

fli4I in der Praxis



## Wireless LAN

im  Schulungszentrum

Projektdokumentation



# Inhalt

1.	Konsequent vernetzt.....	3
1.1	Zielsetzung.....	3
1.2	räumliche Situation.....	4
1.3	Hardware-Voraussetzungen.....	4
1.4	Marktanalyse Hardware / Software.....	5
2.	Realisierung.....	6
2.1	Benötigte Hardware.....	6
2.2	Kostenrechnung.....	7
2.3	Benötigte Software.....	7
3.	Konfiguration.....	8
3.1	Konfigurationsschema Accesspoint 1 und 2.....	8
3.2	Konfiguration Accesspoint 1 und 2.....	9
3.3	Konfigurationsschema Gateway.....	10
3.4	Konfiguration Gateway.....	11
3.5	Konfigurationsschema des Gästezugangs.....	13
3.6	Konfiguration des Gästezugangs.....	14
3.7	Weitere Anmerkungen zur Konfiguration der Pakete.....	15
3.7.1	httpd.....	15
3.7.2	cpmvrmlg.....	15
4.	Inbetriebnahme.....	16
5.	Betrieb.....	17
	Anhang – Literatur und weiterführende Links.....	18
	Anhang – Nutzungserklärung.....	19

Die nachfolgenden Seiten setzen Kenntnisse in den Bereichen Netzwerke, TCP/IP und Routing voraus, die über das normale, im privaten Bereich anzutreffende Niveau hinausgehen. Unerlässlich ist auch die fli4I-Dokumentation. Trotzdem bemühe ich mich, so ausführlich wie möglich zu sein, so dass jeder interessierte Leser meine Schritte nachvollziehen und vielleicht für seine Zwecke nutzen kann. Mein besonderer Dank geht an die fli4I-Entwickler und das fli4I-Testteam, die an dieser Dokumentation mitgeholfen haben. Herausstellen möchte ich vor allem Claas Hilbrecht und Frank Saurbier. Ohne sie wäre weder diese Qualität noch Umfang möglich gewesen. (Stefan Krister, Systemadministrator bei Keimfarben, Januar 2009)

## 1. Konsequenz vernetzt

Die Keimfarben GmbH & Co. KG unterhält auf ihrem Fabrikgelände westlich von Augsburg ein Schulungszentrum. Dort werden neben Produktschulungen und Seminaren für Kunden auch interne Projekte besprochen und befreundeten Künstlern die Möglichkeit gegeben, ihre Werke dort auszustellen. Ein integrierter Showroom zeigt anschaulich die Vielfalt der mineralischen Farbgestaltung. Ein Mangel



war bis vor kurzem die Netzwerkanbindung für dort stattfindende Besprechungen und Seminare. In den 3 Besprechungsräumen gibt es lediglich je 2 Netzwerkanlüsse. Eine Trennung zwischen internem Netz und externem Internet hätte ziemlichen Aufwand bedeutet. Die Alternative war ein WLAN.

### 1.1 Zielsetzung

In den Schulungsräumen soll es möglich sein, dass die Mitarbeiter per WLAN Zugang zu den Netzwerkressourcen von Keimfarben bekommen. Dieser Zugang soll verschlüsselt (WPA2/PSK) [1] sein. Der Schlüssel soll periodisch (1x pro Quartal) wechseln.

Neben dem verschlüsselten Zugang zum Netzwerk soll ein weiterer unverschlüsselter Zugang zum Internet angeboten werden. Dieser soll den Dozenten und Besuchern zur Verfügung stehen. Zur Nutzung dieses Zugangs ist eine Freischaltung des Clients notwendig. Diese Freischaltung soll das Personal im Schulungszentrum übernehmen, nachdem der Nutzer eine Nutzungserklärung unterschrieben hat. Diese Nutzungserklärung enthält alle relevanten Daten, um einem Missbrauch vorzubeugen. Nach dem Einbuchen sollen keinerlei Ressourcen des Keimfarben-Netzwerks sichtbar sein. Es ist ausschließlich ein Zugang zum Internet möglich. Nach Ablauf der Freischaltung ist eine erneute Freischaltung des Clients nötig.

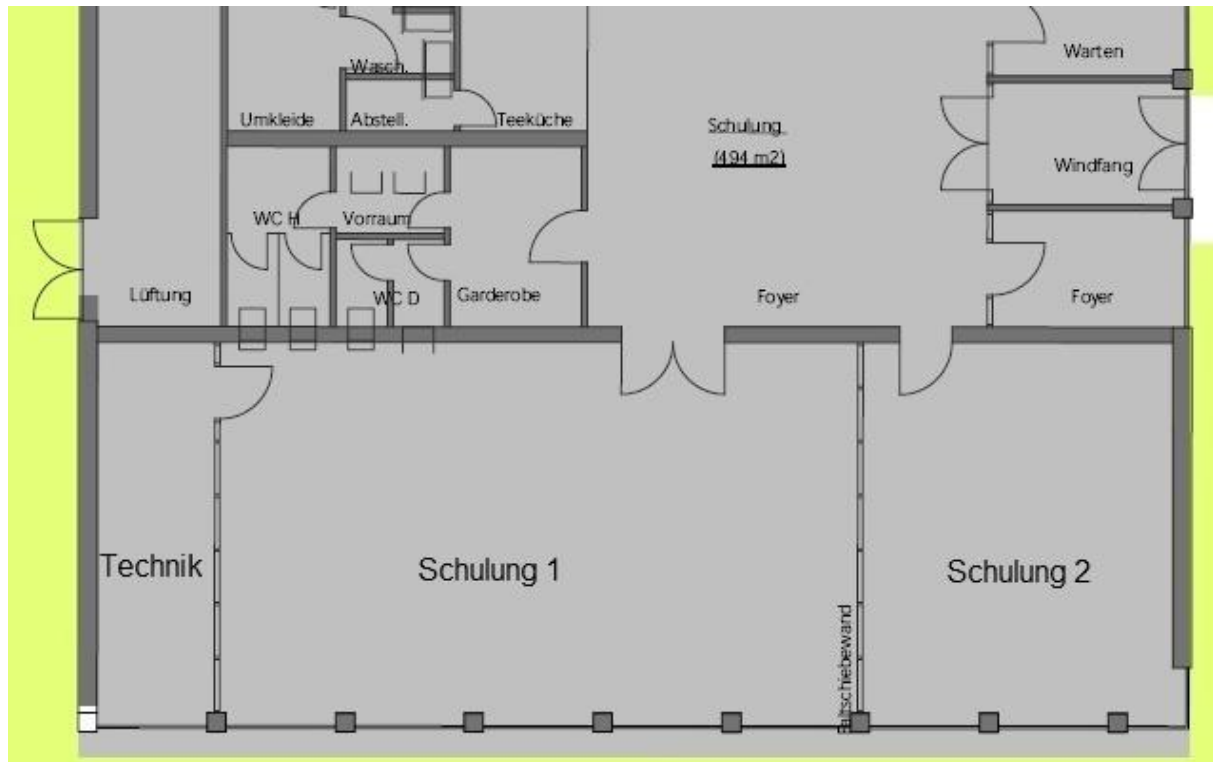
Es sollen 2 Accesspoints und ein geeigneter Gateway installiert werden. Die Funkbereiche der Accesspoints sollen sich überlappen, so dass eine möglichst gute Empfangssituation entsteht. Darüber hinaus soll der Wechsel von der einen Funkzelle in die andere für den Anwender transparent sein. Im Idealfall soll er nicht merken, wenn er die Zelle wechselt.

