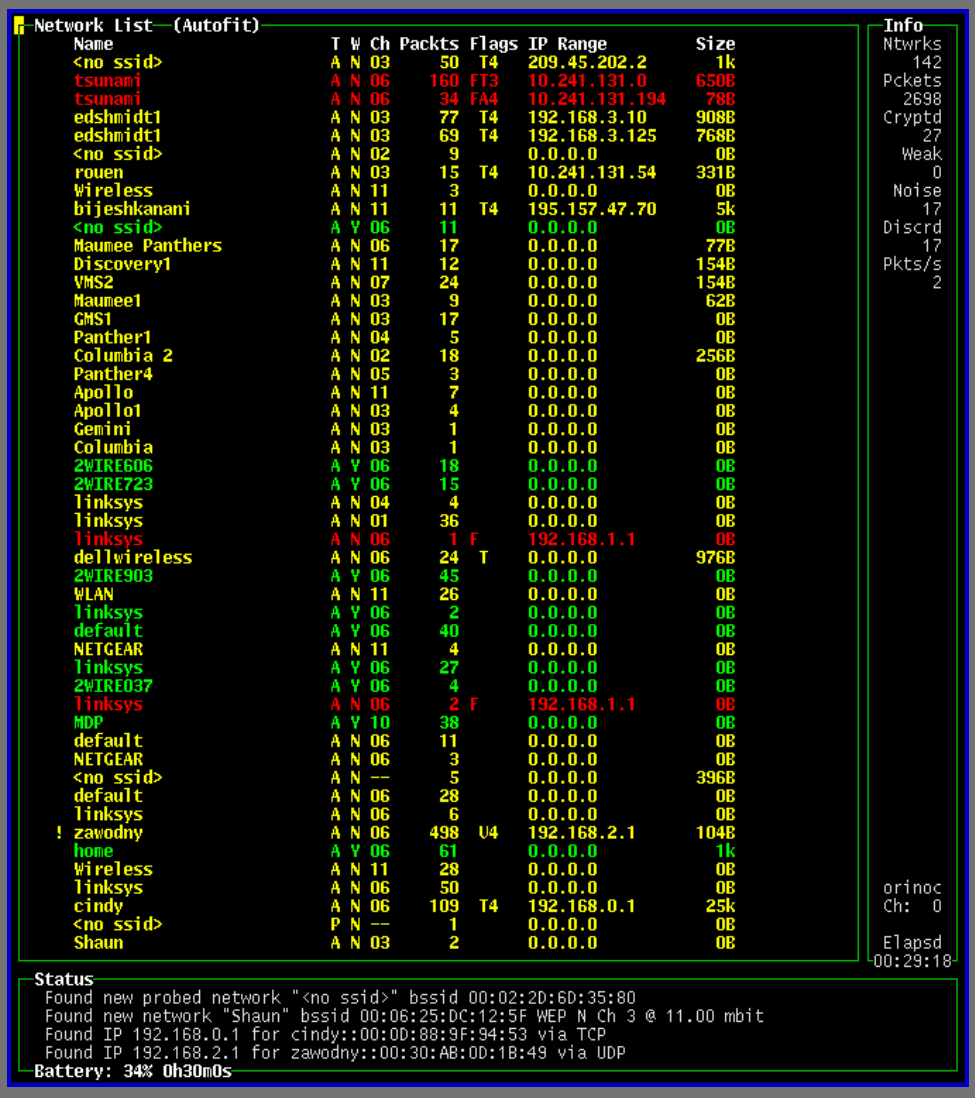
Inf2b

Dokumentation ÜK IT-Com

LAN, WLAN, VLAN und VoIP

Erstellt: 2008-05-26
Kursdauer: 2008-05-26 bis 2008-06-04
Erstellt von Emanuel Duss
Kursleiter: Fredi Ringier



Emanuel Duss
Inf2b

Inhaltsverzeichnis

1 Einführung und Grundlegende Informationen

Wir beginnen mit Herr Meier wieder ein neues Projekt. Herr Meier war sehr erfolgreich mit dem Geschäft und eröffnete mehrere Filialen, die er nun auch in das Netzwerk integrieren will.

1.1 Rahmenbedingungen

- 6 Filialen in der Schweiz
  - Pro Filiale ein Netzwerk mit Server und zwei Arbeitsstationen
- Papierloses Büro
  - Einziger Drucker in der Zentrale
- WLAN einrichten
  - Test zur Sicherheit
- Verkaufsdaten von Zentrale auf Filialen verteilen
  - Synchronisieren
- Tagesdaten der Zentrale der Zentrale schicken
- Trennung zwischen den Daten der Geschäftsführung und den Daten aus dem Tagesgeschäft.
  - Komplett getrennt (VLAN)
- Telefonie auf VoIP migrieren

1.2 Dienste

Wir werden folgende Dienste einrichten:

1.2.1 Dateiserver

Sobald der Server für andere Benutzer im Netzwerk Dateien in freigegebenen Ordnern bereitstellt, fungiert er als Dateiserver. Zu konfigurieren sind dazu Freigaben mit den entsprechenden Sicherheitseinstellungen für die Benutzer und Gruppen.

1.2.2 Druckserver

Die am häufigsten genutzten Dienste eines Servers sind die zur zentralen Bereitstellung und Verwaltung von Druckern. Dieser Dienst ist mit W2k3 Server noch einfacher geworden

1.2.3 Domänencontroller

Die Domänencontroller verwalten die Verzeichnisdatenbank der Domäne, in der unter anderem alle Benutzer, Sicherheitsgruppen und Computer erfasst sind (→ Active Directory)

1.2.4 DNS-Server

Das Domain Name System (DNS) dient der Namensauflösung im Internet oder im LAN.

Bei Active Directory wird DNS vorausgesetzt.

IP-Adresse ←→ Namen

1.2.5 DHCP-Server

Mithilfe des Dynamic Host Configuration Protocol (DHCP) werden IP-Adressen an Clientcomputer automatisch durch einen zentralen DHCP-Server verteilt.

1.3 Teamorganisation

Damit wir zusammen gut arbeiten können, müssen wir die Arbeit im Team fördern. Es bringt nichts, wenn jeder für sich arbeitet und nicht mit den anderen kommuniziert. Es kann nicht jeder immer jede Aufgabe machen. Deshalb müssen wir die Arbeiten aufteilen. Die, die die Arbeit erledigen, müssen den anderen mitteilen, was sie gemacht haben. Damit können alle vom Wissen profitieren.

2 Konzepte

In einem Konzept beschliesst man sich auf ein einheitliches Benennen von PCs und einheitliches vergeben der IP-Adresse

Wir benennen die Geräte einheitlich. So weiss man sofort, wenn etwas Probleme macht anhand des Namens, um was für ein Gerät es sich handelt, und woher es kommt (Standort).

2.1.1 Standort / Gerätename / Nummer

- Standort
  - BAS Basel
  - BER Bern
  - FRE Freiburg
  - GEN Genf
  - BEL Bellinzona
  - LOC Locarno
  - ZUE Zürich
- Gerät
  - SRV Server
  - NB Notebook
  - WS Workstation
  - SW Switch
  - RT Router
  - PR Printer
  - PH Phone
- Nummer
  - Durchnummeriert von 01 bis 99
- Beispiel
  - Den ersten Server von Basel: BAS-SRV-01

2.1.2 IP-Adressen

Wir erstellen ein IP-Adressenkonzept. Es ist viel übersichtlicher, wenn wir pro Filiale IP-Adressen verteilen. Wenn wir dies machen, können wir genau anhand der IP-Adresse bestimmen, wo das Gerät steht.

2.1.2.1 IP-Subnetze

- Hauptagentur
  - 192.168.**1**.0 /24 Management / Zentraler Server
- Deutschschweiz
  - 192.168.**10**.0 /24 Bern
  - 192.168.**11**.0 /24 Zürich
  - 192.168.**12**.0 /24 Basel

- Westschweiz
  - 192.168.**20**.0 /24 Fribourg
  - 192.168.**21**.0 /24 Geneve
- Italienische Schweiz
  - 192.168.**30**.0 /24 Locarno
  - 192.168.**31**.0 /24 Bellinzona

2.1.2.2 IP-Adress-Ranges

- 192.168.xx.1 - 10 Router
- 192.168.xx.11 - 20 Switch
- 192.168.xx.21 - 90 Server
- 192.168.xx.91 - 100 Peripherie
- 192.168.xx.101 - 200 Client
- 192.168.xx.201 - 254 VoIP-Telefone

3 Netzwerk in den Filialen erstellen

Damit es ein wenig schneller geht, installieren wir die Server von einem Image, das auf dem Server liegt.

3.1 Anforderung

- Domäne
- Active-Directory
- 2 Arbeitsstationen
- Windows XP
- Office 2003 mit Outlook
- User
- Gruppen
- Recourcen
- Berechtigungen (Scripts)
- Internetzugriff

3.2 Konfiguration Router bzw. Switch

Unsere Clients verbinden wir mit einem Switch. Hiefür nehmen wir einen US-Robotics-Router, der jedoch als Switch fungiert. Nach dem Reset deaktivieren wir nur den DHCP-Server, damit der Router nicht ins Netzwerk pfuscht. Weitere Einstellungen sind für den Router nicht nötig.

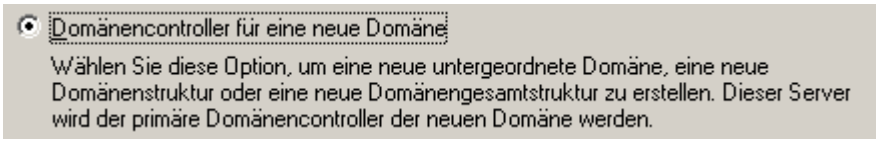
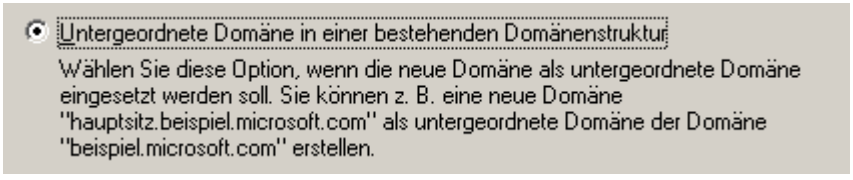
3.3 Konfiguration Server

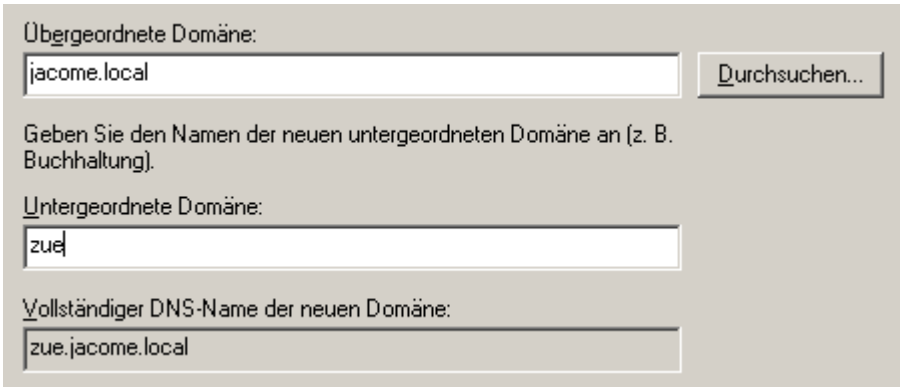
Wir fügten den Server zu der *JACOME.LOCAL*-Domäne hinzu. Dann starteten wir DCPromo und begannen mit dem einrichten der Sub-Domäne.

IP-Adresse: 172.22.58.**21**

DNS-Adresse: Server von Zentrale (172.22.45.21)

3.3.1 DCPromo

DCPROMO.EXE	Wir führen diese EXE aus.
	Wir fügen einen neuen *DOMÄNENKONTROLLER FÜR EINE NEUE DOMÄNE* hinzu.
	Da wir eine Subdomäne erstellen wollen, erstellen wir eine *UNTERGEORDNETE DOMÄNE IN EINER BESTEHENDEN DOMÄNENSTRUKTUR*.



Die übergeordnete Domäne ist die *JACOME.LOCAL-DOMÄNE*. Da wir die Filiale in Zürich sind, heisst unsere untergeordnete Domäne *ZUE*.

Daraus ergibt sich dann *ZUE.JACOME.LOCAL*.

3.3.2 DNS-Server

Ein DNS-Server (Domain Name System) löst IP-Adressen in Namen und Namen in IP-Adressen auf. Der DNS-Server zeigt auch auf gewisse Dienste, die man mit *NSLOOKUP* abfragen kann.

Dazu drei Beispiele:

Mailserver von edulu.ch abfragen	`nslookup –type=mx edulu.ch`
Nameserver von Google.ch abfragen	`nslookup –type=ns google.ch`
Mailserver von edulu.ch auf dem Nameserver von Google abfragen	`nslookup –type=mx edulu.ch ns1.google.com`

Man muss den DNS-Server einrichten, damit die Namensauflösung der Clients funktioniert. Dieser DNS-Server erbt die DNS-Einträge von der oberhalb liegenden Domäne. Das ist eigentlich auch die Sache von der ganzen Namensgeschichte: Der neue DNS-Server *ZUE.JACOME.LOCAL* übernimmt die DNS-Einträge vom DNS-Server *JACOME.LOCAL*.

Die Anfragen sind schneller, wenn wir den Server direkt vor Ort (in Zürich) aufstellen, damit die Anfragen nicht übers Internet gehen müssen.

Problem: Der DNS-Dienst geht nach dem Konfigurieren manchmal in den Manuellen Mode. Das heisst, das der Dienst nach dem Starten nicht automatisch ausgeführt wird. Dies muss man ändern, indem man den Dienst auf Automatisch stellt. Somit funktioniert der DNS-Server!!! Das war ein grosses Problem bei uns!

3.3.3 DHCP-Server

Die Hauptaufgabe eines DHCP-Servers ist die Vergabe einer Konfiguration der Netzwerkkarten-Einstellungen. Die wichtigsten Sachen sind:

- IP-Addresse
- Subnetmaske
- Default-Gateway
- DNS-Server

Man kann den Dienst aber auch noch für andere Zwecke brauchen:

- Vergeben von
  - WINS-Server vergeben
  - Zeitserver vergeben
- Man kann IPs reservieren
- Definition: wie mit Broadcast umgehen

Ein DHCP-Server benötigen wir zum dynamischen zuweisen einer IP-Adresse zu einem Client.

Es gibt dabei folgende DHCP-Typen:

- **DHCPDISCOVER:** Ein Client ohne IP-Adresse sendet eine Broadcast-Anfrage nach Adress-Angeboten an den/die DHCP-Server im lokalen Netz.
- **DHCPOFFER:** Der/die DHCP-Server antworten mit entsprechenden Werten auf eine DHCPDISCOVER-Anfrage.
- **DHCPREQUEST:** Der Client fordert (eine der angebotenen) IP-Adresse(n), weitere Daten sowie Verlängerung der Lease-Zeit von einem der antwortenden DHCP-Server.
- **DHCPACK:** Bestätigung des DHCP-Servers zu einer DHCPREQUEST-Anforderung
- **DHCPNAK:** Ablehnung einer DHCPREQUEST-Anforderung durch den DHCP-Server
- **DHCPDECLINE:** Ablehnung durch den Client, da die IP-Adresse schon verwendet wird.
- **DHCPRELEASE:** Der Client gibt die eigene Konfiguration frei, damit die Parameter wieder für andere Clients zur Verfügung stehen.
- **DHCPINFORM:** Anfrage eines Clients nach Daten ohne IP-Adresse, z. B. weil der Client eine statische IP-Adresse besitzt.

Den DHCP-Server konfigurieren wir folgendermassen:

- Bereich: Clients: 192.168.58.101 – 200

Wir können auch gleich den DNS-Server bei der Konfiguration mitgeben. Damit müssen wir diesen nicht mehr bei jedem Client separat eingeben. Wenn diese einmal wechseln würde, kann man es zentral an einem Ort wechseln und schon sind alle Clients auf dem neusten Stand.

Bei allen Clients stellen wir die IP-Konfiguration auf DHCP. Es ist sehr wichtig, dass man das IP-Adressenkonzept beachtet. Damit können schon einige Probleme aus dem Weg geschaffen werden. Wenn der IT-Administrator sieht, welche IP-Adresse etwas macht, sieht er genau, was für eine Maschine das ist.

