Dokumentation

der betrieblichen Projektarbeit

Kabellose Gebäudevernetzung und Anbindung an eine bestehende Netzwerkstruktur mit Hilfe von Richtfunkantennen

durchgeführt von

Thomas Zirkel
Geburtsort: Nordhorn
Geburtsdatum: 12.03.1970

Auszubildender im Beruf

Fachinformatiker-Systemintegration

im

Niedersächsischen Landesbetrieb für Wasserwirtschaft
Küsten- und Naturschutz (NLWKN)

Inhaltsverzeichnis

Projektdokumentation

Vorwort

Wörter und Begriffe, die im Glossar näher erläutert sind, werden bei erstmaliger Nennung in der Dokumentation *kursiv* dargestellt.
Verweise auf Dokumente im Anhang werden farbig gekennzeichnet.

1 Projektvorphase

1.1 Ausgangslage

Der Niedersächsische Landesbetrieb für Wasserwirtschaft, Küsten- und Naturschutz Betriebsstelle Brake-Oldenburg (NLWKN) hatte bis zum 31.12.2004
78 Mitarbeiter. Nach der Verwaltungsreform in Niedersachsen erhöhte sich diese Zahl auf 169 Mitarbeiter. Hinzu kamen ein Dienstgebäude in Oldenburg sowie ein weiteres in Wilhelmshaven. Das Gebäude in Wilhelmshaven steht in 100 Meter Entfernung zu einem bestehenden Dienstgebäude (Anlage K), welches bereits netzwerktechnisch mit einer 2 MBit Standleitung an das Landesdatennetz angebunden ist. Das zusätzliche Gebäude in Wilhelmshaven muss nun in die bestehende Netzwerkstruktur integriert werden. Dieses Gebäude verfügt über keine strukturierte Verkabelung.

1.2 Kosten/ Nutzen Analyse

Aufgrund der angespannten finanziellen Lage des Land Niedersachsen ist die Finanzierung eines Projektes dieser Art, einer genauen Prüfung zu unterziehen.
Das Projektumfeld lässt mehrere Arten der Primäranbindung des Gebäudes zu und aufgrund dessen müssen alle Möglichkeiten kalkuliert werden.
Weiterhin ist zu prüfen, wie die Gebäudevernetzung umgesetzt werden soll.
Drei Konzepte müssen bei der Kostenanalyse betrachtet werden.
Die Anbindung durch:

- Standleitung an das Landesnetz
- Installation einer strukturierten Verkabelung
- Einsatz der W-LAN Technik.

1.2.1 Standleitung

Durch den Verbindungs- und Benutzungszwang, dem der NLWKN gegenüber dem Informatikzentrum Niedersachsen (IZN) unterliegt, bleiben bei der Auswahl für den Anbieter der Standleitung keine Alternativen. Dies bedeutet, dass dem NLWKN, für die Bereitstellung einer Standleitung durch das IZN, monatliche Kosten in Höhe von **1650,-€** entstehen würden.
Durch eine benötigte Gebäudeverkabelung würden zusätzliche Kosten entstehen.
(siehe 1.2.2)

1.2.2 Strukturierte Verkabelung

Die Anbindung an das Nachbargebäude hätte aufwendige Erdarbeiten und genehmigungsrechtlichen Aufwand zur Folge, da beide Gebäude auf einem Deichabschnitt errichtet sind. Die Kosten für eine Sekundärverkabelung sowie die Gebäudeanbindung ergeben sich nach einer Preisermittlung wie folgt:

2x	24 Port 10/100/1000 GBit Switch 19“	760,00 €
1x	24 Port Patch Panel 19“	35,00 €
1x	19” Schrank, klein	300,00 €
24x	CAT5 TP Kabel 0,5m	15,00 €
300 m	CAT5 TP Kabel	250,00 €
100 m	LWL Kabel, Multimode, duplex SC/SC	700,00 €
4x	Mini-GBIC Modul	576,00 €
16x	Anschlussdosen RJ45	320,00 €
Kleinmaterial (RJ45 Stecker, Leerrohr, Dichtmasse usw.)		300,00 €
Erdarbeiten und Gebäudeverkabelung durch Fremdfirma		
3 Personen, 3 Tage(8 Std.) = 72 Std. x 50 €[1]		3600,00 €
	Gesamt	**6856,00 €**

1 Durchschnittsarbeitslohn für Netzwerkarbeiten

1.2.3 Wireless-LAN

Um letztendlich entscheiden zu können, welches Konzept bei der Gebäudevernetzung und der Anbindung an das Landesnetz zum Einsatz kommen soll, muss der aufkommende Datenverkehr sowie die Anwendungen, die die Benutzer benötigen, betrachtet werden. Es muss den Benutzern ermöglicht werden das Internet, Intranet, den Mail-account sowie das Speichern auf den Netzlaufwerken, zu nutzen. Die Bandbreite von maximal 54 MBit, die im WLAN für diese Dienste zu Verfügung stehen würde, ist ausreichend.
Alle drei Konzepte entsprechen den Anforderungen und sind technisch umsetzbar.

