötigt man ein serielles Kabel, um die Verbindung herzustellen. Dort muss man Deutsch als Landessprache einstellen, da ansonsten die Antennen der Access-Points abgeschaltet sind. Des Weiteren muss die DHCP*-Unterstützung abgeschaltet und eine IP-Adresse vergeben werden, damit man die Access Points per Web – Oberfläche zu Ende konfigurieren kann.

```
Nortel Enterprise AP#configure
Nortel Enterprise AP(config)#interface ethernet
Nortel Enterprise AP(if-ethernet)#no ip dhcp
Nortel Enterprise AP(if-ethernet)#ip address 10.xx.xx.xx 255.xxx.xxx.x 10.xx.xx.xx
Nortel Enterprise AP(if-ethernet)#exit
Nortel Enterprise AP#show interface ethernet
Ethernet Interface Information
=======================================
IP Address        : 10.xx.xx.xx
Subnet Mask       : 255.xxx.xxx.x
Default Gateway   : 10.xx.xx.xx
```

Abbildung 9: Ausschnitt aus der Erstkonfiguration des Access-Points

Über die Web – Oberfläche müssen nun noch die restlichen Einstellungen vorgenommen werden. Darunter fällt die Überprüfung der Netzwerkeinstellungen und das Hinzufügen der DNS*-Server-Adressen,

Abbildung 10: Ausschnitt aus der Konfiguration des Access-Points: DHCP Einstellungen

die IP Adresse des Radius-Servers,

Abbildung 11: Ausschnitt aus der Konfiguration des Access-Points:
Angabe der IP-Adresse des Radius-Server

*im Glossar erklärt

und die Authentication-Einstellungen.

Abbildung 12: Ausschnitt aus der Konfiguration des Access-Points: Authentication Einstellungen

Es werden noch weitere Einstellungen getätigt, diese werden aber per Screenshot im Anhang beigefügt.

6.3 Aufbau der Access Points

Nachdem die Access Points konfiguriert wurden, können sie an ihren Bestimmungsorten aufgebaut werden. Da unsere Access Points die Option „Power over Ethernet“ besitzen, benötigen wir keine Stromanbindung, sondern nur LAN – Dosen, die dann an die vorhandenen „Power over Ethernet“ - Switche angeschlossen werden. Die LAN – Dosen müssen im Anschluss von unserem Administrator mit einem Tool in das richtige VLAN geschaltet werden.

7. Funktions- und Sicherheitstests

7.1 Einrichten eines Laptops

Damit überhaupt Tests durchgeführt werden können, wird ein Laptop mit Wireless-LAN-Technologie benötigt. Der Laptop, der für die Testphase genutzt wird, ist ein Ersatzgerät, welches mir von ICTS Bereit gestellt wurde. Dieses muss passend zu unserem Netz eingerichtet werden. Da es sich um ein Laptop mit Windows XP handelt, wird das Windows XP WPA Rollup Package benötigt, um Windows XP WPA-kompatibel zu machen. http://support.microsoft.com/default.aspx?scid=kb;de;826942(Windows XP WPA Rollup) Zusätzlich muss ein User eingerichtet werden, der Zugriffsrechte besitzt und das Root Zertifikat ist zu installieren. Sind diese Maßnahmen abgeschlossen, kann die Wireless-LAN-Verbindung eingerichtet werden. Wie die Verbindung eingerichtet werden muss, wird im Anhang beschrieben.

7.2 Ausleuchtungsstudie

Um einen Überblick über die Reichweite der Access-Points, die stark von den räumlichen Gegebenheiten abhängig sind, zu bekommen, wird eine Ausleuchtungsstudie durchgeführt. Diese Studie wurde mit Hilfe eines eingerichteten Laptops, der von Windows angegebenen Verbindungsqualität, die sich in unterschiedliche Stufen unterteilt, und dem Raumplan getätigt. Um diesen Test realisieren zu können, geht man zu den aufgebauten Access-Points, verbindet sich mit dem Wireless-LAN und geht dann langsam mit kurzen Pausen immer weiter vom Access-Point weg. Die verschiedenen Verbindungsqualitäten, die Windows anzeigt, werden in einem ausgedruckten Raumplan eingezeichnet. Später wurden die ermittelten Ergebnisse analysiert und in einen, in digitaler Form, vorhandenen Raumplan eingefügt. Dieser Raumplan ist im Anhang B enthalten. Auf dem Plan kann man den Access-Point sowie seine ungefähre Reichweite erkennen. Beruhend auf diesen Ergebnissen wurden die restlichen Access-Points aufgebaut.

7.3 Sicherheitsanalyse

Um Schwachstellen des Wireless-LAN herauszufiltern, wurde der schon vorhandene Laptop genutzt. Dieser Laptop musste so konfiguriert werden, dass man mit ihm keinen Zugriff mehr auf das Wireless-LAN bekommt. Dann wurde eine frei erhältliche Software namens „Netstumbler“ aus dem Internet geladen (www.netstumbler.com) und installiert. Mit dieser Software kann man feststellen, ob und welche Sicherheitseinstellungen am Access Point zur Sicherung des Netzwerks eingestellt wurden. Sobald Netstumbler gestartet wird, sucht dieser sofort nach Wireless-LAN-Netzen. Sobald ein Wireless-LAN entdeckt wird, bekommt man die SSID*, die MAC-Adresse* der Access-Points, die Qualität des Signals, die Art der Verschlüsselung und weitere Informationen. Ein Nachteil dieser Software ist, dass es die WPA-Verschlüsselung nicht richtig anzeigt, sondern diese als WEP* kennzeichnet. Da das Tool sonst alle wichtigen Informationen bereitstellt, wird auf diesen Nachteil nicht weiter eingegangen. Im Anhang B befindet sich ein Screenshot aus dem Programm Netstumbler, der die Informationen über einen Access-Point anzeigt.

Es wurde dann versucht, sich mit dem Wireless-LAN zu verbinden, was nicht funktionierte. Da man keine gültige IP-Adresse zugewiesen bekam, konnte man auch nicht auf das Wireless-LAN zugreifen. Erst, als wieder alle Einstellungen getätigt wurden, wie im Anhang A beschrieben, war ein Verbindungsaufbau zum WLAN wieder möglich.

