

Corporate Wireless LAN

Detailkonzept

Verfasser: Nico Lamberti

Email: nico.lamberti@leuchterag.ch

Version: 1.3

Status: in Arbeit

Datum: 18.03.2005

Änderungskontrolle

Version	Datum	Ausführende Stelle	Bemerkung / Art der Änderung
1.0	30.12.2004	lan	Erstellung des Dokumentes
1.1	17.01.2005	stt	Allgemeine Ergänzungen
1.2	18.03.2005	stt / lan / gat	Allgemeine Ergänzungen
1.3	18.03.2005	lan	Allgemeine Korrektur

Prüfung

Version	Datum	Ausführende Stelle	Bemerkung / Art der Änderung
1.0			

Inhaltsverzeichnis

1.	Einleitung	5
1.1.	Zweck des Dokumentes	5
1.2.	Referenzierte Dokumente	5
2.	Allgemeines	5
2.1.	Komponenten	5
2.2.	Logische Darstellung des Gesamtsystems	6
2.3.	Vorgesehene physische Implementierung	6
3.	Komponente DHCP	7
3.1.	Funktionsbeschreibung	7
3.2.	Funktionale Anforderungen	7
3.2.1.	FUNKTION1	7
3.3.	Use Cases	7
3.3.1.	Use Case „WLAN Access“	7
3.3.2.	Use Case „Netzwerk_Dienste“	7
4.	Komponente DNS	8
4.1.	Funktionsbeschreibung	8
4.2.	Funktionale Anforderungen	8
4.2.1.	FUNKTION1	8
4.3.	Use Cases	8
4.3.1.	Use Case „Netzwerk_Dienste“	8
5.	Komponente AD	9
5.1.	Funktionsbeschreibung	9
5.2.	Funktionale Anforderungen	9
5.2.1.	FUNKTION1	9
5.3.	Use Cases	9
5.3.1.	Use Case „WLAN Access“	9
5.3.2.	Use Case „Passwort Fehleingabe“	10
6.	Komponente RADIUS	11
6.1.	Funktionsbeschreibung	11
6.2.	Funktionale Anforderungen	11
6.2.1.	FUNKTION1	11
6.3.	Use Cases	11
6.3.1.	Use Case „WLAN Access“	11
7.	Komponente Access Point	12
7.1.	Funktionsbeschreibung	12
7.2.	Funktionale Anforderungen	12
7.2.1.	FUNKTION1	12
7.3.	Use Cases	12
7.3.1.	Use Case „WLAN Access“	12
8.	Komponente WLAN Client	13
8.1.	Funktionsbeschreibung	13
8.2.	Use Cases	13
8.2.1.	Use Case „WLAN Access“	13
9.	Komponente Funknetzwerk	13
9.1.	Use Cases	13
9.1.1.	Use Case „WLAN Access“	13
10.	Komponente Layer-3-Switch (Router)	14
10.1.	Funktionsbeschreibung	14
10.2.	Funktionale Anforderungen	14
10.2.1.	FUNKTION1	14
10.3.	Use Cases	14
10.3.1.	Use Case „WLAN Access“	14
10.3.2.	Use Case „Funknetzwerk“	14
10.3.3.	Use Case „Netzwerk_Dienste“	14
11.	Quellenangabe	14
12.	Mittelliste	15
12.1.	Hardware	15

12.1.1.	Computer.....	15
12.1.2.	Netzwerk	15
12.2.	Software.....	15
12.2.1.	Betriebssysteme	15
12.2.2.	Software.....	15

1. Einleitung

1.1. Zweck des Dokumentes

Das Dokument Detailkonzept regelt den Übergang vom IST-Zustand zum SOLL-Zustand sowie die definitive Implementierung.

Der Fokus wird in diesem Projekt auf die Erweiterung eines bestehenden Netzwerkes mit kabellosem LAN gerichtet. Ausgangspunkt ist die Firma Skai Logistik AG. In diesem Dokument wird eine WLAN Lösung beschrieben, welche den Bedürfnissen des Unternehmens optimal gerecht wird.