---

[1] WPA2/PSK = Wi-Fi Protected Access 2 mit Pre-Shared Key

Durch die Verwendung gleichartiger Hardware soll ein Ausfall eines Gerätes kompensiert werden können. Eine künftige Ergänzung auf weitere Accesspoints soll möglich sein.

## 1.2 räumliche Situation



Fabrikgelände / Schulungszentrum

„Schulung 1“ und „Schulung 2“ sind die am häufigsten belegten Räume. Dort sollen die Accesspoints platziert werden.

Hinter der Leinwand von „Schulung 1“ ist der Technikraum mit Switch. Der Accesspoint 1 soll auf dem Netzwerkschrank, der Accesspoint 2 in der Nähe der Netzwerkdose in der nord-östlichen Ecke von „Schulung 2“ installiert werden.

## 1.3 Hardware-Voraussetzungen

- 2x Accesspoint mit je 2 SSIDs [2], VLAN-fähig [3]
- 1x Gateway / Firewall, VLAN-fähig
- Beschaffungsmöglichkeiten über mehrere Jahre
- VLAN auf den beteiligten Switchen

---

[2] SSID = Service Set Identifier, die Kennung eines Funknetzwerkes

[3] VLAN = Virtual Local Area Network ist ein virtuelles lokales Netz innerhalb eines gesamten Netzes. In einem geschichteten Netzwerk ist es notwendig, dass die beteiligten Switches das verwendete VLAN-Protokoll unterstützen und dass die benutzten Switchports richtig konfiguriert werden. Hier wird VLAN nach IEEE 802.1Q eingesetzt.

## 1.4 Marktanalyse Hardware / Software

Keimfarben liegt ein Angebot von einem Cisco-Dienstleister vor, der für die Lösung einen 5-stelligen Betrag veranschlagt. Dies hat den Autor dazu veranlasst, nach Alternativen zu suchen. Trotz meiner Verbundenheit zum Projekt fli4l wollte ich es mir nicht nehmen lassen, eine nachvollziehbare objektive Entscheidung zu fällen.

Aufgrund der unklaren Beschaffungssituation von Billig- und Noname-Accesspoints wurde auf eine eingehende Untersuchung der Möglichkeiten der Firmware auf diesen Geräten verzichtet. Näher betrachtet wurden Geräte des Herstellers AVM und D-Link. Keines der geprüften Geräte konnte mit der unflexiblen Firmware alle Anforderungen erfüllen.

Ein wenig mehr Beweglichkeit bekommt man, wenn man diese Geräte mit einer Linux-Firmware ausstattet, die von der Community veröffentlicht wird. Die Hersteller verwenden bereits z.T. Linux als Firmware. So lassen sich sowohl die Fritz!Box als auch Geräte von Linksys (und deren baugleiche Schwestern) mit alternativen Images flashen um mehr Funktionen zu bekommen.

Leider kranken diese Community-Lösungen an mangelnder Dokumentation. Als krasses Beispiel muss hier DD-WRT dienen. Das an sich leistungsfähige Paket hat sehr viele nicht dokumentierte Einstellmöglichkeiten. Diese mühsam aus den Foren herauszusuchen ist eine Strafarbeit, die der Autor nicht tun wollte.

Es scheint aber, dass Linux prinzipiell die anzustrebende Lösung ist. Eine vollwertige Linux-Distribution übertrifft den eigentlichen Zweck allerdings völlig. Deshalb gibt es speziellere Distributionen – auch für Routing-Zwecke.

Näher betrachtet wurden IPCop, M0n0wall und fli4l. Alle drei setzen eine „Intel-kompatible“ Hardware voraus, sind aber auch mit moderat ausgestatteten Rechnern flott unterwegs. Ausgeschlossen sind ebenfalls aufgrund der mangelnden Flexibilität die ersten beiden Kandidaten. Das liegt bei den beiden Projekten übrigens nicht an der verwendeten Software, sondern an der eher unflexiblen Web GUI die für die Einrichtung benötigt wird. Man müsste bei diesen Projekten die Software selbst erweitern und anpassen und könnte so nicht einfach neue Versionen installieren.

Besonders erwähnen möchte ich den Umfang der fli4l Dokumentation. Auf ca. 400 Seiten werden alle Parameter beschrieben und Szenarien vorgestellt. Howtos auf der Webseite runden die Informationen weiter ab.

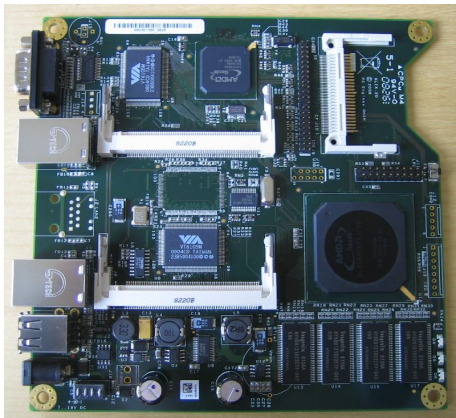
Die jetzt noch in Frage kommende Hardwarepalette beginnt bei normalen Büro-PCs, geht über speziellere Racklösungen bis hin zu Geräten, denen eine Vielzahl der sonst üblichen PC-Komponenten entfernt wurden. Letztere sind dadurch auch noch mit wenigen Watt Leistungsaufnahme wahre Energiesparer. Meine Wahl fiel schließlich auf den Hersteller PC Engines aus der Schweiz. Aus eigener Erfahrung kenne ich die Boards als absolut zuverlässig. Erfahrungsberichte Gleichgesinnter unterstreichen die von mir gemachten Beobachtungen.