*im Glossar erklärt

8. Projektabschluss

Das Projekt ist aus meiner Sicht ganz gut verlaufen und auch der Betrieb war zufrieden mit den Ergebnissen. Das Projekt soll in einer weiteren Testphase von mehreren Kollegen getestet werden und durch deren Feedback können noch nicht aufgetretene Fehler protokolliert und anschließend Beseitigt werden.

9. Tabellen- und Abbildungsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

*im Glossar erklärt

9. Anhang

A Einrichten eines Laptops

B Screenshot aus dem Programm Netstumbler

C Ausleuchtungsstudie mit einem Access-Point

D Konfiguration der Access-Points

E Glossar und Quellenverzeichnis

F Zeit- und Maßnahmenplan

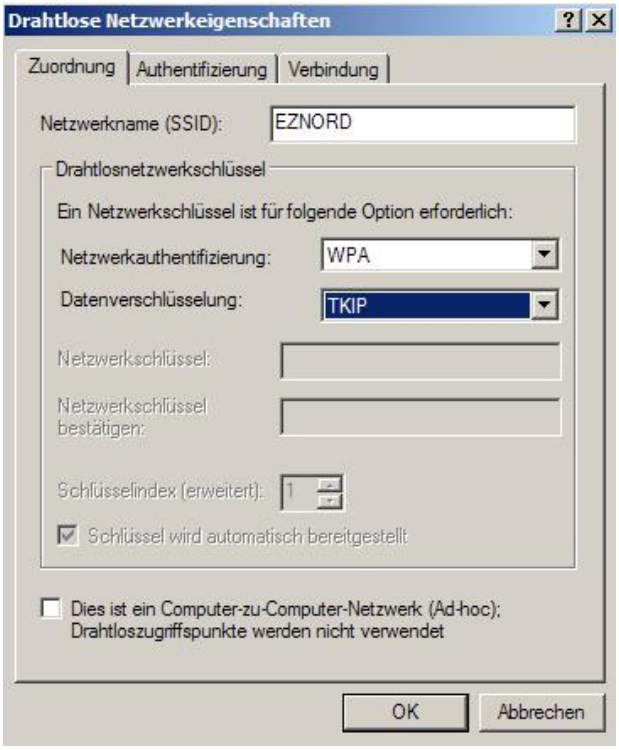
*im Glossar erklärt

Anhang A

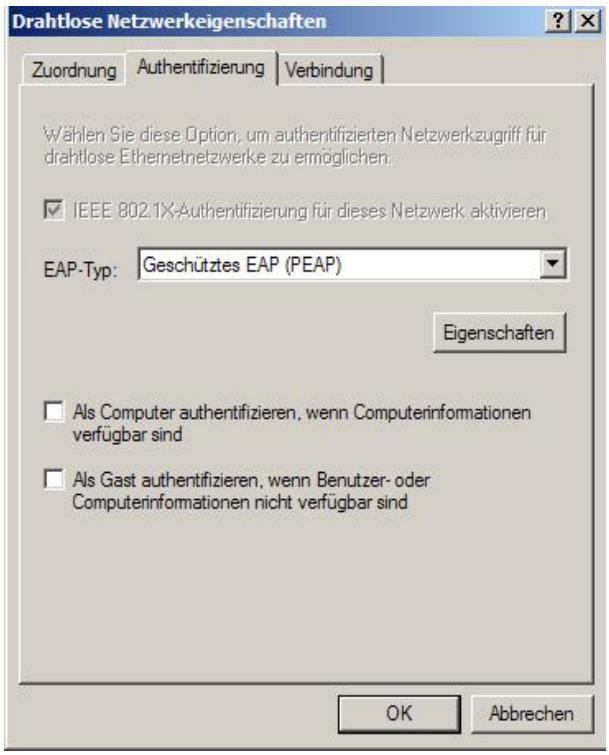
Einrichtung eines Laptops

Dazu geht man unter Netzwerkverbindungen
-> wählt die Wireless LAN Verbindung aus, über die rechte Maustaste kommt man zu den Eigenschaften -> dort wählt man „Drahtlosnetzwerke“ aus

Klick auf „Hinzufügen“ und es öffnet sich ein neues Fenster

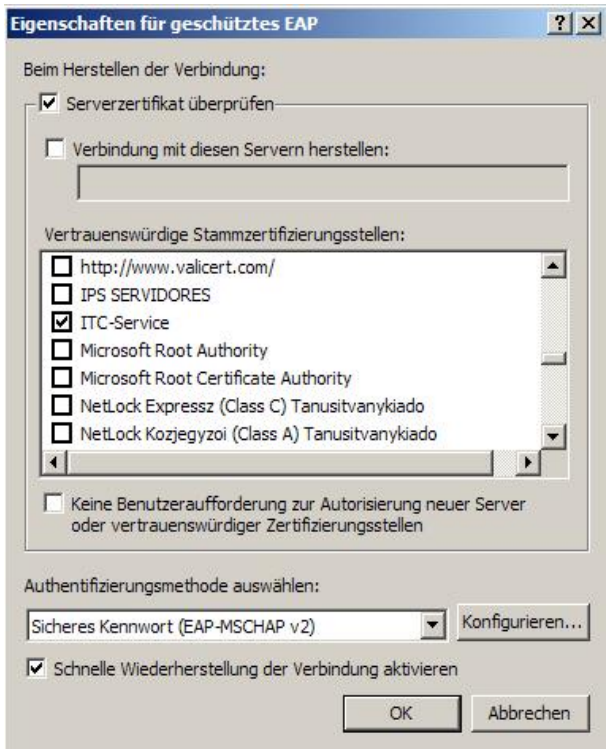


in dem Fenster trägt man die Informationen über den Netzwerknamen, die Netzwerkauthentifizierung und die Datenverschlüsselung ein.
Als nächstes wechselt man den auf Reiter „Authentifizierung“

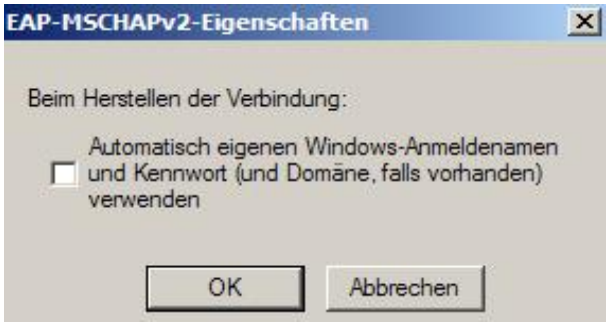


Hier wählt man bei „EAP-Typ“ das „Geschützte EAP (PEAP)“ aus und nimmt den Haken weg von „Als Computer authentifizieren“

