



**3G/4G | In MOBILE ROUTER SERIES**

# **User Manual**

# Bedienungsanleitung

MR-102N

Deutschsprachige Version 1.0.0

# CONTENT

KAPITEL1	Einführung.....	1
1.1	Produkteigenschaften.....	1
1.2	Packungsinhalt .....	2
KAPITEL2	Hardwareinstallation .....	3
2.1	Gehäuseansicht .....	3
2.1.1	Produktansicht .....	3
2.1.2	Frontansicht mit Statusanzeigen.....	3
2.1.3	Seitenansicht mit Anschlüssen .....	4
2.2	Installation der Hardware .....	6
2.2.1	Installation des Akkus .....	6
	Öffnen Sie die hintere Abdeckung und legen den mitgelieferten Akku ein. ....	6
2.2.2	Herstellen der Spannungsversorgung .....	6
2.2.3	Herstellen der LAN Netzwerkverbindung .....	6
2.2.4	Herstellen der WAN Netzwerkverbindung.....	6
KAPITEL3	Netzwerkeinstellungen.....	7
3.1	für Computer mit dem Betriebssystem Windows XP .....	7
3.2	für Computer mit dem Betriebssystem Windows 2000.....	9
3.3	für Computer mit dem Betriebssystem Windows 98 / ME.....	11
3.4	für Computer mit dem Betriebssystem Windows 7 .....	13
KAPITEL4	Konfiguration des Router per WEB – Browser .....	15
4.1	Systemstart und Anmeldung .....	15
KAPITEL5	Grundeinstellungen.....	16
5.1	WAN Netzwerkeinstellungen .....	16
5.1.1	DHCP - IP-Adresszuweisung durch den ISP bei jedem Verbindungsaufbau ....	18
5.1.2	Statische IP – Statische IP-Adresszuweisung durch den ISP .....	19
5.1.3	PPPoE - WAN Verbindung mit Benutzername und Passwort .....	20
5.1.4	VPN Client.....	21
5.1.5	3G/4G Mobile WAN (connected by information related to what your ISP needs)	
	22	
5.1.6	3G / 4G - Verbindung per Windows oder Android Mobiltelefon .....	24
5.1.7	HSPA+ Verbindung.....	25
5.1.8	3G / 4G - Verbindung per iPhone .....	27
5.2	Netzwerkeinstellungen .....	28
5.3	DHCP Server – Einrichtung .....	29
5.4	DDNS - Einrichtung .....	30
5.5	MAC- Adresseinrichtung.....	31

KAPITEL6	Einrichtung des WLAN .....	32
6.1	Einführung .....	32
6.1.1	Grundeinstellungen.....	32
6.1.2	Einrichten der SSID (Service-Set-Identifizier-ID) .....	34
6.1.3	WEP (Wired-Equivalent-Privacy) Sicherheitseinstellungen .....	36
6.1.4	WPA Pre-Shared Key / WPA2 Pre-Shared Key Sicherheitseinstellungen.....	37
6.1.5	WPA (Wi-Fi-Protected-Access) / WPA2 Sicherheitseinstellungen .....	38
6.2	Erweiterte Einstellungen .....	39
6.3	Einrichtung des WDS (Wireless Distributed System) .....	42
6.4	Einrichtung des Repeater Modus .....	44
KAPITEL7	Sicherheitseinstellungen .....	45
7.1	Die Firewall Einstellungen .....	45
7.2	Einrichtung der ACL (Access-Control-List) Zugriffskontrolle.....	47
7.2.1	ACL Einstellungen .....	47
7.3	MAC Adress Steuerung .....	50
7.4	Lokale Einrichtung des Open-DNS .....	52
7.4.1	OpenDNS-Einstellungen .....	52
7.5	Internetfilter .....	53
7.5.1	Einen neuen Internetfilter hinzufügen .....	54
KAPITEL8	Anwendungseinstellungen.....	56
8.1	Einführung in die Port-Range-Forward Funktion.....	56
8.1.1	Port-Range-Forward Einstellungen.....	57
8.1.2	Hinzufügen einer neuen Port-Range-Forward Regel .....	58
8.2	Einstellungen für Medien-Streaming / VPN .....	60
8.3	UPnP (Universal Plug and Play) / NAT-PMP Einstellungen.....	61
KAPITEL9	Administration.....	62
9.1	Geräteverwaltung .....	62
9.2	Netzwerkdienstprogramme.....	64
9.3	Zeiteinstellungen.....	66
KAPITEL10	Gerätestatus .....	67
10.1	<b>Router Informationen</b> .....	67
10.2	Verbindungsuebersicht / DHCP.....	70
10.3	Verbindungsuebersicht / aktuell .....	71
10.4	System-Log .....	72

# KAPITEL1 Einführung

Dieses Produkt wurde für den Small-, Home- und Mobile- Office-Gebrauch entwickelt. Dieser Router ist eine ideale Lösung für einen gemeinsam genutzten mobilen WAN / Internet-Zugang per 3G, 3.5G, 3.75G Modem. Da der WAN / Internet-Zugang gemeinsam genutzt wird, werden die 'Kosten pro Benutzer / Gerät' folglich reduziert. Die AXIMCom Mobile Router Serie verfügt über den 802.11n – Standard. Geniessen Sie Internet mit der zur Zeit höchsten Datenübertragungsrate und Abdeckung. Die Modelle MR-108N und MR-216NV sind darüber hinaus mit weiteren Funktionen, wie iDBM (Intelligentes Bandbreiten Management), TurboNAT und MRTG, zur intelligenten Bandbreitennutzung und Netzwerkverwaltung ausgestattet.

## 1.1 Produkteigenschaften

- **Mobiler, gemeinsamer Breitbandzugang (Unterstützt 3G / 4G, 802.11n und xDSL/Kabel - Modem)**

Dieser AXIMCom-Mobile-Router stellt 4 Breitband – Übertragungstechniken, einschließlich 3G / 4G, 802.11n und xDSL/Kabel – Modem, zur Verfügung. Sie können mit einem 3G / 4G Modem einen mobilen WAN / Internetzugang einrichten, oder einen kabelgebundenen Zugang per xDSL/Kabel – Modem. Es wird auch der 802.11n - Standard unterstützt. Dieser AXIMCom-Mobile-Router ist die ideale Lösung für einen gemeinsam genutzten mobilen WAN / Internet-Zugang!

- **Ermöglicht WAN / Internet – Zugang per 3G / 4G Modem**

Der AXIMCom Mobile Router unterstützt alle gängigen 3G / 4G USB - Modems. Nutzen Sie einfach Ihr vorhandenes 3G / 4G USB – Modem und Ihren Internet Dienstleister um ein mobiles Netzwerk mit WAN / Internet – Zugang zu erstellen.

- **Energie- Effizienz**

Der eingesetzte Low-Power SOC-Chip sorgt für einen niedrigen Energieverbrauch, der nicht nur Energie spart, sondern auch unsere Umwelt und Ihren Geldbeutel schont.

- **Sitzungs-Manager**

AXIMCom Mobile Router supports up to 60000 fast recycling sessions in order to guarantee stable network connection and to accommodate more users/applications in the network. (Session numbers vary between models.)

- **3G / 4G APN und PIN-Code - Unterstützung**

Der AXIMCom Mobile Router unterstützt 3G / 3.5G / 3.75G APN und PIN-Code, um unbefugten Zugriff auf Ihren Mobile Router zu verhindern und die Sicherheit Ihrer mobilen Breitbanddienste zu erhöhen..

- **Universal Repeater**

Mit der Nutzung der Universal Repeater - Funktion des AXIMCom Mobile Router vergrößern Sie Ihre Wireless - Netzwerkabdeckung und beseitigen Verbindungs-löcher im Wireless - Netzwerk in nur wenigen Schritten.

Dieses ermöglicht Ihnen die äußerst komplizierten WDS - Einstellungen zu umgehen. (Hinweis: Sie benötigen mindestens 2 AXIMCom Mobile Router, um diese Funktion zu nutzen.)

## 1.2 Packungsinhalt

- 1 x AXIMCom 3G / 4G Mobile Router
- 1 x Anwenderdokumentations-CD-ROM
- 1 x Gedruckte Kurzanleitung
- 1 x Steckernetzteil
- 1 x Li-ion Akku

# KAPITEL2 Hardwareinstallation

## 2.1 Gehäuseansicht

### 2.1.1 Produktansicht



### 2.1.2 Frontansicht mit Statusanzeigen



Anzeige	Funktion	Farbe	Status	Beschreibung
	USB Aktivität/ Router Status Anzeige	Grün	Ein	Mobile WAN ist verbunden
			Aus	USB Dongle/Modem ist nicht angeschlossen.
			Schnelles Blinken	Das USB Gerät wird aktiviert bzw. Deaktiviert.
			Langsames Blinken	Das Gerät startet und schaltet danach wieder ab. Bitte kontaktieren Sie den AXIMcom Support, sollte dieser Zustand andauernd anhalten.

WLAN 	Drahtlose Aktivität	Grün	Ein	Drahtlose Verbindung aktiviert
			Aus	Drahtlose Verbindung deaktiviert
ETHERNET 	Ethernet Link	Grün	Ein	Der Ethernet-Anschluß ist verbunden
			Aus	Der Ethernet-Anschluß ist nicht verbunden
			Blinken	Daten werden über den Ethernet-Anschluß übertragen
Power 	Status der Spannungsversorgung	Grün / Rot	Grün Ein	Akku wird geladen
			Rot Ein	
			Aus	Gerät ist ausgeschaltet
			Grün Ein	Gerät ist eingeschaltet und Akku ist aufgeladen
			Grün Blinken	Gerät ist eingeschaltet und befindet sich im Akkubetrieb
			Grün Ein Rot Blinken	Gerät ist eingeschaltet. Kein Akku vorhanden oder Akku ist defekt
Rot Ein	Niedriger Akkustatus			

### 2.1.3 Seitenansicht mit Anschlüssen

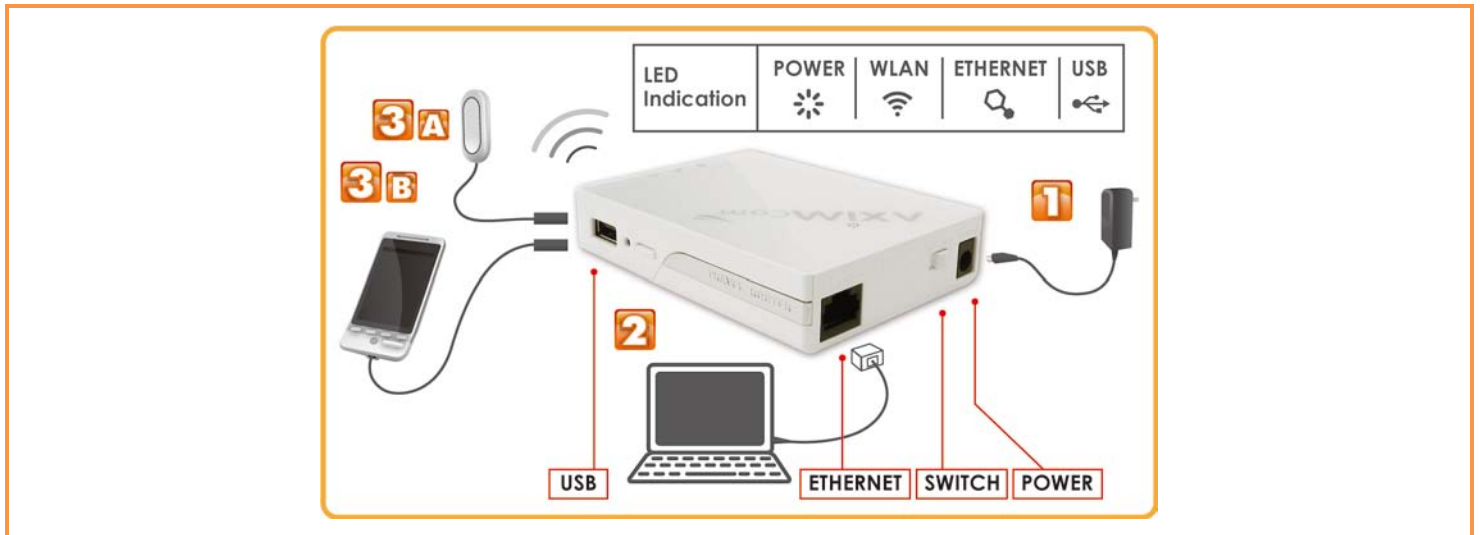


Anschlüsse / Tasten	Beschreibung
Power	Anschluss für Spannungsversorgung
ETHERNET	Wenn als WAN konfiguriert: Der Anschluß für Ihr DSL- oder Kabel-Modem. Wenn als LAN konfiguriert: Der Anschluß für Ihren Computer, Drucker oder andere Geräte.
ON-OFF Schalter	Um den Router EIN- bzw. Auszuschalten



Anschlüsse / Tasten	Beschreibung
USB Port	Zum Anschluss eines 3G/4G USB-Modems um eine mobile WAN-Verbindung aufzubauen.
WPS	Zum sicheren Entfernen des 3G/4G USB-Modems, nicht für WPS-Einstellung.
Reset	Drücken Sie die "Reset"-Taste für 2 Sekunden lassen Sie Diese dan los. Danach wird der AXIMCom Mobile Router auf Werkseinstellungen zurückgesetzt.

## 2.2 Installation der Hardware



### 2.2.1 Installation des Akkus

Öffnen Sie die hintere Abdeckung und legen den mitgelieferten Akku ein.

### 2.2.2 Herstellen der Spannungsversorgung

Entnehmen Sie das mitgelieferte Netzteil der Verpackung und verbinden Sie es mit dem Mobile Router DC-Anschluss und einer freien Steckdose. Der AXIMCom Mobile Router wird, wenn seine Power-LED und Status-LED permanent aufleuchten, in Kürze den Normalbetrieb aufnehmen.

### 2.2.3 Herstellen der LAN Netzwerkverbindung

Verbinden Sie mit einem Ethernet-Kabel den LAN-Port Ihres Computers mit dem LAN-Port des Routers.

### 2.2.4 Herstellen der WAN Netzwerkverbindung

Entscheiden Sie zuerst wie Sie den AXIMCom Mobile Router mit dem Internet verbinden wollen:

A: Anschluss über 3G/4G: Schliessen Sie das 3G/4G USB-Modem an den USB - Anschluss des Mobile Router an. Die Verbindung ist hergestellt, sobald die USB-LED konstant leuchtet.

B: Verbindung über xDSL- oder Kabelmodem: Verbinden Sie Ihr xDSL- oder Kabel - Modem, per Ethernet-Kabel mit dem WAN Anschluss des AXIMCom Mobile Router.

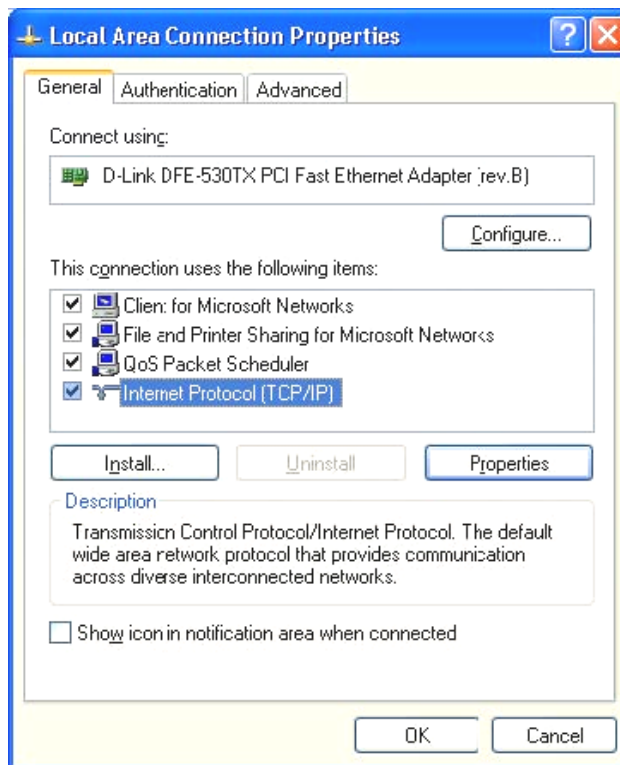
# KAPITEL3 Netzwerkeinstellungen

Bevor Sie den AXIMCom - Mobile Router nutzen können, müssen die Netzwerkeinstellungen in den Client-PCs konfiguriert werden. Sie können entweder DHCP oder Statische IP für die TCP/IP - Einstellungen benutzen.