## 2. Realisierung

Zur Realisierung konnte mit Herrn Hilbrecht von der Linum Software GmbH aus Einbeck ein kompetenter Partner gewonnen werden. Das Projekt wurde innerhalb weniger Wochen geplant und ist am 18.12.2008 produktiv gegangen.

### 2.1 Benötigte Hardware

- 3x alix2d2 [4] (500 MHz AMD Geode LX800 CPU, 256 MB SDRAM, 1 CompactFlash-Slot, 2 FastEthernet-Anschlüsse, 2 MiniPCI-Slots, 1 serielle Konsole)



- 2x Wistron CM 9 (miniPCI-wireless-Modul 54 MBit/s, IEEE 802.11a,b,g, Chipsatz: Atheros AR5213A, MiniPCI Type III, Antennenanschluß: 2x U.FL)



- 2x Pigtail U.FL -> RP-SMA-Buchse 2,4 GHz (Pigtail für die Verbindung zwischen einem RP-SMA-Stecker und einer WLAN-miniPCI-Karte mit U.F.L-Anschluß, Länge: ca. 15 cm)
- 2x WLAN-Antenne RP-SMA-Stecker 2,4GHz (Frequenz: 2,4 GHz, Gewinn: 5dBi, Ausrichtung: Omnidirektional, knickbar)
- 3x Gehäuse



---

[4] ALIX = Name einer Produktserie des Schweizer Herstellers PC Engines. Intel kompatibles Motherboard als Basis für stromsparende Router/Accesspoints:  
<http://www.pcengines.ch/alix.htm>

- 1x CompactFlash-Karte 2GB
- 2x CompactFlash-Karte 512MB
- 3x Steckernetzteil 12V 1200mA

## 2.2 Kostenrechnung

• 3x alix2d2	115,00	345,00
• 2x Wistron CM 9	37,00	74,00
• 2x Pigtail	4,00	8,00
• 2x WLAN-Antenne	4,70	9,40
• 3x Gehäuse	12,00	36,00
• 3x CompactFlash-Karte	10,00	30,00
• <u>3x Steckernetzteil</u>	<u>7,50</u>	<u>22,50</u>
Summe		<u>554,90</u>

Preise in € Stand Januar 2009, incl. MwSt vom PC Engines Distributor Tronico:  
<http://shop.tronico.net>

## 2.3 Benötigte Software

Die speziell an Routingaufgaben anpassbare Linux Distribution „fli4l“ [5] ermöglicht es auf einfache Weise, die ansonsten ziemlich komplex zu konfigurierenden Netzwerkeinstellungen vorzunehmen.

Die möglichen Funktionen eines Routers werden bei fli4l in einzelne Pakete unterteilt. Für die oben beschriebenen Aufgaben kommen die Pakete `advanced_networking`, `base`, `c3surf`, `cpmvrmlg`, `httpd`, `kernel_26` und `wlan` zum Einsatz.

Wegen weiterer Aufgaben, die nicht Teil dieser Dokumentation sind, sind noch die Pakete `chrony`, `easycron`, `hd`, `rrdtool`, `sshd`, `squid`, `tools` und `wol` installiert.

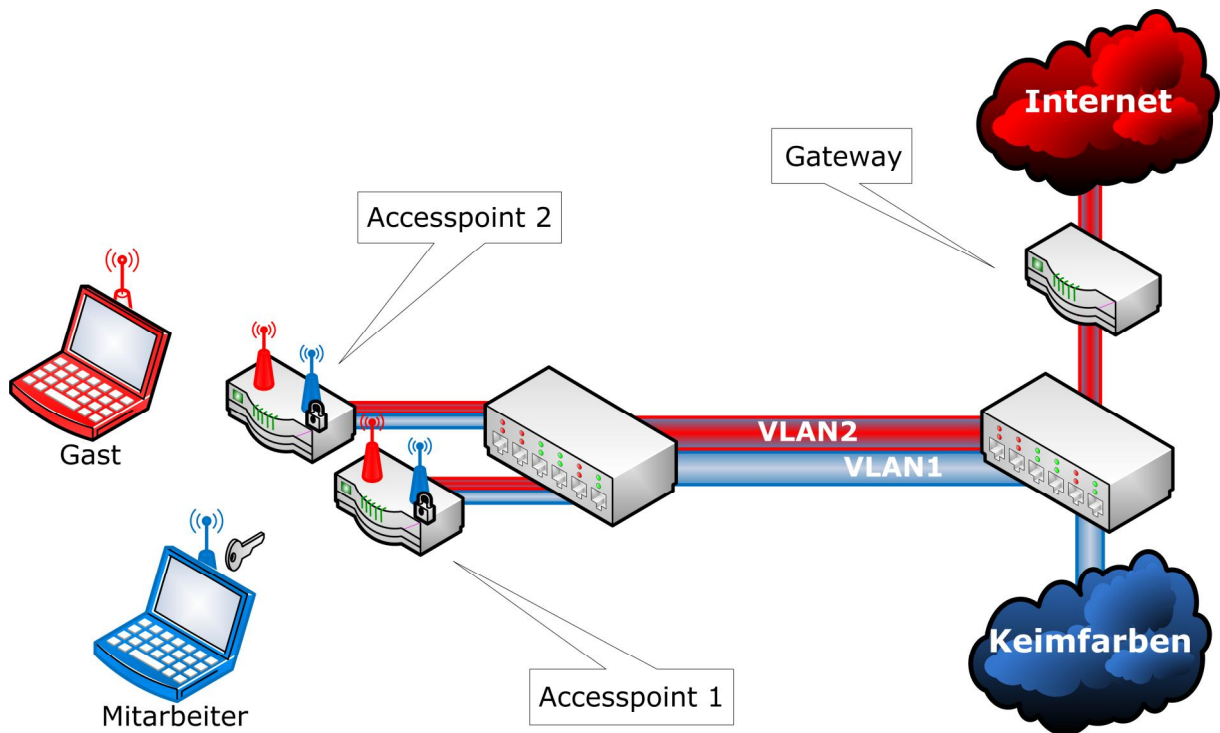
---

[5] <http://www.fli4l.de> Zur Inbetriebnahme wurde die damals aktuelle Entwicklerversion 3.3.0 verwendet.

### 3. Konfiguration

Die Konfigurationsdateien enthalten eine Vielzahl von konfigurierbaren Variablen. Im folgenden werden aber nur diejenigen hier dokumentiert, welche für die genannte Aufgabenstellung relevant sind.