Als nächstes drückt man auf „Eigenschaften“ und es öffnet sich wieder ein neues Fenster



Hier wird der Haken bei „Serverzertifikat überprüfen“ gesetzt und es muss das richtige Zertifikat ausgewählt werden, in diesem Fall das selbst erzeugte „ITC-Service“ Zertifikat.
Des Weiteren wird die Authentifizierungsmethode auf „Sicheres Kennwort (EAP-MSCHAP v2)“ eingestellt und der Haken bei „Schnelle Wiederherstellung der Verbindung“ gesetzt.
Dann noch einmal auf „Konfigurieren“ klicken und es öffnet sich ein neues Fenster,



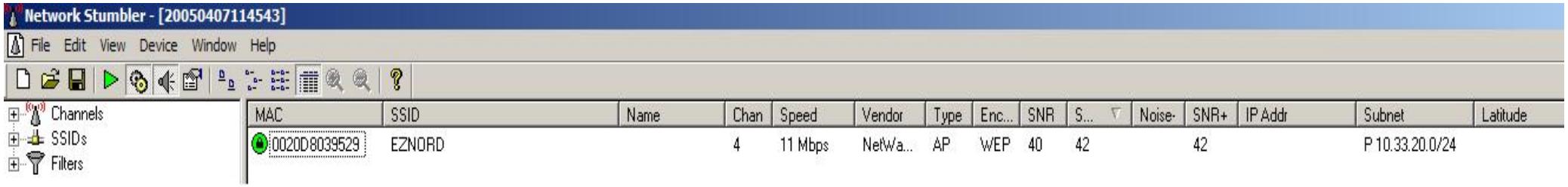
in dem wir den Haken bei „ Automatisch eigenen Windows Anmeldenamen und Kennwort verwenden“ entfernen.

Wenn die Einstellungen in Ordnung sind, öffnet sich das Anmelde-Fenster

Hier muss der User seinen Benutzernamen und Passwort eintragen. Der User muss vorher jedoch dem Radius-Server eingerichtet werden. Die Anmeldedomäne darf nicht ausgefüllt werden.