Da ein Funknetzwerk ohne besondere Massnahmen leicht abhörbar ist, hat die Sicherheit des Netzwerkes eine hohe Priorität.

1.2. Referenzierte Dokumente

Folgende Dokumente referenzieren mit dem Sollkonzept. Die Nummern in den eckigen Klammern werden jeweils im entsprechenden Kontext aufgeführt:

[1] Pflichtenheft Corporate WLAN, Kapitel 2 ff.

[2] Pflichtenheft Corporate WLAN, Kapitel 4.1

2. Allgemeines

2.1. Komponenten

Das Corporate WLAN Soll-Konzept besteht aus acht Hauptkomponenten:

Komponente DHCP

Automatische IP-Adressvergabe im Netzwerk

Komponente DNS

Service zur Namensauflösung

Komponente Active Directory

Benutzerdatenverwaltung

Komponente RADIUS

Authentifizierungs Dienst

Komponente Access Point

Funkstation; WLAN Zugangspunkt

Komponente WLAN Client

Arbeitsgerät der Mitarbeiter

Komponente Funknetzwerk

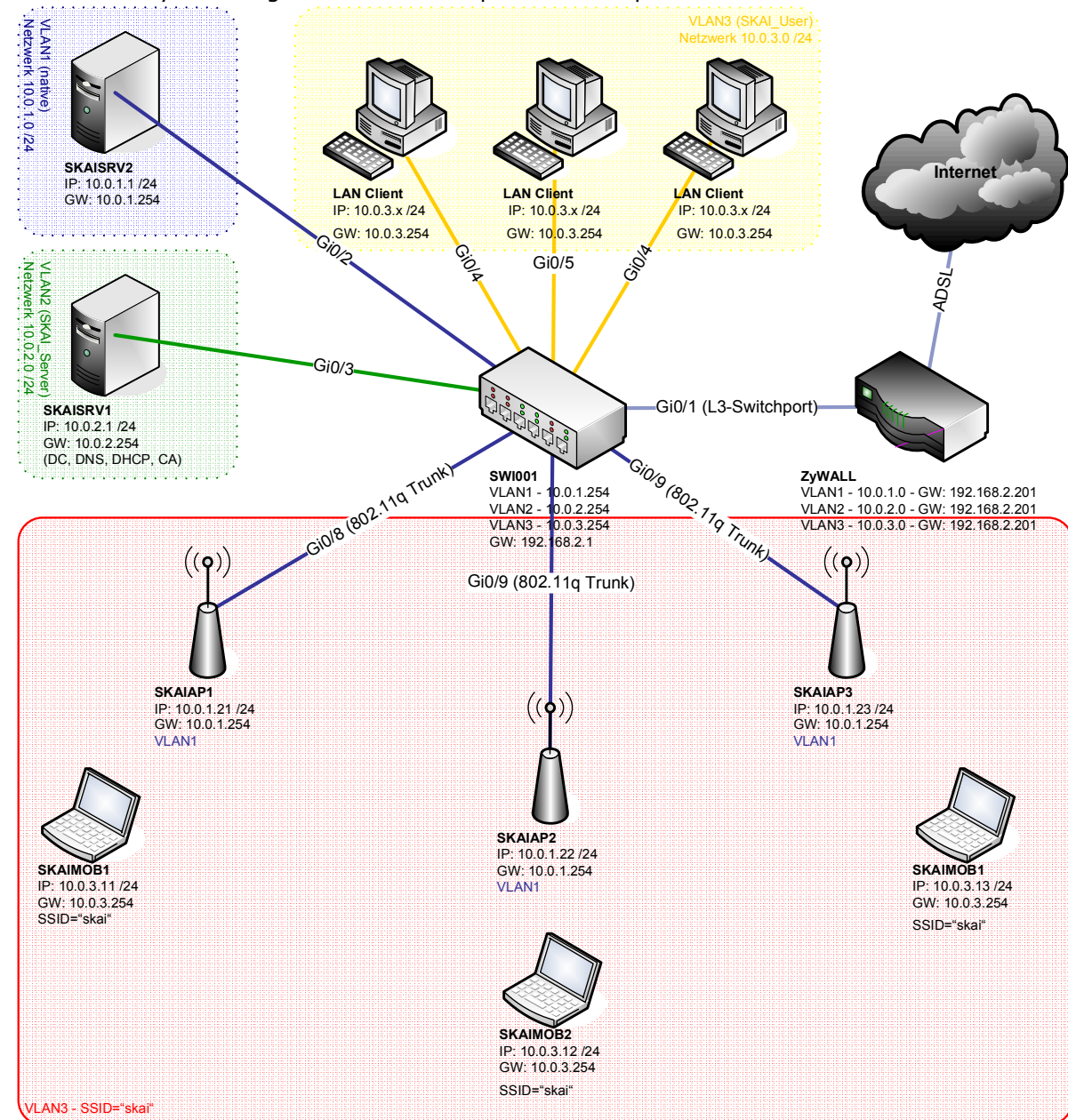
Das drahtlose Netzwerk

Komponente Router (Layer 3 Switch)

Switch mit Routing- Funktion

2.2. Logische Darstellung des Gesamtsystems

Das Gesamtsystem zeigt das Zusammenspiel aller Komponenten auf:



2.3. Vorgesehene physische Implementierung

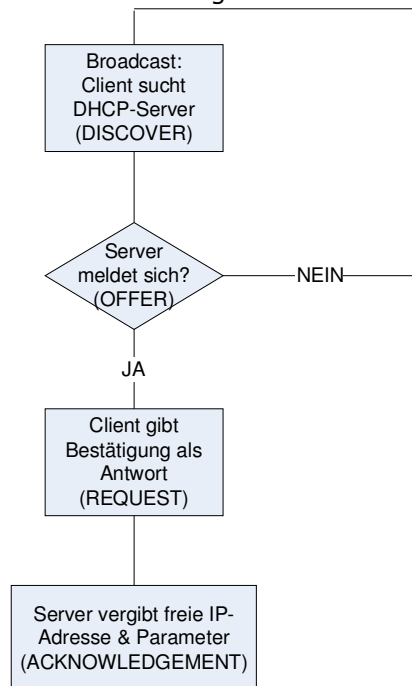