1.2.4 Nutzwertanalyse

		Konzept 1		**Konzept 2**		**Konzept 3**	
		Standleitung		strukturierte Verkabelung		W-LAN	
Auswahlkriterien	**Bewertungs-Faktor**	**Erfüllungs-grad**	**erreichter Wert**	**Erfüllungs-grad**	**erreichter Wert**	**Erfüllungs-grad**	**erreichter Wert**
hohe Verfügbarkeit	20%	100%	20,0%	100%	20,0%	90%	18,0%
gute Skalierbarkeit	5%	90%	4,5%	90%	4,5%	65%	3,25%
Administration	10%	70%	7,0%	80%	8,0%	65%	6,5%
hohe Sicherheit	25%	99%	24,75%	99%	24,75%	80%	20,0%
niedrige Kosten	40%	10%	4,0%	15%	6,0%	100%	40,0%
Summen	100%		**60,25%**		**63,25%**		**87,75%**

2 Konzeptionsphase

2.1 Projektbeschreibung

Dieses Projekt beinhaltet die Gebäudevernetzung mit Hilfe von Access- Points (AP) sowie die Primäranbindung an eine bestehende Netzstruktur mit Richtfunkantennen. Weiterhin muss die Datenübertragung mit größtmöglicher Sicherheit erfolgen, welche mit den zur Zeit verfügbaren W-LAN Standards und VPN Lösungen sichergestellt wird.

2.2 Projektumfeld

2.2.1 Gebäudebesichtigung

Bei der Objektbegehung war es wichtig, die Dämpfungseigenschaften des Gebäudes sowie eventuelle Störquellen auf der Richtfunkstrecke zu lokalisieren.
Um eine optimale Funkausleuchtung innerhalb des Gebäudes zu erreichen, ist es im Vorfeld wichtig, die benötigte Anzahl der AP´s zu ermitteln.
Temporär wurde ein AP aufgestellt, um an den Standorten der jeweiligen Clients die Signalstärke mit Hilfe eines Analysetools *(Netstumbler*) festzustellen.

2.2.2 Ist-Analyse

In dem neuen Gebäude in Wilhelmshaven existiert keine strukturierte Verkabelung. Im Erdgeschoss befinden sich zwei und im Obergeschoss vier Rechner. Alle Rechner sind mit dem Betriebssystem Windows XP+SP2 ausgestattet. Das Gebäude ist ein Altbau mit dicken Stahlbetondecken. Das in einer Entfernung von 100 m gegenüberliegende Gebäude ist strukturiert verkabelt und bereits mit einer 2Mbit Standleitung an das Landesnetz angebunden. Dort ist ein Windows 2003 Server vorhanden, der auch als VPN Server dienen wird. Die Gebäude sind auf einem Deichabschnitt errichtet und zwischen ihnen existieren keinerlei Hindernisse die Reflexionen auf der Richtfunkstrecke erzeugen könnten.

2.2.3 Festlegen des Sollkonzepts

Nach Auswertung aller vorliegenden Erkenntnisse der einzelnen Konzepte sowie Analyse des Projektumfeldes, entschieden sich die EDV-Verantwortlichen im NLWKN für den Einsatz der WLAN Technologie.
Daraus ergeben sich folgende Punkte für das Sollkonzept:

- Installation der AP´s
- Installation der Richtfunkantennen
- Installation der WLAN PCI Karten

- Optimale Funkausleuchtung im Gebäude
- Die Datensicherheit muss gewährleistet sein! Zuteilung der entsprechenden Netzlaufwerke muss umsetzbar sein (sicherstellen der Datensicherung).
- Zugang zum Intra-und Internet
- Abrufen der persönlichen e-mail´s
- Konfigurieren der IP, MAC und Portfilter
- Sicherstellen der gesicherten Datenübertragung (WEP, VPN)

2.2.4 Hardwareauswahl

Bei der Hardwareauswahl wurden folgende Kriterien betrachtet:
- Leistungsdaten der AP´s und Antennen
- Skalierbarkeit mit anderen Herstellern
- Preis- Leistungsverhältnis
- Ausstattung der Geräte (802.11x Standard, Antennenanschlüsse, Sicherheits-Features)
- Hersteller Support (Firmware update, Support usw.)

Hilfreich bei der Auswahl waren Hardwaretests und Erfahrungsberichte in einschlägigen Computer Zeitschriften und Internetseiten. Nach Auswertung dieser Tests fiel die Wahl auf den Hersteller US-Robotics. Die Geräte dieses Herstellers haben, auch unter schwierigen äußeren Einflüssen, eine sehr gute Sendeleistung. Weiterhin unterstützen sie alle zur Zeit verfügbaren 802.11x Standards und sind kompatibel mit anderen Herstellern.
Die *Patch-und Panelantennen* werden von dem Hersteller D-Link beschafft.