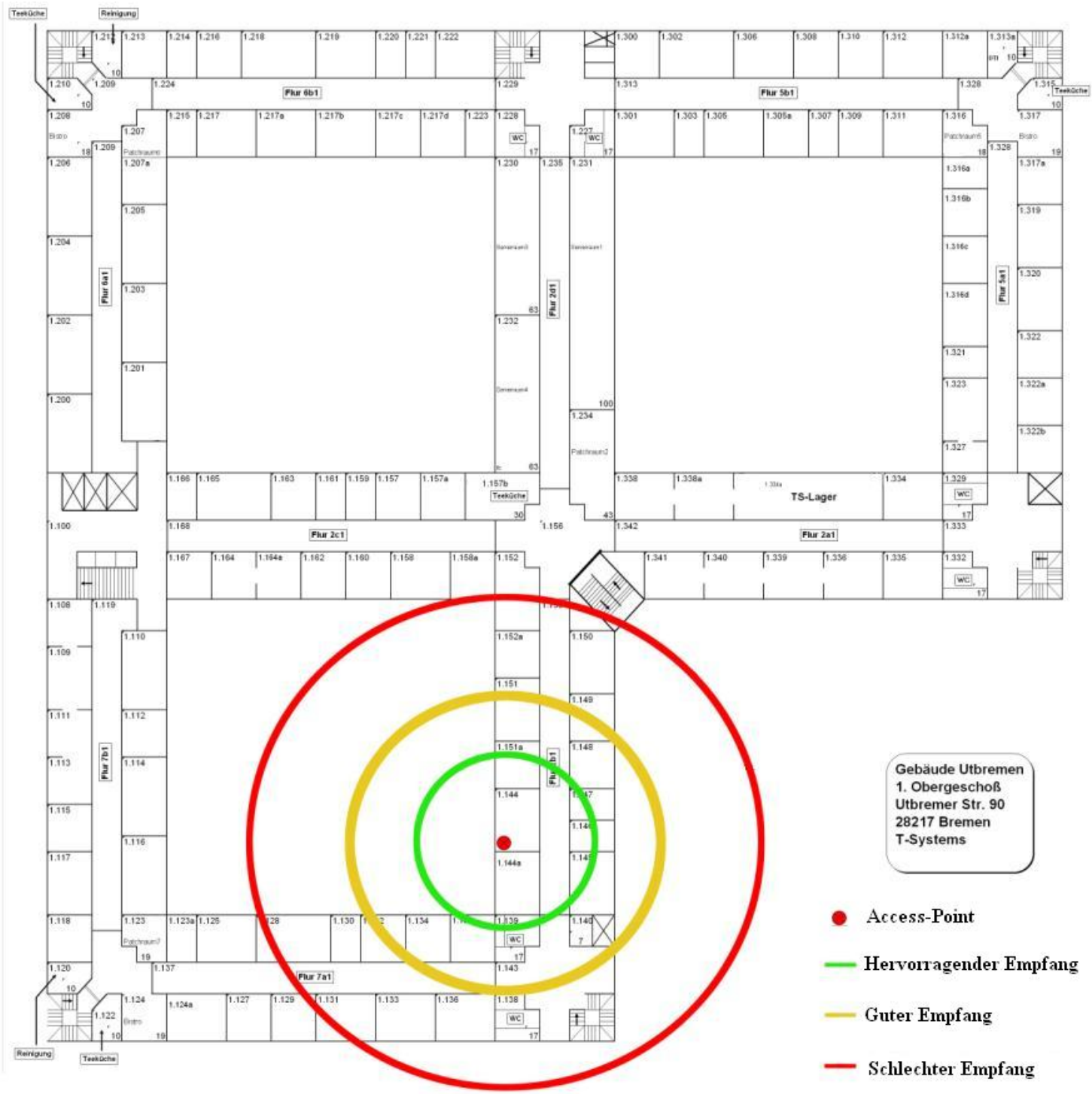
Anhang B

Screenshot aus dem Programm Netstumbler



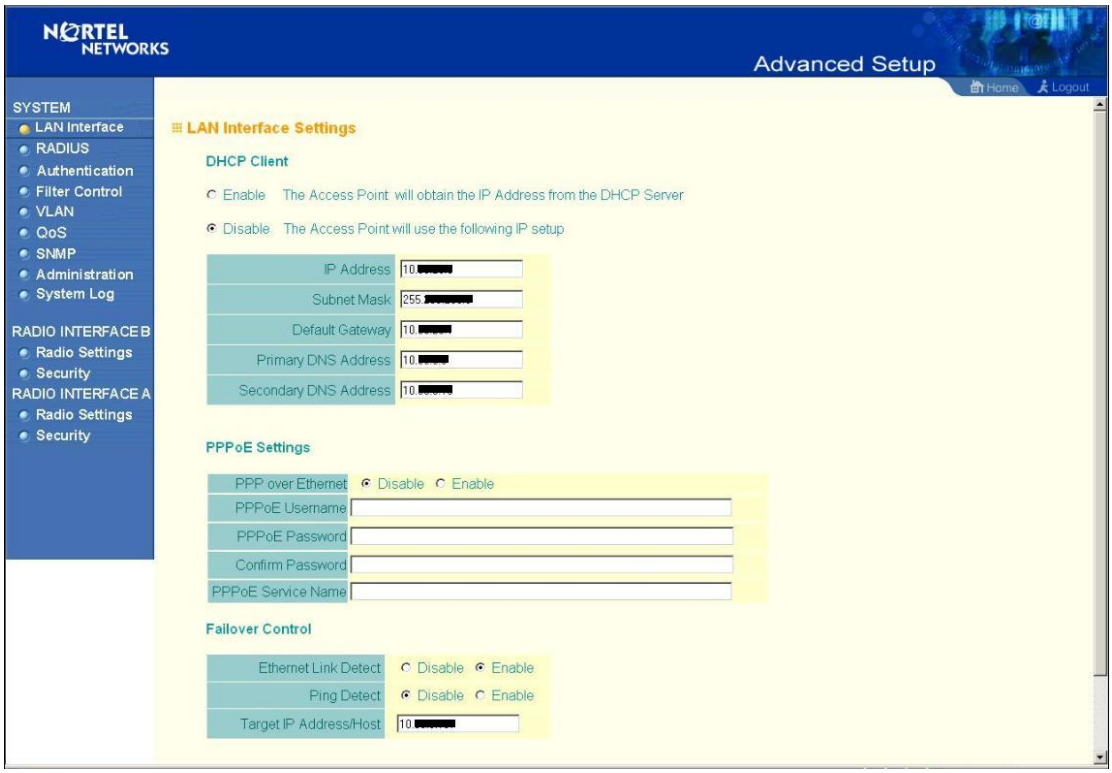
Anhang C

Ausleuchtungsstudie mit einem Access-Point

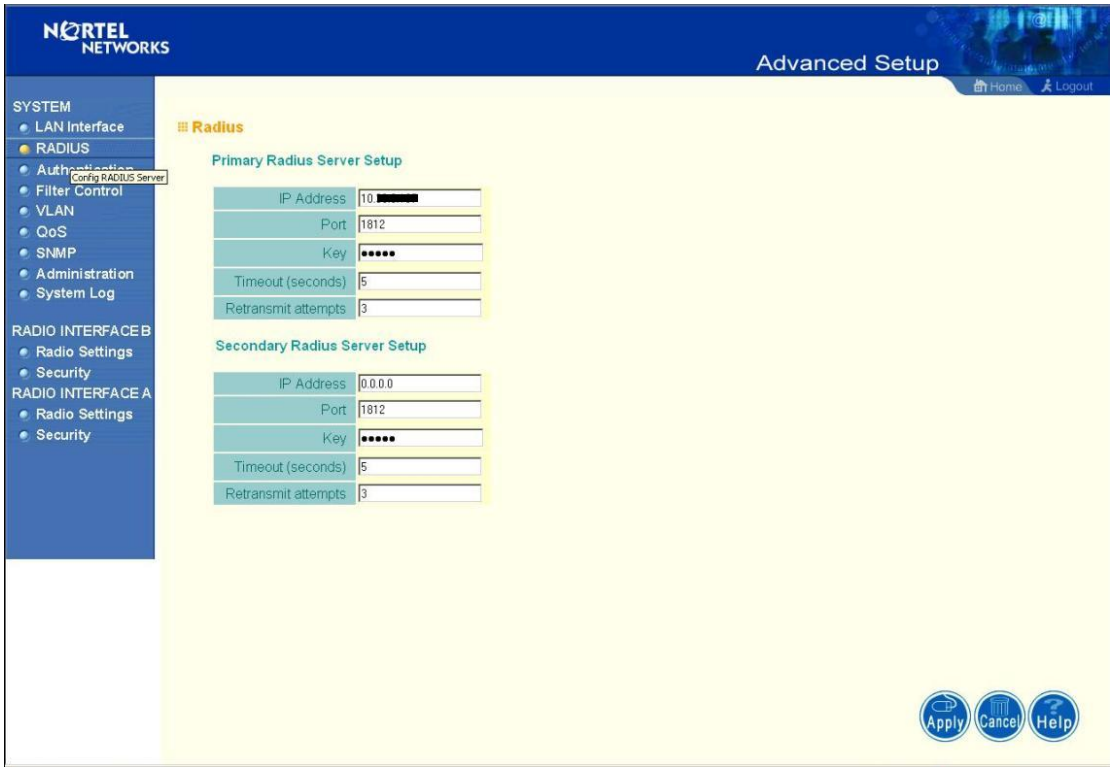


Anhang D

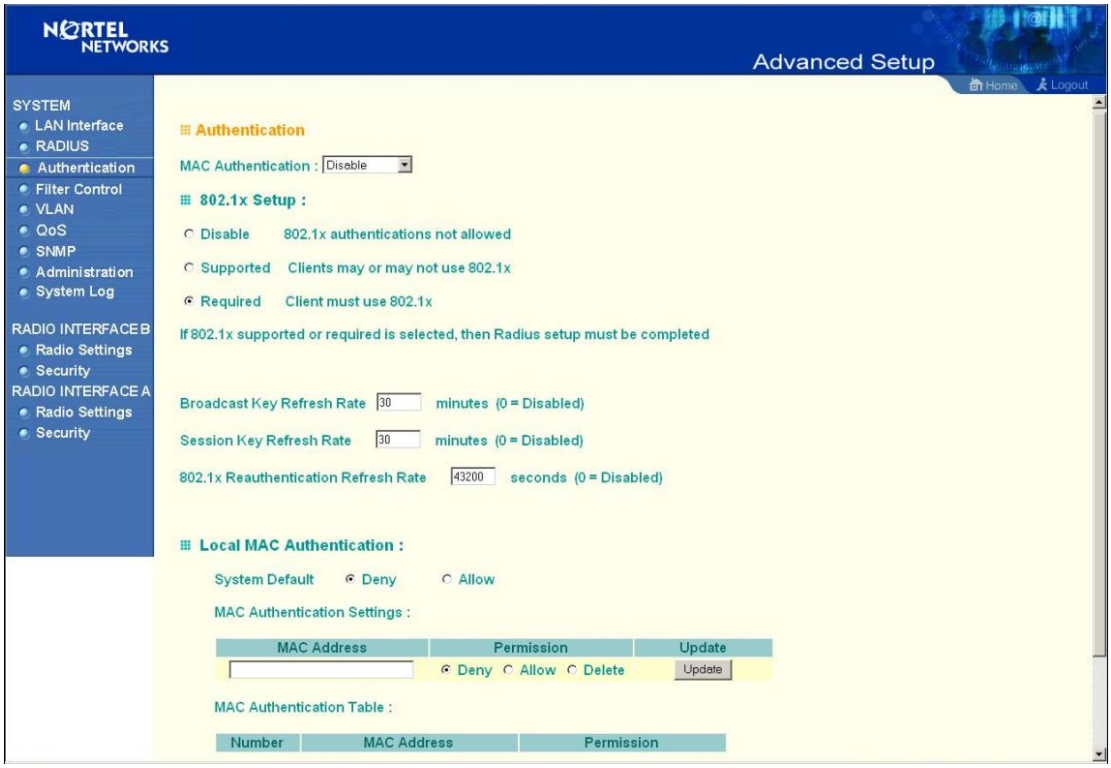
Konfiguration der Access-Points



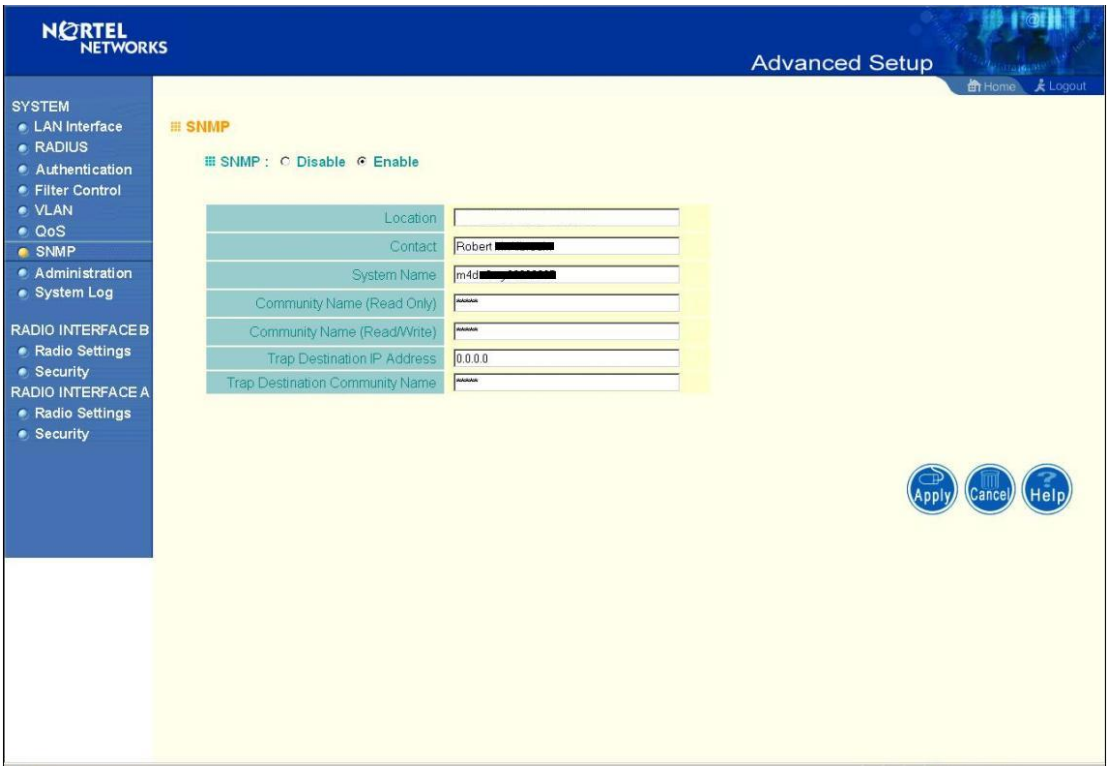
Konfiguration der Access-Points



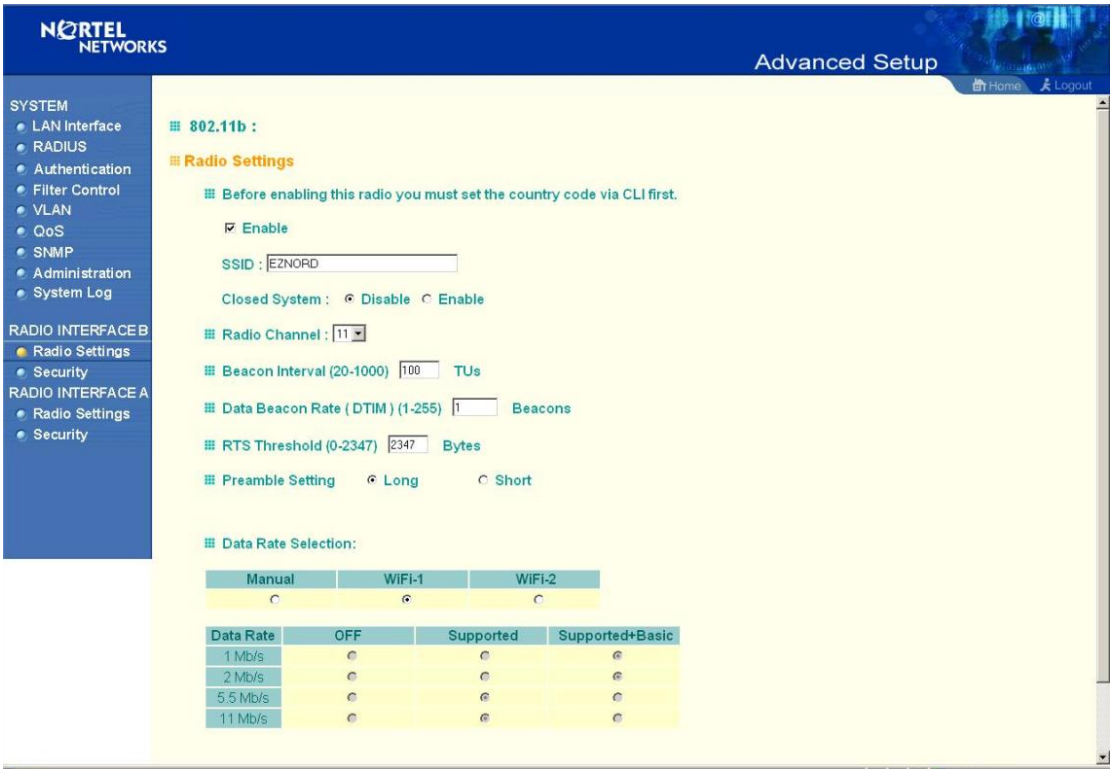
Konfiguration der Access-Points



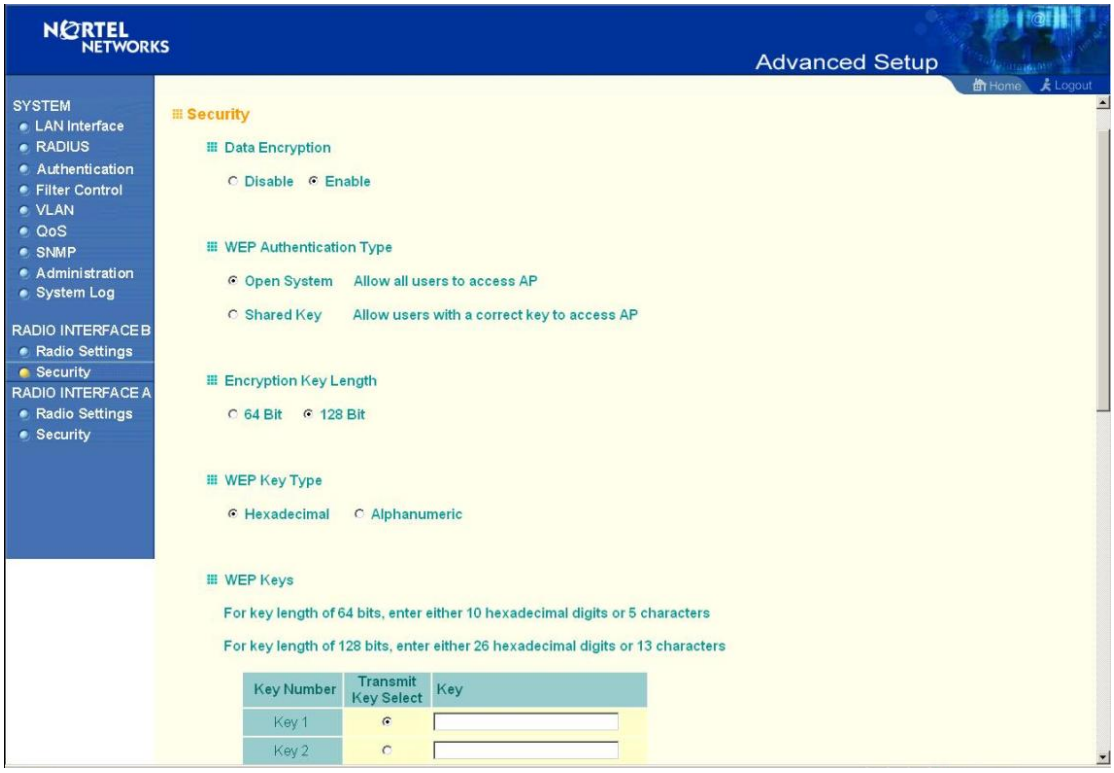
Konfiguration der Access-Points



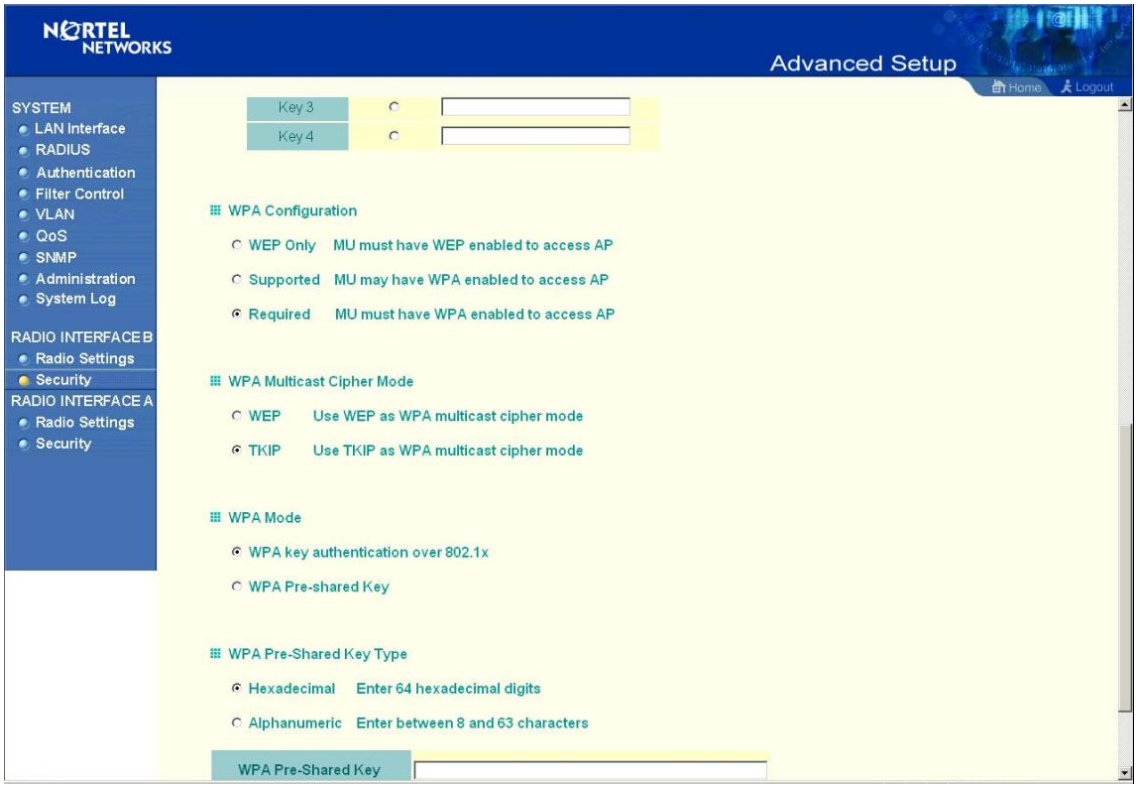
Konfiguration der Access-Points