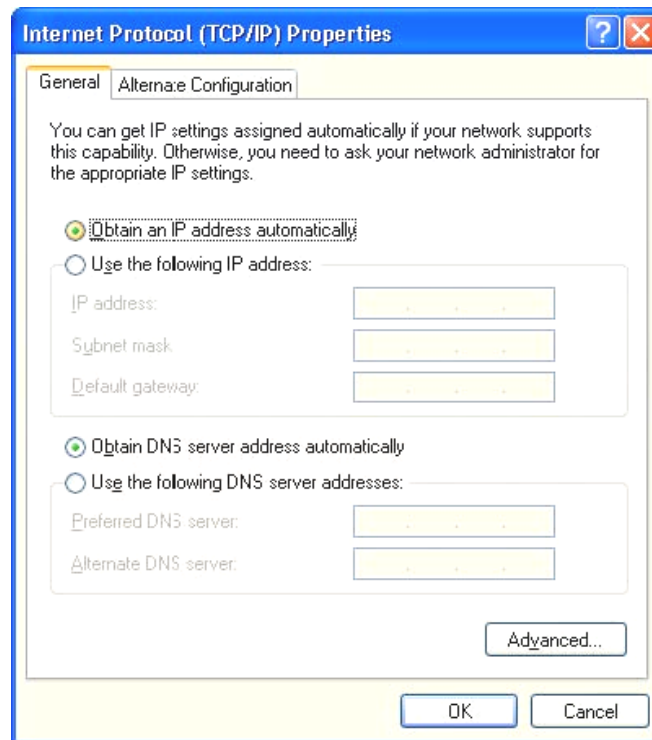
Hinweis: \* DHCP wird auf Grund seiner einfachen Installation empfohlen.

## 3.1 für Computer mit dem Betriebssystem Windows XP

1. Klicken Sie auf „Start“, „Einstellungen“ (Settings) und anschließend auf „Netzwerkverbindungen“ (Network Connections). Klicken Sie auf lokale Netzwerkverbindung(Local Area Connection). Sie werden nun folgendes Fenster sehen.



2. Wählen Sie das TCP/IP Protokoll der Netzwerkkarte aus. Klicken Sie auf Eigenschaften (Properties)



3. Auswahl DHCP oder Statische IP:

- **DHCP benutzen**

Durch Auswahl von „IP Adresse automatisch beziehen“ auf der Registerkarte „Allgemein“ wird die IP-Adresse automatisch vom DHCP - Server des Router bezogen. Wählen Sie dann „DNS Server Adresse automatisch beziehen“ aus. Klicken Sie nun auf OK. Der AXIMCom - Mobile Router wird jetzt diesem Client PC eine IP Adresse automatisch beim Verbindungsaufbau zuweisen.

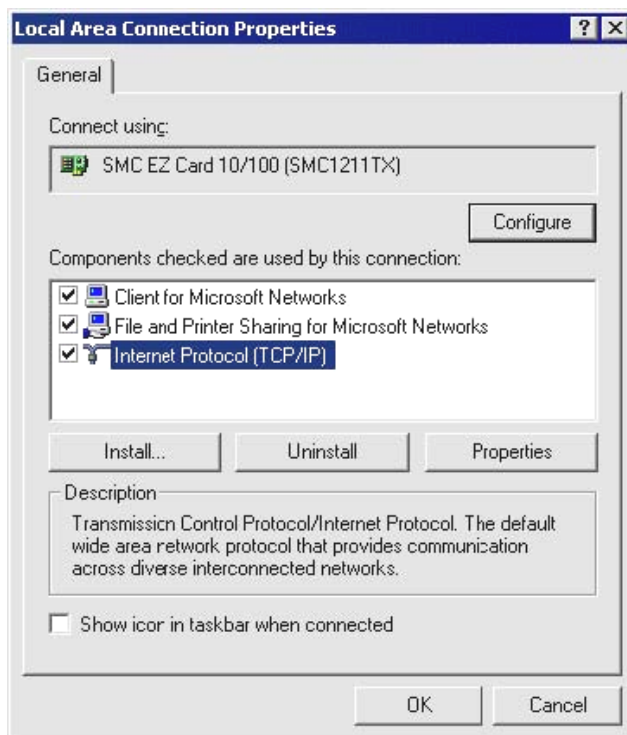
- **Statische IP benutzen**

Wählen Sie zur manuellen Konfiguration "Folgende IP Adresse verwenden" auf der Registerkarte „IP Adresse“ aus. Die Gateway-IP-Adresse des Routers lautet **192.168.1.1**. Geben Sie im Feld „IP Adresse“ folglich bitte **192.168.1.xxx** (für xxx eine Zahl zwischen 1 und 253) ein, und in das Feld „Subnetzmaske“ **255.255.255.0**. Geben Sie auf der Registerkarte „Gateway“ in das Feld „New Gateway“ die IP-Adresse des Routers ein und klicken Sie auf die Schaltfläche „Hinzufügen“ (Add). Geben Sie auf der Registerkarte „DNS Konfiguration“ in das Feld „DNS Reihenfolge“ die folgende Adresse ein: **192.168.1.1**. Klicken Sie dann auf „Hinzufügen“. Zum Abschluss klicken Sie auf OK um die Einstellungen zu übernehmen.

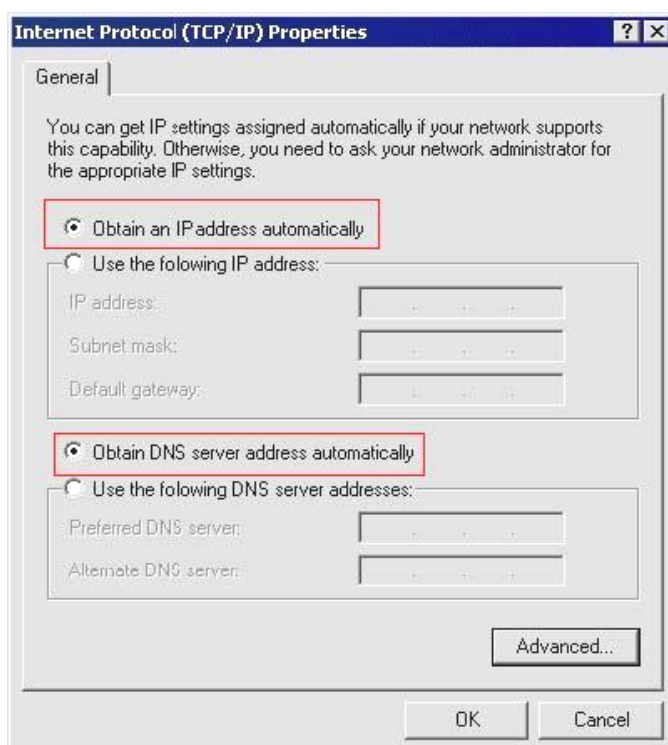
Der Client PC ist nun für den Netzwerkbetrieb konfiguriert. Um mit der Installation fortzufahren schlagen Sie Kapitel 4 auf.

## 3.2 für Computer mit dem Betriebssystem Windows 2000

Klicken Sie auf „Start“, „Einstellungen“ (Settings) und anschließend auf „Netzwerk und Wählerbindungen“ (Network and Dial-up Connection). Klicken Sie mit der rechten Maustaste auf Netzwerkverbindung (Local Area Connection) und wählen Sie „Eigenschaften“ (Properties) aus. Folgendes Fenster öffnet sich:



Wählen Sie das TCP/IP Protokoll der Netzwerkkarte aus. Klicken Sie auf Eigenschaften (Properties)



Auswahl DHCP oder Statische IP:

- **DHCP benutzen**

Durch Auswahl von „IP Adresse automatisch beziehen“ auf der Registerkarte „Allgemein“ wird die IP-Adresse automatisch vom DHCP - Server des Router bezogen. Wählen Sie dann „DNS Server Adresse automatisch beziehen“ aus. Klicken Sie nun auf OK. Der AXIMCom - Mobile Router wird jetzt diesem Client PC eine IP Adresse automatisch beim Verbindungsaufbau zuweisen.

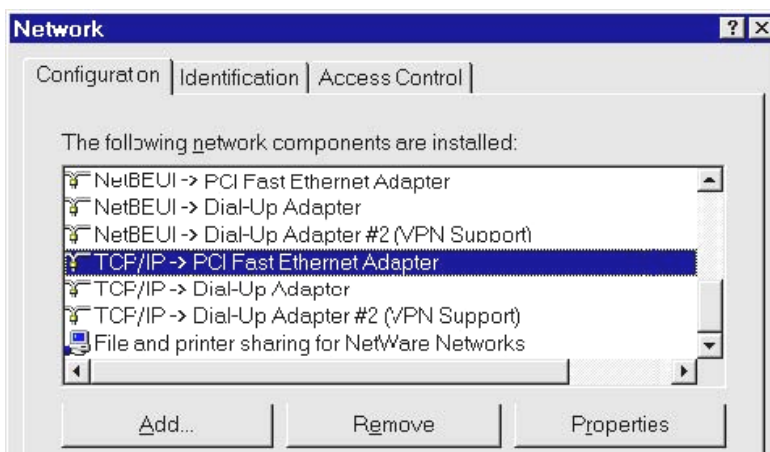
- **Statische IP benutzen**

Wählen Sie zur manuellen Konfiguration "Folgende IP Adresse verwenden" auf der Registerkarte „IP Adresse“ aus. Die Gateway-IP-Adresse des Routers lautet **192.168.1.1**. Geben Sie im Feld „IP Adresse“ folglich bitte **192.168.1.xxx** (für xxx eine Zahl zwischen 1 und 253) ein, und in das Feld „Subnetzmaske“ **255.255.255.0**. Geben Sie auf der Registerkarte „Gateway“ in das Feld „New Gateway“ die IP-Adresse des Routers ein und klicken Sie auf die Schaltfläche „Hinzufügen“ (Add). Geben Sie auf der Registerkarte „DNS Konfiguration“ in das Feld „DNS Reihenfolge“ die folgende Adresse ein: **192.168.1.1**. Klicken Sie dann auf „Hinzufügen“. Zum Abschluss klicken Sie auf OK um die Einstellungen zu übernehmen.

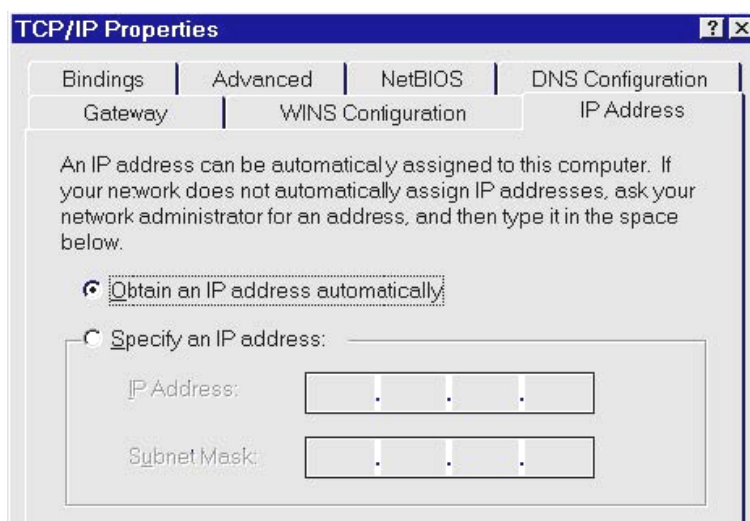
Der Client PC ist nun für den Netzwerkbetrieb konfiguriert. Um mit der Installation fortzufahren schlagen Sie Kapitel 4 auf.

### 3.3 für Computer mit dem Betriebssystem Windows 98 / ME

Klicken Sie auf „Start“, „Einstellungen“ (Settings) und anschließend auf „Netzwerk“ (Network). Folgendes Fenster öffnet sich:



Wählen Sie das TCP/IP Protokoll der Netzwerkkarte aus. Klicken Sie auf Eigenschaften (Properties)



#### Auswahl DHCP oder Statische IP:

- **DHCP benutzen**

Durch Auswahl von „IP Adresse automatisch beziehen“ auf der Registerkarte „Allgemein“ wird die IP-Adresse automatisch vom DHCP - Server des Router bezogen. Wählen Sie dann „DNS Server Adresse automatisch beziehen“ aus. Klicken Sie nun auf OK. Der AXIMCom - Mobile Router wird jetzt diesem Client PC eine IP Adresse automatisch beim Verbindungsaufbau zuweisen.

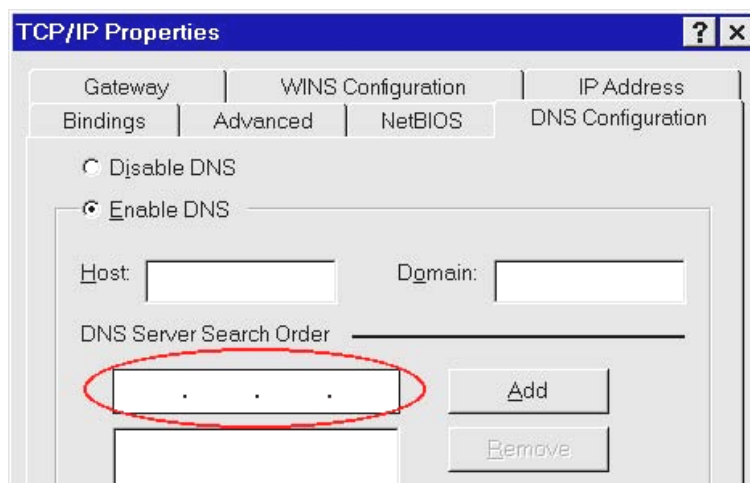
- **Statische IP benutzen**

Wählen Sie zur manuellen Konfiguration "Folgende IP Adresse verwenden" auf der Registerkarte „IP Adresse" aus. Die Gateway-IP-Adresse des Routers lautet **192.168.1.1**. Geben Sie im Feld „IP Adresse" folglich bitte **192.168.1.xxx** (für xxx eine Zahl zwischen 1 und 253) ein, und in das Feld „Subnetzmaske" **255.255.255.0**.

Geben Sie auf der Registerkarte „Gateway" in das Feld „New Gateway" die IP-Adresse des Routers ein und klicken Sie auf die Schaltfläche „Hinzufügen" (Add).



Geben Sie auf der Registerkarte „DNS Konfiguration" in das Feld „DNS Reihenfolge" die folgende Adresse ein: **192.168.1.1**. Klicken Sie dann auf „Hinzufügen".