Die genaue Implementierung wird in einem weiteren Dokument (Implementierungsdokumentation) niedergeschrieben. Die vorgesehene Planung ist im Bild unter Punkt [2.2 Logische Darstellung](#) zu entnehmen.

3. Komponente DHCP

Das DHCP (Dynamic Host Configuration Protocol) ermöglicht mit Hilfe eines entsprechenden Servers die dynamische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter an Computern in einem Netzwerk (z.B. die Angabe der DNS-Server).

3.1. Funktionsbeschreibung

Durch DHCP ist die Einbindung eines neuen Computers in ein bestehendes Netzwerk ohne weitere Konfiguration möglich. Ohne DHCP ist ein relativ aufwendiges Setup nötig, das neben der IP-Adresse die Eingabe weiterer Parameter wie Netzmaske, Gateway, DNS-Server, WINS-Server usw. verlangt. DHCP kann diese Parameter beim Starten eines neuen Rechners automatisch vergeben.



Hinweis zum Flussdiagramm:

Der Anwendungsfall von mehreren DHCP-Servern wurde nicht berücksichtigt, da im Netzwerk der Firma Skai Logistik AG nur ein einzelner DHCP-Server vorhanden ist.

3.2. Funktionale Anforderungen

3.2.1. FUNKTION1

Jeder Client der sich via Funk am Netzwerk meldet, bekommt vom DHCP-Dienst eine Adresse zugewiesen.