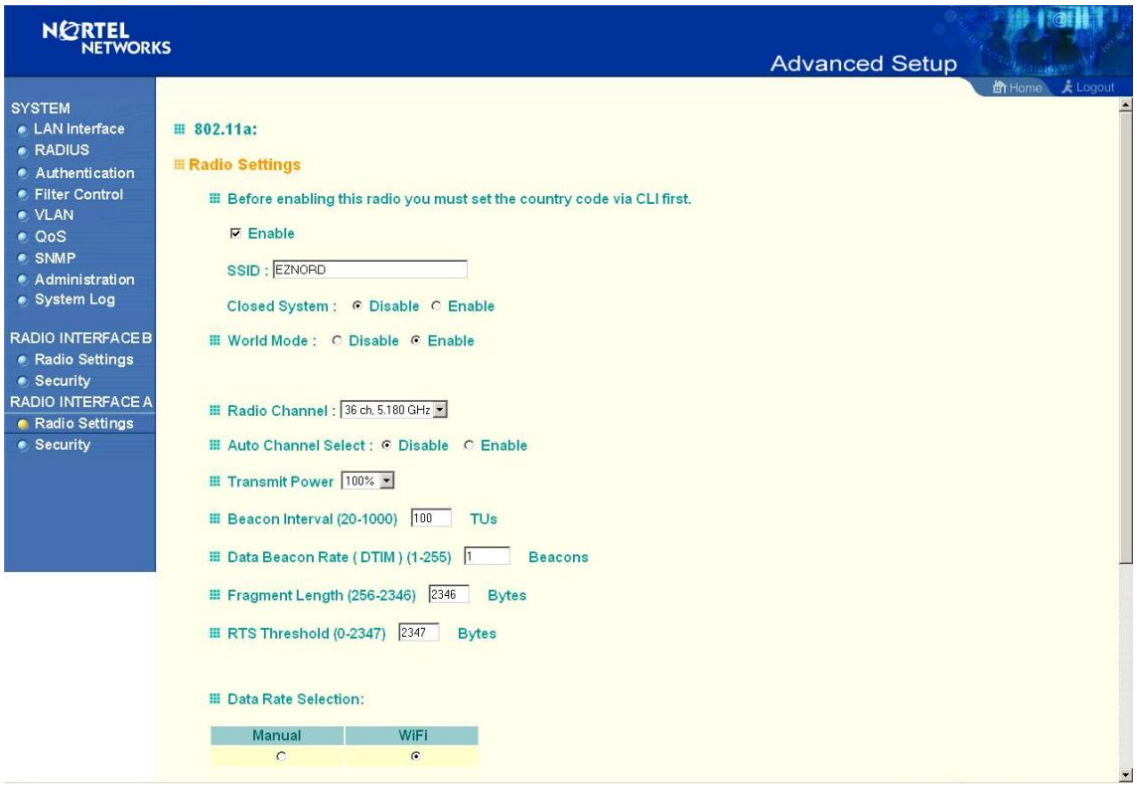
Konfiguration der Access-Points



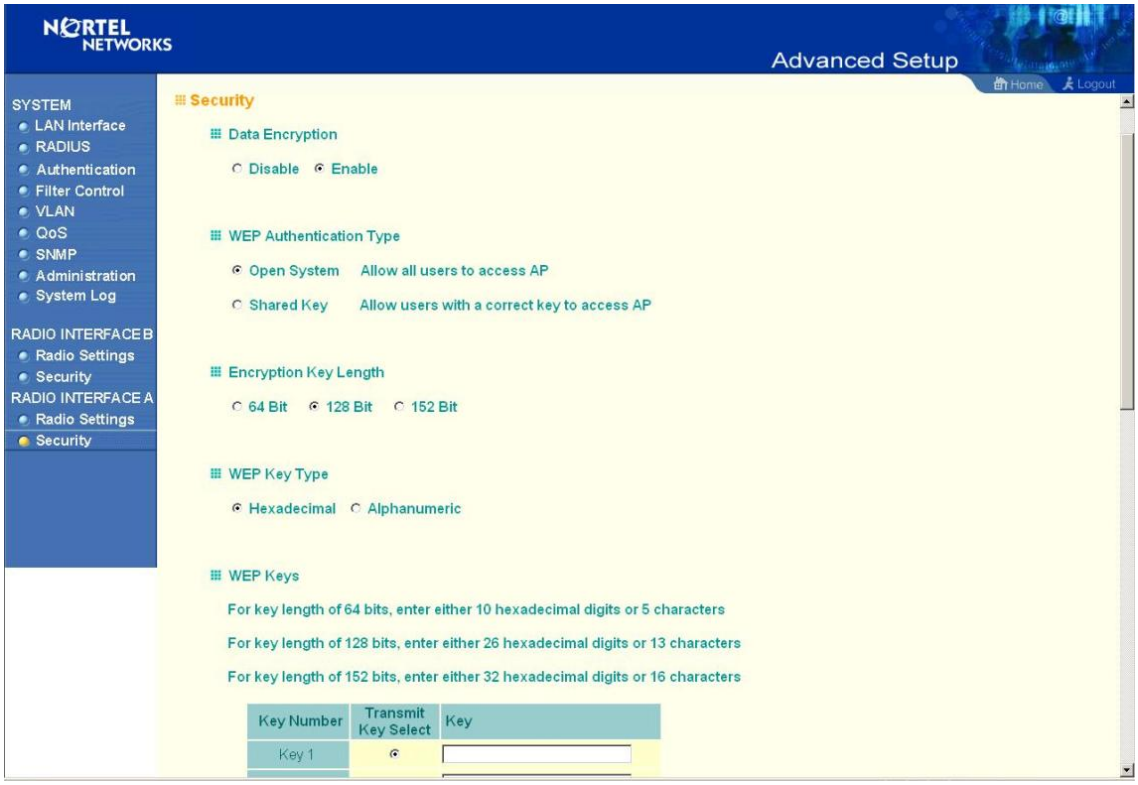
Konfiguration der Access-Points



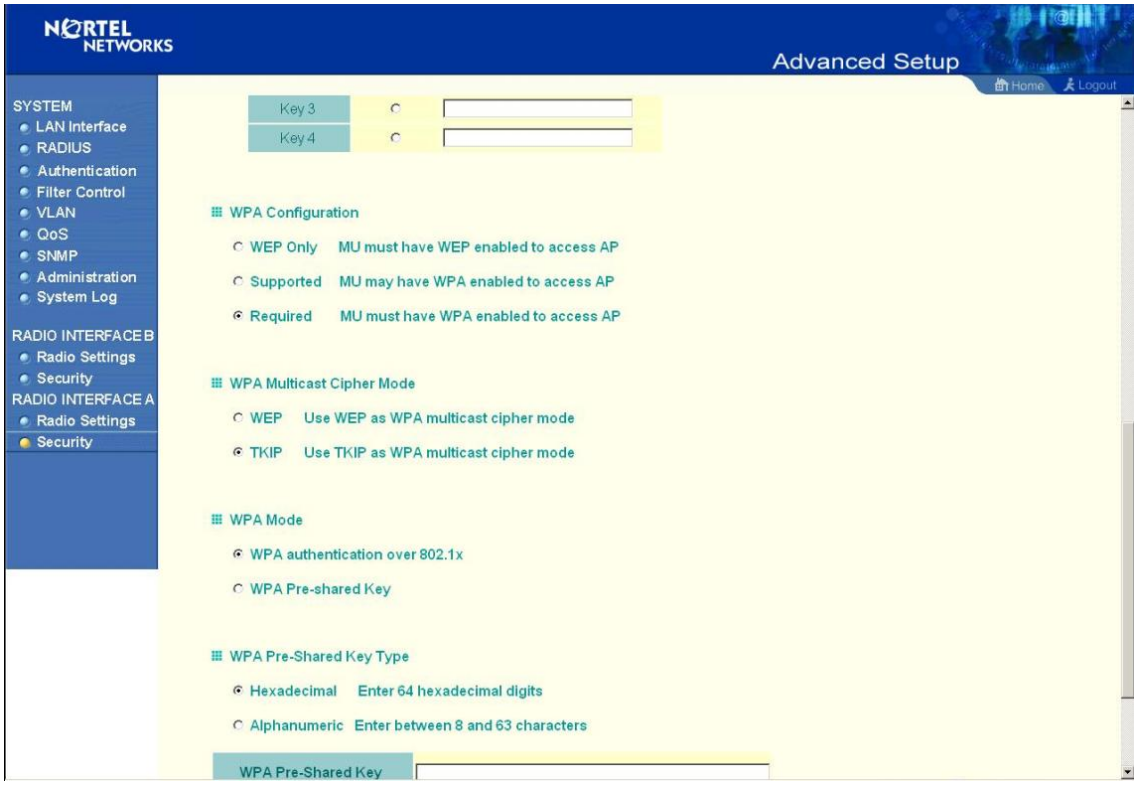
Konfiguration der Access-Points



Konfiguration der Access-Points



Konfiguration der Access-Points



Anhang E

Glossar & Quellenverzeichnis

Glossar

Wireless-LAN	„Wireless Local Area Network“: Drahtloses lokales Netzwerk
Radius-Server	„Remote Authentification Dial-In User Service”: Software, die es ermöglicht, sich über Wahlleitungen an einem Netz anzumelden
WPA	„Wi-Fi Protected Access“: Verschlüsselungsmethode für ein Wireless LAN