3.3.4 Kennwortrichtlinien anpassen

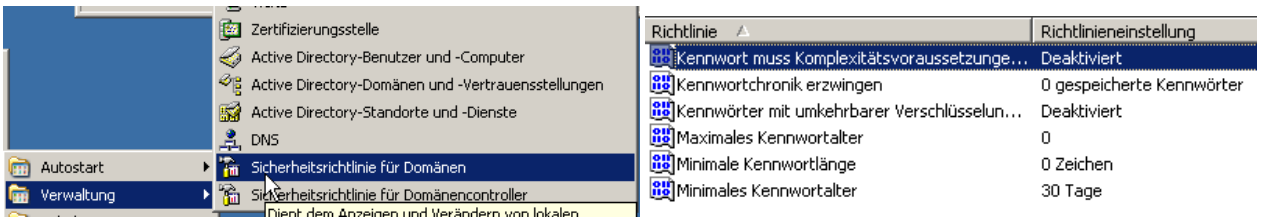
Eine Kennwortrichtlinie besagt, wie das Kennwort aussehen muss. Man kann z.B. die Mindestlänge oder die maximale Länge des Passworts angeben. Windows legt auch eine Chronik an, in welcher die vorhergehenden Passwörter gespeichert werden. Diese darf man dann für eine gewisse Zeit nicht mehr verwenden

Per Konsole:

```
net accounts /minpwlen:6 /maxpwage:90 /minpwage:1 /uniquepw:5
```

Oder über das GUI:

Wir öffnen die Sicherheitsrichtlinien für die Domänen und deaktivieren alle Kennwortrichtlinien. Dies ist ja egal, da wir nur in einer Testumgebung arbeiten. Das schwache Passwort *JUST4US* wird nur akzeptiert, wenn wir diese Kennwortrichtlinien deaktivieren.



Damit die Richtlinien aktiv werden, müssen wir folgenden Befehl ausführen:

```
gpupdate /force
```

3.3.5 Script für den Server

Damit wir den Server möglichst schnell einrichten können, erstellen wir alles mit einem Script. Der Vorteil von einem Script ist es, das danach jeder Server genau gleich aussieht. Das

3.3.6 User einrichten

Hinweis: ä = „ // ö = ” // ü = ü

Achtung: Kennwortrichtlinien deaktivieren und *GPUPDATE /FORCE*

Mit net user kann man ganz einfach neue Benutzer erstellen. Diese bekommen das bekannte „just4us“-Passwort.

```
net user ABBM "just4us" /add /expires:never /fullname:"Martina Abbühl"
/comment:"Zürich" /profilepath:\\zue-srv01\users$\ABBM\Profile /homedir:\\zue-
srv01\users$\ABBM\Home
net user BLUK "just4us" /add /expires:never /fullname:"Kevin Blum"
/comment:"Zürich" /profilepath:\\zue-srv01\users$\BLUK\Profile /homedir:\\zue-
srv01\users$\BLUK\Home
net user EGGA "just4us" /add /expires:never /fullname:"Andy Eggli"
/comment:"Zürich" /profilepath:\\zue-srv01\users$\EGGA\Profile /homedir:\\zue-
srv01\users$\EGGA\Home
net user DUDF "just4us" /add /expires:never /fullname:"Fiorina Dudli"
/comment:"Zürich" /profilepath:\\zue-srv01\users$\DUDF\Profile /homedir:\\zue-
srv01\users$\DUDF\Home
net user BADA "just4us" /add /expires:never /fullname:"Alexandra Bader"
/comment:"Zürich" /profilepath:\\zue-srv01\users$\BADA\Profile /homedir:\\zue-
srv01\users$\BADA\Home
net user BOLJ "just4us" /add /expires:never /fullname:"Jan Bolte"
/comment:"Zürich" /profilepath:\\zue-srv01\users$\BOLJ\Profile /homedir:\\zue-
srv01\users$\BOLJ\Home
net user CHRR "just4us" /add /expires:never /fullname:"Regina Christen"
/comment:"Zürich" /profilepath:\\zue-srv01\users$\CHRR\Profile /homedir:\\zue-
srv01\users$\CHRR\Home
```

Das Home-Laufwerk wird automatisch auf den Laufwerksbuchstaben Z:\ gemappt.

Ergebnis:

Folgende Benutzer wurden erfolgreich angelegt:

```
C:\>net user
Benutzerkonten für \\ZUE-SRV01
-------------------------------------------------------------------------------
ABBM                     Administrator            ASPNET
BADA                     BLUK                     BOLJ
CHRR                     DUDF                     EGGA
Gast                     IUSR_VFI-03              IWAM_VFI-03
krbtgt                   SUPPORT_388945a0
Der Befehl wurde erfolgreich ausgeführt.
```

3.3.7 Globale Groups einfügen!

```
net group GO_Filialleiter /add
net group GO_Verk„ufer /add
net group GO_Supporter /add
```

```
net group GO_Lernende /add
net group GO_Aussendienst /add
net group GO_Reserve /add
```

Wir sehen, dass folgende Gruppen erstellt wurden:

```
C:\>net group
Gruppenkonten für \\ZUE-SRV01
[…]
*GO_Aussendienst
*GO_Filialleiter
*GO_Lernende
*GO_Reserve
*GO_Supporter
*GO_Verk„ufer
[…]
Der Befehl wurde erfolgreich ausgeführt.
```

3.3.8 Lokale Groups einfügen!

```
net localgroup LR_Filialleiter /add
net localgroup LR_Verk„ufer /add
net localgroup LR_Supporter /add
net localgroup LR_Lernende /add
net localgroup LR_Aussendienst /add
net localgroup LR_Reserve /add
```

Hier sehen wir die hinzugefügten Gruppen:

```
C:\>net localgroup
Gruppen für \\ZUE-SRV01
-------------------------------------------------------------------------------
*Administratoren
*Benutzer
[…]
*LR_Aussendienst
*LR_Filialleiter
*LR_Lernende
*LR_Reserve
*LR_Supporter
*LR_Verk„ufer
[…]
Der Befehl wurde erfolgreich ausgeführt.
```

3.3.9 User zu den Lokalen Gruppen hinzufügen

```
net localgroup LR_Filialleiter GO_Filialleiter /add
net localgroup LR_Verk„ufer GO_Verk„ufer /add
net localgroup LR_Supporter GO_Supporter /add
net localgroup LR_Lernende GO_Lernende /add
net localgroup LR_Aussendienst GO_Aussendienst /add
net localgroup LR_Reserve GO_Reserve /add
```

3.3.10 User zu den Globalen Gruppen hinzufügen

```
net group GO_Filialleiter ABBM /add
net group GO_Verk„ufer BLUK /add
net group GO_Supporter EGGA /add
net group GO_Lernende DUDF /add
net group GO_Aussendienst BADA /add
net group GO_Reserve BOLJ /add
net group GO_Reserve CHRR /add
```

3.3.11 Home-Verzeichnis für die Benutzer einfügen

Das Home-Verzeichnis wird im Ordner *D:\Daten\Users\%username%\Home* erstellt.

```
mkdir D:\Daten\Users\ABBM\Home
mkdir D:\Daten\Users\BLUK\Home
mkdir D:\Daten\Users\EGGA\Home
mkdir D:\Daten\Users\DUDF\Home
mkdir D:\Daten\Users\BADA\Home
mkdir D:\Daten\Users\BOLJ\Home
mkdir D:\Daten\Users\CHRR\Home
```

3.3.12 Profile-Ordner für die Benutzer erstellen

Das Profil wird im Ordner *D:\Daten\Users\%username%\Profile* erstellt.

```
mkdir D:\Daten\Users\ABBM\Profile
mkdir D:\Daten\Users\BLUK\Profile
mkdir D:\Daten\Users\EGGA\Profile
mkdir D:\Daten\Users\DUDF\Profile
mkdir D:\Daten\Users\BADA\Profile
mkdir D:\Daten\Users\BOLJ\Profile
mkdir D:\Daten\Users\CHRR\Profile
```

3.3.13 Berechtigungen erstellen

```
cacls D:\Daten /T /C /G Administrator:F Dom„nen-Admins:F
cacls D:\Daten\Users /T /C /G Jeder:R Administrator:F Dom„nen-Admins:F
net share users$=D:\Daten\Users /GRANT:Jeder,FULL
```

3.3.14 Public-Folder erstellen zum Austauschen von Dateien

Wir erstellen den folgenden Ordner, der für alle freigegeben ist. Dabei haben alle die Vollberechtigung (Gruppe Jeder).

```
mkdir D:\Daten\Public
cacls D:\Daten\Public /T /C /G Jeder:F
net share public$=D:\Daten\Public /GRANT:Jeder,FULL
```

3.3.15 Erstelle Gruppenordner

Auf die Gruppenordner haben nur die bestimmten Gruppen Zugriff.

Hinweis: Wir geben nicht den Ordner einer bestimmten Gruppe frei, sondern der übergeordnete Ordner Groups. Damit gehen wir auf die sichere Seite, wenn jemand in mehreren Gruppen ist. Dann kann man nur den Ordner Groups mappen und der Zugriff ist per NTFS-Berechtigung auf die jeweiligen Unterordner vom Netzwerklaufwerk geregelt.

```
net share groups$=D:\Daten\Groups /GRANT:Jeder,FULL
mkdir D:\Daten\Groups\Filialleiter
cacls D:\Daten\Groups\Filialleiter /T /C /G LR_Filialleiter:F Administrator:F
Dom„nen-Admins:F
mkdir D:\Daten\Groups\Verk„ufer
cacls D:\Daten\Groups\Verk„ufer /T /C /G LR_Verk„ufer:F Administrator:F Dom„nen-
Admins:F
mkdir D:\Daten\Groups\Supporter
cacls D:\Daten\Groups\Supporter /T /C /G LR_Supporter:F Administrator:F Dom„nen-
Admins:F
mkdir D:\Daten\Groups\Lernende
cacls D:\Daten\Groups\Lernende /T /C /G LR_Lernende:F Administrator:F Dom„nen-
Admins:F
mkdir D:\Daten\Groups\Aussendienst
cacls D:\Daten\Groups\Aussendienst /T /C /G LR_Aussendienst:F Administrator:F
Dom„nen-Admins:F
mkdir D:\Daten\Groups\Reserve
cacls D:\Daten\Groups\Reserve /T /C /G LR_Reserve:F Administrator:F Dom„nen-
Admins:F
net share groups$=D:\Daten\Groups /GRANT:Jeder,FULL
```

3.3.16 Preislisten-Ordner erstellen und freigeben

In diesem Ordner wird vom Chef eine Preisliste angelegt. Der Filialleiter hat darauf den Vollzugriff. Alle Anderen dürfen aber nur lesen.

```
mkdir D:\Daten\Preislisten
cacls D:\Daten\Preislisten /T /C /G Jeder:R LR_Filialleiter:F Administrator:F
Dom„nen-Admins:F
net share preislisten$=D:\Daten\Preislisten /GRANT:Jeder,FULL
```

3.3.17 Berechtigungen für die User auf das Home- und Profile-Verzeichnis

Auf das Home-Verzeichnis hat natürlich nur der User und der Administrator Zugriff.

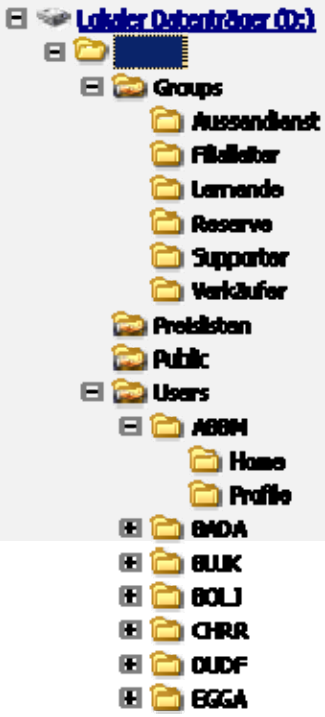
```
cacls D:\Daten\Users\ABBM /T /C /G ABBM:F Administrator:F Dom„nen-Admins:F
cacls D:\Daten\Users\BLUK /T /C /G BLUK:F Administrator:F Dom„nen-Admins:F
cacls D:\Daten\Users\EGGA /T /C /G EGGA:F Administrator:F Dom„nen-Admins:F
cacls D:\Daten\Users\DUDF /T /C /G DUDF:F Administrator:F Dom„nen-Admins:F
cacls D:\Daten\Users\BADA /T /C /G BADA:F Administrator:F Dom„nen-Admins:F
cacls D:\Daten\Users\BOLJ /T /C /G BOLJ:F Administrator:F Dom„nen-Admins:F
cacls D:\Daten\Users\CHRR /T /C /G CHRR:F Administrator:F Dom„nen-Admins:F
```

3.3.18 Ordnerstruktur

Das Script erstellt folgende Ordnerstruktur im Laufwerk *D:*\.

```
D:\>tree /a
Auflistung der Ordnerpfade
Volumeseriennummer : 0006EE50 3049:CD91
D:.
\---Daten
    +---Groups
    |   +---Aussendienst
    |   +---Filialleiter
```

```
    |   +---Lernende
    |   +---Reserve
    |   +---Supporter
    |   \---Verk„ufer
    +---Preislisten
    +---Public
    \---Users
        +---ABBM
        |   +---Home
        |   \---Profile
        +---BADA
        |   +---Home
        |   \---Profile
        +---BLUK
        |   +---Home
        |   \---Profile
        +---BOLJ
        |   +---Home
        |   \---Profile
        +---CHRR
        |   +---Home
        |   \---Profile
        +---DUDF
        |   +---Home
        |   \---Profile
        \---EGGA
```



Diese Ordnerstruktur ermöglicht eine einfache Organisation.

3.3.19 Freigaben / Berechtigungen

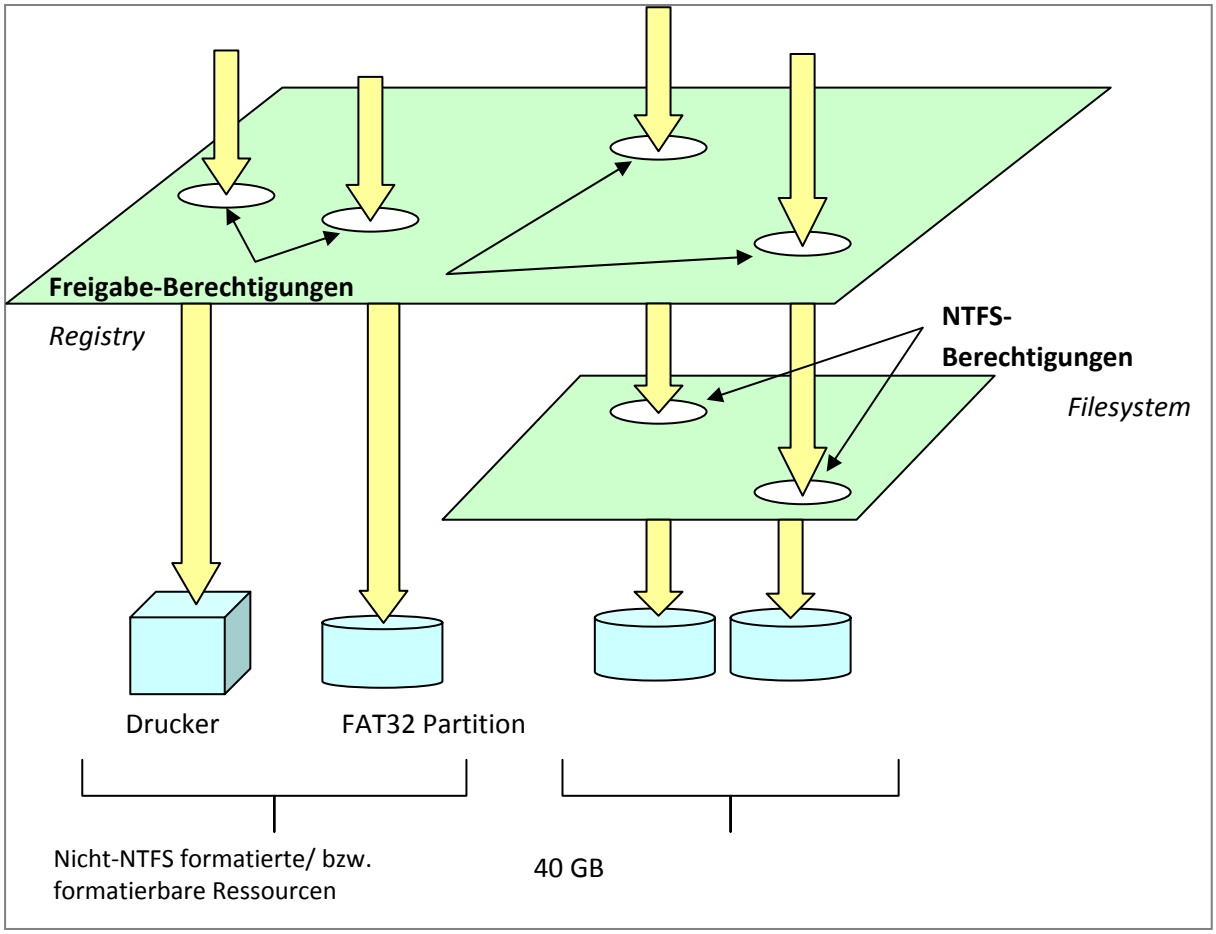
Hier eine Information bzgl. Berechtigungen

Es gibt zwei Arten von Berechtigungen:

- NTFS-Berechtigungen
- Freigabe-Berechtigungen

Die NTFS-Berechtigungen sind im Filesystem gespeichert. Diese sind auch aktiv, wenn der User sich lokal anmelden würde.