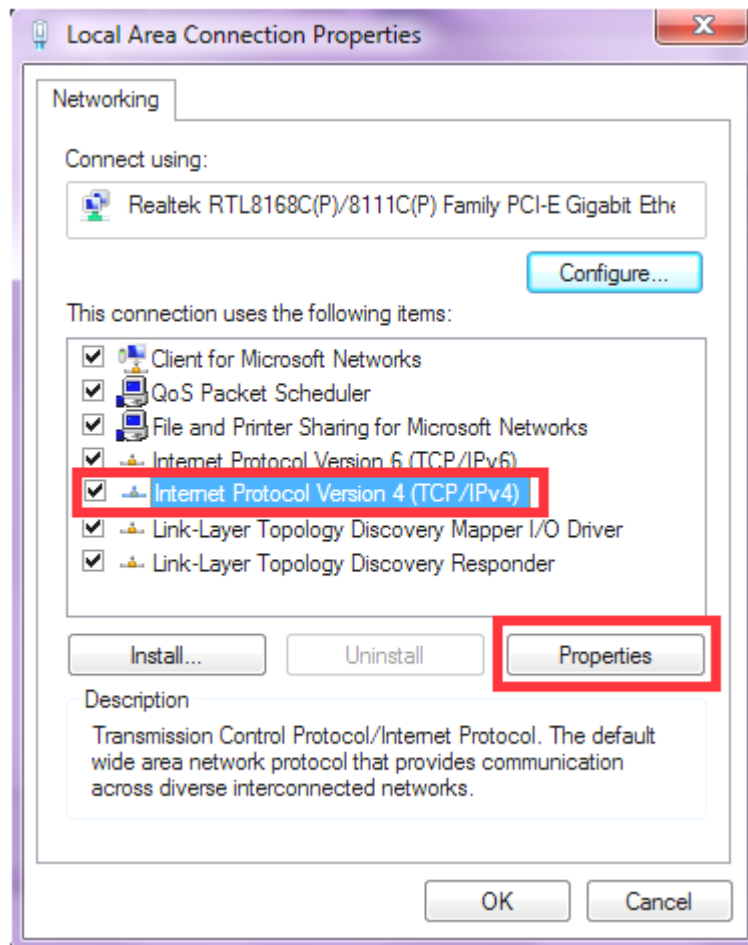


Zum Abschluss klicken Sie auf OK um die Einstellungen zu übernehmen.

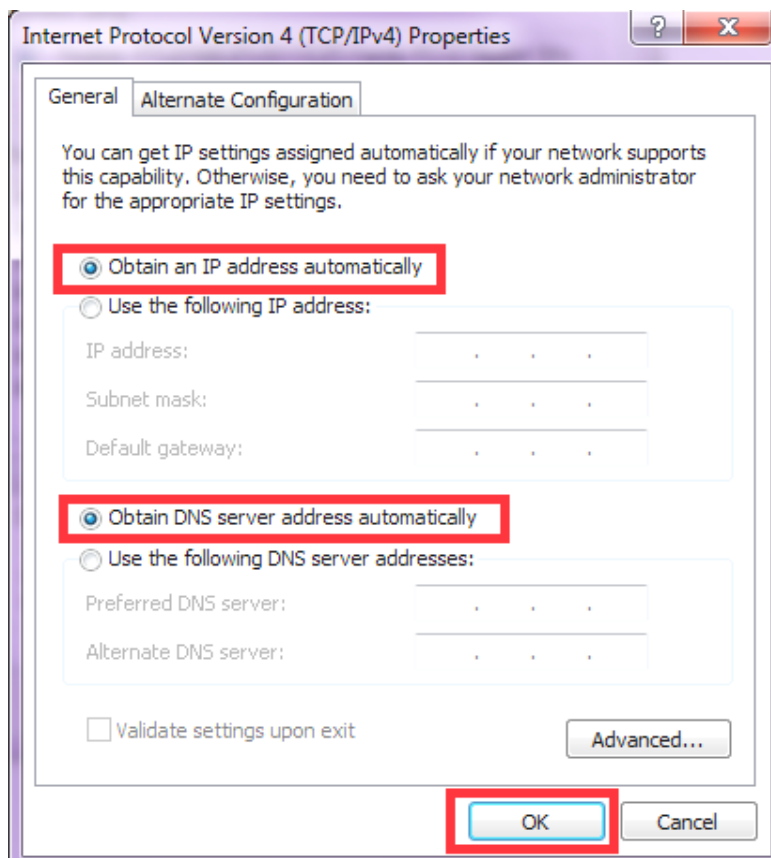
Der Client PC ist nun für den Netzbetrieb konfiguriert. Um mit der Installation fortzufahren schlagen Sie Kapitel 4 auf.

### 3.4 für Computer mit dem Betriebssystem Windows 7

Klicken Sie auf Start> Systemsteuerung> Netzwerk und Internet> Netzwerk- und Freigabecenter> Ändern Netzwerkadaptereinstellungen. Klicken Sie auf „lokales Netzwerk“ (Local Area Connection) und wählen Sie Eigenschaften. Folgendes Fenster öffnet sich:



Wählen Sie das TCP/IP Protokoll der Netzwerkkarte aus. Klicken Sie auf Eigenschaften (Properties)



#### Auswahl DHCP oder Statische IP:

- **DHCP benutzen**

Durch Auswahl von „IP Adresse automatisch beziehen“ auf der Registerkarte „Allgemein“ wird die IP-Adresse automatisch vom DHCP - Server des Router bezogen. Wählen Sie dann „DNS Server Adresse automatisch beziehen“ aus. Klicken Sie nun auf OK. Der AXIMCom - Mobile Router wird jetzt diesem Client PC eine IP Adresse automatisch beim Verbindungsaufbau zuweisen.

- **Statische IP benutzen**

Wählen Sie zur manuellen Konfiguration "Folgende IP Adresse verwenden" auf der Registerkarte „IP Adresse“ aus. Die Gateway-IP-Adresse des Routers lautet 192.168.1.1. Geben Sie im Feld „IP Adresse“ folglich bitte 192.168.1.xxx (für xxx eine Zahl zwischen 1 und 253) ein, und in das Feld „Subnetzmaske“ 255.255.255.0. Geben Sie auf der Register- karte „Gateway“ in das Feld „New Gateway“ die IP-Adresse des Routers ein und klicken Sie auf die Schaltfläche „Hinzufügen“ (Add). Geben Sie auf der Registerkarte „DNS Konfiguration“ in das Feld „DNS Reihenfolge“ die folgende Adresse ein: 192.168.1.1. Klicken Sie dann auf „Hinzufügen“. Zum Abschluss klicken Sie auf OK um die Einstellungen zu übernehmen.

Der Client PC ist nun für den Netzwerkbetrieb konfiguriert. Um mit der Installation fortzufahren schlagen Sie Kapitel 4 auf.

# KAPITEL4 Konfiguration des Router per WEB – Browser

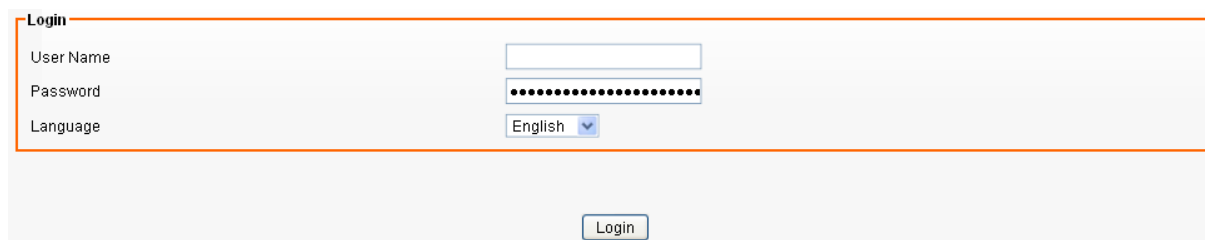
Nach Durchführung der Netzwerkeinstellungen und einem Neustart sollte Ihrem Windows XP / 2000 Client PC eine IP Adresse zugewiesen worden sein. Nun müssen Sie Ihren AXIMCom Mobile Router konfigurieren.

## 4.1 Systemstart und Anmeldung

Starten Sie Ihren WEB / Internet - Browser. Geben Sie in der Adresszeile folgendes ein: **http://192.168.1.1:8080**



Nach erfolgreicher Verbindung öffnet sich der Anmeldebildschirm des AXIMCom – Mobile Router. Geben Sie hier den Benutzernamen (username) und das Kennwort (Password) ein. Der voreingestellte Benutzername lautet **admin**, das Passwort lautet ebenfalls **admin**. Die Startseite der grafischen Benutzeroberfläche des AXIMCom - Mobile Router öffnet sich nun.

A screenshot of the login page for the AXIMCom Mobile Router. The page has a light gray background. At the top left, the word 'Login' is written in bold. Below it, there are three input fields: 'User Name' with an empty text box, 'Password' with a text box containing 12 black dots, and 'Language' with a dropdown menu showing 'English'. At the bottom center, there is a 'Login' button.

# KAPITEL5 Grundeinstellungen

## 5.1 WAN Netzwerkeinstellungen

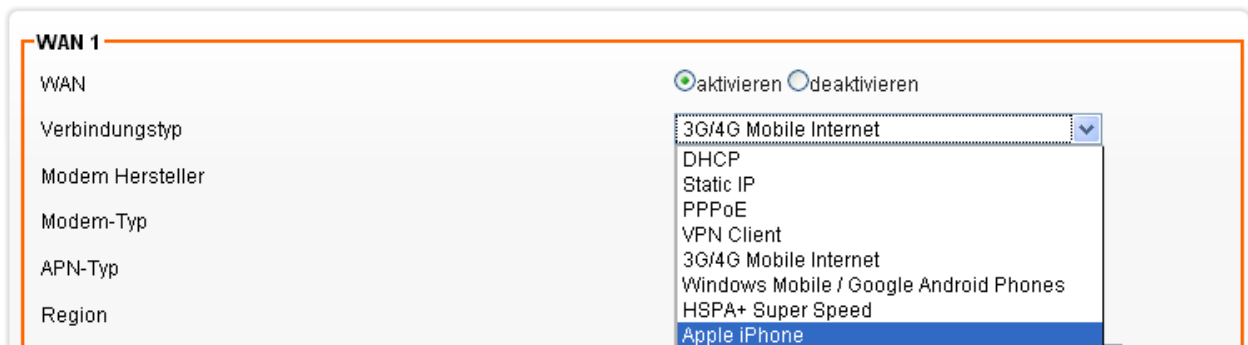
1. Klicken Sie auf [Setup] - [WAN]. Folgendes Fenster öffnet sich: screen.

### Setup - WAN

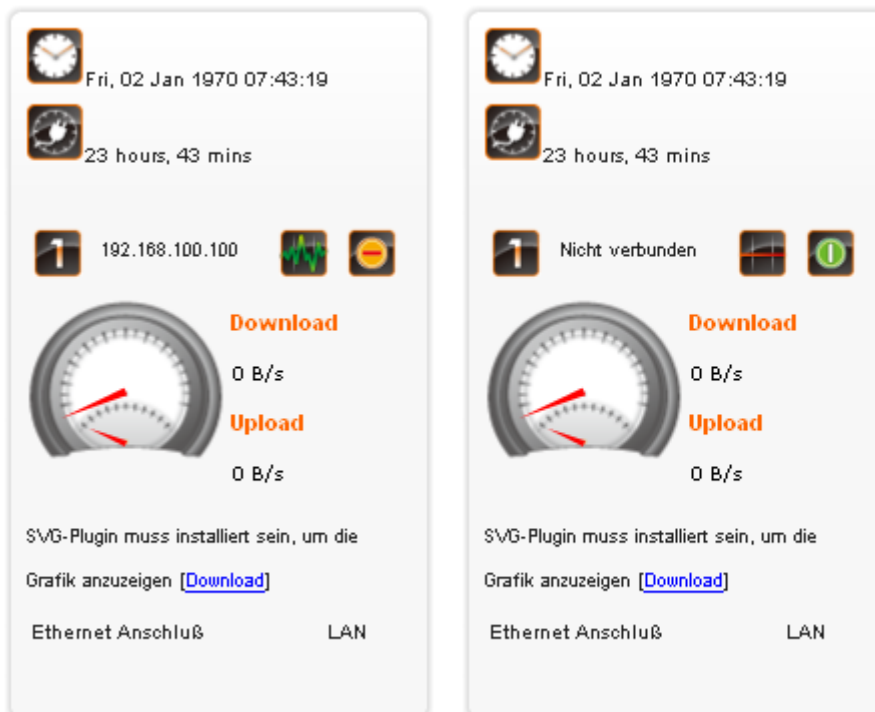
WAN 1	
WAN	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Verbindungstyp	3G/4G Mobile Internet
Modem Hersteller	Automatischer Modus
Modem-Typ	Automatischer Modus
APN-Typ	<input checked="" type="radio"/> Anbieter <input type="radio"/> Manuell
Region	Taiwan
Anbieter	Chunghwa Telecom
Access Point Name (APN)	internet
Persönliche Identifikationsnummer (PIN)	
Authentifizierung	CHAP (Automatischer Modus)
Benutzername	
Kennwort	
Einwahlnummer	*99#
Verbindungs-Modus	Automatischer Modus
PPP-Verbindungsmodus	<input type="radio"/> Ständige Verbindung <input type="radio"/> Manuelle Verbindung
Maximale Pausenzeit	300 Sekunden (60~3600)
PPP Echo Intervall	20 Sekunden (3 ~ 50)
PPP Wiederholungsgrenzwert	20 Zeit (3 ~ 50)
MTU	1492 Bytes (592-1492)
TurboLink (Aktiviert erhöht es eventuell die Gebühr für Ihre 3G Datennutzung)	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
WAN PnP	
WAN PnP	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren

## 2. WAN Einstellungen:

AXIMCom-Mobile Router unterstützt vier Verbindungstypen: DHCP, Static, PPPoE, 3G/4G Mobile internet, Windows Mobile/Google Android phone, HSPA+ Super Speed und Apple iPhone. Stellen Sie sicher welchen Verbindungstyp Sie nutzen wollen, wählen Sie Diesen aus dem Pull-Down Menu aus.



Egal für welche Verbindungsart Sie sich entschieden haben, die Anzeige der externen Verbindung zu einem Client wird wie unten dargestellt. Wenn die Anzeige "nicht verbunden" (Not connected) erscheint, so sind die gemachten WAN Einstellungen falsch. Bitte überprüfen Sie alle Einstellungen und ändern Diese entsprechend.



### 5.1.1 DHCP - IP-Adresszuweisung durch den ISP bei jedem Verbindungsaufbau

Ihnen wird automatisch die IP-Adresse von Ihrem ISP zugewiesen. DHCP ist der Vorgabeverbindungsstyp für den AXIMCom - Mobile Router. Sie werden nun das folgende Fenster sehen, nachdem Sie DHCP ausgewählt haben.

**WAN 1**

WAN  aktivieren  deaktivieren

Verbindungstyp

Host-Name

MTU  Bytes

Bigpond Login  aktivieren  deaktivieren

Bigpond Login Server

Bigpond Login Username

Bigpond Passwort

WAN	Aktivieren / Deaktivieren des WAN / Internet Zugangs
Verbindungstyp	DHCP
Host Name	Einige ISP und DHCP - Server benötigen den Host Namen des Clients um ihm eine IP-Adresse zuzuweisen. Geben Sie in diesem Fall den Host Namen des Client ein..
MTU	Maximum Transmission Unit
Bigpond Login	Aktivieren / Deaktivieren des Bigpond
Bigpond Login Server	Wählen Sie hier den Log-In Server aus
Bigpond Login User Name	Der Bigpond Benutzername, nur wenn benötigt
Bigpond Login Passwort	Das Bigpond Kennwort, nur wenn benötigt

## 5.1.2 Statische IP – Statische IP-Adresszuweisung durch den ISP

Die IP-, Gateway-, DNS-Server Adressen, sowie die Subnetmask Adresse, werden Ihnen von Ihrem ISP bereitgestellt. Geben Sie diese Daten entsprechend hier ein.

**WAN 1**

WAN  aktivieren  deaktivieren

Verbindungstyp Static IP ▼

Externe Netzwerk-IP-Adresse

Netzmaske

Standardgateway

Erster DNS

Zweiter DNS

MTU  Bytes

WAN	Aktivieren / Deaktivieren des WAN / Internet Zugangs
Verbindungstyp	Statische IP
Externe Netzwerk-IP-Adresse	Die vom ISP bereitgestellte IP - Adresse.
Netzmaske	Die vom ISP bereitgestellte Subnetmask.
Standardgateway	Die vom ISP bereitgestellte Gateway - Adresse.
Erster DNS	Die vom ISP bereitgestellte DNS Server Adresse für den primären DNS Server
Zweiter DNS	Die vom ISP bereitgestellte DNS Server Adresse für den sekundären DNS Server
MTU	Größtmögliche Übermittlungseinheit

### 5.1.3 PPPoE - WAN Verbindung mit Benutzername und Passwort

Ihr ISP stellt Ihnen Benutzername (username) und Passwort (password) für den WAN / Internetzugang zur Verfügung. Geben Sie diese Daten entsprechend ein.