Access Point	Sende – und Empfangsstation bei WLAN
IEEE 802.11	Bezeichnet einen Industriestandard für drahtlose Netzwerkkommunikation
Power over Ethernet	Netzwerkgeräte werden über Ethernet mit Strom versorgt
Distributionen	Unterschiedliche Versionen
SSL	„Secure Sockets Layer“: Bietet die Möglichkeit der verschlüsselten Übertragung
PEAP	„Protected Extensible Authentication Protocol“: Wird zur Verschlüsselung verwendet
CA.all Script	Script zur Erstellung von Zertifikaten
DHCP	„Dynamic Host Configuration Protocol“: Protokoll für die automatische IP-Adress-Vergabe
DNS	„Domain Name Service“: Umsetzen von Namen auf IP-Adressen
SSID	„Service Set Identifier“: Bezeichnet den Namen des WLAN
MAC-Adresse	„Media Access Control“: Identifizierungsnummer einer Netzwerkkarte
WEP	„Wired Equivalent Privacy“: Standardverschlüsselungsalgorithmus für WLAN

Quellenverzeichnis

http://www.de.tomshardware.com/network/20030525/index.html

http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/WirelessLAN

www.openssl.org

www.freeradius.org

www.wikipedia.de

Autor: Michael Kofler, „Linux – Installation, Konfiguration, Anwendung“, Addison - Wesley Verlag, Erscheinungsjahr 2000

Anhang F

Zeit- und Maßnahmenplan

	Vorgangsname	Arbeit	Anfang	Ende	Dauer
1	**Projektstart**	0 Std.	Di 29.03.05	Di 29.03.05	0 Tage
2	**Gesamtprojekt**	**35 Std.**	**Di 29.03.05**	**Fr 08.04.05**	**9 Tage**
3	Informationsbeschaffung	3 Std.	Di 29.03.05	Di 29.03.05	3 Std.
4	Planung & Bedarfermittlung	5 Std.	Mi 30.03.05	Mi 30.03.05	5 Std.
5	Bestellphase	0 Std.	Do 31.03.05	Mo 04.04.05	3 Tage
6	Installation & Konfiguration	8 Std.	Di 05.04.05	Di 05.04.05	8 Std.
7	Funktions- und Sicherheitstest	6 Std.	Mi 06.04.05	Mi 06.04.05	6 Std.
8	Dokumentation	13 Std.	Do 07.04.05	Fr 08.04.05	13 Std.
9	**Projektende**	0 Std.	Fr 08.04.05	Fr 08.04.05	0 Tage