Auch ist fli4l in der Lage noch ganz andere Aufgaben zu erfüllen. Diese werden zum Teil bei Keimfarben auch genutzt, spielen aber ebenfalls hier keine Rolle und werden nicht weiter erwähnt.



In der schematischen Darstellung soll die Trennung der beiden Verbindungsmöglichkeiten herausgestellt werden. Ein „blauer“ Client kann nur innerhalb des blauen Netzwerkbereichs kommunizieren. Ein „roter“ Client dagegen ist auf den roten Teil des Netzes beschränkt. Im folgenden verwende ich immer dann wenn es mir sinnvoll erscheint, blaue oder rote Schriftfarbe, um die Trennung zu verdeutlichen.

#### 3.1 Konfigurationsschema Accesspoint 1 und 2

Aus den beiden physischen Geräten eth0 und wlan0 werden je zwei logische Geräte. Je zwei der vier logischen Geräte werden in einer Netzwerkbrücke zusammengefasst:

Physisch	eth0		wlan0	
Logisch	eth0.1	eth0.2	wlan0	wlan1
SSID			keimfarben	keimfarben-gaeste
Brücke br0 „br-sicher“	X		X	
Brücke br1 „br-gaeste“		X		X

Die Brücke br-sicher ist Teil des vorhandenen Netzes 10.1.0.0/16 in dem alle Netzwerkressourcen erreichbar sind. Die Clients erhalten nach erfolgter Authentifizierung am Accesspoint gültige

Netzwerkinformationen per DHCP von einem der beiden W2k3 DHCP-Server. Dabei ist ein Vollzugriff auf alle Netzwerkressourcen gewährleistet.

Die Accesspoints haben keinen Default-Gateway eingetragen, weil sie selbst keine Daten in andere Netze übermitteln! Für die Gäste sind die Accesspoints lediglich WLAN/LAN Bridges.

Die Brücke **br-gaeste** spannt ein eigenes Netz **192.168.99.0/24** auf. Dieses Netz reicht mittels VLAN über die beteiligten Switches bis zum Gateway. Das Einbuchen in dieses Netz gelingt ohne Netzwerkschlüssel oder Passwörter. Die per DHCP zugewiesenen Netzwerkinformationen stammen vom Gateway. Die Netzwerkpakete an eth0 werden um die VLAN-ID ergänzt. Ein „Erschnüffeln“ der Netzwerkressourcen ist damit unmöglich. Die einzige mögliche Kommunikation ist mit dem Webserver des Gateway selbst – um dort den Zugangscode einzugeben.

Im Moment steht für fli4l leider kein SSL fähiger Webserver zu Verfügung, daher ist es möglich, die Anmeldedaten eines Clients abzuhören. Die Unterstützung von SSL für den fli4l Webserver ist geplant und Sie sollten prüfen ob SSL mittlerweile unterstützt wird und die Anmeldeseiten entsprechend auf der SSL Seite ablegen.

Die in Deutschland erlaubten Funkkanäle, die sich nicht in ihren Frequenzen überschneiden sind die Kanäle 1, 6 und 11. Deshalb werden die beiden Accesspoints auf diese eingestellt. Eine Überprüfung der Umgebung hat keine anderen Funknetze angezeigt.

### 3.2 Konfiguration Accesspoint 1 und 2

Die Konfiguration der beiden Accesspoints ist bis auf die IP-Adresse und den Hostnamen identisch.

base.txt

```
HOSTNAME='wlan-schuze-1'
NET_DRV_N='2'
NET_DRV_1='via-rhine'
NET_DRV_2='ath_pci'

IP_NET_N='2'

IP_NET_1='10.1.1.5/16'
IP_NET_1_DEV='br0'

IP_NET_2='192.168.99.2/24'
IP_NET_2_DEV='br1'

HOSTNAME='wlan-schuze-2'
NET_DRV_N='2'
NET_DRV_1='via-rhine'
NET_DRV_2='ath_pci'

IP_NET_N='2'

IP_NET_1='10.1.1.6/16'
IP_NET_1_DEV='br0'

IP_NET_2='192.168.99.3/24'
IP_NET_2_DEV='br1'

IP_ROUTE_N='0'
```

## advanced\_networking.txt

```
OPT_BRIDGE_DEV='yes'
BRIDGE_DEV_N='2'

BRIDGE_DEV_1_NAME='br-sicher'
BRIDGE_DEV_1_DEVNAME='br0'
BRIDGE_DEV_1_DEV_N='2'
BRIDGE_DEV_1_DEV_1_DEV='eth0.1'
BRIDGE_DEV_1_DEV_2_DEV='wlan0'

BRIDGE_DEV_2_NAME='br-gaeste'
BRIDGE_DEV_2_DEVNAME='br1'
BRIDGE_DEV_2_DEV_N='2'
BRIDGE_DEV_2_DEV_1_DEV='eth0.2'
BRIDGE_DEV_2_DEV_2_DEV='wlan1'

OPT_VLAN_DEV='yes'
VLAN_DEV_N='2'

VLAN_DEV_1_DEV='eth0'
VLAN_DEV_1_VID='1'

VLAN_DEV_2_DEV='eth0'
VLAN_DEV_2_VID='2'
```

## wlan.txt

```
WLAN_N='2'

WLAN_1_MAC='00:0b:6b:87:xx:yy'
WLAN_1_ESSID='keimfarben'
WLAN_1_MODE='master'
WLAN_1_CHANNEL='1'

WLAN_1_WPA_KEY_MGMT='WPA-PSK'
WLAN_1_WPA_PSK='WLAN Schluessel'
WLAN_1_WPA_TYPE='1'
WLAN_1_WPA_ENCRYPTION='TKIP'

WLAN_2_MAC='00:0b:6b:87:uu:vv'
WLAN_2_ESSID='keimfarben-gaeste'
WLAN_2_MODE='master'
WLAN_2_CHANNEL='1'

WLAN_2_WPA_KEY_MGMT=''
WLAN_2_WPA_PSK=''
WLAN_2_WPA_TYPE='1'
WLAN_2_WPA_ENCRYPTION='TKIP'
```

### 3.3 Konfigurationsschema Gateway

Auf den beiden physischen Ethernet Anschlüssen eth0 und eth1 werden drei logische Netzwerke betrieben. Die beiden internen Netze 10.1.0.0/16 und 192.168.99.0/24 werden auf eth0 zusammengeführt, auf eth1 ist das Internet terminiert. Der Internet-Provider stellt am Ausgang seines SDSL-Routers ein /29er Netz zur Verfügung.