**WAN 1**

WAN  aktivieren  deaktivieren

Verbindungstyp

Authentifizierung

Benutzername

Kennwort

PPP-Verbindungsmodus  Ständig Verbunden  Manuelle Verbindung

Maximale Pausenzeit  Sekunden (60~3600)

PPP Echo Intervall  Sekunden (3 ~ 50)

PPP Wiederholungsgrenzwert  Zeit (3 ~ 50)

PPP MTU  Bytes (592-1492)

MTU  Bytes (600~1500)

WAN	Aktivieren / Deaktivieren des WAN / Internet Zugangs
Verbindungstyp	PPPoE
Benutzername	Der vom ISP bereitgestellte Benutzername
Kennwort	Das vom ISP bereitgestellte Kennwort
PPP-Verbindungsmodus	Die PPPoE wird ständig aufrechterhalten oder es erfolgt eine manuelle Verbindung
Maximale Pausenzeit	PPPoE Auf Verlangen wird nur aktiviert werden, wenn es Verkehr gibt. Wenn es keinen Verkehr innerhalb größtmöglicher Leerlaufzeit gibt (Vorgabe: 300 Sekunden), wird PPPoE unterbrochen. Die Verbindung wird nur bei aktivem Datenverkehr hergestellt. Ist kein Datenverkehr vorhanden wird die Verbindung nach Ablauf der Max. Idle- Zeit (Maximale Wartezeit), voreingestellt: 300 Sekunden) getrennt
PPP Echo Intervall	Es wird sichergestellt ob der Link noch aktiv oder schon inaktiv ist. (Die Abfrage erfolgt 20 mal)
PPP Wiederholungsgrenzwert	Wenn das PPPoE- Echo den Abfragewert (20 mal) überschreitet, wird die Verbindung als „Nicht verbunden“ behandelt
PPPoE MTU	Die größtmögliche Übertragungseinheit: bis zu 1492 Byte (Die Header – Größe von PPPoE beträgt 8 Byte).
MTU	Größtmögliche Übermittlungseinheit

## 5.1.4 VPN Client

**WAN 1**

WAN aktivieren deaktivieren

Verbindungstyp

VPN Client Type

VPN Connection Type

Externe Netzwerk-IP-Adresse

Netzmaske

Standardgateway

Erster DNS

Zweiter DNS

MTU  Bytes

Benutzername

Kennwort

VPN Host

MPPE128 aktivieren aktivieren deaktivieren

WAN	Aktivieren / Deaktivieren des WAN / Internet Zugangs
Verbindungstyp	VPN Client
VPN Client Type	Wählen Sie PPTP oder L2TP
VPN Connection Type	Wählen Sie zwischen statischer IP oder DHCP
Externe Netzwerk-IP-Adresse	Die vom ISP bereitgestellte IP - Adresse.
Netzmaske	Die vom ISP bereitgestellte Subnetmask.
Standardgateway	Die vom ISP bereitgestellte Gateway - Adresse.
Erster DNS	Die vom ISP bereitgestellte DNS Server Adresse für den primären DNS Server
Zweiter DNS	Die vom ISP bereitgestellte DNS Server Adresse für den sekundären DNS Server
MTU	Größtmögliche Übermittlungseinheit
Benutzername	Benutzername für den VPN Server
Kennwort	Kennwort für den VPN Server
VPN Host	IP Adresse oder Domainname des VPN Servers
MPPE128 aktivieren	Aktivieren/Deaktivieren der MPPE128 Verschlüsselung

### 5.1.5 3G/4G Mobile WAN (abhängig von Informationen Ihres ISP)

Bitte geben Sie den APN, PIN-Code, den Benutzernamen und das Passwort von Ihrem ISP ein.  
(Bitte beachten Sie, dass einige Informationen nicht erforderlich sind)

**WAN 1**

WAN	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Verbindungstyp	3G/4G Mobile Internet
Modem Hersteller	Automatischer Modus
Modem-Typ	Automatischer Modus
APN-Typ	<input checked="" type="radio"/> Anbieter <input type="radio"/> Manuell
Region	Taiwan
Anbieter	Chunghwa Telecom
Access Point Name (APN)	
Persönliche Identifikationsnummer (PIN)	
Authentifizierung	CHAP (Automatischer Modus)
Benutzername	
Kennwort	••••••••••••••••
Einwahlnummer	*99***1#
Verbindungs-Modus	Automatischer Modus
PPP-Verbindungsmodus	<input checked="" type="radio"/> Ständige Verbindung <input type="radio"/> Manuelle Verbindung
Maximale Pausenzeit	300 Sekunden (60~3600)
PPP Echo Intervall	20 Sekunden (3 ~ 50)
PPP Wiederholungsgrenzwert	20 Zeit (3 ~ 50)
MTU	1492 Bytes (592-1492)
TurboLink (Aktiviert erhöht es eventuell die Gebühr für Ihre 3G Datennutzung)	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren

WAN	Aktivieren / Deaktivieren des WAN / Internet Zugangs
Verbindungstyp	3G/4G Mobile Internet
Modem Hersteller	Wählen sie die Modemmarke aus, die Sie benutzen. Für eine automatische Erkennung „auto“ auswählen
Modem-Typ	Wählen sie das Modem aus, das Sie benutzen. Für eine automatische Erkennung „auto“ auswählen
APN-Typ	Wählen Sie „By Service Provider“ um den ISP anzugeben. Oder Sie wählen „Custom“ und geben die Daten manuell ein.
Region	Geben Sie hier Ihren Standort ein.
Anbieter	Wählen Sie hier Ihren ISP aus und der Zugangs-Punkt-Name (APN) wird automatisch zugewiesen werden.
Access Point Name (APN)	Geben Sie hier den vom ISP bereitgestellten APN- String ein, wenn Sie zuvor beim APN Type „Custom“ gewählt haben. Sonst lassen Sie diese Feld leer.
Persönliche Identifikationsnummer (PIN)	Geben Sie hier den vom ISP bereitgestellten PIN- Kode ein, nur wenn benötigt
Authentifizierung	
Benutzername	Der vom ISP bereitgestellte Benutzername, nur wenn benötigt
Kennwort	Das vom ISP bereitgestellte Kennwort, nur wenn benötigt
Einwahlnummer	Geben Sie hier die vom ISP bereitgestellte Einwahlnummer ein (Vorgabe *99***1#).
Verbindungs-Modus	Die PPPoE wird ständig aufrechterhalten oder es erfolgt eine manuelle Verbindung
Maximale Pausenzeit	Die Verbindung wird nur bei aktivem Datenverkehr hergestellt. Ist kein Datenverkehr vorhanden wird die Verbindung nach Ablauf der Max. Idle-Zeit (Maximale Wartezeit), voreingestellt: 300 Sekunden) getrennt
PPP Echo Intervall	Es wird sichergestellt ob der Link noch aktiv oder schon inaktiv ist. (Die Abfrage erfolgt 20 mal)
PPP Wiederholungsgrenzwert	Wenn das PPPoE Echo den Abfragewert (20 mal) überschreitet, wird die Verbindung als „Nicht verbunden“ behandelt
MTU	Die größtmögliche Übertragungseinheit: bis zu 1492 Byte (Die Header – Größe von PPPoE beträgt 8 Byte).
TurboLink (Aktiviert erhöht es eventuell die Gebühr für Ihre 3G Datennutzung)	Die TurboLink Funktion verbessert die Verbindungsstabilität und sorgt für höhere Datenübertragungsraten. (Hinweis: Die TurboLink Aktivierung erhöht mitunter die Kosten für die Datenübertragung)

## 5.1.6 3G / 4G - Verbindung per Windows oder Android Mobiltelefon

Wenn Sie den Windows / Android Smart Phone Zugang wählen, verbinden Sie Ihr Smart Phone per HUSB mit dem Router und stellen sicher das eine Verbindung zu Ihren Netzbetreiber besteht. Nehmen Sie nun alle erforderlichen Einstellungen am Router vor. Dann, um den gemeinsamen Internetzugang zu aktivieren, erstellen Sie in Ihrem Smart Phone eine neue Verbindung. Der Router wird nun automatisch dieser Verbindung zugeordnet.

**WAN 1**

WAN  aktivieren  deaktivieren

Verbindungstyp  ▼

Host-Name

MTU  Bytes

TurboLink (Enable it might increase your 3G data charge)  aktivieren  deaktivieren

WAN	Aktivieren / Deaktivieren des WAN / Internet Zugangs
Verbindungstyp	3G/4G Windows Mobile / Google Android Phones
Host Name	Einige ISP und DHCP - Server benötigen den Host Namen des Clients um ihm eine IP-Adresse zuzuweisen. Geben Sie in diesem Fall den Host Namen des Client ein
MTU	Größtmögliche Übermittlungseinheit
TurboLink	Die TurboLink Funktion verbessert die Verbindungsstabilität und sorgt für höhere Datenübertragungsraten. (Hinweis: Die TurboLink Aktivierung erhöht mitunter die Kosten für die Datenübertragung)

## 5.1.7 HSPA+ Verbindung

Wenn Ihr Modem ein HSPA+ Modem ist, wählen Sie den HSPA+ Super Speed Modus aus. Bitte geben Sie hier, die von Ihrem ISP bereitgestellten APN, PIN-Code, Benutzernamen und Passwort ein. (Hinweis: Bitte beachten Sie, dass einige Informationen nicht erforderlich sein könnten)

**WAN 1**

WAN	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Verbindungstyp	HSPA+ Super Speed
Modem Hersteller	Automatischer Modus
Modem-Typ	Automatischer Modus
APN-Typ	<input type="radio"/> Anbieter <input checked="" type="radio"/> Manuell
Region	Taiwan
Anbieter	Chunghwa Telecom
Access Point Name (APN)	<input type="text"/>
Persönliche Identifikationsnummer (PIN)	<input type="text"/>
Verbindungs-Modus	Automatischer Modus
WAN MTU	1500 Bytes
Bigpond Login	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren
Bigpond Login Server	New South Wales (61.9.192.13)
Bigpond Login Username	<input type="text"/>
Bigpond Passwort	<input type="password"/>
TurboLink (Enable it might increase your 3G data charge)	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren

WAN	Aktivieren / Deaktivieren des WAN / Internet Zugangs
Verbindungstyp	HSPA+ Super Speed
Modem Hersteller	Wählen sie die Modemmarke aus, die Sie benutzen. Für eine automatische Erkennung „auto“ auswählen
Modem-Typ	Wählen sie das Modem aus, das Sie benutzen. Für eine automatische Erkennung „auto“ auswählen
APN-Typ	Wählen Sie „By Service Provider“ um den ISP anzugeben. Oder Sie wählen „Custom“ und geben die Daten manuell ein
Region	Geben Sie hier Ihren Standort ein.
Anbieter	Wählen Sie hier Ihren ISP aus und der APN-Name wird automatisch zugewiesen
Access Point Name (APN)	Geben Sie hier den vom ISP bereitgestellten APN-String ein, wenn Sie zuvor beim APN Type „Custom“ gewählt haben. Sonst lassen Sie diese Feld leer
Persönliche Identifikationsnummer (PIN)	Geben Sie hier den vom ISP bereitgestellten PIN- Kode ein, nur wenn benötigt
Verbindungs-Modus	Wählen Sie hier den Verbindungsmodus, bitte wählen Sie „auto“ aus
WAN MTU	Größtmögliche Übertragungseinheit
Bigpond Login	Aktivieren / Deaktivieren des Bigpond
Bigpond Login Server	Wählen Sie hier den Log-In Server aus
Bigpond Login User Name	Der Bigpond Benutzername, nur wenn benötigt
Bigpond Login Passwort	Das Bigpond Kennwort, nur wenn benötigt
TurboLink	Die TurboLink Funktion verbessert die Verbindungsstabilität und sorgt für höhere Datenübertragungsraten. (Hinweis: Die TurboLink Aktivierung erhöht mitunter die Kosten für die Datenübertragung)

## 5.1.8 3G / 4G - Verbindung per iPhone

**WAN 1**

WAN  aktivieren  deaktivieren

Verbindungstyp

Host-Name

MTU  Bytes

TurboLink (Enable it might increase your 3G data charge)  aktivieren  deaktivieren

WAN	Aktivieren / Deaktivieren des WAN / Internet Zugangs
Verbindungstyp	Apple iPhone
Host-Name	Einige ISP und DHCP - Server benötigen den Host Namen des Clients um ihm eine IP-Adresse zuzuweisen. Geben Sie in diesem Fall den Host Namen des Client ein
MTU	Größtmögliche Übermittlungseinheit
TurboLink	Die TurboLink Funktion verbessert die Verbindungsstabilität und sorgt für höhere Datenübertragungsraten. (Hinweis: Die TurboLink Aktivierung erhöht mitunter die Kosten für die Datenübertragung)

Die Verbindungseinstellungen sind komplett. Klicken Sie auf "Save Settings" um die Einstellungen zu übernehmen.

## 5.2 Netzwerkeinstellungen

1. Klicken Sie auf [Setup] - [LAN]. Folgendes Fenster öffnet sich:

**LAN 1**

Interne Netzwerk-IP-Adresse	<input type="text" value="192.168.1.1"/>
Netzmaske	<input type="text" value="255.255.255.0"/> ▾
Spanning Tree Protokoll (STP)	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren
MTU	<input type="text" value="1500"/> Bytes

2. Konfigurieren Sie das Netzwerk entsprechend den folgenden Anweisungen:

Interne Netzwerk-IP-Adresse	Geben Sie hier die Router IP- Adresse ein
Netzmaske	Wählen Sie die Netmask aus der Auswahlliste aus
Spanning Tree Protokoll (STP)	Klicken Sie auf „Enable“ um redundante Netzsleifen, verursacht durch fehlerhafte Verkabelung innerhalb Ihres Netzwerkes zu vermeiden. (Hinweis: Redundante Netzsleifen können den Datenverkehr erheblich beeinträchtigen oder gar unmöglich machen!)
MTU	Größtmögliche Übertragungseinheit: bis 1500 Byte

## 5.3 DHCP Server – Einrichtung

AXIMCom Mobile Router provides DHCP server service in order to offer IP addresses to the computers within a LAN.

1. Klicken Sie auf [Setup] - [DHCP-Server]. Folgendes Fenster öffnet sich:

**DHCP-Server - LAN 1**

DHCP-Dienst  aktivieren  deaktivieren

DHCP erste IP-Adresse 192.168.1. 20

Max. Anzahl DHCP-Clients 8

Gültigkeit 1 Tag ▼

Domain lan

DHCP DNS-Server-Typ OpenDNS Server ▼

DHCP DNS-Server IP-Adresse 208.67.220.220  
208.67.222.222

2. Konfigurieren Sie den DHCP Server entsprechend den folgenden Anweisungen:.

DHCP-Dienst	Aktivieren / Deaktivieren des DHCP Server Dienstes
DHCP erste IP-Adresse	Die vom DHCP Server zu vergebende Start IP Adresse
Max. Anzahl DHCP-Clients	Die größtmögliche Anzahl von den vom DHCP-Client IP-Adressen
Gültigkeit	Hier stellen Sie die Gültigkeitsdauer ein, nach deren Ablauf die IP Adresse der DHCP-Clients verfällt. Sie Können zwischen <A[zeit   mal]>1 Stunde, 3 Stunden, 6 Stunden, 1 Tag, 3 Tage, oder 7 Tage auswählen.
Domain	Geben Sie hier den Domain Namen ein.
DHCP DNS-Server-Typ	
DHCP DNS-Server IP-Adresse	

## 5.4 DDNS - Einrichtung

DDNS (Dynamic Domain Name Service) ermöglicht einen "Internet-Domain-Namen" auf einen Computer oder Router, mit dynamische IP- Adresse, zu übertragen. Dies macht es für andere Internet-Geräte möglich sich zu verbinden ohne eine dynamisch wechselnde IP-Adresse dauernd zu verfolgen. Um DDNS zu nutzen, müssen Sie sich zunächst für den DDNS Dienst bei DynDNS.org, TZO.com oder ZoneEdit.com registrieren.