2.2.5 Projektschnittstellen

Hardwareinstallation:

Im Vorfeld wurden die Termine mit dem Haustechniker abgesprochen. Es wurde sichergestellt, dass bei Lieferung der Hardware sofort mit der Wandmontage der AP´s und Antennen begonnen werden kann. Weiterhin müssen zusätzliche Stromleitungen installiert werden, um die optimale Gerätepositionierung zu gewährleisten.

Verfügbarkeit des Domainservers:

Parallel zu diesem Projekt wird das Projekt Windows Server 2003 von einer weiteren Auszubildenden durchgeführt. Dieser Server wird in dem bereits bestehenden Gebäude eingesetzt. Um die spätere VPN Verbindung einrichten zu können, muss die Konfiguration des Verzeichnisdienst Active Directory Service abgeschlossen sein. Terminabsprachen aufgrund der verschiedenen Projektabläufe sind zwingend notwendig.

3 Preisvergleich und Beschaffung

Der Preisvergleich für die benötigte Hardware erfolgte ausschließlich über das Internet. Mehrere Onlineshops wurden auf Angebotspreis, Service, Lieferbedingungen und Garantieleistungen verglichen. Hierbei war nicht nur der günstigste Preis ausschlaggebend. Service und Garantiebedingungen flossen bei der Kaufentscheidung mit ein, da bei einem Hardwareausfall schnelle Ersatzlieferung im Garantiefall von großer Bedeutung ist. Vorsorglich wird ein AP und AP-Router zusätzlich beschafft, um bei einem Hardwareausfall die laufenden Arbeitsprozesse sicherstellen zu können.

Folgende Hardware wurde beschafft:

Hersteller: US.Robotics

Menge	Artikel		Einzelpreis	Gesamtpreis
2	Access Point Router	USR 805050	76,59 €	162,56 €
3	Access Point	USR 805450	115,00 €	345,00 €
4	PCI-Wireless Karte	USR 805416	40,53 €	162,12 €

Hersteller: D-Link

2	Outdoor-Antenne 18dBi Panel	137,46 €	274,92 €
2	Indoor-Antenne 5dBi Patch	28,12 €	56,24 €
2	Antennen Verlängerungskabel	9,35 €	18,70 €
2	PCI-Wireless Karte DWL 520	64,70 €	129,40 €
	Sromkabel und Überputzsteckdosen		20,00 €
		Gesamt:	1168,94 €

Die Geräte wurden bei dem Onlineshop Mindfactory, Reichelt Elektronik und Future Vertriebs GmbH gekauft (Rechnungen siehe Anlage I1-7) Kosten für Software oder zusätzliche Lizenzen fielen nicht an. Die Arbeitsleistung für die Montagearbeiten durch den Haustechniker ist bei allen drei Konzepten etwa gleich hoch und wird daher nicht gesondert betrachtet. Eine Kalkulation der Personalkosten ist in diesem Fall schwierig, da Arbeiten durch hauseigenes Personal kostenmäßig nur bedingt zu erfassen sind.

4 WLAN Standard

Die Arbeitsgruppe Institute of Electrical and Electronical Engineers (IEEE) ist zuständig für die Definition der WLAN-Standards. Im Jahr 2003 wurde der Standard 802.11g von der IEEE definiert. Dieser ermöglicht Datenraten bis 54 MBit/s. Er arbeitet im 2,4 GHz Frequenzband und mit dem Übertragungsverfahren *OFDM*.
Der Hersteller US.Robotics erreicht eine Bruttodatenrate von 100 MBit/s. Dies wird erreicht, indem im MAC-Frame die Nutzdatenlänge von durchschnittlich 1500 Bytes auf 4000 Bytes vergrößert wurde. Angewandt wird dieses Verfahren erst ab einer Datenrate von 11MBit/s, da wegen der längeren Übertragungsdauer die Gefahr der Beeinflussung zu groß währe. US.Robotics arbeitet mit dem *PBCC* Übertragungsverfahren.