Wird fli4l als Ethernet-Router betrieben, muss man eine Default-Route (IP\_ROUTE\_1) ins Internet definieren.

Bei den Firewall-Regeln muss man zunächst die Kommunikation zur Anmeldeseite erlauben (Regel PF\_INPUT\_6). Die Regeln 12, 13 und 14 sorgen dafür, dass auch Clients mit statischer IP-Adresse nicht kommunizieren können. Namensauflösungen über den DNS des Providers sind erlaubt (Regel 15 und 16). Regel 17 verweist in die Chain c3surf\_control des Paketfilters. Entweder werden die Pakete dort verworfen, weil der Client noch nicht angemeldet ist, oder gelangen wieder zurück und werden wegen der Regel 18 ins Internet weitergeleitet. Regel 4 in PF\_POSTROUTING sorgt schließlich für das Masquerading der abgehenden Pakete.

Die Clients im Gäste-WLAN bekommen vom Gateway per DHCP Netzwerkinformationen. Zur Namensauflösung wird der DNS des Internetproviders verwendet, damit keine internen Informationen über Hostnamen vom internen Netz durchsickern können und auch dafür keine Ausnahmen im Paketfilter gemacht werden müssen.

Die von den Accesspoints getaggtten Netzwerkpakete werden über die Switches zum Gateway gebracht. Deswegen muss der Gateway ebenfalls die VLAN-Konfiguration erhalten. Bitte beachten Sie bei der VLAN Konfiguration dass auch die VID1 getaggt zu Verfügung gestellt wird. Dafür gibt es zwei Gründe: Zum einem ist es so nicht möglich an den entsprechenden Ports durch einfaches "abziehen" der Accesspoints doch wieder in das interne Netz zu kommen. Dafür müsste jemand mindestens seinen Notebook entsprechend konfigurieren, dass er mit den getaggtten Ethernetframes klarkommt. Eine deutlich höhere Hürde als nur den AP abziehen zu müssen. Zum zweiten gab es noch ungeklärte Probleme mit dem Linuxkernel, der teilweise eine falsche IP für das Masquerade benutzt hat, wenn VID1 nicht getaggt war.

### 3.4 Konfiguration Gateway

base.txt

```
HOSTNAME='gateway'
NET_DRV_N='1'
NET_DRV_1='via-rhine'

IP_NET_N='3'

IP_NET_1='10.1.1.40/16'
IP_NET_1_DEV='eth0.1'

IP_NET_2='vv.ww.xx.yy/29'
IP_NET_2_DEV='eth1'

IP_NET_3='192.168.99.1/24'
IP_NET_3_DEV='eth0.2'

IP_ROUTE_N='1'
IP_ROUTE_1='0.0.0.0/0 vv.ww.xx.yy'

PF_INPUT_6='prot:tcp IP_NET_3 IP_NET_4_IPADDR:4444 ACCEPT'
PF_INPUT_6_COMMENT='SchuZe c3surf REDIRECT erlauben'

PF_FORWARD_12='if:IP_NET_3_DEV:any 0.0.0.0/0 10.0.0.0/8 REJECT'
PF_FORWARD_12_COMMENT='SchuZe in 10.0.0.0/8 -> REJECT'
```

```
PF_FORWARD_13='if:IP_NET_3_DEV:any 0.0.0.0/0 172.16.0.0/12 REJECT'  
PF_FORWARD_13_COMMENT='SchuZe in 172.16.0.0/12 -> REJECT'  
PF_FORWARD_14='if:IP_NET_3_DEV:any 0.0.0.0/0 192.168.0.0/16 REJECT'  
PF_FORWARD_14_COMMENT='SchuZe in 192.168.0.0/16 -> REJECT'  
  
PF_FORWARD_15='if:IP_NET_3_DEV:IP_NET_2_DEV tmpl:dns IP_NET_4  
ip1.dns.ser.ver ACCEPT'  
PF_FORWARD_15_COMMENT='DNS fuer SchuZe immer erlauben'  
  
PF_FORWARD_16='if:IP_NET_3_DEV:IP_NET_2_DEV tmpl:dns IP_NET_4  
ip2.dns.ser.ver ACCEPT'  
PF_FORWARD_16_COMMENT='DNS fuer SchuZe immer erlauben'  
  
PF_FORWARD_17='if:IP_NET_3_DEV:any c3surf_control'  
PF_FORWARD_17_COMMENT='Anfragen vom SchuZe via c3surf_control'  
  
PF_FORWARD_18='if:IP_NET_3_DEV:IP_NET_2_DEV IP_NET_4 0.0.0.0/0 ACCEPT'  
PF_FORWARD_18_COMMENT='SchuZze ins Internet -> ACCEPT'  
  
PF_POSTROUTING_4='if:any:IP_NET_4_DEV MASQUERADE'
```

## dns\_dhcp.txt

```
OPT_DNS='yes'  
DNS_LISTENIP_N='1'  
DNS_LISTENIP_1='IP_NET_3_IPADDR'  
  
OPT_DHCP='yes'  
  
DHCP_TYPE='dnsmasq'  
  
DHCP_VERBOSE='no'  
DHCP_LS_TIME_DYN='3600'  
DHCP_MAX_LS_TIME_DYN='7200'  
DHCP_LS_TIME_FIX='86400'  
DHCP_MAX_LS_TIME_FIX='604800'  
DHCP_LEASES_DIR='/boot'  
DHCP_WINSERVER_1=''  
DHCP_WINSERVER_2=''  
  
DHCP_RANGE_N='1'  
DHCP_RANGE_1_NET='IP_NET_3'  
DHCP_RANGE_1_START='192.168.99.10'  
DHCP_RANGE_1_END='192.168.99.200'  
DHCP_RANGE_1_DNS_SERVER1='ip1.dns.ser.ver'  
DHCP_RANGE_1_DNS_SERVER2='ip2.dns.ser.ver'
```

## advanced\_networking.txt

```
OPT_VLAN_DEV='yes'  
VLAN_DEV_N='2'  
  
VLAN_DEV_1_DEV='eth0'  
VLAN_DEV_1_VID='1'  
  
VLAN_DEV_2_DEV='eth0'  
VLAN_DEV_2_VID='2'
```

### 3.5 Konfigurationsschema des Gästezugangs

Die Paketfilter des Gateways werden durch c3surf so beeinflusst, dass der Gast beim Aufrufen einer beliebigen Internetseite zuerst auf der Login-Seite landet. Erst nach einem gültigen Login wird diese Umleitung aufgehoben und es gelten für den Gast die im Paketfilter konfigurierten Regeln. Zum Beispiel wird der Zugriff auf das Internet erlaubt. Nach Ablauf der Gültigkeit wird wieder die Umleitung auf die Anmeldeseite eingestellt und die normalen Regeln des Routers gelten für den Gast nicht mehr, was einer Sperre gleichkommt.