3.3. Use Cases

3.3.1. Use Case „WLAN Access“

Auslöser	Client fordert Adresse vom Funknetzwerk
Arbeitsablauf	Client senden Broadcast, worauf er Antwort vom DHCP-Server bekommt
Schlussfolgerung	Netzwerkdaten wurden dem WLAN Client übergeben

3.3.2. Use Case „Netzwerk_Dienste“

Auslöser	Client fordert Adresse
Arbeitsablauf	Client senden Broadcast, worauf er Antwort vom DHCP-Server bekommt
Schlussfolgerung	Netzwerkdaten wurden dem Client übergeben

4. Komponente DNS

Das Domain Name System (DNS) verknüpft IP Adressen mit Hostnamen. In einem simplen TCP/IP Netzwerk können normalerweise die Hosts nur direkt über die IP Adresse angesprochen werden. Mit dem DNS-Dienst ist es folglich möglich, bequem über die Hostnamen zu arbeiten. z.B. im Internet – www.google.ch

4.1. Funktionsbeschreibung

Der Client muss zur Namensauflösung mindestens ein DNS-Server eingetragen haben. Um sich eine manuelle Eingabe bei den Hosts zu ersparen, kann man diese Einträge dem DHCP mitgeben.

Unter den Bereichsoptionen des DHCP-Servers kann dies mitgegeben werden.

Da der DNS-Funktion in diesem Projekt keine allzugrosse Bedeutung zukommt, wird auf die Funktion der Namensauflösung nicht weiter eingegangen. Der Zuweisungsvorgang der DNS-Einstellungen ist unter [Punkt 3.1.](#) ersichtlich.

4.2. Funktionale Anforderungen

4.2.1. FUNKTION1

Wichtig ist die Auflösung der Access Points und der Computer. Damit die auf die Freigaben unkompliziert zugegriffen werden kann, werden diese als „Namen“ angegeben, und nicht als IP-Adresse.

4.3. Use Cases

4.3.1. Use Case „Netzwerk_Dienste“

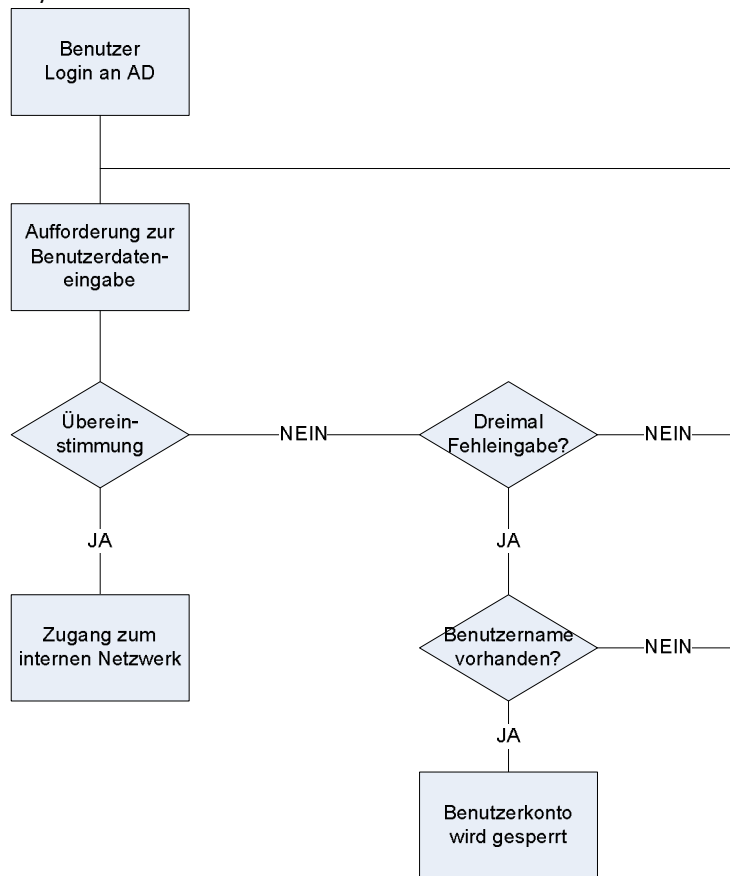
Auslöser	Namensauflösung
Arbeitsablauf	Server nimmt Angaben und löst sie in IP / Namen auf
Schlussfolgerung	Die IP-Adresse / Namen wurde vom DNS aufgelöst

5. Komponente AD

Das Active Directory (AD) ist die Verwaltungsdatenbank über Benutzer und Clients. Um in der Geschäftsdomäne zu arbeiten, muss sich der User am Active Directory anmelden. Der User wird zur Benutzerdaten eingabe aufgefordert. Diese Daten werden mit den Einträgen im AD verglichen. Stimmen diese Überein (Benutzername, Passwort), wird dem Client über den RADIUS-Server Zugang zum internen Netzwerk gewährt.