Die Freigabe-Berechtigungen sind dazu da, einem User zu ermöglichen auf einen Ordner/Drucker den Zugriff zu geben.



Bei den Freigaben vergeben wir immer die Vollberechtigung für die Gruppe Jeder. Damit kann jeder auf die freigegebenen Ordner zugreifen. Die weiteren Berechtigung bestimmt immer die NTFL-Dateiberechtigung. Anhand von dieser NTFS-Berechtigung wird der Zugriff geregelt.

```
C:\>net share
Name         Ressource                       Beschreibung
------------------------------------------------------------------------------
[…]
preislisten$ D:\Daten\Preislisten
Daten$       D:\Daten
groups$      D:\Daten\Groups
users$       D:\Daten\Users
public$      D:\Daten\Public
[…]
Der Befehl wurde erfolgreich ausgeführt.
```

3.3.20 Infos zu den Gruppen

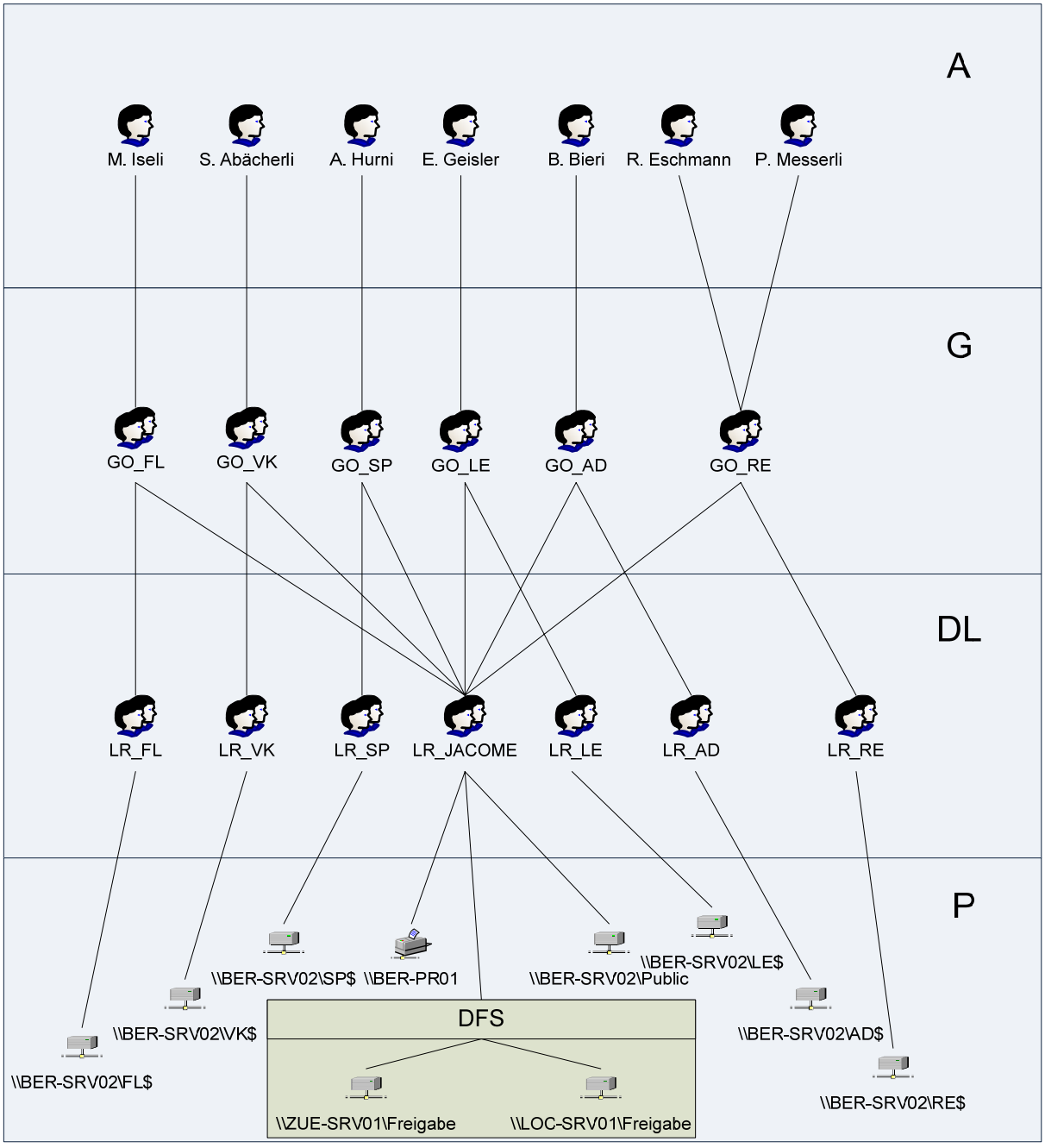
Wir arbeiten nach dem Prinzip: A G DL P

- A (Acout) Dies ist ein Benutzeraccount.
- G (Global Group)
- DL (Domain Local Group)
- P (Permission)

Globale Gruppen: Diese verwenden wir für die eigene Domäne. Man kann keine Benutzer von einer anderen Domäne in diese Gruppe einfügen. Wir vergeben keiner Ressource Berechtigung für diese Gruppen.

Lokale Gruppen: Diese verwenden wir für die Berechtigungen. Man fügt in diese lokalen Gruppen keine User, sondern globale Gruppen ein. Nun kann man auch globale Gruppen von einer anderen Domäne hinzufügen.

Das ist folgendermassen am Beispiel Bern zu sehen:[1]

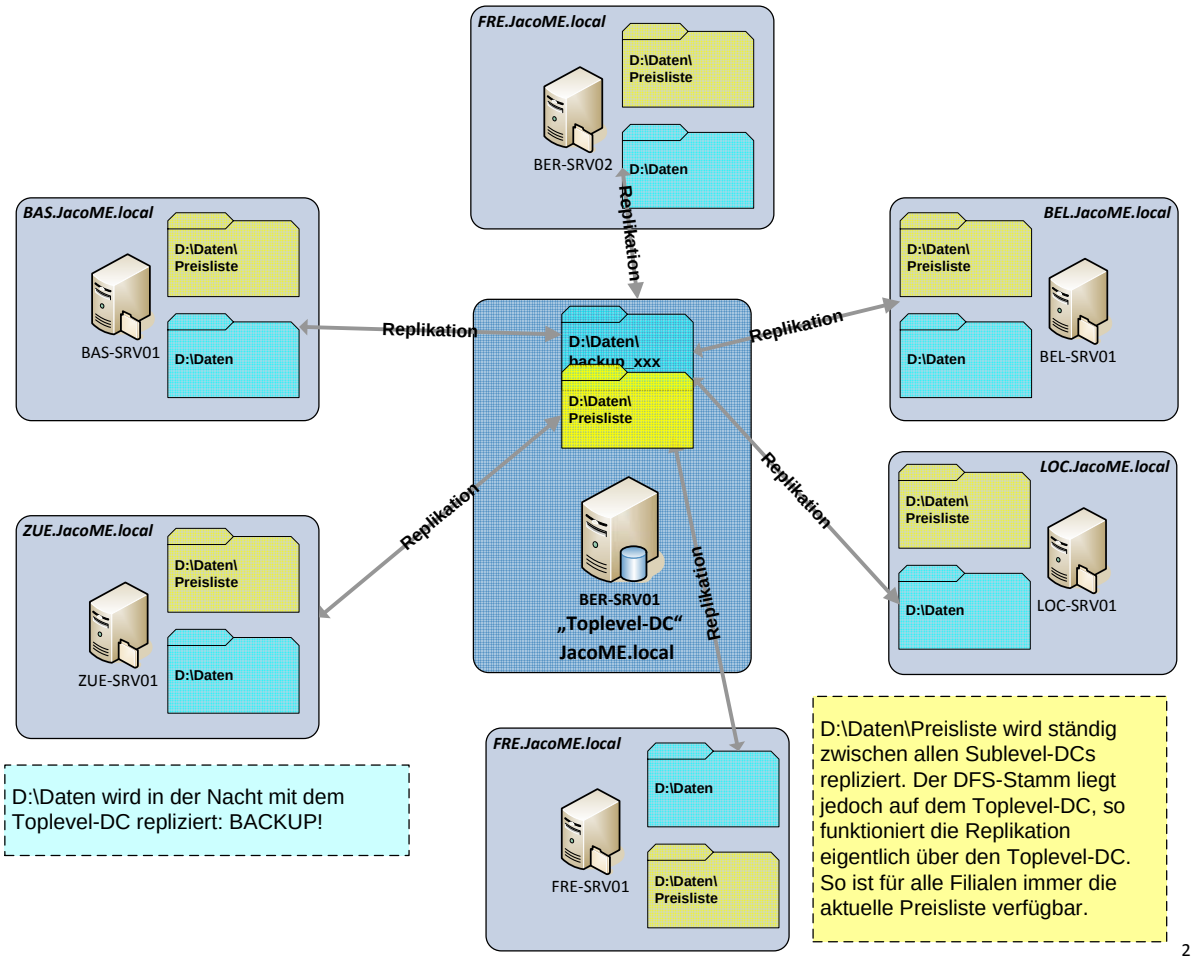


Folgendermassen sind die Bezeichnungen zu verstehen:

- **GO**_XX **G**lobal **O**rganisation
- **LR**_XX **L**ocal **R**essource

[1] Quelle: Roman Bachmann

3.4 DFS (Distributed File System) einrichten



[2]

Erklärung dazu: Wir benötigen das DFS für zwei Sachen:

1. Datenbackup: Die Daten von D:\Daten bei den Filialen werden beim Zentralserver auf D:\Daten\backup_zue gesichert.
2. Datenaustausch: Damit auf allen Agenturen immer dieselbe Preisliste vorhanden ist, synchronisiert der Zentral-Server die Preisliste mit allen Agenturen.

3.4.1 Grundfunktion

Die Grundfunktion von DFS ist es, verschiedene Freigaben auf mehreren Servern zu einer Freigabe zusammenzufassen.

- Client ermittelt durch ActiveDirectory den nächstgelegenen DFS Root-Server. Ist ein DFS Root-Server nicht verfügbar, suchen die Clients einen weiteren.
- DFS leitet die Clients nun zu den DFS-Zielen (Targets), also den Servern mit den entsprechenden Freigaben. Wenn ein solcher Server ausfällt, leitet DFS die Clients zu einem Server, dessen Freigabe als DFS-Target für dieselbe DFS-Verknüpfung konfiguriert ist.

[2] Grafik by Arno Galliker

Der Client connectet zum DFS-Server. Dort schaut der Client, wo die eigentliche Freigabe ist, und connectet dann direkt darauf. Es passiert kein Umweg über den DFS-Server. Es muss nicht zwingend eine Windows-Freigabe sein (der Client muss das Protokoll einfach unterstützen).

Wenn ein AD vorhanden ist, erstellt man einen DFS-Domänenstamm.

DFS-Domänenstamm	\\domain.int\stammname
Eigenständiger Stamm	\\computername\stammname

3.4.2 Voraussetzungen

OS	DFS-Client	DFS-Root	DFS-Ziel
W2k3	Ja	Ja	Ja
Windows XP	Ja	Nein	Ja
W 2k Server	Ja	Ja	Ja
W2K Professional	Ja	Nein	Ja
Windows NT4 Server	Ja	Ja (kein Domain-Mode)	Ja
Windows NT4 Workstation	Ja	Nein	Ja
Windows 98	Ja (kein Domain Mode)	Nein	Ja

3.4.3 FRS (File Replication Service)

Das funktioniert nur beim **DFS-Domänenstamm** (setzt ActiveDirectory voraus).

Eine DFS-Verknüpfung kann auch auf mehrere Ziele Zeigen, die auf verschiedenen Servern liegen. (zwei Ziele)

Wenn eine DFS-Verknüpfung auf 4 Ordner zeigt, möchte man diese 4 Freigaben synchron halten! (Replikationssatz hinzufügen)

Bei Verwendung eines „eigenständigen DFS-Stammes“ (also ohne die Mitarbeit einer Domain) kann man zwar mehrere Ziele definieren, diese jedoch nicht automatisch synchronisieren (das muss dann anders gelöst werden.).

3.4.4 Ausfallsicherheit

Sehr wichtig natüürli!!!

Klassischerweise verwendet man Cluster. Doch das DFS kann auch eine preisgünstigere Alternative sein.

DFS ist an zwei Stellen „empfindlich“: am DFS-Root (also die Anlaufstelle der Clients) und die DFS-Zeile (die Freigabe von den Servern).

So macht man es sicherer:

- DFS-Domänenstamm verwenden
- Redundante ActiveDirectory-Domainkontroller. Wenn kein DC vorhanden ist dann finden die Clients überhaupt nichts (/dev/null ☺).
- Redundante DFS-Roots: Wird über die MMC konfiguriert.
- Redundante DFS-Ziele: Mindestens 2 Ziele pro DFS-Verknüpfung. Diese sollten z.B. mit dem File Replication Service synchron gehalten werden.

Die redundanten Maschinen sollten physikalisch getrennt stehen…

3.4.5 Verteilen von Daten / Standortübergreifendes DFS

Damit die Mitarbeiter in Chur nicht über die WAN-Strecke auf den Server in Luzern zugreifen müssen, stellt man in Chur einen Server auf und erstellt eine Freigabe. Diese Freigabe definiert man dann als zusätzliches Ziel. Nun können die Mitarbeiter von Chur auf den Chur-Server zugreifen. Das macht man mit dem Domain Controller, dem DFS-Root und dem FileServer.

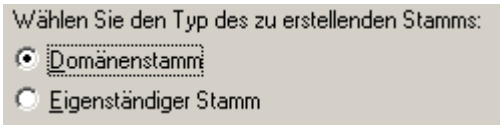
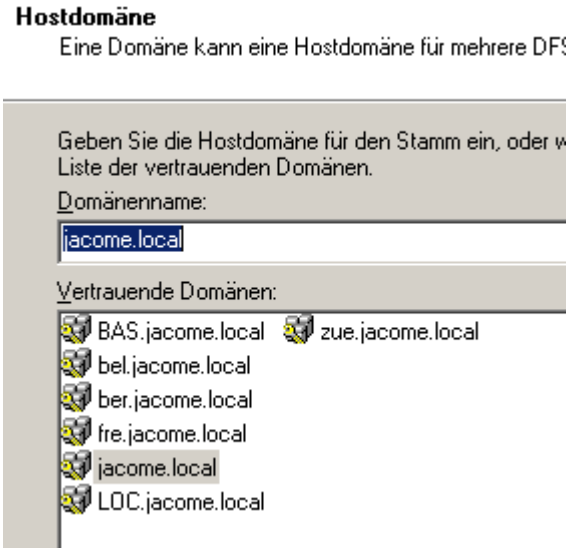
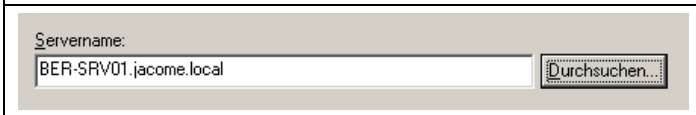
→ Man muss Das Datenvolumen beachten, damit die Synchronisation nicht die WAN-Strecke belastet.