Um das zu erreichen, bindet c3surf in das Regelwerk des Gateways eigene Chains ein. Verweise auf diese Chains stehen in den Chains "INPUT", "FORWARD" und "PREROUTING". Über die zusätzlichen Regeln in der Chain "INPUT" wird gesteuert, auf welche Ports des Gateways ein Gastsystem Zugriff hat. Dabei können die Ports komplett gesperrt werden oder nach einer gültigen Anmeldung auch freigegeben werden. Schließlich sollen die Ports, die auch der Administration des Gateways dienen nicht für Gäste offen sein. Eine zentrale Rolle spielt die zusätzliche Chain "c3surf\_control" in der Chain "FORWARD". Denn sie steuert den Zugriff auf andere Netze. Dabei ist die Logik so ausgelegt, dass ohne gültige Anmeldung ein weiteres Verarbeiten des normalen Regelwerkes des Gateways gesperrt ist. Erst nach einer erfolgreichen Anmeldung gelten dann für den Gast auch alle Regeln der Chain "FORWARD".

Entsprechend kann der Gast dann z. B. das Internet nutzen, wie es im Regelwerk erlaubt ist. Die Änderung in der Chain "PREROUTING" beschränkt sich darauf, einen Gast zuerst auf die Anmeldeseite umzuleiten, falls er nicht angemeldet ist. Es ist vergleichbar mit einer "transparent Proxy" Konfiguration. Nur dass nicht auf einen Proxy, sondern auf den mini-httpd zur Anmeldung verwiesen wird.

Um den Anforderungen bei Keimfaben gerecht zu werden, wurden ein paar der c3surf Dateien und Scripte verändert. Hauptsächlich geht es dabei um den Eintrag der Chain „c3surf\_control“ in der Chain „FORWARD“ des Paketfilters. Der würde ansonsten durch das Script „/etc/rc.d/rc655.c3surf“ erzeugt werden und zu früh einige Regeln blockieren. Daher wurde das Einbinden dieser Chain abgeschaltet und dann mittels eines Eintrages in der "base.txt" (siehe dort "PF\_FORWARD\_17") manuell eingefügt. Damit sind die Regeln 1-16 auch schon vor einer gültigen Anmeldung wirksam. Die Chain „c3surf\_control“ selbst wird jetzt durch das Script „/etc/rc.d/fwrules.pre.c3surf\_control“ erzeugt, aber nicht mehr ins Regelwerk des Routers automatisch eingebunden.

Eine weitere Änderung betrifft den Wortlaut und das Layout der Anmeldeseite. Diese wurde an die Keimfarben CI angepasst. Diese Änderungen werden derzeit durch den Paketverantwortlichen geprüft und in geeigneter Weise (auch konfigurierbar) in das Paket c3surf eingebaut.

Die Standardeinstellungen für c3surf wurden so gewählt, dass jeder Gast mit seiner Anmeldung 720 Minuten Zugriff auf des Internet erhält. Ist die Zeit abgelaufen, so wird sein Zugang für 240 Minuten gesperrt. Dabei darf der Gast sich beliebig oft an- und wieder abmelden, was durch einen Zähler von "-1" bewirkt wird. Sollte der Gast sich nicht abmelden, aber seinen Rechner ausschalten, so wird der Gast automatisch von c3surf abgemeldet. Dies wird anhand der ARP-Tabelle überprüft.

Free Surf Admin (LoginUsr v. 2.2.1)

3Surf Admin -- LoginUsr Anmeldeseite --

Online Accounts Quota Blocklist MAC Backlist ARP System Logdateien

---==== Arbeitsbereich Benutzer ===---

UID	Vorname	Name	e-mail	Password	Zeit Minuten	Blockzeit Minuten	Zähler	Aktion
								<input type="button" value="Hinzufügen"/>
					Geltender Standardwert der Konfiguration, wenn Feld leer bleibt: 720 240 -1			

UID	Vorname Name	e-mail	Zeit Minuten (Sekunden)	Blockzeit Minuten (Sekunden)	Zähler	Quota-Stand		Aktion
						Zeit Sekunden	Zähler / Max.	
bogert	John none	none	3000 (180000)	240 (14400)	-1	-	- / -1	Benutzer: Bearbeiten Löschen Quota: Zurücksetzen
musterm	Elke Muster	none	720 (43200)	240 (14400)	-1	-	- / -1	Benutzer: Bearbeiten Löschen Quota: Zurücksetzen

Die Einstellungen für die Steuerung der Gastquota sind Vorgabewerte für die spätere Einrichtung der Zugangs-Accounts im laufenden Betrieb. Beim Einrichten dieser Zugangsdaten können diese Vorgaben bei Bedarf noch überschrieben werden.

### 3.6 Konfiguration des Gästezugangs

#### c3surf.txt

```

C3SURF_QUOTA='yes'
C3SURF_COUNTER='-1'
C3SURF_TIME='720'
C3SURF_BLOCKTIME='240'

C3SURF_CHECK_ARP='yes'

C3SURF_CONTROL_HOST_OR_NET_N='1'
C3SURF_CONTROL_HOST_OR_NET_1='IP_NET_4'

C3SURF_CONTROL_PORT_N='0'
C3SURF_CONTROL_PORT_1='515'
C3SURF_CONTROL_PORT_2='21'

C3SURF_BLOCK_PORT_N='2'
C3SURF_BLOCK_PORT_1='5000'
C3SURF_BLOCK_PORT_2='5001'

C3SURF_HTTPD_PORT='4444'
C3SURF_HTTPD_LISTENIP='192.168.99.1'

OPT_LOGINUSR='yes'

LOGINUSR_DELETE_PERSISTENT_DATA='no'

LOGINUSR_ACCOUNT_N='0'

```

## 3.7 Weitere Anmerkungen zur Konfiguration der Pakete

### 3.7.1 httpd

Damit das Personal im Schulungszentrum die Benutzerkonten der Gäste selbst anlegen und pflegen kann, wurde im httpd ein Pflegeaccount eingerichtet, welcher nur Zugriff auf die c3surf Benutzerverwaltung hat.