5.1. Funktionsbeschreibung

Auf dem folgenden Flussdiagramm ist ersichtlich, wie der Anmeldevorgang mittels Active Directory erfolgt. Voraussetzung hierbei ist die abgeschlossene Authentifizierung am AP/Radius-Server



5.2. Funktionale Anforderungen

5.2.1. FUNKTION1

Das AD ist die Vertrauensstelle des RADIUS-Servers. Die Anfragen der WLAN Clients werden über den RADIUS-Server an das AD übergeben und dort auf Berechtigung geprüft.

5.3. Use Cases

5.3.1. Use Case „WLAN Access“

Auslöser	Benutzer will sich an der Domäne anmelden
Arbeitsablauf	Radius stellt Tunnelverbindung zum Client her. Dieser wird aufgefordert Kennungsdaten für Domäne anzugeben. Die Daten werden an das AD weitergeleitet. Das AD vergleicht die eingegeben Benutzerdaten mit den vorhandenen Angaben. Ist eine Übereinstimmung feststellbar, wird dem Client Zugang zum internen Netzwerk gewährt.

Schlussfolgerung	Client hat Zugang zum Firmennetzwerk
-------------------------	--------------------------------------

5.3.2. Use Case „Passwort Fehleingabe“

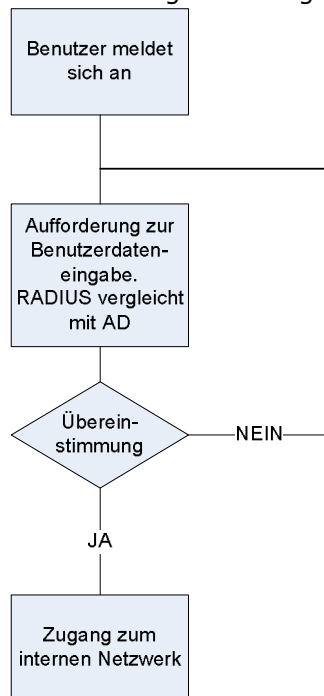
Auslöser	Benutzer will sich am System anmelden
Arbeitsablauf	Gibt der Benutzer beim Login sein Passwort dreimal falsch ein, wird sein Konto gesperrt. Dies dient als Schutzmechanismus gegen Brute-force Angriffe von Hackern. Wird bei der Anmeldung ein falscher Benutzername verwendet, passiert nichts, da dieses Konto nicht besteht.
Schlussfolgerung	Konto muss entsperrt werden.

6. Komponente RADIUS

Der RADIUS (engl. Remote Authentication Dial-In User Service) ist ein Client-Server-Protokoll, das zur Authentifizierung von Benutzern bei Einwahlverbindungen in ein Computernetzwerk dient. Er erlaubt das Einwählen von Geräten, wie zum Beispiel über Wireless LAN.

6.1. Funktionsbeschreibung

Das Flussdiagramm zeigt den WLAN Access auf, der über den RADIUS-Server läuft.



6.2. Funktionale Anforderungen

6.2.1. FUNKTION1

Der RADIUS hat die Access Points als 'Clients' eingetragen. Diese leiten anfangs die Daten vom Client zum RADUIS weiter. Nach der Authentifizierung funktioniert der Access Point quasi als Bridge zwischen WLAN Client und RADIUS.