3.4.6 Sicherung von Daten

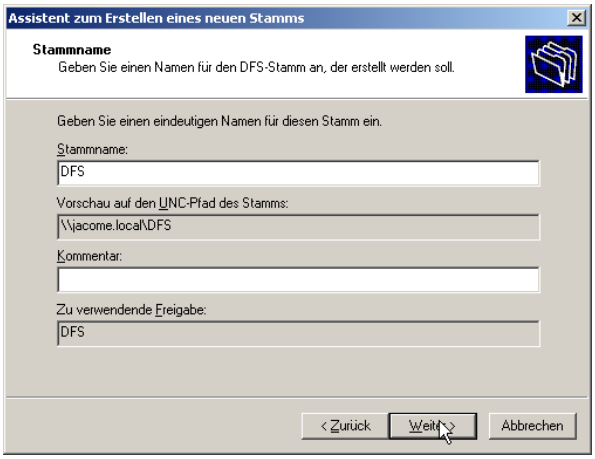
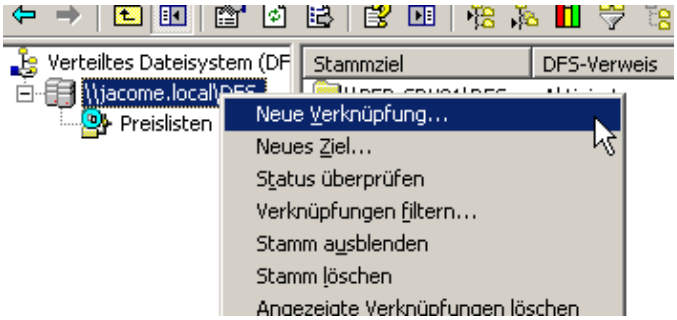
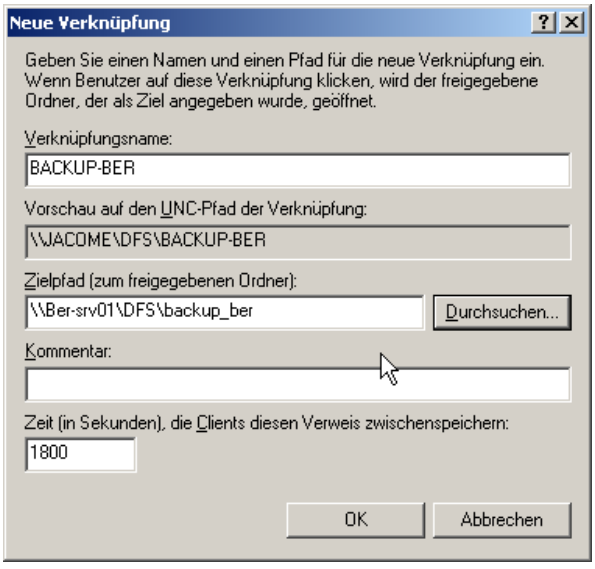
Die verschiedenen Ziele auf den verschiedenen Lokationen werden mit dem FRS synchronisiert. Somit muss man nur an einem Ort einen Tape-Roboter aufstellen.

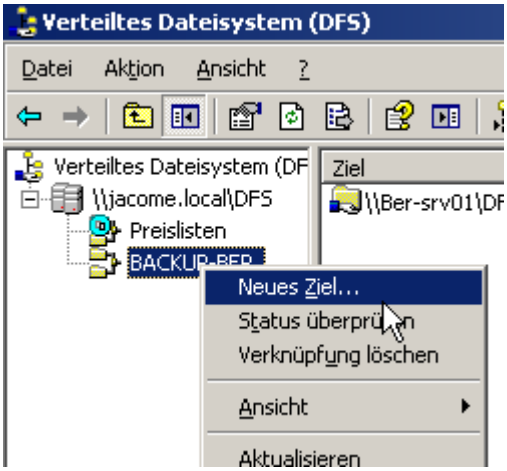
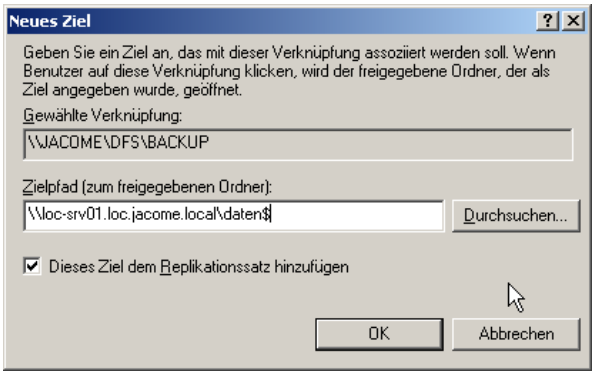
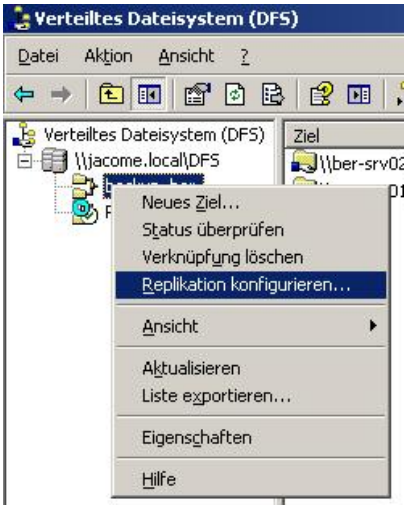
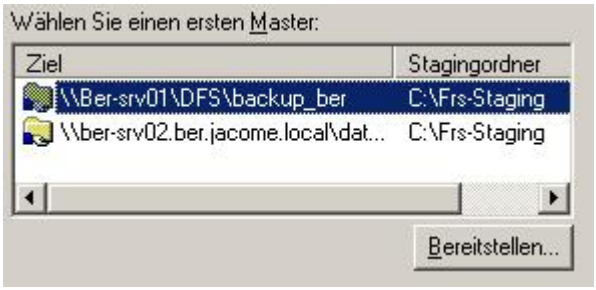
Sollte der Fileserver auf der Agentur ausfallen, so greifen die Clients auf die Daten im Hauptsitz zu. Ein Störfallkonzept ist also schon integriert ;).

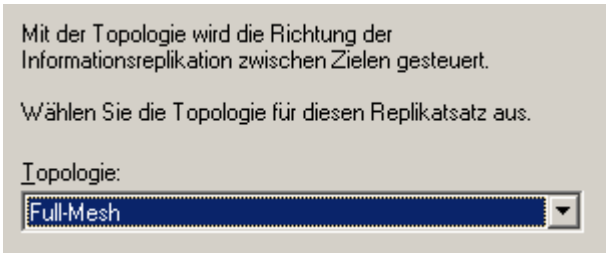
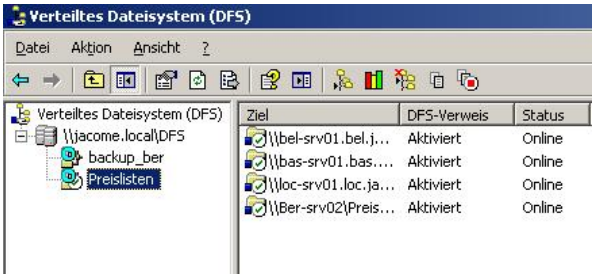
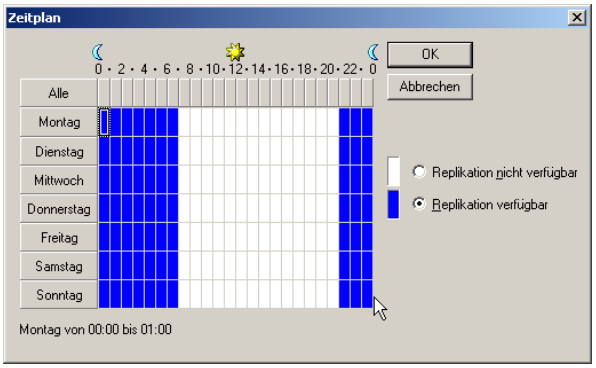
3.4.7 Anleitung[3]

	Domänenstamm auswählen (für Replikation)
	Top Domäne anwählen (*JACOME.LOCAL*)
	Als Hostserver nehmen wir den Top-Level Server.

[3] Erstellt von Reto Gobat

	Stammname: DFS (beliebig wählbar, möglichst aussagenkräftig.
	Es muss eine Verknüpfung erstellt werden.
	Der Name ist beliebig wählbar, sollte aber dennoch aussagekräftig sein. Der Zielpfad, muss auf den Top Server zeigen.

	Um eine Replikation zu ermöglichen, muss ein zweites Ziel erstellt werden.
	Hier geben wir als Zielpfad, den zu replizierenden Server ein.
	Die Replikation muss mit einem Rechtsklick auf die Verknüpfung eingerichtet werden. → „Replikation konfigurieren“.
	Zuerst muss der erste Master angegeben werden. Was in unserem Fall der Top-Level Domain Controller ist.

	Als Topologie wird „Full Mesh“ verwendet. Was in alle Richtungen funktioniert. (Totale Vermaschung)
	Nach erfolgreicher Konfiguration, sehen wir ein grünes „Kreislein“ neben der Verknüpfung.
	Wenn man nun auf die Domäne zugreift, sieht man den DFS Stamm. Von hier aus kann man auch auf die Daten im DFS zugreifen.
	Bei der Replikation kann man zudem noch einen Zeitplan erstellen. Aus performance Gründen setzten wir die Replikationszeiten von 22.00 – 06.00 Uhr.

3.4.8 Weitere Infos

Auf dieser Seite findet man viele nützliche Infos für DFS:

- http://www.serverhowto.de/Planung-Installation-und-Konfiguration-des-Distributed-File-System-DFS-unter-Windows-Server-2003.338.0.html

3.5 Konfiguration der Clients

Wir fügen die Clients der Subdomäne hinzu: *ZUE.JACOME.LOCAL*, damit wir uns an diesem Domänencontroller anmelden können.

Auf der Netzwerkkarte aktivieren wir DHCP, damit der Computer automatisch eine IP-Adresse bezieht.

3.5.1 SID (Computer Security Identifier)

Jeder PC muss für seine eindeutige Erkennung im LAN sein individuelles Erkennungsmerkmal haben. Dies ist der Computername und die SID, wie beim Menschen der Fingerabdruck. Kopiert man eine Festplatte mit einem Betriebssystem und würde beide Rechner gleichzeitig ins Netz bringen, würde eine Fehlermeldung kommen, dass der Rechner zweimal im Netz vorhanden ist. Hierbei hilft ein Freeware-Tool von SysInternals, welches die SID und den Rechnernamen ändert.

Der Befehl lautet:

```
newsid /a newname
```

Der Parameter "a" steht dabei für den automatischen Ablauf und "newname" ist die Variable für den neuen Computernamen. Anschliessend braucht nur noch die IP geändert werden, falls sie statisch ist. Weitere Informationen gibt es auch auf der angegebenen Seite.

Da wir die Computer per Image installierten, müssten wir eigentlich die SID ändern. Aber:

Hinweis: Die SID wird jedoch verändert, wenn wir einen Computer in eine Domäne einbinden. Deshalb müssen wir die SID nicht ändern!

4 WLAN Security

Bei WLAN kann jeder die Signale, die in der Luft sind, mit einer kompatiblen Antenne auffangen und analysieren, um unberechtigt Informationen zu erhalten oder gar zu manipulieren. Dies ist auch so, weil man die Funkweite nicht auf ein Gebäude beschränken kann und somit die Strahlen bis auf die Strasse gelangen.

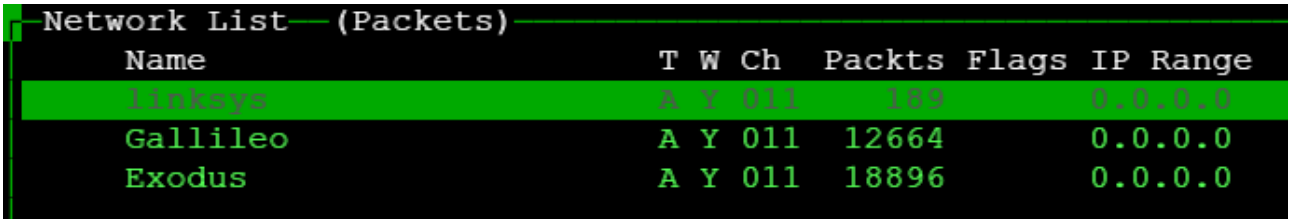
4.1 Viele Schutzmassnahmen, die nichts bringen

Es gibt verschiedene Methoden, ein WLAN sicher zu machen. Es gibt grundlegende Schutzmassnahmen wie z.B. MAC-Filter aktivieren oder das aussenden der SSID zu unterbinden.

Mit Kismet kann man jedoch auch nach Netzen suchen, die „versteckt“ sind. Kismet zeigt ausserdem auch die MAC-Adressen der Clients an, die mit dem Netz verbunden sind. Praktisch. Somit sind die ersten zwei Schutzmassnahmen nichts wert.

4.2 Hide SSID bei Kismet

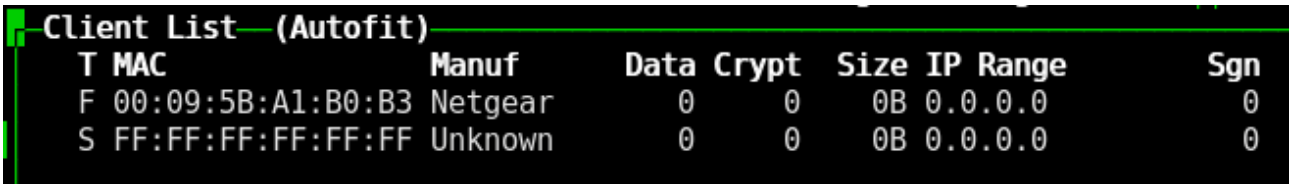
Kismet zeigt eine versteckte SSID an:



Über diese können wir uns nun mit dem WLAN verbinden, oder beginnen den WEP-Schlüssel zu berechnen.

4.3 MAC-Adressen fälschen

Kismet zeigt die MAC-Adressen der Clients an:



Diese können wir nun fälschen: Man kann die MAC-Adresse auf verschiedene Arten ändern:

Wir können die MAC mit dem Standard-Tool *IFCONFIG* oder über *MACCHANGER* ändern. Simpel!

```
root@discordia:~# ifconfig eth0 | grep Hardware
eth0      Link encap:Ethernet  Hardware Adresse 00:1c:25:74:cd:06
root@discordia:~# ifconfig eth0 hw ether AA:AA:AA:AA:AA:AA
root@discordia:~# ifconfig eth0 | grep Hardware
eth0      Link encap:Ethernet  Hardware Adresse aa:aa:aa:aa:aa:aa
root@discordia:~# macchanger eth0 -m 00:1c:25:74:cd:06
Current MAC: aa:aa:aa:aa:aa:aa (unknown)
Faked MAC:   00:1c:25:74:cd:06 (unknown)
root@discordia:~# ifconfig eth0 | grep Hardware
eth0      Link encap:Ethernet  Hardware Adresse 00:1c:25:74:cd:06
```

4.4 Netzwerkdetails mit Kismet auflisten

```
Network Details
Name     : Exodus

SSID     : GALILEO
Server   : localhost:2501
BSSID    : 00:09:5B:88:CA:E0
Carrier  : IEEE 802.11a
Manuf    : Netgear
Model    : Unknown
Matched  : 00:09:5B:00:00:00/FF:FF:FF:00:00:00
Max Rate: 36.0
BSS Time: ca3a7ee037
Max Seen: 1000 kbps
First    : Fri May 30 23:20:17 2008
Latest   : Fri May 30 23:54:02 2008
Clients  : 0
Type     : Access Point (infrastructure)
Info     :
Channel  : 11
Privacy  : Yes
Encrypt  : WEP
Decryptd: No
Beacon   : 25600 (26.214400 sec)
Packets  : 18896
  Data     : 0
  LLC      : 18896
  Crypt    : 0
  Weak     : 0
  Dupe IV  : 0
Data     : 0B
Signal   :
  Power    : -87 (best -74)
  Noise    : 0 (best 0)
IP Type  : None detected
Min Loc  : N/A
Max Loc  : N/A
Range    : N/A
```

Daraus können wir schon viel ablesen. Die Verschlüsselung ist z.B. WEP. Wir sehen die MAC-Adresse vom Router und der Hersteller. Somit können wir in einer Tabelle das Standardpasswort nachschauen. Damit wir mehr Pakete sammeln können, sehen wir, dass wir auf Channel 11 lauschen müssen. In *KISMET* kann man das mit Shitf + L einstellen.

4.5 WEP-Verschlüsselung

Man kann das eindringen in ein Netzwerk mittels Verschlüsselung verbieten. Eine schwache Verschlüsselung ist WEP (Wired Equivalent Privacy). Wir sniffen den Netzwerkverkehr mit *AIRODUMP-NG* oder *KISMET* und schreiben ihn in ein Dumpfile. Danach entschlüsseln wir ihn mit *AIRCRACK-NG*.

AIRODUMP-NG in Action

```
                                Aircrack-ng 1.0 beta1

                [00:00:12] Tested 3537600 keys (got 49 IVs)

   KB    depth   byte(vote)
    0    0/  1   A3(1024) 1B( 512) 2B( 512) 82( 512) B7( 512)
    1    0/  1   7F( 768) 6E( 512) A5( 512) B4( 512) 01( 256)
    2    0/  1   E4( 512) BA( 512) 04( 256) 10( 256) 1A( 256)
    3    0/  1   13( 512) 65( 512) 00( 256) 01( 256) 0F( 256)
    4    0/  1   0D( 512) 79( 512) C0( 512) D0( 512) DA( 512)
    5    0/  1   E6( 512) 4C( 512) 58( 512) DA( 512) E5( 512)
    6    0/  1   FF( 512) 98( 512) BF( 512) E9( 512) 01( 256)
    7    0/  1   74( 768) 0D( 512) A6( 512) F2( 512) 22( 256)
    8    0/  1   F6( 768) 9C( 512) B7( 512) E8( 512) 03( 256)
    9    0/  9   5E( 512) 66( 512) 85( 512) C7( 512) E9( 512)
   10    0/  1   40( 768) 67( 768) 2D( 512) 9B( 512) DA( 512)
   11    0/  1   69( 768) 23( 512) 43( 512) 6A( 512) 87( 512)
   12    0/ 12   44( 440) 69( 440) 90( 440) D2( 440) 0C( 256)
```

Damit man den WEP-Schlüssel berechnen kann, braucht man zwischen 500'000 und 700'000 Pakete. Entweder wartet man sehr lange, oder man erzeugt mit der richtigen Netzwerkkarte und dem richtigen Treiber selber Netzwerkverkehr. Dazu benutzt man das Tool *AIREPLAY-NG*. Dieses schickt ARP-Requests in das betroffene WLAN und erzeugt somit Traffic.