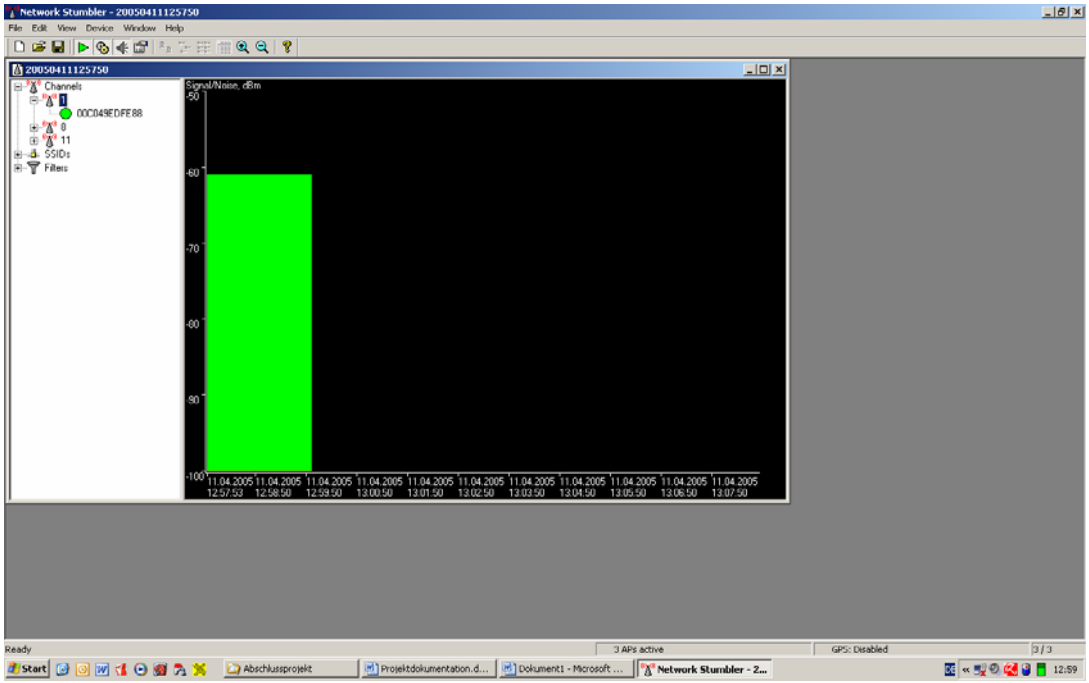
5 Installation der Hardware

5.1 Antennen

Da die Richtfunkstrecke auf einem Deichabschnitt an der Nordsee (Jadebusen) betrieben wird, muss von erheblichen Witterungseinflüssen ausgegangen werden. Die Anforderung an die mechanische Sicherheit ist hierbei sehr hoch. Die Antennenanlagen müssen so befestigt werden, dass sie sich bei starker Windlast nicht dejustieren. Das Einschleifen eines Blitzschutzes sollte grundsätzlich erfolgen, da bei einem Blitzschlag die aktive Hardware des WLAN beschädigt werden kann.
Bei den eingesetzten Richtfunkantennen handelt es sich um so genannte *Panel-Antennen* mit einem *Öffnungswinke*l von 15° und einem Antennengewinn von 18 *dBi* (Datenblatt siehe Anlage F3). Weiterhin wurden Patch-Antennen verwendet, mit denen innerhalb des Gebäudes eine Reichweitensteigerung durch eine Richtfunkcharakteristik erreicht wird. Diese besitzen einen Öffnungswinkel von 65° und einen Antennengewinn von 5 dBi.

5.2 Access Points

Um eine fehlerfreie Datenübertragung sowie eine optimale Bandbreite in der WLAN-Infrastruktur sicherzustellen, müssen die AP´s optimal platziert werden. Hierbei ist nun die bei der Gebäudebesichtigung durchgeführte Funkausleuchtung hilfreich. Die AP´s wurden an den vorher festgelegten Standorten montiert (Datenblatt siehe Anlage F1+2).
Die Panel-Antennen wurden, mit Hilfe der mitgelieferten *Pigtails*, an die AP`s angeschlossen und justiert. Die Justierung wurde ebenfalls mit dem Tool Netstumbler überprüft. Hierbei wurde an dem gegenüberliegendem Gebäude, auf Höhe der zweiten Antenne, ein Laptop platziert und die Signalstärke festgestellt. In Abhängigkeit der Signalstärke wurde dann die Antenne optimal ausgerichtet.



5.3 Clients

Die Clients wurden mit den PCI WLAN Karten USR 805416 ausgestattet. Die Installation war mit wenig Aufwand abgeschlossen. Die WLAN PCI Netzwerkkarten wurden in den PCI Slot des PC´s eingebaut und nach Installation der Gerätesoftware sofort von dem Betriebssystem erkannt.
Die Mindestanforderungen an die Hardware und die Leistung sind bei allen Clients gegeben.

5.4 Gesetzliche Bestimmungen

Es ist jedermann gestattet, grundstücksübergreifende Datenübertragungen vorzunehmen. Dabei ist aber zu beachten, dass die 2,4 GHz WLAN Funkstrecke bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) angemeldet werden muss. Die Richtfunkstrecke wird nun bei der RegTP zentral registriert. Hierdurch entstehen dem Betreiber keinerlei Genehmigungskosten. Es müssen der RegTP formlos folgende Informationen mitgeteilt werden:

- Genauer Standort der Funkanlage
- Antennenparameter (Antennengewinn und Öffnungswinkel)
- Höhe der Antennen über Grund
- Datum der Inbetriebnahme
- Voraussichtliches Datum der Außerbetriebnahme

Die regionale Zuständigkeit kann auf der Homepage der RegTP nachgelesen werden.
Die Richtfunkstrecke dieses Projektes wurde ordnungsgemäß bei der RegTP angemeldet. (siehe Anlage G)