The screenshot shows the 'Free Surf Admin (LoginUsr v. 2.2.1)' interface. The 'Accounts' tab is active, displaying a table of users. The table has columns for UID, Vorname, Name, e-mail, Passwort, Zeit Minuten, Blockzeit Minuten, Zähler, and Aktion. Two users are listed: 'bogert' and 'musterme'. The 'Aktion' column contains links for 'Bearbeiten', 'Löschen', and 'Quota: Zurücksetzen'.

UID	Vorname	Name	e-mail	Passwort	Zeit Minuten	Blockzeit Minuten	Zähler	Aktion	
								Hinzufügen	
Geltender Standardwert der Konfiguration, wenn Feld leer bleibt:					720	240	-1		
UID	Vorname	Name	e-mail	Passwort	Zeit Minuten (Sekunden)	Blockzeit Minuten (Sekunden)	Zähler	Quota-Stand	Aktion
								Zeit Zähler / Max.	
bogert	John	none	none		3000 (180000)	240 (14400)	-1	- / -1	Benutzer: Bearbeiten Löschen Quota: Zurücksetzen
musterme	Elke	Muster	none		720 (43200)	240 (14400)	-1	- / -1	Benutzer: Bearbeiten Löschen Quota: Zurücksetzen

```
HTTPD_USER_2_USERNAME='Gaestepflege'  
HTTPD_USER_2_PASSWORD='sag-ich-nicht'  
HTTPD_USER_2_RIGHTS='c3surf:view,admin'
```

### 3.7.2 cpmvrmlog

Um die Logbuchdateien von c3surf zu rotieren, wird cpmvrmlog verwendet.

```
CPMVRMLOG_4_ACTION='move'  
CPMVRMLOG_4_SOURCE='/data/var/log/c3surf'  
CPMVRMLOG_4_DESTINATION='/data/var/log/rotate'  
CPMVRMLOG_4_CUSTOM=''  
CPMVRMLOG_4_MAXCOUNT='15'  
CPMVRMLOG_4_CRONTIME='10 0 * * *'
```

#### 4. Inbetriebnahme

Das beschriebene Setup wurde fertig konfiguriert von der Linum Software GmbH geliefert und sollte in der KW 51 in Betrieb gehen. Leider verzögerte sich die Konfiguration des VLANs auf den Switchen bis 18.12.2008. Auch dabei konnte auf die Kompetenz von Herrn Hilbrecht zurückgegriffen werden.

Der Accesspoint 1 wurde auf dem Netzwerkschrank im Technikraum des Schulungszentrums aufgestellt. Der Accesspoint 2 im Schulungsraum 2 in der nord-östlichen Ecke.

Am 19.12.2008 wurden mehrere Zugriffsszenarien an den beiden Accesspoints durchgeführt. Die beabsichtigte Ausleuchtung ist im Ergebnis sehr zufriedenstellend. Die Funkzellen reichen über den Showroom und der Werkstatt bis zu einem dritten Schulungsraum.

Die zunächst vorkonfigurierten 20 Benutzerkonten im Gäste-WLAN haben sich im nachhinein als unnötig herausgestellt und wurden wieder gelöscht. Das Personal im Schulungszentrum wurde geschult, um die Konten selbst anzulegen.

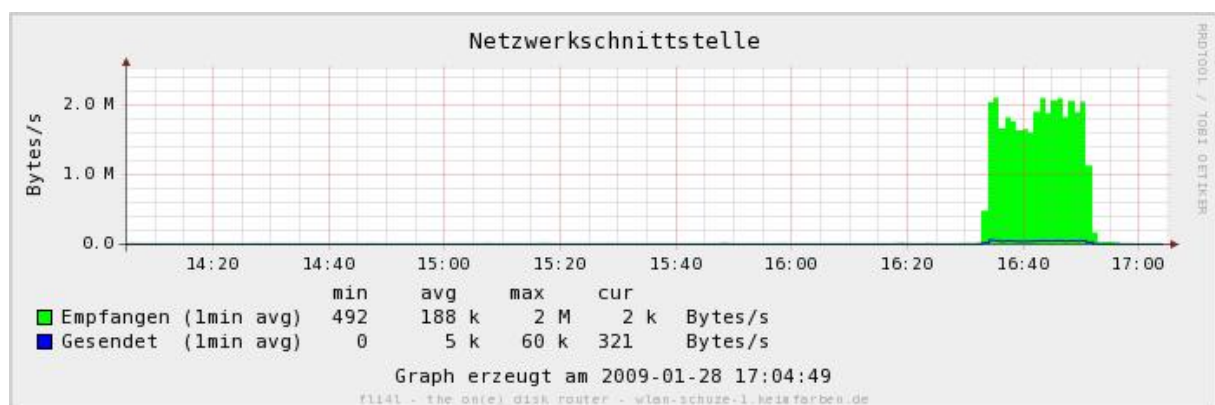
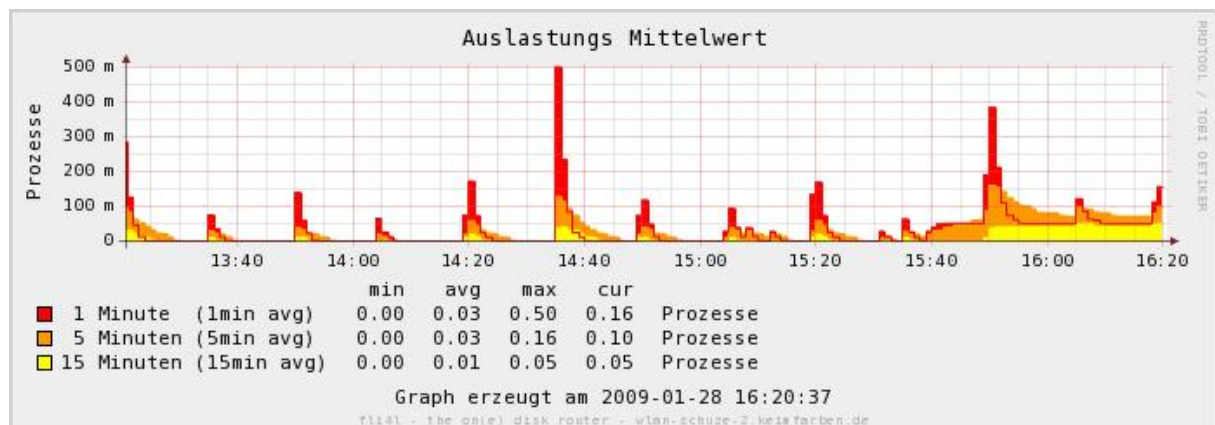
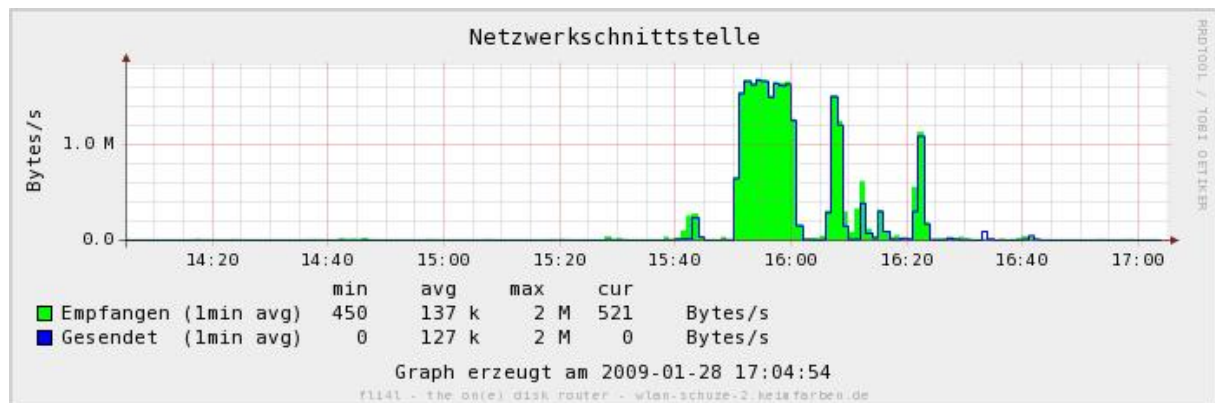
Das Einbuchen in das WLAN gelingt problemlos. Ein Hinweis von Windows, dass die Funkzelle gewechselt wurde konnte nicht festgestellt werden.