Hier ist ein Auszug aus der Manpage von *AIREPLAY-NG*:

```
DESCRIPTION
       aireplay-ng injects specially generated ARP-request packets into an
       existing wireless network in order to generate traffic. By sending
       these ARP-request packets again and again, the target host will respond
       with encrypted replies, thus providing new and possibly weak IVs.

       aireplay-ng supports single-NIC injection/monitor.
       This feature needs driver patching.
```

Wenn man so ca. 700 MB Traffic mithören konnte, kann man das Dumpfile an *AIRCRACK-NG* übergeben und dieses knackt das Kennwort innert Sekunden/Minuten:

```
root@discordia:~# aircrack /var/log/kismet/Kismet-May-29-2008-1.dump
Opening /var/log/kismet/Kismet-May-29-2008-1.dump
Read 6062 packets.

   #  BSSID              ESSID                     Encryption

   1  00:19:CB:03:E7:6A  discordia                 WPA (0 handshake)
   2  00:18:39:22:B5:FA  EXODUS                    WEP (49 IVs)
   3  00:18:39:2C:E3:46  U     No data - WEP or WPA
   4  00:09:5B:88:CA:E0  GALILEO                   WEP (36 IVs)
   5  00:13:10:05:D4:D0  linksys                   WEP (2 IVs)
```

```
Index number of target network ? 2

Not enough IVs available. You need about 250.000 IVs to crack
40-bit WEP, and more than 800.000 IVs to crack a 104-bit key.
```

Wir sehen, dass ich zu wenige Pakete gesammelt habe. Wenn wir *AIREPLAY-NG* einsetzen könnten, wäre das WEP-Passwort innert Minuten geknackt.

4.6 Fazit

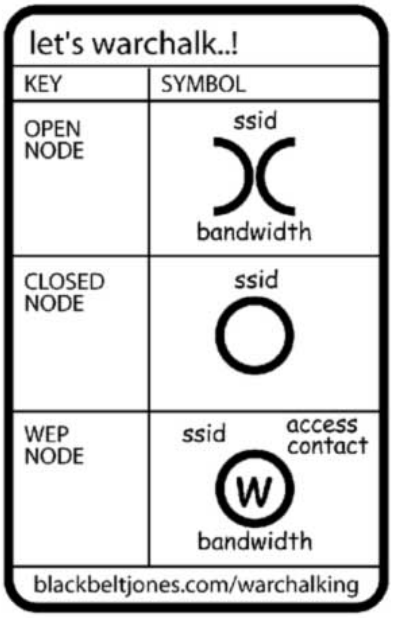
Wir sehen: WEP ist sehr einfach zu knacken. Hierfür braucht man keine Hacker-Fähigkeiten. Man liest sich in die MAN-Pages der Tools ein (*AIRCRACK-NG* und *KISMET*) und probiert ein bisschen rum...

Hinweis: Das unerlaubte eindringen in Netzwerke ist strafbar! Daher gilt: Man soll sich nicht erwischen lassen und deshalb gar nicht probieren. Man darf am eigenen Netz rumspielen und üben ein WEP-Schlüssel zu knacken. Wir selber lernen auch daraus, dass wir uns selber besser schützen müssen.

WPA ist eher dazu gedacht, dass sich nicht jemand zufällig mit dem Netzwerk verbindet… ☺

Ein wesentlich besserer Schutz ist WPA. Diesen Schutz kann man nicht zurück berechnen. Man kann zwar Bruteforce oder Dictionary-Attaken machen, aber Mathematisch ist der WPA-Schlüssel nicht knackbar. Wenn man also ein sichere Passwort wählt und es sicher aufbewahrt (digital verschlüsselt!), kann „nichts“ passieren.

4.7 Wardriving



Ein neuer Volkssport ist Wardriving. Leute suchen nach (offenen) WLANs. Das ziel ist nicht etwas zu beschädigen, oder in geschützte Netze einzubrechen. Man will legidlich schauen, wo etwas offen ist und was es dort zu schauen gibt. Oft findet man Musik, Bilder oder auch sogar einen Netzwerkdrucker.

Nach dem einloggen in das Netzwerk, lässt man *NMAP* laufen. Das ist ein IP- bzw. Portscanner. Er scannt einen Bereich von Ips ab und prüft, welche Ports offen sind:

Wenn man eine Man-in-the-Middle-Attacke machen würde, könnte man Daten manipuliert weiterschicken.

Wir sehen nun was es gibt. Wir mounten Windows-Freigaben und können vielleicht sogar Familienfotos bestaunen. Eventuell hinterlässt man noch einen Ausdruck auf dem freigegebenen Drucker, dass das Netzwerk nicht verschlüsselt ist.

Wenn man nur über ein offenes Netz surft, macht man nichts illegales, solange man nichts manipuliert oder irgendwo einbricht. Es könnte auch eine Falle sein: Mitten in der Statt steht ein offenes WLAN. Super, wir connecten und loggen uns auf FTP-Servern, POP3-Konten, VNC-Hosts etc ein. Jeder (!) kann den Datenverkehr mithören und solange nichts verschlüsselt ist, kann jeder (!) mit *DSNIFF* die Logindaten abhören. Man kann sich davor schützen, indem man sich per VPN in ein anderes (virtuelles) Netzwerk einwählt (verschlüsselt) und in diesem Netz mit den Arbeiten beginnt.

4.8 Demo-Attacke

4.8.1 Netzwerkkarte vorbereiten

`root@discordia:~# ifconfig wlan0 down`	WLAN Interface deaktivieren
`root@discordia:~# iwconfig wlan0 mode monitor`	WLAN Interface in Monitoring-Modus (nur hören)
`root@discordia:~# ifconfig wlan0 up`	WLAN Interface starten

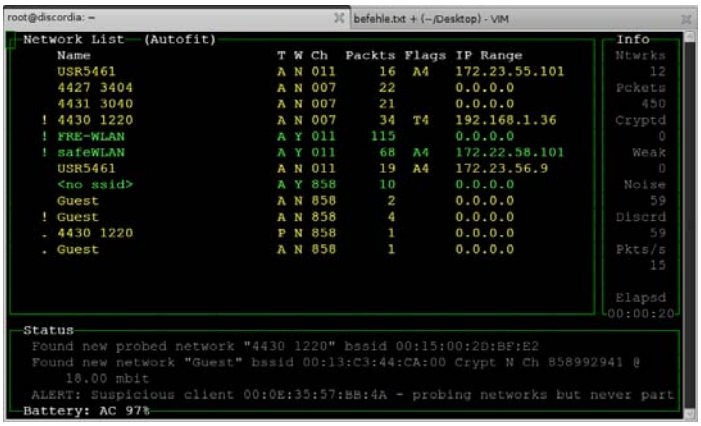
4.8.2 Datenverkehr erzeugen

Damit wir den Datenverkehr mithören können, müssen wir zuerst Datenverkehr erzeugen. Dies machen wir mit einem passenden Treiber für die WLAN-Karte, damit man gleichzeitig senden und empfangen kann (im monitoring-Modus), oder wir nehmen ein zweites Notebook und erzeugen mit diesem Notebook Traffic. Dazu nutzen wir das Tool *AIREPLAY-NG*. Das Tool sendet ARP-Requests an den AP und erzeugt somit Traffic.

```
aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:11:22:33:44:55 wlan0
```

- *-3* bedeutet, dass es normale arp requests erzeugt
- *-B* ist die BSSID vom AP
- *-H* ist die source MAC-Adresse vom ARP-Request. Hier kann ein Fake eintragen.
- *WLAN0* ist das WLAN-Interface

4.8.3 Datenverkehr mithören mit Kismet

`root@discordia:~# kismet` 	Kismet starten Kismet schreibt im Hintergrund alle Pakete die herumschwirren in eine Datei.
s p	Sortieren nach Pakete
shift L	Nur noch den Kanal des markierten WLANs sniffen
shift Q	Kismet verlassen

4.8.4 Datenverkehr mithören mit Airodump-ng

`airodump-ng –i wlan0 –w file.dump –c 11`	Wir hören mit der WLAN-Karte *WLAN0* auf dem Kanal *11* und speichern den

	Dump in das File *FILE.DUMP*.

4.8.5 Knacken mit Aircrack 2.3

`root@discordia:~# aircrack /var/log/kismet/Kismet-Jun-02-2008-1.dump`	Aircrack starten und das dumpfile von kismet mit den gespeicherten Paketen mitgeben
Read 3598511 packets.	Aircrack list die Pakete ein…

root@discordia:~# aircrack /var/log/kismet/Kismet-Jun-02-2008-1.dump
Opening /var/log/kismet/Kismet-Jun-02-2008-1.dump
Read 3598511 packets.
 	
  # BSSID ESSID Encryption
 	
  1 00:0F:CC:91:8D:5C 4430 1220 WPA (0 handshake)
  2 00:0F:CC:91:78:C8 4427 3404 WEP (4 IVs)
  3 00:13:C3:44:C7:B0 Guest None (0.0.0.0)
  4 00:0F:CC:91:99:EC 4431 3040 WPA (0 handshake)
  5 00:C0:49:FF:38:28 USR5461 No data - WEP or WPA
  6 00:C0:49:F1:29:00 FRE-WLAN WPA (0 handshake)
  7 00:C0:49:FF:30:92 USR5461 WEP (7 IVs)
  8 00:C0:49:FE:F9:1C safeWLAN EAPOL+WEP (3070729 IVs)
  9 00:14:C1:1D:31:82 USR5461 WEP (445 IVs)
 10 00:13:C3:44:C7:E0 [illegible] None (0.0.0.0)
 	
Index number of target network ?
	Das zuhackende WLAN wählen: 8 safeWLAN

aircrack 2.3 [00:00:05] Tested 1 keys (got 3070729 IVs) KB depth byte(vote) 0 0/ 1 46(765) 9F(27) 35(19) B3(15) 93(10) EA(10) B6(1) 0E(-3) 21(-7) 34(-9) 78(-12) 59(-22) 1 0/ 1 49(773) EB(38) 55(20) A0(18) 6C(-5) EA(-11) 93(-12) 69(-13) 2E(-14) B1(-15) 18(-21) 4C(-21) 2 0/ 1 52(530) 9D(47) 07(29) 9C(28) AB(27) 1B(21) 1E(9) 63(0) 62(-9) E0(-9) 45(-12) C1(-15) 3 0/ 1 45(1692) 53(72) AF(47) 52(43) 0B(20) 1E(15) 09(8) 44(6) C3(5) 0A(4) 69(0) 9F(0) 4 0/ 1 77(802) 05(39) A9(31) 52(30) 06(25) 53(24) BD(23) D2(19) BF(18) 63(17) BC(17) 3C(15) 5 0/ 1 69(809) E4(66) 3F(49) 3C(45) 74(38) 86(37) 40(34) 88(32) D2(30) 29(29) 87(28) FB(20) 6 0/ 1 72(995) 12(54) CE(43) 60(42) 02(40) 14(40) 01(38) E1(36) 15(33) 2C(32) 7F(32) B6(32) 7 0/ 1 65(812) 52(51) 86(43) 84(39) 9A(39) 03(38) 73(35) 99(32) 8B(30) 50(28) 3A(26) 96(25) 8 0/ 1 5F(421) 71(65) 1B(54) 02(53) 16(51) E2(50) 73(49) DE(44) 2A(40) 03(38) 15(36) 91(36) 9 0/ 1 32(525) 6F(58) AA(53) BE(53) 70(51) B9(50) 72(44) 96(44) B0(44) BD(42) 73(41) 74(41)]	Aircrack findet den Key anhand der gespeicherten Pakete innerhalb von 5 Sekunden! Pwned!

4.9 Weitere Infos

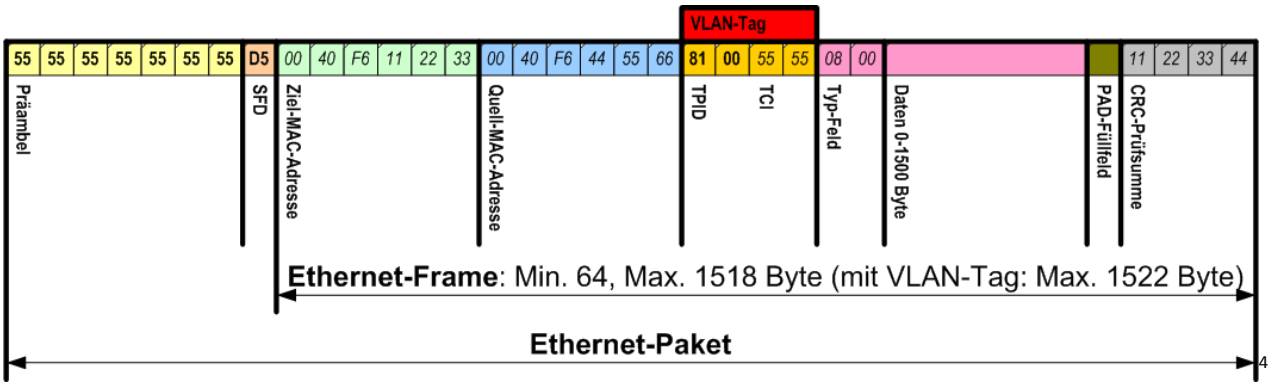
- http://www.wardriving.ch
-

5 VLAN realisieren

5.1 Theorie

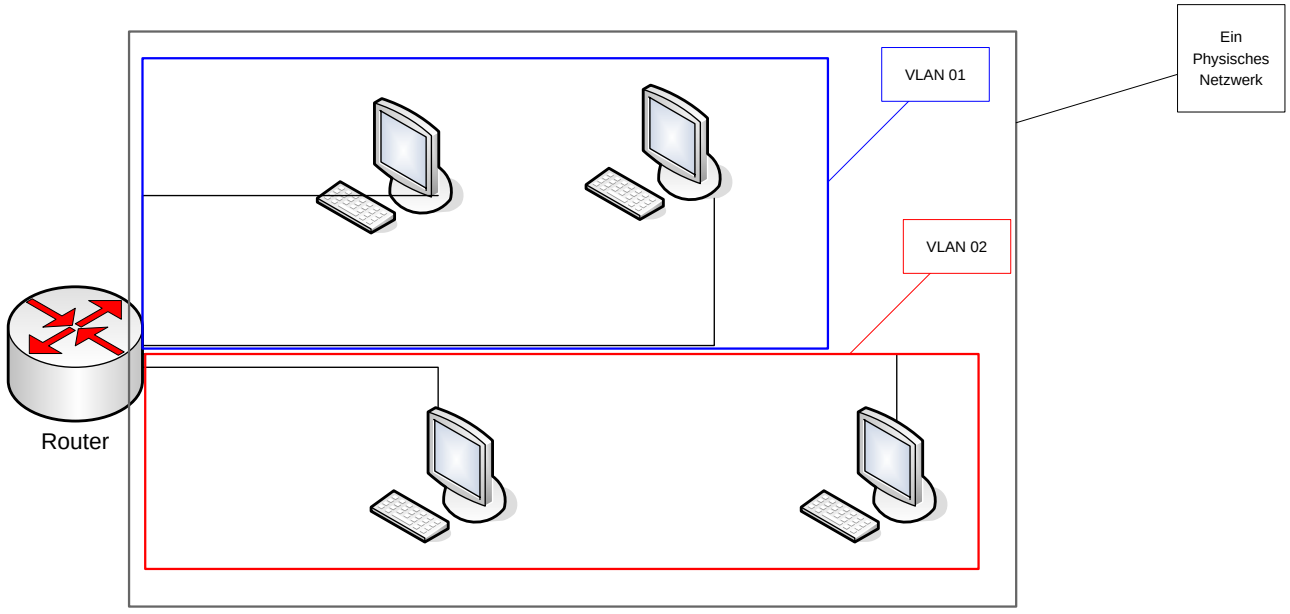
Wir nehmen ein normales Frame und hängen ein VLAN-Tag daran. Dieses wird durch eine VLAN fähigen Switch hinzugefügt und danach wieder entfernt.