DDNS ist nützlich, wenn es mit der Virtual Server Funktion kombiniert wird. Andere Internet-Nutzer können nun mit dem Domain Namen, statt der IP Adresse eine Verbindung zu Ihrem virtuellen Server herstellen. Der DDNS- Dienst hilft den Benutzern, die richtige IP- Adresse durch den Domain-Namen zu finden.

Zum Beispiel, Sie wollen einen persönlichen Web-Server einrichten. Allerdings erhalten Sie jedesmal wenn Sie eine Verbindung herstellen eine andere IP- Adresse von Ihrem ISP. Diese dynamische IP- Adresse führt dazu, das andere Internet-Nutzer Schwierigkeiten haben Internet-Nutzer Ihren Webserver zu finden. In diesem Fall müssen Sie DDNS aktivieren, damit andere Benutzer sich mit einem Domain-Namen mit Ihrem Web-Server verbinden, so dass die unterschiedlichen IP- Adressen hinter dem Server ignoriert werden können.

Registrieren Sie sich zuerst bei einem der DDNS- Anbieter (DynDNS.org, TZO.com oder ZoneEdit.com), bevor Sie DDNS den AXIMCom Mobile Router konfigurieren.

1. Klicken Sie auf [Setup] - [DDNS]. Folgendes Fenster öffnet sich:.

**Dynamic Domain Name Service - WAN 1**

DDNS Service  aktivieren  deaktivieren

DDNS Typ

Benutzername

Kennwort

Host-Name

Aktion

2. Konfigurieren Sie den DDNS Dienst entsprechend den folgenden Anweisungen:

DDNS Service	Aktivieren / Deaktivieren des DDNS Dienstes
DDNS Typ	Wählen Sie den DDNS-Dienstleister aus der Liste aus, bei dem Sie sich registriert haben .
Benutzername	Geben Sie hier Ihren Benutzernamen ein
Kennwort	Geben Sie hier Ihr Passwort ein
Host-Name	Geben Sie hier Ihren zugewiesenen Domain Namen ein
Aktion	Änderung sofort Aktualisieren

## 5.5 MAC- Adresseinrichtung

Einige Internet-Anbieter erlauben nur mit einer registrierten MAC- Adresse auf das Internet zuzugreifen. Um diese Regelung zu umgehen, müssen Sie eine geklonte MAC- Adresse mittels einer bereits registrierten MAC- Adresse hier einrichten

1. Klicken Sie auf [Setup] - [MAC Adresse Klonen]. Folgendes Fenster öffnet sich.:

The screenshot shows two configuration panels. The top panel is titled "MAC Adresse Klonen - WAN 1" and contains the text "Kopieren der MAC-Adresse des externen Netzes" with radio buttons for "aktivieren" (unselected) and "deaktivieren" (selected). Below this is a label "MAC-Adresse" and an empty text input field. The bottom panel is titled "MAC Adresse Klonen - LAN 1" and contains the same text and radio buttons. Below this is a label "MAC-Adresse" and a text input field with a light grey background.

2. Konfigurieren Sie die MAC Adresse entsprechend den folgenden Anweisungen.:

Kopieren der MAC-Adresse des externen Netzes	Wenn Ihr ISP eine Verbindung nur mit einer festen MAC-Adresse gewährt, wähl klicken Sie auf „aktivieren“ . Sonst lassen Sie die Einstellung auf „deaktivieren“
MAC-Adresse	Wenn der zur Zeit genutzte PC die richtige MAC Adresse besitzt um auf das Internet zu zugreifen, klicken Sie auf „Get Current PC MAC-Adress“ . Oder Sie geben die MAC Adresse manuell ein..

Mit Hilfe von "MAC Adresse Klonen-LAN1", kann die LAN MAC eingestellt warden.

# KAPITEL6 Einrichtung des WLAN

## 6.1 Einführung

Multiple SSIDs geben Ihnen die Möglichkeit für getrennte Sicherheits- und Schlüsseinstellungen, für einen besseren Komfort und einen verstärkten Schutz. Sie können Ihre Clients so konfigurieren, dass sie auf die erste SSID mit WPA2 PSK (Pre-Shared Key- Zugang) und geheimen Schlüssel zugreifen, während sie, mit einem Besucher Benutzerkonto auf die zweite SSID mit WEP und regelmäßig wechselndem Schlüssel zugreifen. Darüber hinaus sind Sie in der Lage, diese SSIDs zu isolieren, um böswilligen WLAN Angriffen vorzubeugen und Diese zu verhindern, weiterhin bestimmte Zugänge für Besucher, welche die zweite SSID nutzen, zu sperren. Dieses bietet Ihnen dann einen höchst komfortablen, gemeinsamen, drahtlosen (WLAN) Netzzugang, während Sie über einen stabilen und effizienten Schutz Ihres drahtlosen Netzwerkes (WLAN) verfügen.

### 6.1.1 Grundeinstellungen

1. Klicken Sie auf [Wireless] - [Basic]. Folgendes Fenster öffnet sich:

**WLAN 1**

Wireless-Verbindung	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Wireless-Modus	B/G/N Mixed
Sendeleistung	100%
Kanäle	Channel 6 [2.437GHz]
Wireless Isolation zwischen SSIDs	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren

**WLAN 1 - SSID 1**

Wireless Netzwerk-SSID	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Wireless Netzwerk-SSID-Namen	AXIMCom1
Wireless SSID Ausstrahlung	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Wireless Multimedia (WMM)	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Wireless Isolation	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren
Verschlüsselungs-Typ	deaktivieren

**WLAN 1 - SSID 2**

Wireless Netzwerk-SSID	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren
Wireless Netzwerk-SSID-Namen	AXIMCom2
Wireless SSID Ausstrahlung	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Wireless Multimedia (WMM)	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Wireless Isolation	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren
Verschlüsselungs-Typ	deaktivieren

2. Konfigurieren Sie das WLAN entsprechend den folgenden Anweisungen:.

Wireless-Verbindung	Aktivieren / Deaktivieren des drahtlosen Netzwerkes (WLAN)
Wireless-Modus	Wählen Sie hier den Übertragungsstandard aus (b/g/n oder mixed, so dass Client PCs mit unterschiedlichem Übertragungsstandard auf das WAN / Internet zugreifen können)
Sendeleistung	Wählen Sie hier die Übertragungsleistung aus (10 %, 25 %, 50 %, 75 %, oder 100 %)
Kanäle	Stellen Sie hier den Übertragungskanal, welcher genutzt werden soll, ein
Wireless Isolation zwischen SSIDs	Aktivieren Sie diese Funktion, wenn Sie den Zugriff von einer SSID auf die Andere unterbinden wollen. Deaktivieren Sie diese Funktion, wenn Sie Dieses erlauben möchten

## 6.1.2 Einrichten der SSID (Service-Set-Identifizier-ID)

Benutzer können jede SSID separat konfigurieren. Weiterhin stehen Ihnen verschiedene Sicherheits-Modi zur Verfügung, die Sie basierend auf Ihren Bedürfnissen einrichten und konfigurieren können: Deaktiviert, WEP, WPA Pre-Shared Key, WPA, WPA2 Pre-Shared Key und WPA2.

(Hinweis: Es ist jedoch wichtig zu beachten, dass alle Clients in diesem drahtlosen Netzwerk die gleichen Sicherheitseinstellungen verwenden müssen.)

Sie können die Sicherheitseinstellungen Ihres drahtlosen Netzwerks Ihren gewünschten Vorgaben entsprechend anpassen. Verschiedene Methoden gewähren unterschiedliche Sicherheitsstufen. Beim Einsatz von Verschlüsselung werden Datenpakete vor der Übertragung verschlüsselt, das verhindert somit das Auslesen von, das Eindringen in und das Verändern von Datenpaketen.

(Hinweis: Beachten Sie, dass je höher die Sicherheitseinstellungen, desto geringer wird der Datendurchsatz sein.)

1. Klicken Sie auf [Wireless] - [Basic]. Folgendes Fenster öffnet sich:.

The screenshot displays a configuration window for wireless settings, organized into three main sections:

- Wireless-Modus:** B/G/N Mixed (dropdown)
- Sendeleistung:** 100% (dropdown)
- Kanäle:** Channel 6 [2.437GHz] (dropdown)
- Wireless Isolation zwischen SSIDs:**  aktivieren  deaktivieren

**WLAN 1 - SSID 1**

- Wireless Netzwerk-SSID:  aktivieren  deaktivieren
- Wireless Netzwerk-SSID-Namen: AXIMCom1 (text input)
- Wireless SSID Ausstrahlung:  aktivieren  deaktivieren
- Wireless Multimedia (WMM):  aktivieren  deaktivieren
- Wireless Isolation:  aktivieren  deaktivieren
- Verschlüsselungs-Typ: deaktivieren (dropdown menu is open, showing options: deaktivieren, WEP, WPA PSK (Pre-Shared Key), WPA (Radius), WPA2 PSK (Pre-Shared Key), WPA2 (Radius))

**WLAN 1 - SSID 2**

- Wireless Netzwerk-SSID:  aktivieren  deaktivieren
- Wireless Netzwerk-SSID-Namen: AXIMCom2 (text input)
- Wireless SSID Ausstrahlung:  aktivieren  deaktivieren
- Wireless Multimedia (WMM):  aktivieren  deaktivieren
- Wireless Isolation:  aktivieren  deaktivieren
- Verschlüsselungs-Typ: deaktivieren (dropdown)

2. Konfigurieren Sie die SSIDs entsprechend den folgenden Anweisungen:

Wireless Netzwerk-SSID	Aktivieren / Deaktivieren der SSID
Wireless Netzwerk-SSID-Namen	Geben Sie hier den Stationsnamen ein, den Sie verwenden möchten.
Wireless SSID Ausstrahlung	<p>Der AXIMCom Mobile Router sendet die SSID periodisch. Sie können diese Funktion hier Aktivieren / Deaktivieren</p> <p>Die Aktivierung dieser Funktion dient nur dem Komfort des Client PC Nutzers, da er das drahtlose Netzwerk (WLAN) und diesen Router einfacher finden kann, um sich dann mit Diesem zu verbinden.</p> <p>Eine Deaktivierung dieser Funktion dient der Sicherheit und kann im ersten Schritt unberechtigtem Zugriff auf das drahtlose Netzwerk und den Router vorbeugen.</p>
Wireless Multimedia (WMM)	Aktivieren Sie diese Option um den Datenverkehr, anhand seiner Merkmale zu priorisieren. Zum Beispiel: VoIP- oder Mediendatenverkehr hat eine höhere Priorität gegenüber gewöhnlichen Datenverkehr.
Wireless Isolation	Aktivieren Sie diese Option, wenn Sie möchten, das der Zugriff auf andere Netzwerk-Geräte ueber diese SSID deaktiviert wird. Deaktivieren Sie diese Funktion, wenn Sie den Zugriff erlauben möchten
Verschlüsselungs-Typ	Wählen Sie den gewünschten Verschlüsselungs-Typ (WEP, WPA, WPA2)

### 6.1.3 WEP (Wired-Equivalent-Privacy) Sicherheitseinstellungen

**WLAN 1 - SSID 1**

Wireless Netzwerk-SSID  aktivieren  deaktivieren

Wireless Netzwerk-SSID-Namen

Wireless SSID Ausstrahlung  aktivieren  deaktivieren

Wireless Multimedia (WMM)  aktivieren  deaktivieren

Wireless Isolation  aktivieren  deaktivieren

Verschlüsselungs-Typ

ID des bevorzugten Schlüssels

Schlüssel 1

Schlüssel 2

Schlüssel 3

Schlüssel 4

(WEP-Schlüssel für 5 oder 13 ASCII-String, oder 10 oder 26 hexadezimale Zeichenfolge)

Wenn WEP aktiviert wird, muss der WEP-Index und der Schlüssel manuell eingestellt werden..

ID des bevorzugten Schlüssels	Der WEP Key Index (1-4) gibt an, welcher WEP-Schlüssel zur Verschlüsselung von Daten verwendet wird.
Schlüssel (1-4)	64-Bit-WEP: Geben Sie 10 hexadezimale Ziffern oder 5 ASCII-Zeichen ein. 128-Bit-WEP: Geben Sie 26 hexadezimale Ziffern oder 13 ASCII Zeichen ein.

#### 6.1.4 WPA Pre-Shared Key / WPA2 Pre-Shared Key Sicherheitseinstellungen

**WLAN 1 - SSID 1**

Wireless Netzwerk-SSID	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Wireless Netzwerk-SSID-Namen	<input type="text" value="AXIMCom1"/>
Wireless SSID Ausstrahlung	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Wireless Multimedia (WMM)	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Wireless Isolation	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren
Verschlüsselungs-Typ	<input type="text" value="WPA PSK (Pre-Shared Key)"/>
Schlüssel	<input type="text"/>
Verschlüsselungs-Methode	<input type="text" value="TKIP"/>

(Encryption Key als ASCII-String von 8 bis 63 Zeichen oder 64 hexadezimale Zeichenfolge.)

Wenn Sie WPA Pre-shared Key oder WPA2 Pre-shared Key wählen, muss der Pre-shared Key eingestellt werden

Pre-shared Key	Der Pre-shared Key dient als Qualifikationsnachweis für die Paket-Verschlüsselung
Encryption Mode	TKIP/AES wird unterstützt.

## 6.1.5 WPA (Wi-Fi-Protected-Access) / WPA2 Sicherheitseinstellungen

**WLAN 1 - SSID 1**

Wireless Netzwerk-SSID  aktivieren  deaktivieren

Wireless Netzwerk-SSID-Namen

Wireless SSID Ausstrahlung  aktivieren  deaktivieren

Wireless Multimedia (WMM)  aktivieren  deaktivieren

Wireless Isolation  aktivieren  deaktivieren

Verschlüsselungs-Typ

Schlüssel

Verschlüsselungs-Methode

(Encryption Key als ASCII-String von 8 bis 63 Zeichen oder 64 hexadezimale Zeichenfolge.)

**WLAN 1 - SSID 1**

Wireless Netzwerk-SSID  aktivieren  deaktivieren

Wireless Netzwerk-SSID-Namen

Wireless SSID Ausstrahlung  aktivieren  deaktivieren

Wireless Multimedia (WMM)  aktivieren  deaktivieren

Wireless Isolation  aktivieren  deaktivieren

Verschlüsselungs-Typ

Radius-Server IP-Adresse

Radius-Server-Port

Radius Schlüssel

Verschlüsselungs-Methode

Rekey-Methode

Rekey Zeitintervall

Rekey Paketintervall

(Encryption Key als ASCII-String von 8 bis 63 Zeichen oder 64 hexadezimale Zeichenfolge.)

Wenn WPA oder WPA2 ausgewählt wird, sollte die Radiusserver Informationen dementsprechend eingegeben werden.