6 Konfiguration der Hardware

6.1 Access Point

Da in der Domainstruktur des NLWKN-Brake statische IP-Adressen vergeben werden, wird auch den AP´s eine statische IP zugeteilt.
Die AP´s der WLAN-Infrastruktur in Wilhelmshaven sind wie folgt konfiguriert:
(siehe Netzwerkplan Anlage C)

Access Point Router:

IP	:10.xxx
Subnet Mask	:255.255.255.0
Gateway	:10.xxx
SSID	: [redacted]
Channel	: x
DHCP	: disable
SSID broadcast	: disable

Access Point, client:

IP	:10.xxx
Subnet Mask	:255.255.255.0
Gateway	:10.xxx
SSID	: [redacted]
Channel	: x
DHCP	: disable
SSID broadcast	: disable

Access Point:

IP	:10.xxx
Subnet Mask	:255.255.255.0
Gateway	:10.xxx
SSID	: [redacted]
Channel	: x
DHCP	: disable
SSID broadcast	: disable

Alle Geräte innerhalb der WLAN-Infrastruktur müssen im gleichen IP-Adressbereich und der gleichen *SSID* betrieben werden.
Es werden die Kanäle x, x, x auf den AP´s verwendet, damit die Geräte auf überlappungsfreien Frequenzen arbeiten und es zu keiner Kanalbeeinflussung kommt.
Alle Geräte in dieser WLAN-Infrastruktur werden mit dem *802.11g* Standard betrieben.

6.2 Clients

Alle Clients in der WLAN-Infrastruktur bekommen ebenfalls eine statische IP-Adresse zugewiesen. In den Eigenschaften der Drahtlosnetzwerkeinstellungen werden die SSID und das Verhalten beim Verbindungsaufbau konfiguriert. Dabei wird festgelegt, ob der Client sich sofort oder manuell mit dem AP verbindet. Weiterhin wird festgelegt, ob der Client im Ad-hoc oder Infrastrukturmodus arbeiten soll.

7 Konfiguration der Sicherheitsmechanismen

7.1 Access Point

Die Schnittstelle zum LAN des NLWKN Brake-Oldenburg ist ein Access-Point Router. Dieser wurde anstatt eines AP eingesetzt, weil er über eine zusätzliche Firewall und Filtereigenschaften verfügt und somit einen weiteren Schutz gegen ungewolltes Eindringen in das Netzwerk bietet.
Die DHCP-Funktion wird auf den Ap´s ausgeschaltet. Dies hat einen gewissen Sicherheitsaspekt, da bei einem unbefugten Verbindungsversuch diesem Client keine IP-Adresse zugewiesen wird. Weiterhin wird der SSID Broadcast auf den AP´s abgeschaltet. Dadurch wird erreicht, dass der AP nach außen hin nicht sichtbar ist. Den Mitarbeitern wird strikt untersagt „wilde Access Points“ in die WLAN-Infrastruktur einzubinden, da hierbei die eingerichteten Sicherheitsmechanismen umgangen werden.
Zusätzlich zu der *VPN* Verschlüsselung wird die *WEP* Verschlüsselung verwendet. Der Zugang zum Netzwerk und die zu übertragenden Daten werden durch die VPN-Verbindung abgesichert. Die Kommunikation, zwischen Client und AP würde aber ohne WEP unverschlüsselt stattfinden. Ohne WEP könnten relevante Zugangsdaten zum AP mit Netzwerk-Sniffern ohne viel Aufwand ausspioniert werden.
Zusätzlich werden Filtermechanismen wie MAC, IP, Port und Protokollfilter angewandt.
Um eine zusätzliche Sicherheit zu erlangen werden die Access Points mit Zeitschaltuhren versehen, die das WLAN von 19.00 Uhr bis 06.00 Uhr und am Wochenende abschalten.

7.1 Clients

Standardmäßig ist bei allen Clients die Windows-Firewall und ein Virenprogramm installiert. Der VPN-Client wird nachträglich über die Netzwerkumgebung installiert und konfiguriert. Die Einstellungen für die drahtlose Netwerkverbindung werden in den Eigenschaften der Netzwerkkarte vorgenommen. Hier werden die vorher festgelegten Verschlüsselungen und Authentifizierungen übernommen.

7.3 Einrichten der VPN-Verbindung

7.3.1 Server

Das Einrichten von VPN-Verbindungen setzt bestimmte Hardwareanforderungen voraus. In unserem Fall ist der Server mit der Dualprozessor Technik und 2GB Arbeitsspeicher ausreichend ausgestattet.
Da die VPN-Verbindung von maximal sechs Clients genutzt wird, muss mit keinem Leistungseinbruch während des Betriebes gerechnet werden.