6.3. Use Cases

6.3.1. Use Case „WLAN Access“

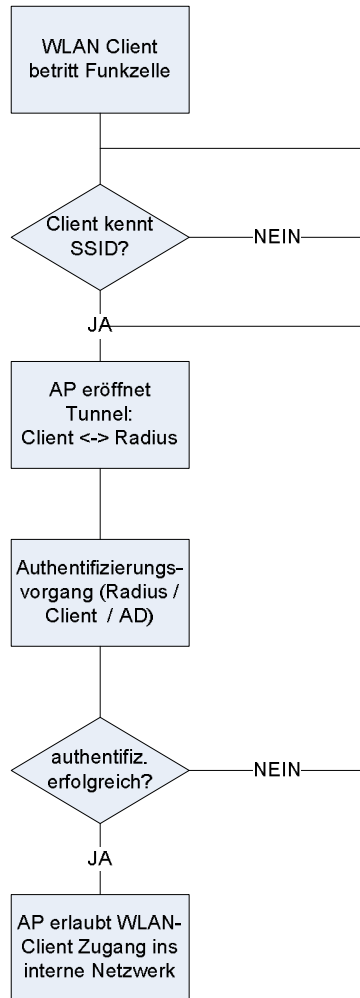
Auslöser	User betritt Funkzelle
Arbeitsablauf	Der User wird mit dem Access Point verbunden. Dieser fordert zur Authentifizierung auf; ist diese richtig, gelangt der User ins Firmennetzwerk
Schlussfolgerung	Der User hat Netzwerkzugriff

7. Komponente Access Point

Der Access Point (AP) hat eine SSID, welche sein Funknetz definiert. Oft werden Broadcasts versenden, damit die Clients das Funknetzwerk erkennen und verbinden. Um eine grössere Sicherheit zu gewähren, wird die SSID auch oft verdeckt, wie hier in unserem Fall.

7.1. Funktionsbeschreibung

Ist der Client an einem Funknetzwerk angeschlossen, eröffnet der AP einen 'Tunnel' zwischen Client und RADIUS-Server. Diese Verbindung ist für andere nicht sichtbar.



7.2. Funktionale Anforderungen

7.2.1. FUNKTION1

Der Access Point leitet User anfragen weiter. Jene ohne Authentifizierung werden automatisch vom Netzwerk ausgeschlossen, bzw. erhalten keinen Zugriff. Die anderen User werden vom AP in ein höheres und berechtigteres Netz eingestuft.

7.3. Use Cases

7.3.1. Use Case „WLAN Access“

Auslöser	User meldet sich am Netzwerk an
Arbeitsablauf	User wird je nach eingestellter SSID in ein VLAN zugewiesen
Schlussfolgerung	Je nach Recht hat der User Zugriff.

8. Komponente WLAN Client

Der WLAN Client ist meistens ein Notebook, welches über Funk eine Netzwerkverbindung hat. So ein Client kann auch in Form eines PDA oder ähnlicher Geräte vorkommen.

8.1. Funktionsbeschreibung

Der Client ist der Hauptnutzer des Funknetzwerkes. Er selber hat keinen Einfluss auf das Netzwerk. Der Funkuser kann mit der Standard-Windows Netzwerkumgebung das Funknetzwerk verbinden (bei XP mindestens SP1). Es müssen lediglich die Einstellungen angepasst werden (siehe Benutzerhandbuch).

8.2. Use Cases

8.2.1. Use Case „WLAN Access“

Auslöser	Client betritt Funkzelle
Arbeitsablauf	Client muss sich authentifizieren
Schlussfolgerung	Client hat Zugang zum Netzwerk

9. Komponente Funknetzwerk

Ein Funknetz ist ein Netzwerk, in welchem Informationen mittels elektromagnetischer Wellen übertragen werden. In unserem Fall handelt es sich um WLAN, ein kabelloses lokales Netzwerk.

Das Funknetzwerk hat selber kein Flussdiagramm, da wir diese Komponente als logischen Sammelbegriff für das WLAN erstellt haben.

9.1. Use Cases

9.1.1. Use Case „WLAN Access“

Auslöser	Gebrauch des Funknetzwerkes
Arbeitsablauf	Sendet die Daten zum Empfänger / Sender
Schlussfolgerung	Verfügbares WLAN

10. Komponente Multi-Layer-Switch

Der Multi-Layer-Switch hat zwei Aufgaben, einerseits fungiert er als Switch im Netzwerk, andererseits arbeitet er als Router.

Ein Router ist ein Vermittlungsrechner, der in einem Netzwerk dafür sorgt, dass bei ihm eintreffende Daten eines Protokolls zum vorgesehenen Zielnetz bzw. Subnetz weitergeleitet werden.