Radius-Server IP-Adresse	Geben Sie die IP- Adresse des RADIUS- Server hier ein
Radius-Server-Port	Geben Sie die Anschluss-Nummer des RADIUS- Server hier ein. Die Standard-Anschluss Nummer ist 1812
Radius Schlüssel	Geben Sie hier den Radius-Schlüssel ein
Verschlüsselungs-Methode	Wählen Sie hier TKIP oder AES für die Datenpaketverschlüsselung aus

## 6.2 Erweiterte Einstellungen

1. Klicken Sie auf [Wireless] - [Fortgeschritten]. Folgendes Fenster öffnet sich:

**Regionale Einstellung**

Region Vereinigten Staaten, Kanada, Taiwan (Kanal 1 - 11) ▾

---

**WLAN 1**

Fragmentation	<input type="text" value="2346"/> Bytes (256 ~ 2346)
RTS	<input type="text" value="2347"/> Sekunden (1 ~ 2347)
DTim	<input type="text" value="1"/> (1 ~ 255)
Beacon Interval	<input type="text" value="100"/> Millisekunden (20 ~ 1024)
Header Preamble	<span>Lang ▾</span>
Tx-Modus	<span>None ▾</span>
MPDU	<input type="text" value="4"/> <span>▾</span> Mikrosekunden
MSDU Aggregate	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren
Tx Burst	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Packet Aggregate	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
HT Control-Feld	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Reverse Direction Grant	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Link Adapt	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren
Short Guard Interval(GI)	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Operation Modus	<span>Mixed Mode ▾</span>
HT-Bandbreite	<input type="text" value="20/40"/> <span>▾</span> MHz
Block Ack Setup Automatically	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Block Ack Window Size	<input type="text" value="64"/> x16 Bits (1 ~ 64)
Reject Block Ack	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren
MCS	<span>Automatischer Modus ▾</span>

2. Konfigurieren Sie die Einstellungen entsprechend den folgenden Anweisungen:

Region	Wählen Sie die Region aus in der Sie sich gerade befinden
Fragmentation	Geben Sie die hier die Fragmentierungsgröße in Bytes ein. Der Standardwert ist 2346 Bytes
RTS	Geben Sie den RTS (Request To Send) Wert in Sekunden ein. Der Standardwert ist 2347 Sekunden
DTim	Geben Sie den DTIM (Delivery Indication Message) Wert in Sekunden ein. Der Standardwert ist 1
Beacon Interval	Geben Sie hier das Intervall für das Senden eines Beacon (Das Intervall zwischen 2 Signal Frames) ein. Der Standardwert ist 100 Millisekunden
Header Preamble	Wählen Sie hier zwischen Long oder Short Header Präambel
TxMode	Stellen Sie hier den „diversity“ Wert ein: -1, 0, 1 oder 3
MPDU	Wählen Sie hier den Übertragungsmodus aus. Der CCK Modus ist kompatibel zu IEEE 802.11b, OFDM ist kompatibel zu IEEE 802.11g
MSDU Aggregate	Wählen Sie hier die Länge der MPDU (MAC Protocol Data Unit) Nachricht aus. größere Werte erhöhen die Effizienz, aber nur bei unterstützten Modellen. Generell ist ein Wert von 4 einzugeben
Tx Burst	Aktivieren / Deaktivieren. Wenn aktiviert, können mehrere MSDU zu einer Paketübertragung kombiniert werden. Das erhöht die Effizienz, ist aber nicht kompatibel zu älteren Netzwerkadaptern und Treibern
Packet Aggregate	Aktivieren / Deaktivieren. Aktivieren Sie diese Funktion wenn Sie über einen IEEE 802.11g kompatiblen Netzwerkadapter verfügen. Die Aktivierung kann die Übertragungsgeschwindigkeit erhöhen, führt aber auch zu einem höheren Energieverbrauch
HT Control Field	Aktivieren / Deaktivieren. Ähnlich der A-MSDU Funktion werden hier mehrere Pakete im drahtlosen Netzwerk zu einer Übertragungseinheit zusammengefasst. Der verwendete Netzwerkadapter muss diese Funktion jedoch ausdrücklich unterstützen
Reverse Direction Grant	Aktivieren / Deaktivieren. Diese Funktion wird für High-End Netzwerkadapter oder für das Debugging / Fehlersuche benötigt. Diese Funktion ist normalerweise deaktiviert
Link Adapt	Aktivieren / Deaktivieren. Die Antwortzeiten reduzieren sich im drahtlosen Netzwerk. Die Kompatibilität mit den eingesetzten Netzwerkadaptern muss aber zuvor sichergestellt worden sein
Short Guard Interval (SGI)	Aktivieren / Deaktivieren. Aktivieren Sie diese Funktion wenn die drahtlosen Geräte die Modulationsart und den "Code" dynamisch ändern. . Die

	Kompatibilität mit den eingesetzten Netzwerkadaptern muss aber zuvor sichergestellt worden sein
Operation Mode	Aktivieren / Deaktivieren. Ist diese Funktion aktiviert, wird das SGI den Systemverwaltungs- Overhead reduzieren und somit die Systemeffizienz erhöhen
HT Band Width	Wählen Sie zwischen "Mixed mode" und "Greenfield" Übertragungsmodus aus. Wenn Sie "Greenfield" auswählen kann die IEEE 802.11n Übertragungsrate ansteigen , aber die Kompatibilität zu einigen IEEE 802.11g und IEEE 802.11n drahtlosen Netzwerkadaptern kann sinken
Block Ack Setup Automatically	Wählen Sie hier das Übertragungsfrequenzband aus: HT20MHz oder HT20/40MHz
Block Ack Window Size	Aktivieren / Deaktivieren. Aktivieren Sie diese Funktion um die Übertragungsleistung zu erhöhen, die Antwortzeiten können sich jedoch etwas verlängern
Reject Block Ack	Legen Sie hier die ACK Blockgröße fest
MCS	Aktivieren / Deaktivieren. Aktiviert, wird das ACK Signal anderer drahtloser Netzwerkgeräte ignoriert.

## 6.3 Einrichtung des WDS (Wireless Distributed System)

WDS (Wireless Distributed System) ermöglicht die drahtlose Verbindung (Wireless bridging) zwischen mehreren drahtlosen Geräten. Die drahtlosen Geräte werden durch die WDS MAC- Adresse identifiziert.

1. Klicken Sie auf [Wireless] - [WDS]. Folgendes Fenster öffnet sich:

### Wireless - WDS

The screenshot displays the 'Wireless - WDS' configuration window. It is divided into several sections:

- WLAN 1:** WDS-Modus is set to 'Repeater-Modus (AP aktiviert)'.
- WDS 1:** WDS MAC-Adresse is an empty text field; Verschlüsselungs-Typ is 'deaktivieren'.
- WDS 2:** WDS MAC-Adresse is an empty text field; Verschlüsselungs-Typ is 'deaktivieren'.
- WDS 3:** WDS MAC-Adresse is an empty text field; Verschlüsselungs-Typ is 'deaktivieren'.
- WDS 4:** WDS MAC-Adresse is an empty text field; Verschlüsselungs-Typ is 'deaktivieren'.

At the bottom of the window are two buttons: 'Einstellungen speichern' and 'Stornieren'.

2. Konfigurieren Sie die WDS Einstellungen entsprechend den folgenden Anweisungen:

WDS	Aktivieren / Deaktivieren der WDS Funktion
WDS MAC-Adresse [1-4]	Geben Sie die MAC- Adressen der anderen "bridged wireless" Geräte an. Maximal 4 Geräte können "gebridged" werden.

Hinweis: Bitte stellen Sie sicher, dass die folgenden Einstellungen richtig sind, damit das WDS effektiv arbeiten kann:

(1) Alle WDS Geräte müssen den gleichen Funkkanal (Wireless Channel) verwenden.

(2) Alle WDS Geräte müssen die gleiche Verschlüsselung und den gleichen Schlüssel-Modus verwenden.

Bitte beachten Sie: Wenn eine der oben genannten Funktionen nicht ordnungsgemäß eingestellt ist, können die WDS Geräte nicht miteinander kommunizieren!

## 6.4 Einrichtung des Repeater Modus

Die Universal Repeater Funktion ist ähnlich der des WDS, da sie im wesentlichen verwendet wird um die drahtlose Netzabdeckung zu erweitern. Doch anders als WDS ist die Universal Repeater Funktion einfacher einzurichten, da Sie nur den aktuellen AP (Access Point) als Client einrichten müssen, um ihn dann mit der SSID (oder BSSID) des zweiten AP (Access Point) zu verbinden. Allerdings müssen Sie sicherstellen, dass die beiden APs über den gleichen Funkkanal und Sicherheits-Modus (sowie Schlüssel) verfügen, damit die Universal Repeater Funktion effektiv arbeiten kann.

1. Click on [Wireless] – [Universal Repeater] tab. You will see the following screen.

### Wireless - Universal Repeater

WLAN 1

Universal Repeater aktivieren  aktivieren  deaktivieren

Ziel SSID

Ziel BSSID (MAC)

Kanäle

Site Survey

Verschlüsselungs-Typ

2. Configure universal repeater settings following the instructions below.

Universal Repeater aktivieren	Aktivieren / Deaktivieren der Universal Repeater Funktion
Ziel SSID	Geben Sie die Ziel SSID des APs ein, mit dem eine Verbindung aufgebaut werden soll
Ziel BSSID (MAC)	Geben Sie die Ziel BSSID des APs ein, mit dem eine Verbindung aufgebaut werden soll. Diese Einstellung ist optional und wird nur benötigt wenn keine Ziel SSID eingegeben wurde
Kanäle	Die verwendbaren Kanäle
Site Survey	Ein Pop-Up Fenster öffnet sich und Sie können die SSID wählen
Verschlüsselungs-Typ	Stellen Sie hier den Sicherheitsmodus des Ziel AP ein, und geben, wenn nötig den Schlüssel ein

# KAPITEL7 Sicherheitseinstellungen

## 7.1 Die Firewall Einstellungen

1. Klicken Sie auf [Security] - [Firewall]. Folgendes Fenster öffnet sich:

### Sicherheit - Firewall

Firewall-Schutz	
SPI-Firewall-Schutz	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
TCP SYN DoS-Schutz	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
ICMP Broadcasting Protection	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
ICMP Redirect Protection	<input checked="" type="radio"/> aktivieren <input type="radio"/> deaktivieren
Broadcast Storming	<input type="radio"/> aktivieren <input checked="" type="radio"/> deaktivieren

2. Konfigurieren Sie die Firewall entsprechend den folgenden Anweisungen:

SPI Firewall-Schutz	Aktivieren / Deaktivieren der SPI Firewall
TCP SYN DoS-Schutz	<p>Aktivieren / Deaktivieren des TCP SYN DoS Schutzes</p> <p>TCP SYN DoS Angriffe senden eine Flut von TCP / SYN-Paketen. Jedes dieser Pakete arbeitet wie eine Verbindungsanfrage, so dass der Server sehr viele Ressourcen (zB. CPU, Speicher) benötigt um zu antworten und kontinuierlich auf die eingehenden Pakete zuwarten.</p> <p>Ohne TCP SYN DoS Schutz, werden die Ressourcen des Server nahezu vollständig verbraucht. Dieses wird dann in Folge zum Versagen des Server führen.</p> <p>Der AXIMCom Mobile Router ist in der Lage TCP SYN DoS Angriffe zu erkennen und den Ressourcenverbrauch, durch eine Minderung der eingehenden Anfragerate, zu senken. Daher ist der AXIMCom Mobile Router weiterhin in der Lage den normalen Datenverkehr zu steuern, während ein solcher Angriff erfolgt.</p>

<p>ICMP Broadcasting Protection</p>	<p>Aktivieren / Deaktivieren des ICMP Broadcasting Schutzes</p> <p>Der ICMP Broadcast Angriff ist eine Art DoS Angriff. Eine Flut von ICMP Broadcast Paketen wird generiert und an einen Server geschickt (zB. AXIMCom Mobile Router). Folglich wird dieser Server unter einer großen Menge an Unterbrechungen und dem Verbrauch von Rechenleistung leiden.</p> <p>Der AXIMCom Mobile Router ist in der Lage nicht mehr auf diese ICMP Broadcast Echo Pakete zu antworten, um einen potenziellen ICMP Broadcast DoS Angriff zu verhindern.</p>
<p>ICMP Redirect Protection</p>	<p>Aktivieren / Deaktivieren des ICMP Redirect Schutzes</p> <p>Eine ICMP Redirect Message ist ein Weg, den vorhandenen Routing-Pfad zu ändern. Generell sollten ICMP Redirect Pakete nicht gesendet werden, und falls ICMP Redirect Pakete gesendet werden, so ist es wichtig zu beachten, dass es sich sehr wahrscheinlich um einen Angriff auf das Netzwerk handelt.</p>
<p>Broadcast Storming</p>	<p>Aktivieren um "broadcast storming" zu verhindern.</p>

## 7.2 Einrichtung der ACL (Access-Control-List) Zugriffskontrolle

### 7.2.1 ACL Einstellungen

1. Klicken Sie auf [Sicherheit] - [Zugriffskontrolle]. Folgendes Fenster öffnet sich:

Hinweis: Ändern Sie diese Einstellungen nur wenn Sie mit der ACL Funktion vertraut sind und diese Funktion Ihren Bedürfnissen anpassen müssen!

#### Sicherheit - Zugangskontrolle

2. Konfigurieren Sie die ACL Funktion entsprechend den folgenden Anweisungen:

Zugangskontrolle	Aktivieren / Deaktivieren der ACL Funktion
Standard-Zugriffskontrolle	<p>Aktivieren Sie eine bestimmte MAC Filter Regel</p> <p>Deaktivieren Sie eine bestimmte MAC Filter Regel</p> <p>Geben Sie die MAC Adresse des Clients ein, dem Sie erlauben auf das Netzwerk zuzugreifen.</p> <p>* Die Aktivierung der MAC Filterung sperrt alle MAC Adressen, die nicht in den MAC Filter Regeln aufgeführt sind. Seien Sie sich bewusst, dass die MAC Adresse Ihres Computers zum Zugriff auf den AXIMCom Mobile Router und zur Verwaltung des Router erforderlich ist!</p>

3. Konfigurieren Sie die [Hinzufügen] ACL Einstellungen entsprechend den folgenden Anweisungen::

Lfd. Nummer	<input type="text" value="4"/>
Regel Name	<input type="text"/>
Regel aktivieren	<input checked="" type="checkbox"/>
Externe Schnittstelle	<input type="text" value="WAN1"/>
Interner IP-Bereich	Von: <input type="text"/> Zu: <input type="text"/>
Externer IP-Bereich	Von: <input type="text"/> Zu: <input type="text"/>
Protokoll	<input type="text" value="*"/>
Service Port Bereich	Von: <input type="text"/> Zu: <input type="text"/>
Aktion	<input type="text" value="Erlauben"/>

Lfd. Nummer	Dies definiert die Reihenfolge der ACL-Regeln. Wenn ein Paket den Bedingungen der ACL-Regeln entspricht, wird das Paket dann nach der ersten ACL-Regel in der Liste sortiert werden
Regel Name	Geben Sie hier einen Namen für die ACL-Regel ein
Regel aktivieren	Markieren Sie dieses Kästchen um die Regel zu aktivieren
Externe Schnittstelle	Wählen Sie die externe Schnittstelle (WAN1 oder WAN2) die ein Paket passieren soll, wenn es den Bedingungen dieser ACL-Regel entspricht
Interner IP-Bereich	Legen Sie hier den internen IP-Adressbereich für diese Regel fest
Externer IP-Bereich	Legen Sie hier den externen IP-Adressbereich für diese Regel fest
Protokoll	Legen Sie hier das Übertragungsprotokoll (TCP oder UDP) fest für das die Regel aktiviert sein soll
Service Port Bereich	Richten Sie den Service Port Bereich ein (z. B. HTTP ist TCP/80), für den die Regel aktiviert sein soll
Aktion	Wählen Sie hier Zugriff Zulassen / Verweigern als Regelziel

#### 4. Beispiel: Filterung und Blockierung der MSN Messenger Nutzung

Ein Unternehmen will zum Beispiel Ihren Angestellten nicht erlauben den MSN Messenger am Arbeitsplatz zu nutzen. Der Administrator kann nun eine ACL Regel generieren die diesen Datenverkehr zur externen IP Adresse 207.46.110.\* /24 unterbindet.