Um die VPN-Verbindung nutzen zu können, muss auf dem Windows Server 2003 der *RAS* (Remote Access Service) Dienst sowie der *IIS-Server* installiert werden. Die Konfiguration des Active Directory Service war bereits abgeschlossen.
Als VPN-Protokoll wird das *L2TP/ IPSec* genutzt. Mit diesem Protokoll ist es möglich, eine 168-Bit-Triple-DES Verschlüsselung (3DES) herzustellen. Um dieses Protokoll nutzen zu können, ist die Installation eines Zertifikates notwendig. Dieses Zertifikat wird später von den VPN-Clients benötigt, um sich gegenüber dem VPN-Server authentifizieren zu können. Als Authentifizierungsprotokoll wird EAP-TLS verwendet.
Es wurde eine Zertifikatsbasierte Authentifizierung gewählt, da sie erheblich sicherer als eine Kennwortbasierte Authentifizierung ist.
Bei der Konfiguration des RAS-Servers wird ein IP-Adressenpool festgelegt. In diesem Adressenpool wird der Adressbereich von 10.x.x.x bis 10.x.x.x eingerichtet. Dies bedeutet, dass es maximal sechs Clients möglich ist, sich mit dem VPN-Server zu verbinden.
Die Adressenzuteilung erfolgt nur für die VPN-Server/Client Verbindung über DHCP und ist unabhängig von der Hardwarekonfiguration im Bereich der Netzwerkeinstellungen.

7.3.2 Clients

Über die Eigenschaften der Netzwerkumgebung wird ein VPN-Client installiert und konfiguriert. Weiterhin ist Vorraussetzung, dass die Clients bereits in der Domainstruktur integriert sind, damit eine Verwaltung über die Active Directory möglich ist. Damit eine gesicherte VPN-Verbindung zum RAS-Server hergestellt werden kann, ist es nötig, die Zertifikatsstruktur auf dem Client einzurichten. Dies erfolgt webbasiert, indem der VPN-Client das benötigte Zertifikat von der Zertifizierungsstelle (VPN-Server) erhält.
Nach Abschluss der Konfiguration muss bei der Benutzeranmeldung die Verbindung über DFÜ stattfinden, um die VPN-Verbindung direkt bei der Anmeldung sicherzustellen.

8 Testphase

Die Überprüfung des WLAN erfolgte im laufenden Betrieb und wurde während der Hardwareinstallation sowie bei Aktivierung der einzelnen Sicherheitsmechanismen wiederholt. Da die Testphasen im Realbetrieb stattfanden, konnten festgestellte Probleme in den Arbeitsabläufen sofort lokalisiert und abgestellt werden.
Im laufenden Betrieb des WLAN wurden erhebliche Schwankungen in den Pingzeiten festgestellt. Dies resultierte aus den hohen Dämpfungseigenschaften des Gebäudes. Die hohen Dämpfungseigenschaften störten erheblich den fehlerfreien Datenaustausch. Daraufhin wurden der AP im Obergeschoss und der AP im Untergeschoss mit einem CAT 5 TP/Netzwerkkabel verbunden, um diese Funkstrecke zu überbrücken. Damit wurde eine erhebliche Performancesteigerung bei der Datenübertragung erreicht.
Während der Access Point Konfiguration wurden auf diesen Firmwareupdates installiert. Dies hatte zur Folge, dass das gesamte WLAN Netz ohne Funktion war.

Nach Rücksprache mit dem Support von US. Robotics und der eigenen Fehlereingrenzung wurde festgestellt, dass das Firmwareupdate Fehler in den Access Point Funktionen (AP-Client) verursachte. Mit Installation der älteren Firmwareversion wurde das Problem behoben.Nach dem Aktivieren der Verschlüsselung auf den AP`s und den Clients, konnten keine Einbußen in der Höhe des Datendurchsatzes festgestellt werden. Nach dem Einrichten der VPN-Verbindung ist die Benutzeranmeldung aufgrund der Authentifizierungsmethode etwas langsamer.

9 Erweiterungen des 802.11 Standard

Die Arbeitsgruppe IEEE arbeitet ständig an Erweiterungen des 802.11x Standard. Geplant ist eine Datenratenerhöhung von 108 bis 320 MBit/s. In der folgenden Tabelle werden die wichtigsten Standards, die zur Zeit in Arbeit sind, aufgeführt.
Die neuen Standards werden sich nicht mehr mit Firmwareupdates integrieren lassen. Wenn in naher Zukunft die neuen Standards eingesetzt werden sollen, wird dies nur mit neuer Hardware möglich sein.