10.1. Funktionsbeschreibung

Auf die Funktionen des Switches wird nicht weiter eingegangen, hauptsächlich wird das Routing behandelt.

Der Router leitet die Datenpakete zum anderen Netzwerken weiter. Falls VLANs eingerichtet werden, kann er unter den einzelnen virtuellen Netzen die Daten weiterleiten. Jeder Funknetzwerkuser greift über den Multi-Layer-Switch auf das Netzwerk zu.

10.2. Funktionale Anforderungen

10.2.1. FUNKTION1

Der Multi-Layer-Switch hat die Aufgabe, die Datenpakete je nach Einstellung weiterzuleiten. Unter den verschiedenen Subnetzen (VLAN) muss der Multi-Layer-Switch routen.

10.3. Use Cases

10.3.1. Use Case „WLAN Access“

Auslöser	Verbindung über das Netzwerk
Arbeitsablauf	Router (bzw. Switch) leitet die Daten weiter
Schlussfolgerung	Netzwerk nutzbar

10.3.2. Use Case „Funknetzwerk“

Auslöser	Verbindung über das Netzwerk
Arbeitsablauf	Router (bzw. Switch) leitet die Daten weiter
Schlussfolgerung	Netzwerk nutzbar

10.3.3. Use Case „Netzwerk_Dienste“

Auslöser	Dienste werden beansprucht
Arbeitsablauf	Router (bzw. Switch) leitet die Daten weiter
Schlussfolgerung	Dienste nutzbar

11. Quellenangabe

- www.wikipedia.de

12. Mittelliste

Unter diesem Punkt sind alle benötigten Materialien für das Projekt aufgelistet. Von der Cisco gelieferte Artikel sind leicht grau hinterlegt.

12.1. Hardware

12.1.1. Computer

Erforderliche Hardware Komponenten:

Beschreibung	Spezifikation	Zweck	Anzahl
Server Hardware	min. 1.8GHz, 1GB Ram, 2 HDD (ca. 2x 10GB), 100Mbps NW-Interface	Domain Controller, DNS, DHCP, RADIUS, Certificate Services	2
Client Hardware	min. 1.8GHz, 512MB Ram, 100Mbps NW-Interface	Dokumentation	2
Portable Hardware	WLAN Interface (802.11a, b oder g) [*]	WLAN Testclient	2
	WLAN Interface (802.11a/b/g) [*]	WLAN Sniffer [**]	1

12.1.2. Netzwerk

Erforderliche Netzwerk Komponenten:

Beschreibung	Spezifikation	Zweck	Anzahl
Switch	min. 8 Ports, 100Mbps (optional 1Gbps)	Core Switch	1
	min. 8 Ports, 100Mbps (optional 1Gbps)	Distribution Switch	1
	min. 8 Ports, 100Mbps	Access Switch	1
Patchkabel	RJ45, Kategorie 5 (bzw. 1Gbps mit Kat.6), 3-10m	Netzwerk-Verbindungskabel	10
Access Point	802.11a/b/g (2.4GHz / 5GHz), Wireless-Bridging, Roaming	Wireless LAN Zugangspunkt	3
WLAN Adapter	WLAN Interface (802.11a, b oder g)	Wireless LAN Adapter Karten für Portable Hardware [*]	3
ZyWall10 (BBZS)	Interfaces: - Ethernet	Internetzugang	1

12.2. Software

12.2.1. Betriebssysteme

Erforderliche Betriebssysteme:

Betriebssystem	Bemerkung	Anzahl
Windows 2003 Enterprise Edition		2
Windows XP Professional	inkl. Service Pack 1 / SP2	5

12.2.2. Software

Erforderliche Software:

Beschreibung	Bemerkung	Anzahl
Microsoft Office 11	für Dokumentations-PC's	2
Root Certificate	eigene Zertifikate (ggf. VerySign)	1
Network Associates Sniffer	Ethernet Sniffer [**]	1
AirMagnet Sniffer	WLAN Sniffer [**]	1