Anhand dieses Tags erkennt der VLAN-Fähige Switch, woher das Ethernet-Frame kommt und wohin es muss. Das Frame wechselt das VLAN nie! Die Clients, die in unterschiedlichen VLANS sind, sehen sich nie. Das kommt denen vor, als ob sie in einem eigenen physischen Netzwerk sind.



[4]

5.1.1 Einfaches Beispiel



Ein VLAN unterteilt ein Physisches Netz in mehrere (virtuelle) Netze. Die Kommunikation funktioniert nur über den Router = grössere Sicherheit im Netz. Die Unterteilung erfolgt entweder auf dem Router, per Software (anhand der MAC Adresse) oder auch nach Benutzername. Die sicherste ist die 1. Variante, da man Physisch an der bestimmten Dose sein muss.

[4] Quelle: Wikipedia: http://de.wikipedia.org/wiki/Virtual_Local_Area_Network

5.1.2 Dynamisches VLAN

Dynamsiche VLANS sind sehr flexibel und leicht anzupassen. In dynamischen VLANs erkennt der Switch beim Anschluss des Systems an einen anderen Port diesen anhand seiner MAC-Adresse und liest aus der VLAN-Management-Datenbank aus, zu welchem VLAN-Segment er gehört. Ortsunabhängigkeit eines dynamischen VLANs ist ein entscheidender Vorteil, wenn Mitarbeiter beispielsweise öfter denStandort wechseln.

Sogar räumlich entfernte Mitarbeiter – etwa im Heimbüro – bleiben automatisch Mitglied des jeweiligen VLAN-Segments. Broadcasts aus einem Segment werden nicht in ein anderes weitergeleitet. VLAN-Segmente sind voneinander weitgehend unabhängig.

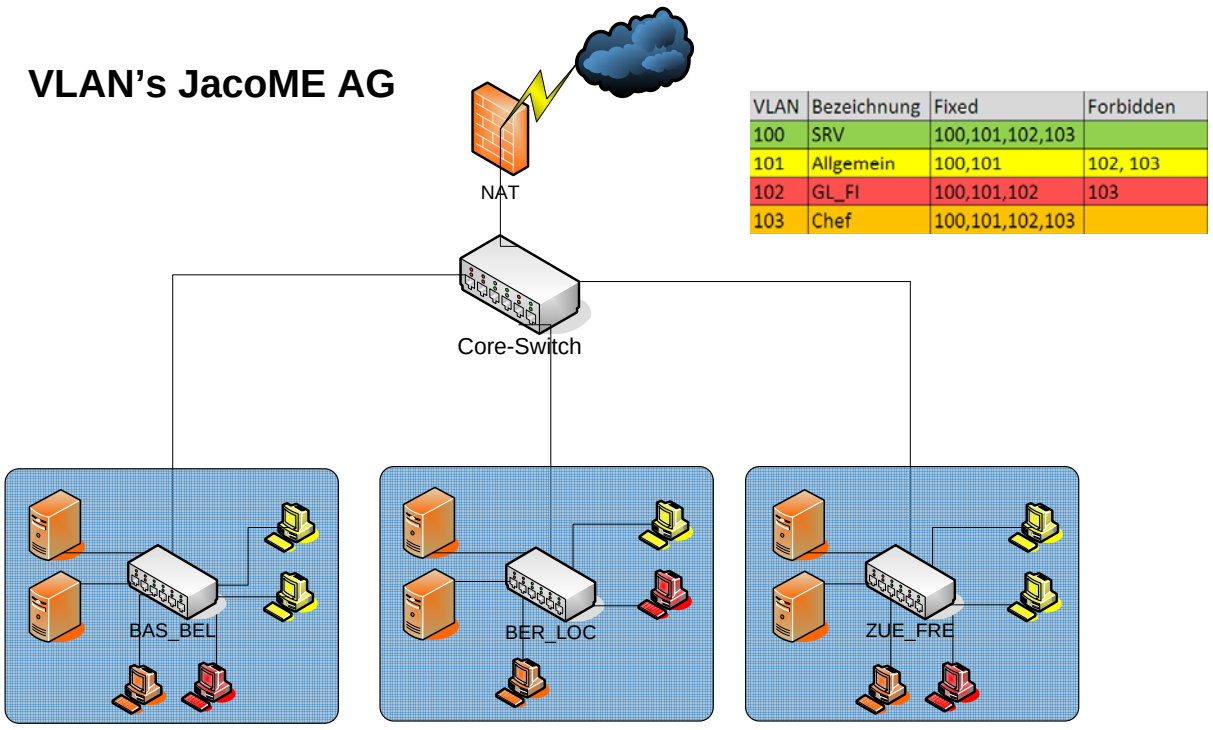
Dynamische VLANs sind im Gegensatz zu Statischen VLANs eher unsicher, da eine MAC-Adresse eines Rechners geändert werden kann und somit eine falsche Identität vorgetäuscht werden könnte.

5.1.3 Static-VLAN

Beim Statischen VLAN werden die VLANS auf den Port eingestellt. Damit werden alle Geräte, die an einem gewissen Port angeschlossen sind, auf dieses voreingestellte VLAN gestellt.

5.2 Praxis

Wir erstellen folgendermassen die VLANS:



VLAN	Bezeichnung	Fixed	Forbidden
100	SRV	100,101,102,103	
101	Allgemein	100,101	102, 103
102	GL_FI	100,101,102	103
103	Chef	100,101,102,103	

Port	Bezeichnung	VLAN
1-2	Allgemein	101
3	Chef	103
4	GL_FI	102
5-6	SRV	100

Port	Bezeichnung	VLAN
1-2	Allgemein	101
3	Chef	103
4	GL_FI	102
5-6	SRV	100

Port	Bezeichnung	VLAN
1-2	Allgemein	101
3	Chef	103
4	GL_FI	102
5-6	SRV	100

Das Ziel ist die logische Unterteilung unseres Netzes in 2 virtuelle LANs „Allgemein“ und „GL_FI“. Weiter wurde noch ein VLAN 103 definiert, welches auf beide anderen VLANs sieht.

Der Chef und die Server sehen also beide VLANs.

5.2.1 Die Verschiedenen VLANS

5.2.1.1 VLANs

VLAN	Bezeichnung	Fixed	Forbidden
100	SRV	100,101,102,103	
101	Allgemein	100,101	102, 103
102	GL_FI	100,101,102	103
103	Chef	100,101,102,103	

5.2.1.2 Ports

Auf jedem Switch sind die Ports folgdendermassen konfiguriert

Port	Bezeichnung	VLAN
1-2	Allgemein	101
3	Chef	103
4	GL_FI	102
5-6	SRV	100

5.2.2 VLAN für VoIP

Für VoIP haben wir ein VLAN 104 definiert.

Die VLAN-Konfig sieht nur folgendermassen aus:

VLAN	Bezeichnung	Fixed	Forbidden
100	SRV	100,101,102,103	
101	Allgemein	100,101	102, 103
102	GL_FI	100,101,102	103
103	Chef	100,101,102,103	
104	VoIP	104	100,101,102,103

Die Ports 10-27 wurden für VoIP konfiguriert:

Port	Bezeichnung	VLAN
1-2	Allgemein	101
3	Chef	103
4	GL_FI	102
5-6	SRV	100
10-27	VoIP	104

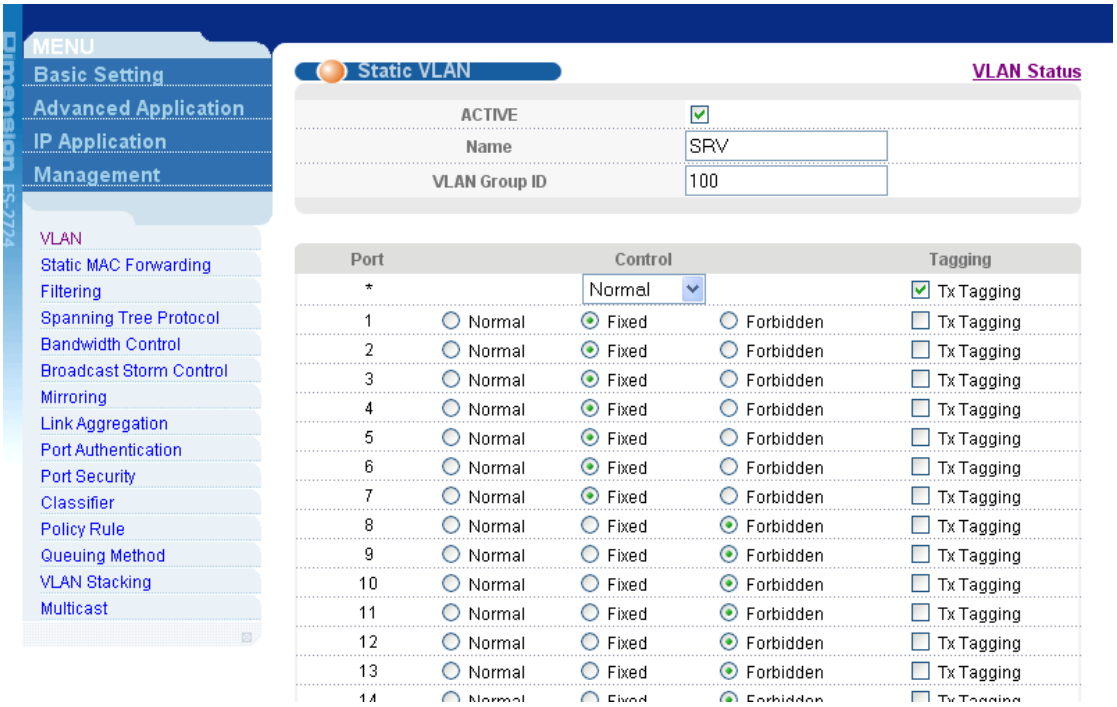
5.2.3 Konfiguration auf dem Switch (Web-Interface)

Hiersind die 4 VLAN's in der Übersicht der existierenden VLAN's auf den Switches welche man in der Grafik unten siehtDie genaue Erläuterung von *Fixed* und *Forbidden* wird während der Installationsbeschreibung noch geklärt.

Das VLAN 104 entspricht dem VOIP VLAN welches in diesem Arbeitsschritt noch nicht gebraucht wurde.

VLAN	Bezeichnung	Fixed (erlaubt)	Forbidden (nicht erlaubt)
100	SRV	100,101,102,103	
101	Allgemein	100,101	102, 103
102	GL_FI	100,101,102	103
103	Chef	100,101,102,103	

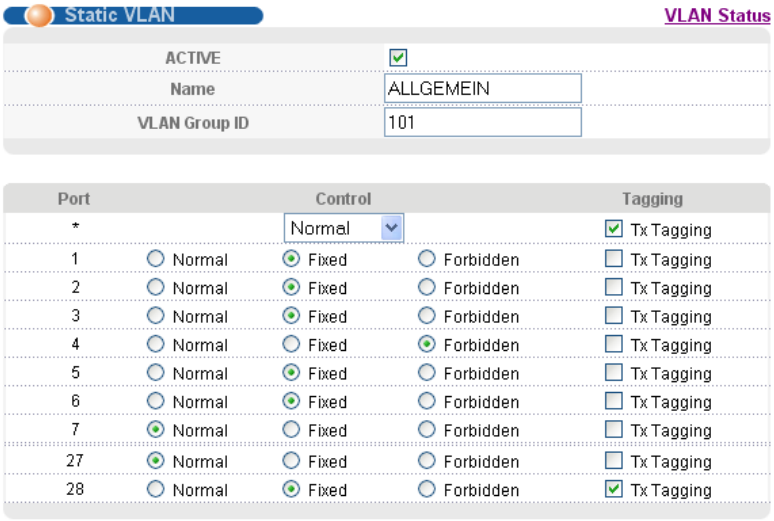
Die Eigenschaften des *VLAN's 100 SRV* sehen folgendermassen aus:



Die Server können von allen Ports aus gesehen werden, daher sind die Ports von 1-7 alle auf Fixed gesetzt. Von allen anderen Ports kann nicht auf die Server gesehen werden.

5.2.3.1 VLAN 101 Allgemein

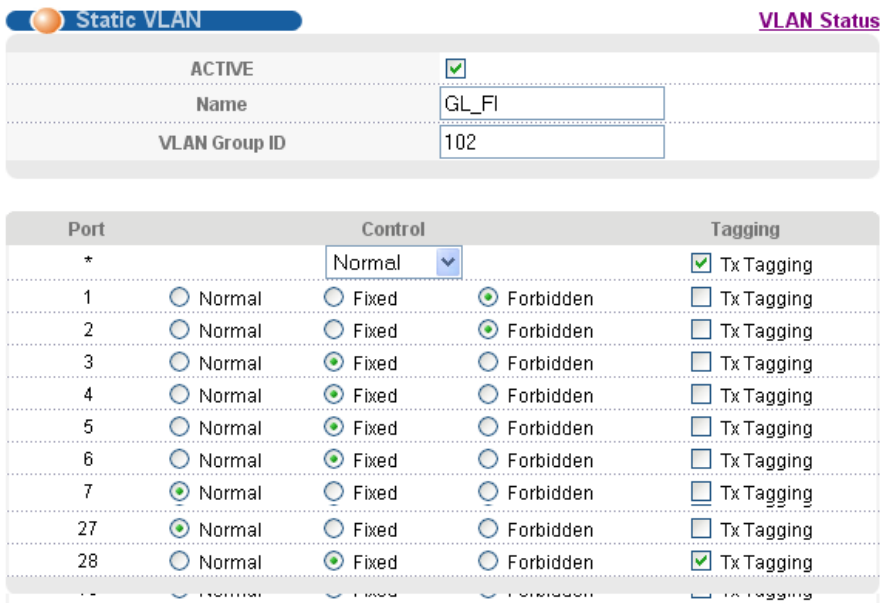
Die Eigenschaften des *VLAN's 101 ALLGEMEIN* sehen folgendermassen aus:



In diesem VLAN befinden sich die Allgemeinen Clients. Diese sind an den Switchports 1 und 2 angeschlossen, daher sind diese Punkte auf Fixed gesetzt worden. An Port 3 hängt der Chef PC welcher ebenfalls die allgemeinen Arbeitsstationen sehen darf. Die Server welche an Port 5 und 6 angeschlossen sind können die Allgemeinen Arbeitsstationen auch sehen.

5.2.4 VLAN 102 GL_FI

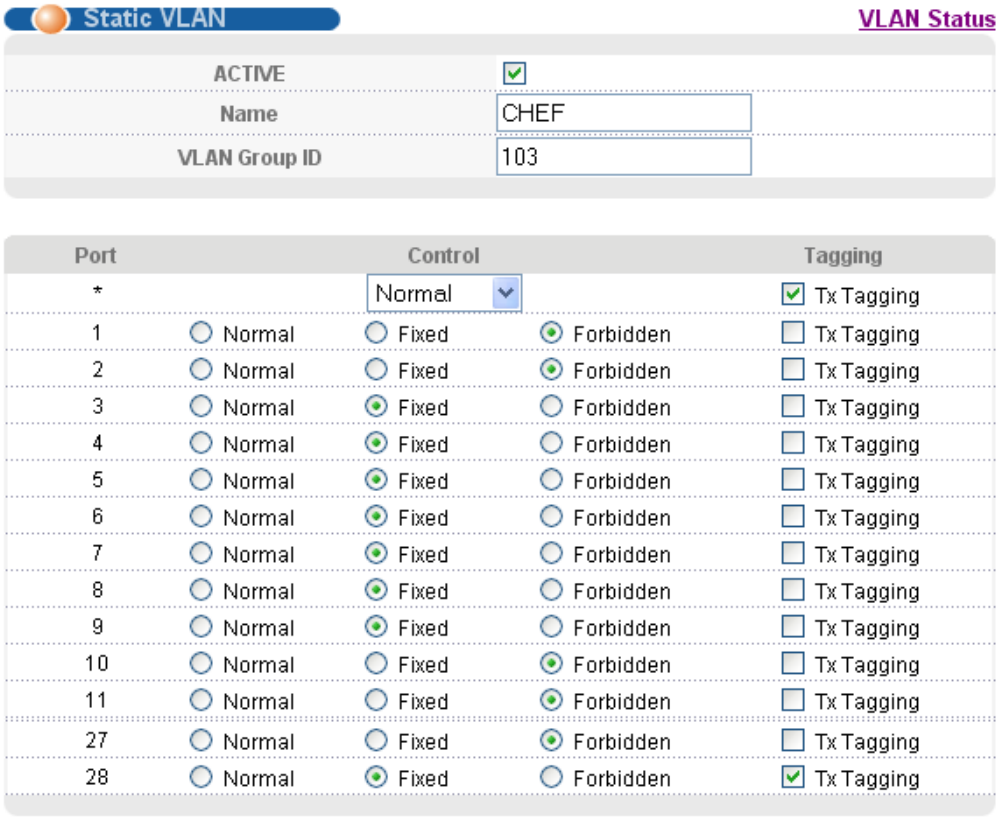
Die Eigenschaften des *VLAN's 102 GL_FI* sehen folgendermassen aus:



Auf das VLAN 102 können alle angeschlossenen Clients und Server sehen ausser die zwei allgemeinen Arbeitsstationen.