Regel Name	MSN-Sperren
Regel aktivieren	Enabled (Aktiviert)
Externe Schnittstelle	* (All complies) (alle WAN Zugänge entsprechend)
Interner IP-Bereich	--leer-- (Alle IP Adressen entsprechend)
Externer IP-Bereich	207.46.110.1:207.46.110.1.254 (IP Adressbereich für MSN Messenger Dienst)
Protokoll	TCP
Service Port Bereich	--leer-- (Alle Anschluss (Port) Adressen entsprechend)
Aktion	Deny (Verweigern)

## 7.3 MAC Adress Steuerung

1. Klicken Sie auf [Sicherheit] - [MAC Access Control]. Folgendes Fenster öffnet sich:

### Sicherheit - MAC Access Control

2. Konfigurieren Sie die MAC Adresssteuerung entsprechend den folgenden Anweisungen:

MAC Access Control	Aktivieren / Deaktivieren der MAC- Adresssteuerung
Standard MAC Zugriffskontrolle	Hier legen Sie das Regelziel fest: Verbindung erlauben (ALLOW) oder verweigern (Deny)

3. Klicken Sie auf [Add]. Folgendes Fenster öffnet sich:

Lfd. Nummer	Hier definieren Sie die Priorität der Regel
Regel Name	Hier geben Sie einen Namen für die Regel ein
MAC	Geben Sie hier die MAC Adresse des Clients ein, der Ziel dieser Regel ist
Aktion	Hier legen Sie das Regelziel fest: Verbindung erlauben (ALLOW) oder verweigern (Deny)
ACL aktivieren	Markieren Sie dieses Kästchen um die Regel zu aktivieren
Static ARP aktivieren	Markieren Sie dieses Kästchen um die MAC Adresse entsprechend dem statischen ARP Eintrag zu verwenden
Static DHCP aktivieren	Markieren Sie dieses Kästchen um die MAC Adresse entsprechend dem statischen DHCP Eintrag zu verwenden
IP	Die dem statischen ARP / DHCP entsprechende IP-Adresse

4. Beispiel einer MAC Adressregel

1:1 Mapping, MAC Adresse eines Client zu einer IP Adresse. Diese Einstellung gibt dem Client eine statische IP Adresse bei der Verbindung zum Router.

Lfd. Nummer	User1
Regel Name	Enable
MAC	00:33:44:55:66:77
Aktion	Allow Access
ACL aktivieren	Enable
Static ARP aktivieren	Enable
Static DHCP aktivieren	Enable
IP	192.168.1.100

## 7.4 Lokale Einrichtung des Open-DNS

### 7.4.1 OpenDNS-Einstellungen

1. Klicken Sie auf [Sicherheit] - [OpenDNS]. Folgendes Fenster öffnet sich:

#### Sicherheit - OpenDNS

OpenDNS - WAN 1

OpenDNS Service  aktivieren  deaktivieren

OpenDNS-Benutzername

OpenDNS Passwort

Abfrageumleitung zum OpenDNS DNS Server  aktivieren  deaktivieren

OpenDNS Label

2. Konfigurieren Sie die OpenDNS Einstellungen entsprechend den folgenden Anweisungen:

OpenDNS Service	Aktivieren / Deaktivieren des OpenDNS Dienstes
OpenDNS-Benutzername	Der vom OpenDNS Dienstleister bereitgestellte Benutzername
OpenDNS Passwort	Das vom OpenDNS Dienstleister bereitgestellte Kennwort
Abfrageumleitung zum OpenDNS DNS Server	Aktivieren oder deaktivieren Sie hier die DNS Abfrageumleitung zum OpenDNS DNS Server.
OpenDNS Label	Geben Sie hier den Namen für Ihr Netzwerk ein, den Sie auch bei der Registrierung des OpenDNS Dienstes eingegeben haben.

Hinweis: Informationen zur Registrierung bei einem Open DNS Dienstleister finden Sie im Anhang dieser Bedienungsanleitung!

## 7.5 Internetfilter

1. Klicken Sie auf [Sicherheit] - [Web Filtering]. Folgendes Fenster öffnet sich:

### Sicherheit - Web Filtering

**Web Filtering**

Web Filtering  aktivieren  deaktivieren

**Web Content Filtering**

ActiveX-Filter  aktivieren  deaktivieren

Java / JavaScript-Filterung  aktivieren  deaktivieren

Proxy-Filter  aktivieren  deaktivieren

**Web Filter Regeln**

Regel aktivieren	Keyword Filter	Filtertyp	Aktion
<input type="button" value="Hinzufügen"/>	<input type="button" value="Löschen"/>	<input type="button" value="Bearbeiten"/>	<input type="button" value="Auf"/> <input type="button" value="Ab"/>

2. Konfigurieren Sie die Filtereinstellungen entsprechend den folgenden Anweisungen:

Web Filtering	Aktivieren / Deaktivieren des WEB Filters
ActiveX-Filter	Aktivieren / Deaktivieren des ActiveX Filters
Java / JavaScript-Filterung	Aktivieren / Deaktivieren des Java Filters
Proxy-Filter	Aktivieren / Deaktivieren des Proxy Filters

## 7.5.1 Einen neuen Internetfilter hinzufügen

1. Klicken Sie auf [Hinzufügen]. Folgendes Fenster öffnet sich:

The screenshot shows a configuration window for an Internet filter. It contains the following fields and controls:

- Lfd. Nummer:** A text input field containing the number '1'.
- Regel aktivieren:** A checkbox that is currently unchecked.
- Keyword Filter:** A text input field containing 'web-page-name'.
- Filtertyp:** A dropdown menu with 'Webseite' selected.
- Aktion:** A dropdown menu with 'Verweigern' selected.
- Buttons:** Two buttons at the bottom: 'Bestätigen' (Confirm) and 'Stornieren' (Cancel).

2. Konfigurieren Sie den Filter entsprechend den folgenden Anweisungen:

Lfd. Nummer	Hier definieren Sie die Priorität des Filters. Wenn mehr als ein Datenpaket die Bedingungen der Internetfilterregeln trifft, wird zuerst das Datenpaket verarbeitet das die Regel mit der höchsten Priorität erfüllt
Regel aktivieren	Aktivieren oder deaktivieren Sie hier die Regel
Keyword Filter	Hier können Sie Schlüsselwörter eingeben um das Ziel des Filters zu spezifizieren
Filtertyp	Wählen Sie hier zwischen Website oder Host
Aktion	Hier legen Sie das Filterziel fest: Verbindung erlauben oder verweigern

3. Beispiel eines Internetfilters

Um zum Beispiel die Internetseite von Facebook zusperrern, müssen Sie die Regel aktivieren, als Schlüsselwort facebook eingeben, den Filtertyp auf url setzen und die Verbindung verweigern (Aktion > Verweigern)

Lfd. Nummer

Regel aktivieren



Keyword Filter

Filtertyp

Webseite ▾

Aktion

Verweigern ▾

Bestätigen

Stornieren

# KAPITEL8 Anwendungseinstellungen

## 8.1 Einführung in die Port-Range-Forward Funktion

Durch Aktivierung der Port-Bereich Forwarding Funktion erhalten Remote- Benutzer Zugriff auf das lokale Netzwerk über die öffentliche IP- Adresse. Sie können einen bestimmten externen Anschlussbereich einem lokalen Server zuweisen. Darüber hinaus können Sie einen internen Anschlussbereich, welcher einer Port Forwarding Regel zugeordnet ist, angeben. Wenn der AXIMCom Mobile Router eine externe Anfrage erhält, auf einen konfigurierten externen Anschluss Zugriff zu gewähren, wird der Router die Anfrage an den entsprechenden internen Server umleiten und den Ziel-Anschluss zu dem angegebenen internen Anschluss hin ändern. Wenn Sie nicht wünschen das der Zielanschluss für eine Verbindungsanfrage geändert wird, lassen Sie den internen Anschlussbereich leer.

Bestimmte Anwendungen in einem LAN sind erst nach Aktivierung des Port Range Forwarding verfügbar, einschließlich Server und Online- Gaming. Wenn eine Internetanfrage auf einen Anschluss zugreifen will, wird der AXIMCom Mobile Router diese and die angegebene IP- Adresse weiterleiten. Aus Sicherheitsgründen wird empfohlen, die Port Range Forwarding Verwendung zu begrenzen und zu deaktivieren, wenn die Anwendung nicht verwendet wird.

Indem Sie die DMZ Host Funktion aktivieren, können Sie einen DMZ-Host einem nun ungeschützten Client zuweisen. Auf diese Weise sind einige Anwendungen, vor allem Online-Spiele (wenn die Anschlussnummern der Anwendungen sich immer ändern), leichter zugänglich.

## 8.1.1 Port-Range-Forward Einstellungen

1. Klicken Sie auf [Anwendungen] - [Port Range Forward]. Folgendes Fenster öffnet sich:

### Anwendungen - Port Range Forward

**DMZ - WAN 1**

DMZ  aktivieren  deaktivieren

DMZ-IP-Adresse

**Regeln für spezielle Anwendungen**

Port Weiterleitung  aktivieren  deaktivieren

**Regeln für spezielle Anwendungen**

Regel Name	Regel aktivieren	Externe Schnittstelle	Protokol	Externer Port Bereich	Interne IP	Interner Port Bereich
HTTP	✘	WAN1	TCP	Von:80 Zu:80	192.168.1.20	Von: Zu:
HTTPS	✘	WAN1	TCP	Von:443 Zu:443	192.168.1.20	Von: Zu:
POP3	✘	WAN1	TCP	Von:110 Zu:110	192.168.1.20	Von: Zu:
POP3S	✘	WAN1	TCP	Von:995 Zu:995	192.168.1.20	Von: Zu:
SMTP	✘	WAN1	TCP	Von:25 Zu:25	192.168.1.20	Von: Zu:
SMTPS	✘	WAN1	TCP	Von:465 Zu:465	192.168.1.20	Von: Zu:
SSH	✘	WAN1	TCP	Von:22 Zu:22	192.168.1.21	Von: Zu:
eMule	✘	WAN1	TCP/UDP	Von:4662 Zu:4672	192.168.1.21	Von: Zu:

2. Konfigurieren Sie die DMZ Einstellungen entsprechend den folgenden Anweisungen:

DMZ	Aktivieren oder deaktivieren Sie hier die DMZ Funktion
DMZ-IP-Adresse	Geben Sie hier die IP- Adresse eines bestimmten lokalen Host in Ihrem LAN ein, der alle Pakete erhalten soll, welche ursprünglich an den WAN-Anschluss oder eine öffentliche IP- Adresse gehen sollten.

3. Konfigurieren Sie die Port Forwarding Einstellungen entsprechend den folgenden Anweisungen:

Port Weiterleitung Aktivieren oder deaktivieren Sie hier die Port Forwarding Funktion

### 8.1.2 Hinzufügen einer neuen Port-Range-Forward Regel

1. Klicken Sie auf [Hinzufügen]. Folgendes Fenster öffnet sich:

2. Konfigurieren Sie die Port Forwarding Regel entsprechend den folgenden Anweisungen:

Lfd. Nummer	Dies definiert die Reihenfolge der Port Forwarding -Regeln. Wenn ein Paket den Bedingungen der Port Forwarding -Regeln entspricht, wird das Paket dann nach der ersten Port Forwarding -Regel in der Liste sortiert werden
Regel Name	Geben Sie hier einen Namen für die Regel ein
Regel aktivieren	Markieren Sie dieses Kästchen um die Regel zu aktivieren
Externe Schnittstelle	Wählen Sie die externe Schnittstelle (WAN1 oder WAN2) für das Port Forwarding fest
Protokoll	Legen Sie hier das Übertragungsprotokoll (TCP oder UDP) fest für das die Regel angewendet werden soll
Externer Port Bereich	Legen Sie hier den externen Anschlussbereich fest, auf den die Regel angewandt wird.

Interne IP	Legen Sie hier die internen IP- Adresse fest, auf den die Regel angewandt wird.
Interner Port Bereich	Legen Sie hier den internen Anschlussbereich fest, auf den die Regel angewandt wird.

## 8.2 Einstellungen für Medien-Streaming / VPN

Sie können Ihre Media-Streaming Qualität verbessern, indem Sie die RTSP, MSS und H.323 Protokolle aktivieren. Darüber hinaus können Sie auch die VPN-Passthrough Funktion aktivieren

1. Klicken Sie auf [Anwendungen] - [Streaming / VPN]. Folgendes Fenster öffnet sich:

### Anwendungen - Streaming / VPN

The screenshot shows a configuration window titled "Anwendungen - Streaming / VPN". It is divided into three main sections, each with a header and a list of options with radio buttons for "aktivieren" (checked) and "deaktivieren".

- Streaming**
  - RTSP:  aktivieren  deaktivieren
  - MMS:  aktivieren  deaktivieren
- Video-Konferenz**
  - H.323:  aktivieren  deaktivieren
- VPN**
  - IPSec:  aktivieren  deaktivieren
  - PPTP:  aktivieren  deaktivieren

At the bottom of the window are two buttons: "Einstellungen speichern" and "Stornieren".

2. Konfigurieren Sie die Streaming Funktion entsprechend den folgenden Anweisungen:

RTSP	Aktivieren oder deaktivieren Sie hier RTSP
MMS	Aktivieren oder deaktivieren Sie hier MMS

3. Konfigurieren Sie die Video Conference Funktion entsprechend den folgenden Anweisungen:

H.323	Aktivieren oder deaktivieren Sie hier H.323
-------	---

4. Configure [VPN] Settings following the instructions below

IPSec	Aktivieren oder deaktivieren Sie hier IPsec Pass-Through
PPTP	Aktivieren oder deaktivieren Sie hier PPTP Pass-Through

## 8.3 UPnP (Universal Plug and Play) / NAT-PMP Einstellungen

1. Klicken Sie auf [Anwendungen] - [UPnP / NAT-PMP]. Folgendes Fenster öffnet sich:

### Anwendungen - UPnP / NAT-PMP

UPnP  aktivieren  deaktivieren

NAT-PMP  aktivieren  deaktivieren

UPnP Port

2. Konfigurieren Sie die Einstellungen entsprechend den folgenden Anweisungen:

UPnP	Aktivieren oder deaktivieren Sie hier UPnP
NAT-PMP	Aktivieren oder deaktivieren Sie hier NAT-PMP
UPnP Port	Geben Sie hier die Anschlussnummer für den UPnP- Anschluss ein

# KAPITEL9 Administration

## 9.1 Geräteverwaltung

1. Klicken Sie auf [Admin] - [Management]. Folgendes Fenster öffnet sich:

### Admin - Management

**Ethernet Anschluß**

Ethernet Anschluß LAN ▾

**Management-Schnittstelle**

Spracheinstellungen Deutsch ▾

Administrator-Passwort

Neues Passwort bestätigen

Remote-Management  aktivieren  deaktivieren

Management-Port HTTP 8080

**Reboot**

Reboot Neustart des Routers

**Konfiguration**

Speichern der Einstellungen Speichern

Werkseinstellungen wiederherstellen Standard

Laden der Einstellungen  Browse... Laden

**Firmware**

Firmware-Update  Browse...