Arbeitsgruppen	Beschreibung
IEEE 802.11e	MAC-Erweiterungen für die Implementierung von Quality of Service und eine Performance-Steigerung
IEEE 802.11f	Definition des Inter Access Point Protocols (IAPP)
IEEE 802.11i	MAC-Erweiterungen zur Verbesserung der Datensicherheit und Authentifizierung
IEEE 802.11n	Neuer MAC- und PHY-Layer für Datenraten von 108 bis 320 MBit/s

10 Resümee

Die vorgegebenen 35 Stunden für die Projektarbeit (Anlage E) konnten eingehalten werden. Von dem geplanten zeitlichen Ablauf in dem Projektantrag (Anlage B) musste ich nicht abweichen.
Das Projekt konnte so umgesetzt werden, dass das Sollkonzept erfüllt wurde. Das WLAN des NLWKN ist im Realbetrieb stabil und unterstützt alle geforderten Anforderungen. Durch den Einsatz der VPN-Verbindung und den zusätzlichen Sicherheitsmechanismen ist das kabellose Netzwerk so sicher, dass nur mit dem Erlangen von internen Daten einem Hacker möglich ist, in das WLAN bzw. Netzwerk von außerhalb einzudringen.
Das WLAN wird ständig, durch Auswertung von Log-Dateien überwacht und Eindring-versuche können sofort unterbunden werden. Auch wechselnde Schlüssel und Passwörter erhöhen die Sicherheit. Eine Änderung der Verschlüsselungsmethode von WEP auf WPA zur Erhöhung der Sicherheit ist für die Zukunft geplant, war jedoch nicht Gegenstand dieser Projektarbeit.
Bei Betrachtung der Kosten für dieses Projekt, im Vergleich zu den Alternativkonzepten ist der Einsatz einer WLAN-Infrastruktur dieser Art, für den NLWKN, vollkommen zufrieden stellend und jederzeit vertretbar.

Anlagenverzeichnis

Anlage A

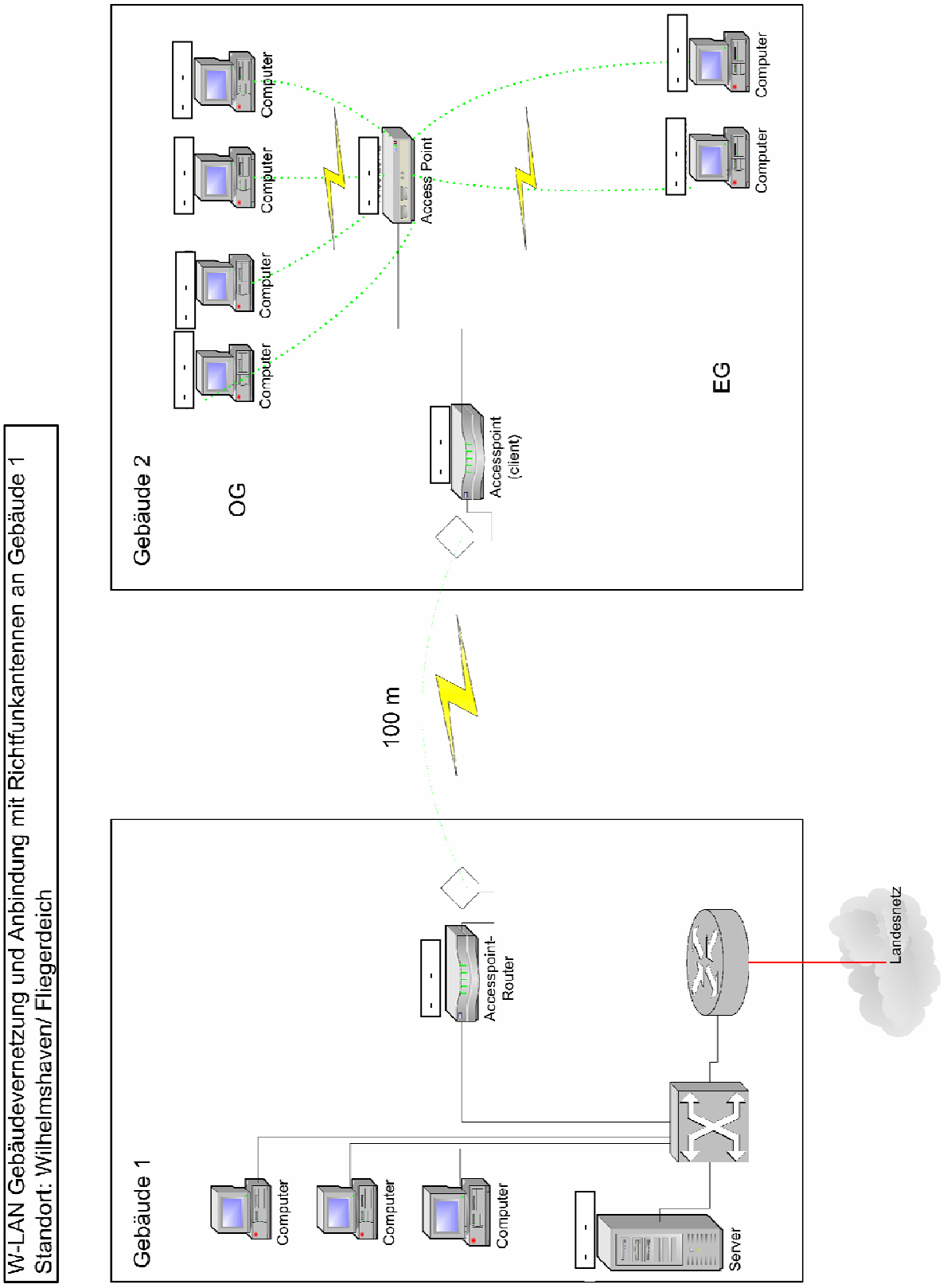
Quellenverzeichnis

Literatur:

Microsoft Press	Einführung von Netzwerkdiensten für Windows Server 2003, Die Technische Referenz
Wireless LANs	Jörg Rech, Heise Verlag, 802.11-WLAN Technologie und praktische Umsetzung im Detail
PC-Chip	Heft 5/2004 Access Points (Hardwaretest)

Internet

Download	Netstumbler: http://www.netstumbler.com/downloads/?op=getit&lid=24 Zugriff: 28.02.05
Hardwaretest	http://www.pc-magazin.de/common/tests/hard.php?m=ih_faz&id=1167 Zugriff:16.02.05


W-LAN Gebäudevernetzung und Anbindung mit Richtfunkantennen an Gebäude 1
Standort: Wilhelmshaven/ Fliegerdeich
Gebäude 2
OG
EG
Computer
Computer
Computer
Computer
Access Point
Computer
Computer
Accesspoint (client)
100 m
Gebäude 1
Accesspoint-Router
Computer
Computer
Computer
Server
Landesnetz

Nds. Landesbetrieb für Wasserwirtschaft, Küsten- und Naturschutz
Regulierungsbehörde für
Telekommunikation und Post
Benningsenstr. 3

28205 Bremen

Dienstgebäude
☒ 26919 Brake, Heinestraße 1
☐ 26122 Oldenburg, Ratsherr-Schulze-Str. 10

Bearbeitet von

Ihr Zeichen, Ihre Nachricht vom	Mein Zeichen (Bei Antwort angeben)	Durchwahl	Ort/ Datum
			Brake 18.03.05

Grundstücksübergreifende Datenübertragung

Sehr geehrte Damen und Herren!

Es wird eine WLAN Richtfunkstrecke in Betrieb genommen.

Standort:
NLWKN
Fliegerdeich 1
26382 Wilhelmshaven

Antennenparameter:
Antennengewinn 18 dBi
Öffnungswinkel 15°

Höhe der Antennen über Grund:
3 m

Datum der Inbetriebnahme:
21.03.05

Datum der Außerbetriebnahme:
Nicht bekannt

Mit freundlichen Grüßen

Thomas Zirkel

Glossar

dBi	(Dezibel isotrop) Dies ist der Wert, mit dem die Antenne, ihre Leistung abgibt bzw. aufnimmt.
3DES	Data Encryption Standard**,**168-Bit Schlüssel, jeder Datenblock wird drei mal mit DES mit verschiedenen Schlüsseln chiffriert.
Öffnungswinkel	Gibt an in welchem Winkel einer Antenne ihre Funkwellen aussendet.
IIS-Server	Internet Information Service (MS-Webserver)
IPSec	IP- Encapsulating Security Payload (Verschlüsselungsmethode)
L2TP	Layer 2 Tunneling Protocol, verwendet für VPN
MS-CHAPv2	Microsoft Challenge Handshake Authentication Protocol Version 2, Client muss Mitglied der Domäne sein, bietet beidseitige Authentifizierung
Netstumbler	Tool zum aufspüren von Access Points (freeware)
OFDM	Orthogonal Frequency Division Multiplexing (Übertragungsverfahren)
PBCC	Packet Binary Convolutional Code (Übertragungsverfahren)
Panel-Antenne	Richtfunkantenne, Flache Bauweise, geringer Öffnungswinkel
Patch-Antenne	Flache Bauweise, Zusatzantenne für Access Point´s, Reichweitensteigerung von bis zu 100%
Pigtails	Verbindungskabel für WLAN Antennen, SMA auf N Stecker
RAS-Server	Remote Access Service (wird benötigt für MS-VPN Server)
RegTP	Die Regulierungsbehörde für Telekommunikation und Post ist für die Frequenzvergabe, Vergabe von Rufnummern, Einhaltung der Grenzwerte für die Stärke elektromagnetischer Felder usw. zuständig.
SSID	Service Set Identifier (Netzwerkname für das WLAN)
WEP	Wired Equivalent Privacy, bis zu 256 Bit verschlüsselte Datenpackete
Wi-Fi	Wireless Fidelity (Diese Organisation prüft Kompatibilität von 802.11-WLAN Produkten
WPA	Wi-Fi Protected Access (Abwärtskompatibel zu WEP, Authentifizierung über Radius-Server, in dem PSK-Verfahren (Pre-Shared-Key) wird im Vorfeld temporär ein Schlüssel verteilt.