5.2.5 VLAN 103 CHEF

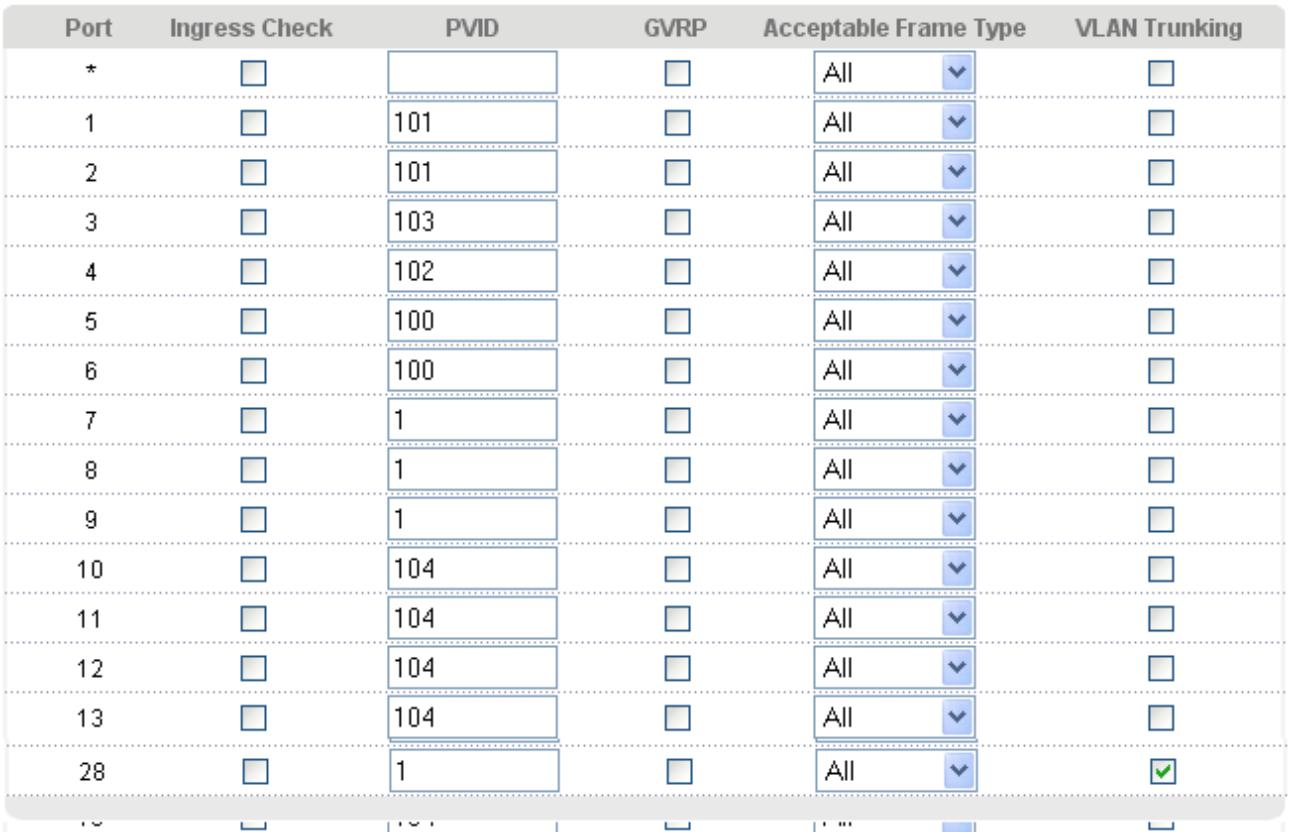
Die Eigenschaften des *VLAN's 103 CHEF* sehen folgendermassen aus:



Auf das VLAN CHEF können nur die Server und der Client des Chefs sehen.

Hinweis: In diesem Printscreen ist ein Konfigurationsfehler, der GL_FI Client an Port 4 dürfte das Chef VLAN auch nicht sehen.

5.2.6 3.4.2 Portkonfiguration auf den normalen Switches



Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
*	☐		☐	All	☐
1	☐	101	☐	All	☐
2	☐	101	☐	All	☐
3	☐	103	☐	All	☐
4	☐	102	☐	All	☐
5	☐	100	☐	All	☐
6	☐	100	☐	All	☐
7	☐	1	☐	All	☐
8	☐	1	☐	All	☐
9	☐	1	☐	All	☐
10	☐	104	☐	All	☐
11	☐	104	☐	All	☐
12	☐	104	☐	All	☐
13	☐	104	☐	All	☐
28	☐	1	☐	All	☑

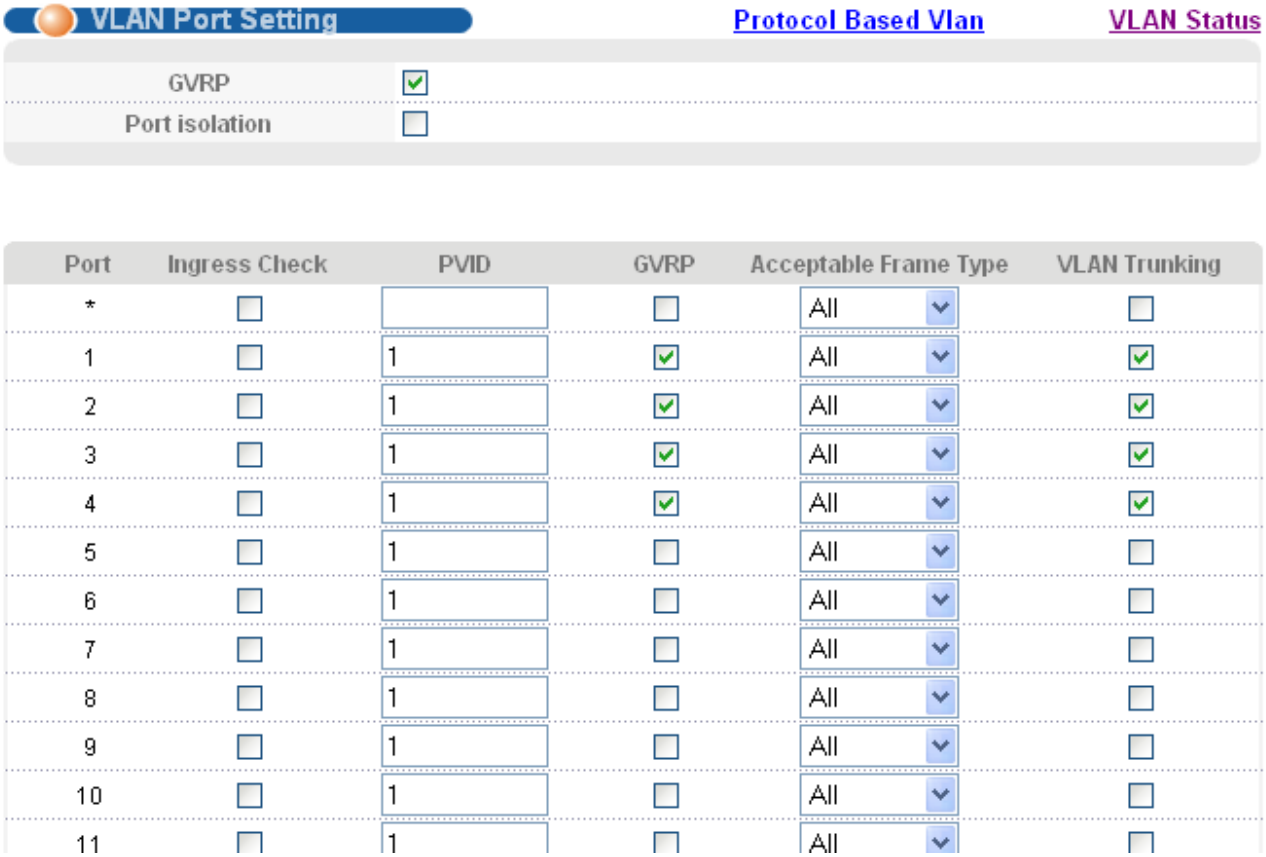
In der Übersicht oben sieht man, an welchen Ports welches VLAN definiert worden ist.

Auf Port 28 ist ein VLAN Trunking definiert worden, durch diesen Port sind die Switches mit dem Core-Switch verbunden.

Wenn dieser Arbeitsschritt fertig ist, hat man den Switch vollständig auf unsere VLAN's abgestimmt und ist fertig.

Port	Bezeichnung	VLAN
1-2	Allgemein	101
3	Chef	103
4	GL_FI	102
5-6	SRV	100

5.2.7 3.4.3 Portkonfiguration auf dem Core-Switch



Auf dem Core-Switch ist nichts anderes zu tun, als dass man bei den Ports an welchen die normalen Switches angehängt sind das VLAN Trunking einzuschalten die Häckchen bei GVRP sind nicht zu setzen.

Hinweis: Das Generic VLAN Registration Protocol (GVRP) ist ein Netzprotokoll zur Verwaltung von VLANs.

6 VoIP

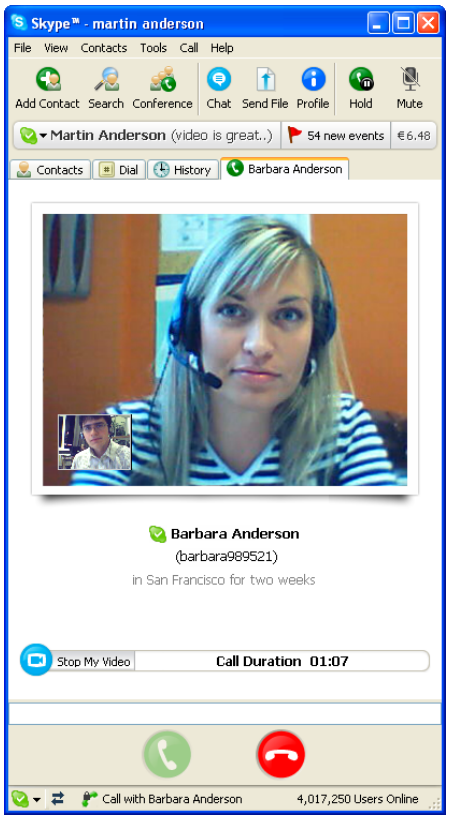
6.1 Theorie

6.1.1 Was ist VoIP

VoIP kann erst seit kurzem professionell genutzt werden. Die verschiedenen Lösungen haben Vor- und Nachteile.

Mit VoIP kann man über das Internet telefonieren.

6.1.2 Skype[5]



Skype ist eine unentgeltlich erhältliche, proprietäre VoIP-Software mit „Instant Messenger"-Funktion, Dateiübertragung und Videotelefonie.

Sie ermöglicht das kostenlose Telefonieren via Internet von Computer zu Computer, sowie das gebührenpflichtige Telefonieren ins Festnetz und zu Mobiltelefonen (SkypeOut). Der ebenfalls gebührenpflichtige Dienst SkypeIn ermöglicht es, auch Anrufe aus dem herkömmlichen Telefonnetz entgegenzunehmen. In der aktuellen Windows-Version sind Konferenzschaltungen mit bis zu 25 Gesprächsteilnehmern möglich.

Die Kritik an Skype ist, dass es nicht mit anderen VoIP-Angeboten kompatibel ist, welche mit offenen Standards wie SIP oder H.323 arbeiten.

Der Leistungsumfang reicht also (noch) nicht für den professionellen Bedarf.

Bei Skype kommt mir immer der Blogeintrag von Marc Ruef in den Sinn: http://www.computec.ch/comment.php?comment.news.215

6.1.3 Gesprächsübertragung[6]

Wie bei herkömmlicher Telefonie werden die akustischen Signale der Sprache zunächst analog mit einem Mikrofon (z. B. über den Telefonhörer) in elektrische Signale gewandelt. Diese analogen elektrischen Signale werden dann digitalisiert (kodiert). Optional können sie auch komprimiert werden (verbreitet sind dafür z. B. ITU-T G.723.1 oder G. 729 Annex A), um die zu übertragende Datenmenge zu reduzieren. Der Transport der so umgewandelten Daten erfolgt dann über ein öffentliches oder privates Telekommunikationsnetz. Bedingt durch das für den Transport verwendete Verfahren der Paketvermittlung werden die Daten dazu in viele kleine Pakete aufgeteilt.

6.1.4 Business Connect Professional (BCON)

BCON ist ein Servicepaket, das Swisscom bereitstellt. Man kann es rasch und flexibel Einbinden und geografisch getrennt benutzen. Man kann sogar die Firmenhandys integrieren.

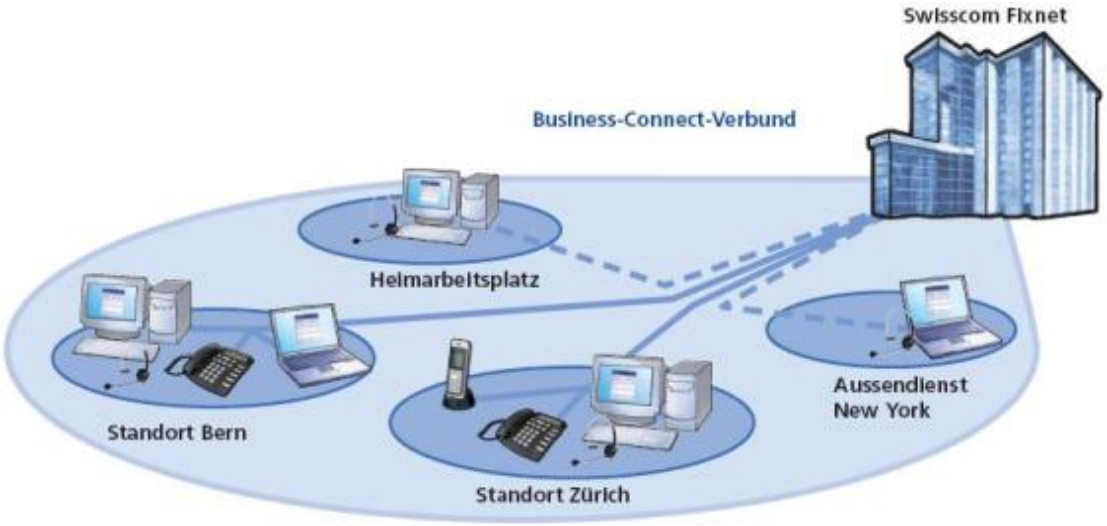
[5] Quelle: Wikipedia // http://de.wikipedia.org/wiki/Skype
[6] http://de.wikipedia.org/wiki/Voip#Gespr.C3.A4chs.C3.BCbertragung

Die Hauptzentrale liegt im Hause Swisscom und die Clien ts (Hard- und Softphones) melden sich an der Zentrale an.

Folgende Vorteile bringt BCON:

- Reduktion der Kosten
- Steigerung der Effizienz
- Flexiblität, Einfachheit
- Hohe Qualität

Der Hauptanschluss muss via Swisscomanschluss angebunden sein. Nur so kann QoS (Quality of Service) garantiert werden. Der Internetanschluss muss zuerst auf die Bedürfnisse der Kunden angepasst werden.



6.2 Praxis

6.2.1 VoIP auf dem iPhone[7]

Das iPhone ist ein neuartiges Smartphone mit einer Reihe von Funktionen, auch ein Skype-Client ist vorhanden. Dieser nennt sich Fring, indem man das iPhone hackt und sich die Source http://fring.com/iphone.xml hinzugefügt.