Aktualisierung

Einstellungen speichern Stornieren

2. Konfigurieren Sie die Administration Interface Einstellungen entsprechend den folgenden Anweisungen:

Spracheinstellungen	Wählen Sie hier die Sprache der Administrationsoberfläche aus, die Sie benutzen wollen
Administrator-Passwort	Die maximale Passwortlänge beträgt 36 alphanumerische Zeichen (Groß- und Kleinschreibung) * Bitte ändern Sie das Kennwort des Administrators, wenn das Remote-Management aktiviert ist. Andernfalls kann ein böswilliger Nutzer Zugriff auf die Management-Schnittstelle erlangen. Dieser Benutzer hat dann die Möglichkeit, die Einstellungen zu ändern und Schäden an Ihrem Netzwerk zu verursachen.
Neues Passwort bestätigen	Geben Sie das Kennwort erneut ein.
Remote-Management	Aktivieren oder deaktivieren Sie hier die das „Remote Management“  Wenn aktiviert, können Benutzer, die nicht im LAN sind, mit dem AXIMCom Mobile Router Verbindung aufnehmen und es vom Internet aus konfigurieren.
Management-Port	HTTP- Anschluss, mit dem Benutzer Verbindung aufnehmen können. (Vorgabeanschluss ist 8080)

3. Sichern Sie Ihre Einstellungen, Importieren Sie sie oder stellen Sie diese wieder her:

Speichern der Einstellungen	Klicken Sie hier um die Konfigurationseinstellungen in eine Datei zu sichern
Werkseinstellungen wiederherstellen	Klicken Sie hier um die Vorgabeeinstellungen zu laden
Laden der Einstellungen	Klicken Sie hier um gesicherte Konfigurationseinstellungen wieder herzustellen

4. Das Firmware Upgrade:

Firmware-Update	Klick Sie hier um eine neue Firmwareversion aufzuspielen.
-----------------	---

## 9.2 Netzwerkdienstprogramme

1. Klicken Sie auf [Admin] - [System-Tools]. Folgendes Fenster öffnet sich:

### Admin - System-Tools

#### Ping

Schnittstelle

Ziel-Host

Anzahl Übertragungs-Pakete  Pakete (1 ~ 10)

Ping

#### ARPing (Innerhalb der gleichen Broadcast-Domain)

Schnittstelle

Ziel-Host

Anzahl Übertragungs-Pakete  Pakete (1 ~ 10)

ARPing

#### Trace Route

Schnittstelle

Ziel-Host

Hop Count  Counts (1 ~ 15)

Trace route

2. Benutzung des "Ping" Tools gemäß untenstehender Anleitung

Schnittstelle	Wählen Sie die Schnittstelle, zu welcher ein Ping gesendet werden soll. Z.B. LAN, WAN.
Ziel-Host	Geben Sie die Ziel IP Adresse an
Anzahl Übertragungs-Pakete	Geben Sie die Anzahl der zu versendeten ICMP Pakete an.
Ping	Starten der Ping-Aktion

3. Benutzung des "ARPing" Tools gemäß untenstehender Anleitung

Schnittstelle	Wählen Sie die Schnittstelle, zu welcher ein ARPing gesendet werden soll. Z.B. LAN, WAN.
Ziel-Host	Geben Sie die Ziel MAC Adresse an
Anzahl Übertragungs-Pakete	Geben Sie die Anzahl der zu versendeten ARP Pakete an.
ARPing	Starten der ARPing-Aktion

4. Benutzung des "Trace Route" Tools gemäß untenstehender Anleitung

Schnittstelle	Wählen Sie die Schnittstelle, zu welcher ein Trace Route gesendet werden soll. Z.B. WAN1, WAN2.
Ziel-Host	Geben Sie die Ziel IP Adresse oder den Domain-Namen an
Hop Count	Spezifizieren Sie die Anzahl der Hops.
Trace route	Starten der Trace Route-Aktion

## 9.3 Zeiteinstellungen

1. Klicken Sie auf [Admin] - [Zeit]. Folgendes Fenster öffnet sich:

### Setup - Zeit

**Zeitsynchronisation**

Zeitsynchronisation  aktivieren  deaktivieren

Zeit-Server-Typen  Zeit-Server-Gruppe  Manuell

Zeit-Server-Region Automatisch ▼

Zeit-Server IP-Adresse

Zeitzone UTC+08:00 Taiwan, China, Hong Kong, Western Australia, Singapore ▼

Regelmäßige Synchronisation  aktivieren  deaktivieren

Synchronisation Intervall Täglich ▼

Aktion Aktualisierung

Einstellungen speichern
Stornieren

2. Konfigurieren Sie die Einstellungen entsprechend den folgenden Anweisungen:

Zeitsynchronisation	Aktivieren oder deaktivieren Sie hier die Zeit-Synchronisierung
Zeit-Server-Typen	Wählen Sie hier einen „Time Server“ entsprechend Ihrem Standort. Sie können unter Automatik, Asien, Europa, Nordamerika, Südamerika, oder Afrika auswählen.
Zeitzone	Wählen Sie hier die Zeitzone entsprechend Ihres Standortes aus. (Sommerzeit / Winterzeit Einstellung erfolgt automatisch).
Regelmäßige Synchronisation	Aktivieren oder deaktivieren Sie hier die Periodische Synchronisierung
Synchronisation Intervall	Wenn Sie die periodische Synchronisierung aktiviert haben, stellen Sie hier die Häufigkeit ein: jede Stunde, jede 6. Stunde, jede 12. Stunde, jeder Tag, oder jede Woche

# KAPITEL10 Gerätestatus

## 10.1 Router Informationen

1. Klicken Sie auf [Status] - [Router].

### Status - Router

Router Information	
Modell Name	MR-102N
Software Version	2.0.5 (P.1)
Lizenz	Autorisiert
Aktuelle Zeit	Thu, 01 Jan 1970 00:03:53
Laufzeit	3 mins

WAN 1	
MAC-Adresse	00:50:18:60:DD:35
Verbindungstyp	wwan
IP-Adresse	
Subnetz-Maske	
Standardgateway	

LAN 1	
MAC-Adresse	00:50:18:60:DD:30
IP-Adresse	192.168.1.1
Subnetz-Maske	24
DHCP-Dienst	Enabled
DHCP erste IP-Adresse	192.168.1.20
DHCP letzte IP-Adresse	192.168.1.27
Max. Anzahl DHCP-Clients	8

Wireless-Netzwerk 1	
Kanäle	6
Wireless Netzwerk-SSID 1	AXIMCom1
MAC-Adresse	00:50:18:60:DD:30
Wireless Netzwerk-SSID 2	AXIMCom2
MAC-Adresse	00:50:18:60:DD:31

2. Folgende Router Informationen werden angezeigt

Modell Name	Router Model
Software Version	Die Firmwareversion, dieses Router
Lizenz	Authorized" sollte angezeigt werden. Wenn Unauthorized" angezeigt wird, setzen Sie sich bitte mit dem Verkäufer<A[Verkäufer   Verkäuferin]> oder AXIMCom für einen Ersatz in Verbindung
Aktuelle Zeit	Gegenwärtige Systemzeit
Laufzeit	Die Zeit die der AXIMCom-Mobile Router in Betrieb ist

3. Folgende WAN Informationen werden angezeigt

MAC-Adresse	MAC-Adresse
Verbindungstyp	Der gegenwärtige Verbindungstyp (PPPoE, Static IP, und DHCP)
IP-Adresse	Die WAN IP-Adresse
Subnetz-Maske	Die Subnet Mask.
Standardgateway	Die IP-Adresse des Gateways

4. Folgende LAN Informationen werden angezeigt

MAC-Adresse	Die MAC-Adresse
IP-Adresse	Die interne IP-Adresse
Subnetz-Maske	Die Subnet Mask des lokalen Netzwerks
DHCP-Dienst	DHCP Dienst aktiv oder deaktiviert
DHCP erste IP-Adresse	Die DHCP Start IP-Adresse
DHCP letzte IP-Adresse	Die DHCP End-IP-Adresse
Max. Anzahl DHCP-Clients	Die maximale Anzahl an IP Adressen, die Clients zugewiesen werden kann

5. Folgende WLAN Informationen werden angezeigt

Wireless Netzwerk-SSID	SSID dieser Wi-Fi-Station
Kanäle	Der Funkkanal (Vorgabe ist 6)
MAC-Adresse	Die MAC-Adresse

## 10.2 Verbindungsuebersicht / DHCP

1. Klicken Sie auf [Status] - [DHCP]. Folgendes Fenster öffnet sich:

### Status - Benutzer

**DHCP Tabelle (20 Benutzer)**

Name	IP-Adresse	MAC-Adresse	Gültigkeitsdauer
•	10.1.1.22	00:13:11:11:aa:23	23:49:57
•	10.1.1.25	00:16:67:03:0d:38	23:09:27
•	10.1.1.67	00:05:9e:91:0e:6d	22:52:00
•	10.1.1.37	00:04:23:5d:52:fb	22:40:42
•	10.1.1.29	00:1d:e0:00:e1:ab	22:00:42
•	10.1.1.28	00:0c:43:30:52:77	22:00:39
•	10.1.1.65	00:12:0e:ba:99:fa	23:31:28
•	10.1.1.63	00:24:d6:0d:c2:e2	22:39:11
•	10.1.1.27	00:13:e8:35:2d:f7	18:36:08
•	10.1.1.35	00:15:af:e5:a6:40	19:30:34
•	10.1.1.53	00:12:0e:b5:5a:32	03:18:46
•	10.1.1.24	00:1f:c8:14:41:5a	18:19:21
•	10.1.1.32	00:06:4f:6e:5d:eb	21:39:52
•	10.1.1.42	00:23:4e:d8:a7:e6	19:06:45
•	10.1.1.31	00:06:4f:66:21:ef	18:44:28
•	10.1.1.36	00:25:56:11:03:80	21:47:48
•	10.1.1.77	00:25:d3:7b:fe:48	19:42:35
•	10.1.1.62	00:1a:a0:8e:05:9a	17:35:25
•	10.1.1.50	00:0f:66:fd:01:6b	13:58:55
•	10.1.1.71	00:13:20:f9:00:05	20:46:15

Aktualisierung

2. Angezeigte DHCP-Informationen

Name	DHCP-Client Name
IP-Adresse	Die IP-Adresse, die diesem Client zugewiesen wurde
MAC-Adresse	Die MAC-Adresse dieses Client
Gültigkeitsdauer	Die gültige Zeit der IP-Adress Zuweisung

## 10.3 Verbindungsuebersicht / aktuell

1. Klicken Sie auf [Status] - [Benutzer]. Folgendes Fenster öffnet sich:

### Status - Benutzer

**ARP Tabelle (17 Benutzer)**

IP-Adresse	MAC-Adresse	ARP Typ
10.1.1.27	00:13:e8:35:2d:f7	Dynamic
10.1.1.32	00:06:4f:6e:5d:eb	Dynamic
10.1.1.77	00:25:d3:7b:fe:48	Unbekannt
10.1.1.83	00:24:d6:0d:c2:e2	Dynamic
10.1.1.31	00:06:4f:66:21:ef	Dynamic
10.1.1.40	00:1e:65:eb:ec:ba	Dynamic
10.1.1.202	00:1f:d0:97:84:94	Dynamic
10.1.1.237	00:25:d3:7b:fe:48	Dynamic
10.1.1.210	2a:fd:bf:97:57:8b	Dynamic
10.1.1.42	00:23:4e:d8:a7:e6	Dynamic
10.1.1.28	00:1d:e0:00:e1:ab	Dynamic
10.1.1.53	00:12:0e:b5:5a:32	Unbekannt
10.1.1.36	00:25:56:11:03:80	Dynamic
10.1.1.205	00:11:6b:97:d0:04	Dynamic
10.1.1.62	00:1a:a0:8e:05:9a	Dynamic
10.1.1.24	00:1f:c8:14:41:5a	Dynamic
10.1.1.35	00:15:af:e5:a6:40	Dynamic

Aktualisierung

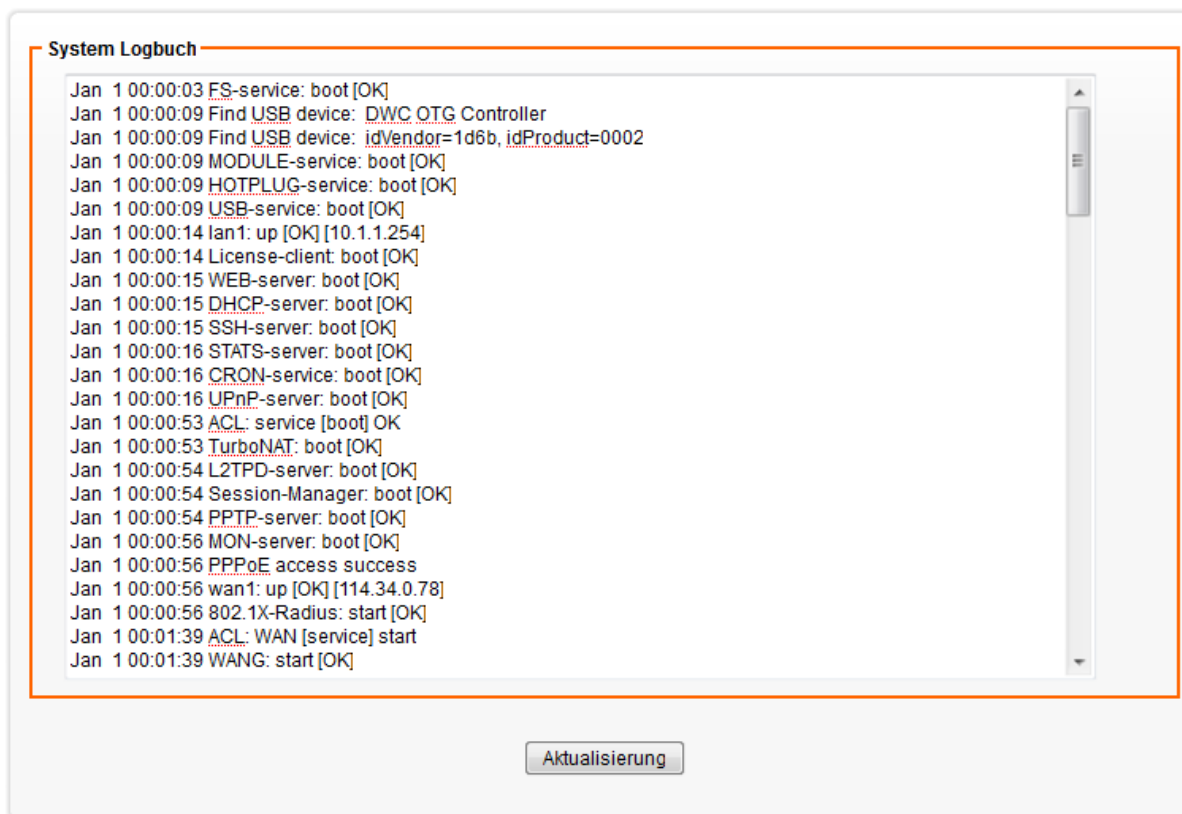
2. Angezeigte ARP-Informationen

IP-Adresse	Die vom Statischen ARP zugewiesene IP-Adresse
MAC-Adresse	MAC-Adresse im statischen ARP
ARP Typ	Statisch oder dynamisch

## 10.4 System-Log

1. Klicken Sie auf [Status] - [Logbuch]. Folgendes Fenster öffnet sich:

### Setup - Logbuch



The screenshot shows a window titled "System Logbuch" with a scrollable list of system events. The events are as follows:

```
Jan 1 00:00:03 FS-service: boot [OK]
Jan 1 00:00:09 Find USB device: DWC OTG Controller
Jan 1 00:00:09 Find USB device: idVendor=1d6b, idProduct=0002
Jan 1 00:00:09 MODULE-service: boot [OK]
Jan 1 00:00:09 HOTPLUG-service: boot [OK]
Jan 1 00:00:09 USB-service: boot [OK]
Jan 1 00:00:14 lan1: up [OK] [10.1.1.254]
Jan 1 00:00:14 License-client: boot [OK]
Jan 1 00:00:15 WEB-server: boot [OK]
Jan 1 00:00:15 DHCP-server: boot [OK]
Jan 1 00:00:15 SSH-server: boot [OK]
Jan 1 00:00:16 STATS-server: boot [OK]
Jan 1 00:00:16 CRON-service: boot [OK]
Jan 1 00:00:16 UPnP-server: boot [OK]
Jan 1 00:00:53 ACL: service [boot] OK
Jan 1 00:00:53 TurboNAT: boot [OK]
Jan 1 00:00:54 L2TPD-server: boot [OK]
Jan 1 00:00:54 Session-Manager: boot [OK]
Jan 1 00:00:54 PPTP-server: boot [OK]
Jan 1 00:00:56 MON-server: boot [OK]
Jan 1 00:00:56 PPPoE access success
Jan 1 00:00:56 wan1: up [OK] [114.34.0.78]
Jan 1 00:00:56 802.1X-Radius: start [OK]
Jan 1 00:01:39 ACL: WAN [service] start
Jan 1 00:01:39 WANG: start [OK]
```

Below the log list is a button labeled "Aktualisierung".