## 5. Betrieb

Da die Mitarbeiter bislang kaum in der Lage waren, mit ihren Notebooks ein WLAN zu nutzen, waren die häufigsten Probleme beim Einbuchen eine abgeschaltete oder deaktivierte WLAN-Karte. Gäste hatten bislang keine derartigen Probleme.

Vom 19.01. bis 30.01. fand in den beiden Schulungsräumen das jährliche Vertriebsseminar statt. In vier Gruppen zu je ca. 20 Personen tagte die komplette Außendienstmannschaft – alle ausgestattet mit einem WLAN-fähigen Notebook. Nachfolgende Graphen der Netzwerk- und Systemlast entstammen dem Paket rrdtool.



## Anhang – Literatur und weiterführende Links

- Dokumentation zu fli4l: <http://www.fli4l.de/hilfe/dokumentation/>
- Dissertation „Rechtsfragen offener Netze“ von Reto Mantz:  
<http://www.retosphere.de/php/download.php?fileId=25>
- Netzmafia-Scripte von Prof. Jürgen Plate, Fachhochschule München, Fachbereich Elektrotechnik und Informationstechnik: <http://www.netzmafia.de/skripten/index.html>
- PC-Netzwerke von Axel Schemberg, Martin Linten, Planen und sicheres Einrichten von LAN und WLAN, Galileo Computing:  
<http://openbook.galileocomputing.de/pcnetzwerke/>
- Linux-Firewalls - Ein praktischer Einstieg, 2. Auflage, Andreas G. Lessig, O'Reilly:  
<http://www.oreilly.de/german/freebooks/linuxfire2ger/toc.html>
- Linux Netzwerker-Handbuch, Tony Bautts, Terry Dawson & Gregor N. Purdy, 3. Auflage Juli 2005, O'Reilly:  
[http://www.oreilly.de/german/freebooks/linag3ger/418\\_LinuxIVZ.html](http://www.oreilly.de/german/freebooks/linag3ger/418_LinuxIVZ.html)
- Sicherheit im Internet, 3. Auflage, Krzysztof Janowicz, 3. Auflage Juli 2007, O'Reilly:  
<http://www.oreilly.de/german/freebooks/sii3ger/>
- Auf <http://www.fli4l-support.de> wird kommerzieller Support für fli4l angeboten. Die Firma Linum Software GmbH bietet Dienstleistungen rund um fli4l-Router an. Der Schwerpunkt liegt dabei in der Realisierung von Spezialanwendungen auf dem fli4l-Router, dem Verkauf fertig konfigurierter Hardware mit vorinstalliertem fli4l und dem Aufbau von VPNs.

Anhang – Nutzungserklärung

Vereinbarung über eine Haftungsbeschränkung  
NUTZUNG EINES WLAN-ACCESS-POINTS

KEIMFARBEN GmbH & Co. KG  
Keimstraße 16  
86420 Diedorf  
- Betreiber -

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
- Nutzer -

- 1.) Der Betreiber gestattet hiermit dem Nutzer die Nutzung seines betrieblichen WLANs inklusive des Übertritts ins Internet.
- 2.) Mit dieser Vereinbarung wird die Haftung des Betreibers für Schäden, die dem Nutzer durch oder während der Benutzung des WLANs entstehen, ausgeschlossen. Ebenso ist die Haftung des Auftragnehmers und seiner Erfüllungsgehilfen auf Fälle der groben Fahrlässigkeit beschränkt, sofern es nicht Ansprüche aus der Verletzung der Gesundheit, des Körpers oder des Lebens des Auftraggebers oder der auftragsgemäß in den Schutzbereich des Vertrages einbezogenen Dritten betrifft.
- 3.) Der Nutzer erklärt, den zur Verfügung gestellten Zugang zum WLAN und Internet nur zu legalen Zwecken zu nutzen, ebenso untersagt der Betreiber die Nutzung zu Zwecken, die jugendgefährdender oder anstößiger Natur sind.
- 4.) Der Nutzer erklärt, dass ihm bekannt ist, dass diese Vereinbarung von der gesetzlichen Regelung abweicht.
- 5.) Es gilt ausschließlich deutsches Recht mit Ausnahme internationaler Kodifikationen wie z.B. das CISG, auch bei Auslandsbezug. Falls einzelne Bestimmungen dieser Vereinbarung unwirksam sein sollten oder dies werden, so wird die Wirksamkeit der übrigen Bestimmungen hiervon nicht berührt. Die unwirksame Bestimmung ist durch die Parteien durch eine gültige zu ersetzen, die dem wirtschaftlich angestrebten Zweck möglichst nahekommt.

Diedorf, den

Diedorf, den

\_\_\_\_\_  
Nutzer  
Benutzername: \_\_\_\_\_  
Kennwort: \_\_\_\_\_

\_\_\_\_\_  
Betreiber  
gültig bis: \_\_\_\_\_