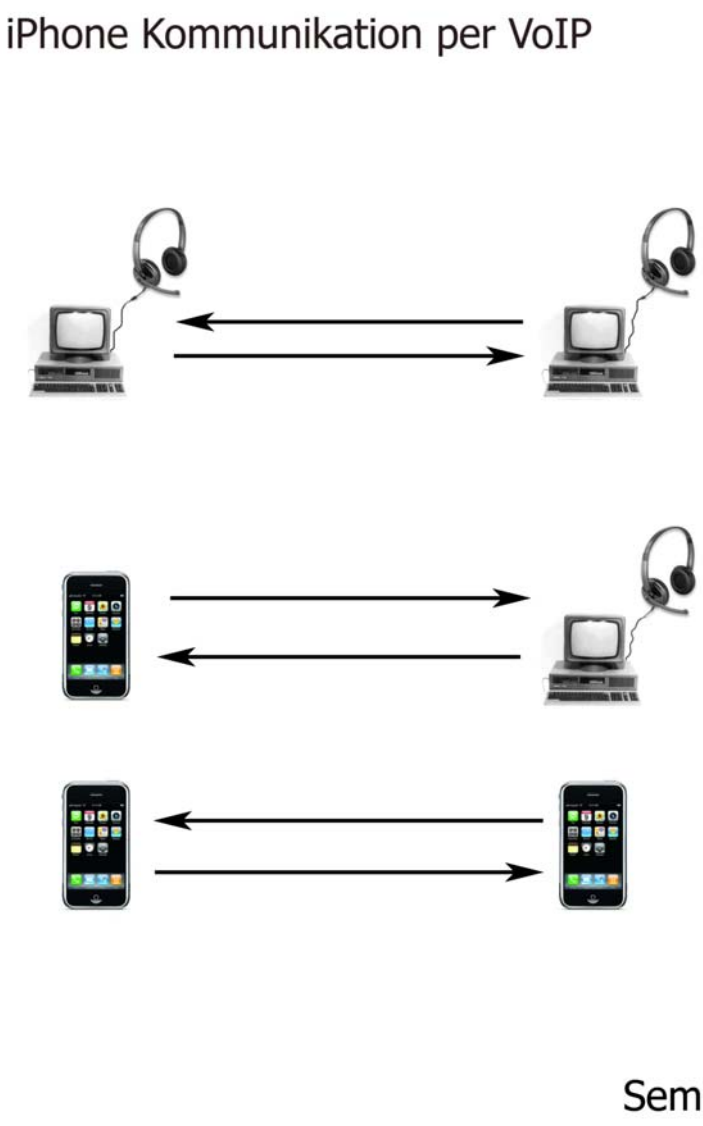
[7] Text von Semir Jahic

Hier das Logo von fring Logo. Es ist ein von freien Entwicklern gefördert es Programm. Die iPhone Community wächst immer mehr und die Technik revolutioniert eine Technik nach der anderen. Bei uns ist es konkret die VoIP Technologie.

Nachdem man sich einen fring Account erstellt hat, kann man sein Skypeprofil da aktivieren und nutzen. Desn fring nutzt auch andere Dienste wie ICQ. Die Kommunikation war äusserst erfolgreich, wir konnten über alle möglichen Wege kommunizieren.

Die Verbindung von PC-to-PC war sehr erfolgreich, die Headsets sind voll funktionsfähig und konnten per Plug'n'Play genutzt werden.

Erstaunlich war der Erfolg von der Kommunikation von iPhone zu iPhone. Denn dies war sehr einfach, nachdem fring installiert war. Da heute häufig ein funktionsfähiges WLAN zur Verfügung steht, kann man so kostenlos über iPhones auf andere iPhones oder in das Internet telefonieren. Sogar das Nutzen von Skype-Out wäre ein Möglichkeit, um sich Kostensparend ins Mobil-und Festnetz einzuwählen. So stellt die fring Alternative eine gute Möglichkeit zur kostenlosen oder günstigen Telefonie dar.



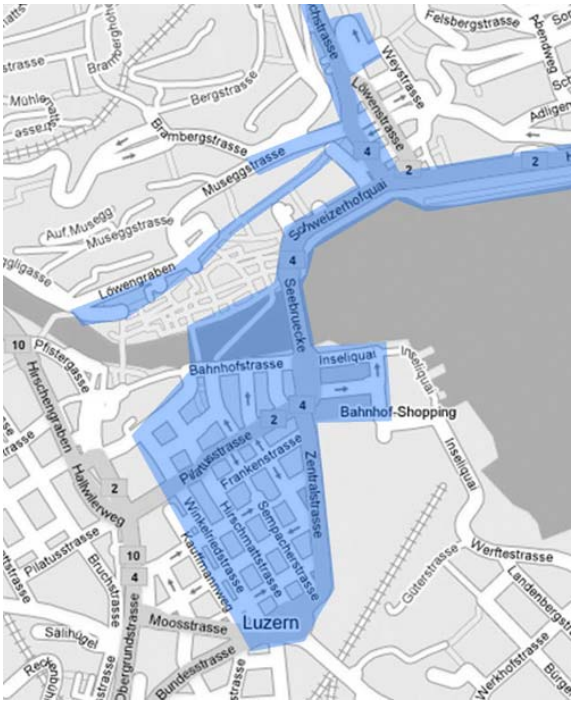
6.2.1.1 Die einzige Bedingung - WLAN

Die Grundlage für das Telefonieren mit Skype per iPhone ist das vorhanden sein eines Funknetzes. Heutzutage gibt es überall kostenlose Zugänge. Diese Zugänge sind legal verfügbar und einfach nutzbar. Beispiele sind:

- Starbucks Coffeeshops
- McDonalds
- viele Hotels
- verschiedene Städte: Luzern, Bern…

Ein gutes Beispiel für öffentlich unterstütztes WLAN ist das PulicWLAN Luzern, dies wird von den Behörden zur Verfügung gestellt.

„Der lokale Energie- und Wasserversorger ewl energie wasser luzern bietet gemeinsam mit Sponsoren ein öffentliches WLAN in der Stadt Luzern an. In Teilen der Alt- und Neustadt kann gratis und kabellos auf das Internet zugegriffen werden. Einfach ***Luzern.WLAN*** *anwählen und lossurfen. Luzern ist die erste Stadt in der Schweiz mit einem grossflächigen WLAN.“ (http://www.luzern.org/de/navpage-FactsLU-LuzernAZLU-211925.html)*



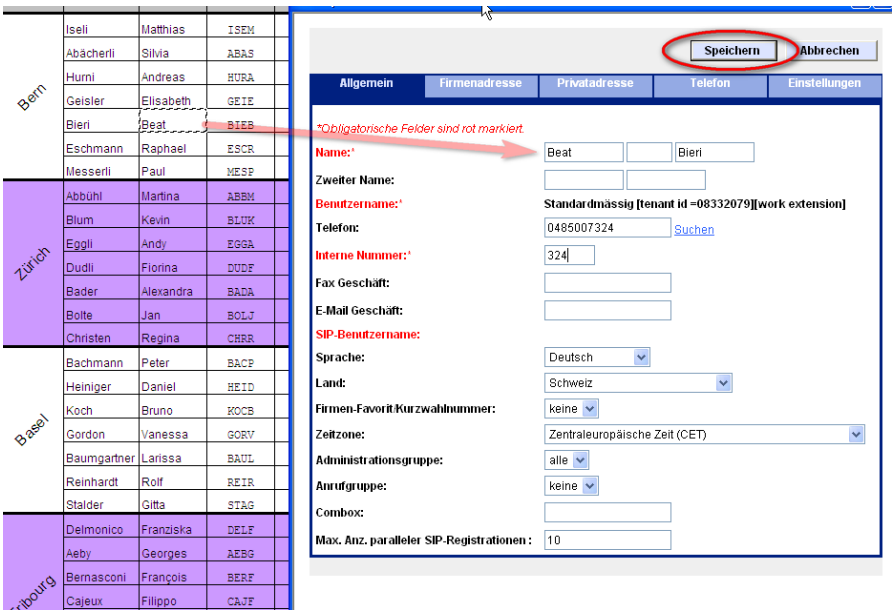
Die Abdeckung erstreckt sich über das blau markierte Gebiet. Genauso wie bei der Stadt Bern. Und so ist man immer und überall erreichbar, egal ob per Mail oder in der neusten Möglichkeit per Skype.

Durch Sponsoring von solchen WLANs ist es möglich, die Technologie weiter voranzutreiben. Denn Fortschritt ist etwas, wofür man offen sein muss und immer neues wagen

6.2.2 BCON in Betrieb nehmen

Wir loggen uns auf dieser Site der Swisscom ein: https://wastest.bluewin.ch/adminportal/Welcome.do. Der Username und das Passwort bekommen wir vom Provider (Swisscom).

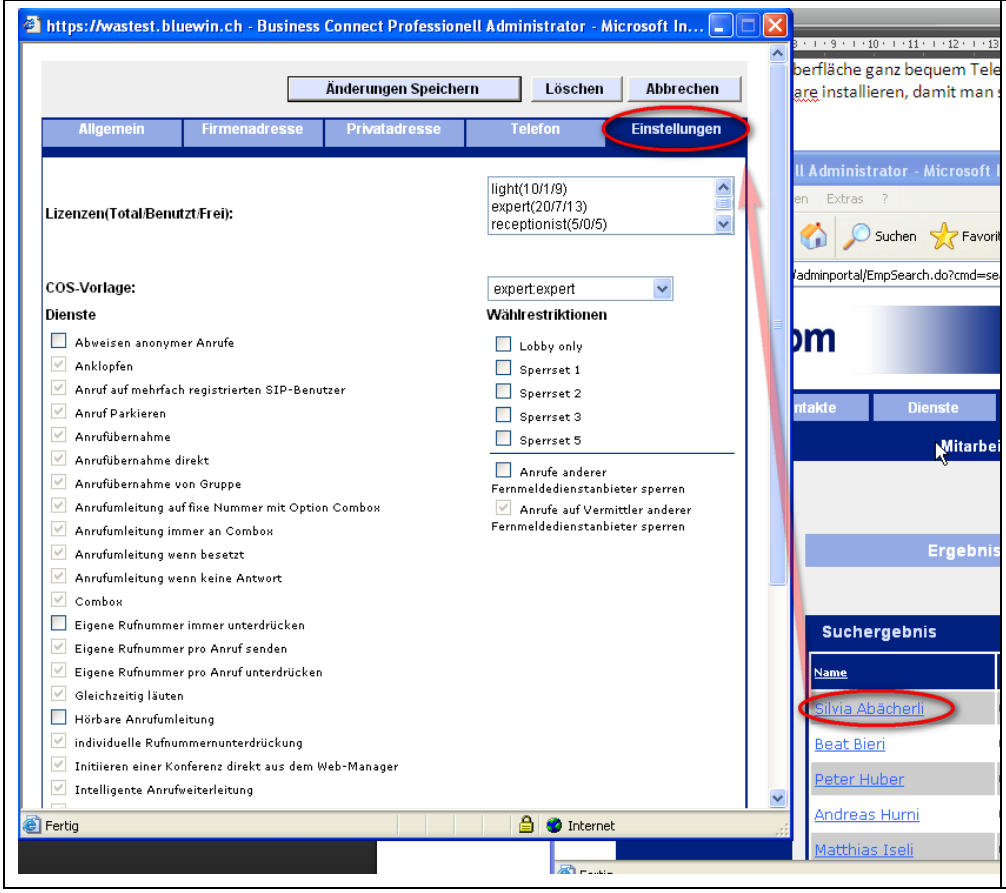
Wir klicken auf *Neu*.



Dann erfassen wir den User in der Maske.

Der Benutzername wird anhand der Tenant-ID erstellt.

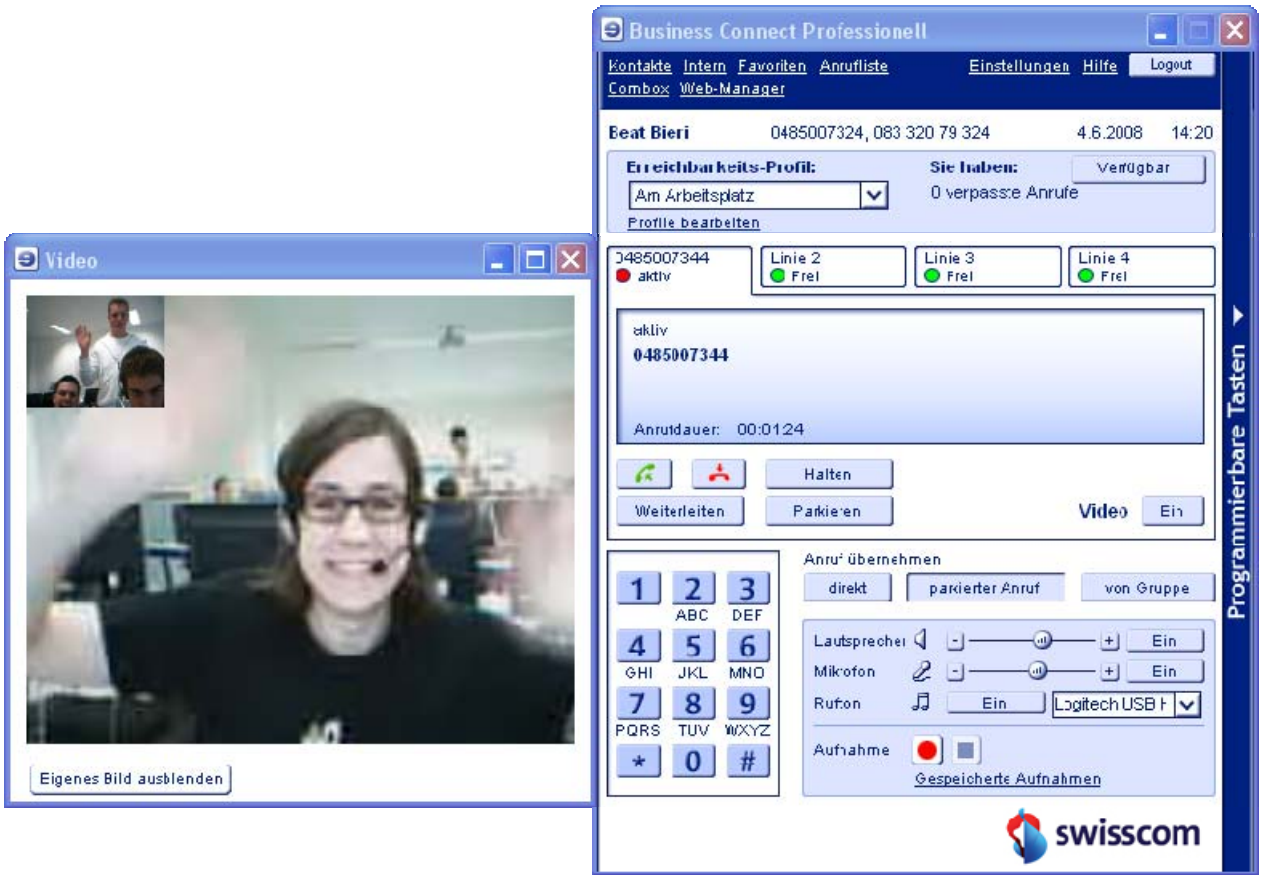
Wir können auch ein Kurzwahl für Innerhalb auswählen.



In dieser Konfigurationsoberfläche kann man sehr viel einstellen. Dabei ist auch auf die Lizenz zu achten!

6.2.2.1 Telefonieren über BCON

Nach dem Einloggen kann man über die Oberfläche ganz bequem Telefonieren. Auf dem Client muss man nur die BCON-Software installieren, damit man sich übers Internet mit Swisscon verbinden kann.



Auf dem Screenshot sieht man die Oberfläche zum Telefonieren. Diese erklärt sich mehrheitlich von alleine. Es hat sogar eine Funktion für die Webcam. Diese Funktion funktionierte bei uns aber nicht so gut. Wir hatten viele Probleme damit. Oft konnte die Webcam-Verbindung gar nicht aufbauen, oder es stockte.

7 Reflexion

Dieser Kurs war einfach genial! Ich lernte sehr viel dazu. Beim LAN erstellen schrieb ich ein grosses Script, das für alle Filialen alles erstellt. Das machte sehr viel Spass.

Mit dem Kursleiter konnten wir über Gott, Göttin und über die Welt reden. Freddi war sehr „human“.

Ich habe das erste Mal mit VLAN und VoIP gearbeitet. Endlich hatte ich die Möglichkeit ein WLAN legal zu „hacken“. Ich las schon sehr viel darüber und probierte schon sehr viel aus. Doch nun geht es super.

- Das Kursziel war nicht ganz bekannt, da wir keine Hanoks hatten.
- Der Kursleiter war sehr human / menschlich. Ich lernte auch viel Nicht-Informatisches dazu!! Buchtipps und Filmtipps!
- Wir hatten gute Unterlagen, Google und Wikipedia. Viele Schüler hatten schon ein grosses Vorwissen.
- Wenn wir Probleme hatten, fragten wir. Er sagte uns nicht direkt die Lösung sondern führte uns zum Ziel! Super!
- Ich habe alles gegeben beim Kurs. Ich machte es mir selber auch sehr spannend!
- Da dies der erste Kurs war, kann man an den Unterlagen noch Verbesserungen anbringen.
- Vieles werden wir in der Praxis wiederfinden.
- Die Kursdauer war viel zu kurz! Vieles konnten wir nicht ganz fertig machen und man könnte noch viel mehr probieren.
- VoIP, VLAN und WLAN hatten wir noch gar nie in der Schule.... Deshalb lernten wir viel.
- Das Image funktionierte am Anfang nicht richtig. Die sonstige Infrastruktur ist sehr gut! Wir bekamen neue Headsets und Webcams von Logical! ☺
- Wir wussten immer, was wir zu tun haben.

Der gebastelte Drache machte Spass! Irgendwie unheimlich!

8 Glossary

Replizieren	Kopieren von Daten von einem Ziel zu einem anderen.
Synchronisieren	Man bringt zwei Datenbestände auf denselben Stand.