

hama[®]

Hama GmbH & Co KG
D-86651 Monheim/Germany
www.hama.com

All listed brands are trademarks of the corresponding companies. Errors and omissions excepted, and subject to technical changes. Our general terms of delivery and payment are applied.

0053120/10.09

hama®

W I R E L E S S L A N

WLAN Modem Router 54 Mbps



00053120

ⓓ Bedienungsanleitung

Inhaltsverzeichnis:

1	Anschluss des ADSL2+ WLAN Modem Routers	3
2	Konfiguration von Betriebssystem und Computer	4
3	Konfiguration des ADSL2+ WLAN Modem Router	5
3.1	Konfiguration der Internetverbindung mit Hilfe des Assistenten (Quick Start)	5
3.1.1	Neues Router Passwort vergeben (Set Password):	5
3.1.2	Zeitzone Festlegen (Time Zone)	5
3.1.3	Breitbandverbindung auswählen (ISP Connection Type)	6
3.1.4	PPPoE Benutzerdaten (PPPoE/PPPoA)	6
4	Konfiguration des Wireless LAN	7
4.1	WEP Verschlüsselung:	8
4.2	WPA und WPA2 Verschlüsselung:	8
4.3	WDS Settings: (Wireless Distributed System)	8
4.3.1	WDS mit WEP 64/128 Bit Verschlüsselung:	8
4.3.2	WDS mit WPA oder WPA2 Verschlüsselung.	9
4.4	Wireless MAC Address Filtering: (WLAN Zugangskontrolle)	10
5	Interface Setup: (LAN Einstellungen konfigurieren)	11
5.1	Router local IP: (IP Adresse des Routers ändern)	11
5.2	DHCP-Server:	11
6	Advanced Setup: (Erweiterte Internet Einstellungen)	12
6.1	ATM VC: (DSL-Modem Einstellung)	12
6.2	Encapsulation: (DSL- Protokoll)	12
6.3	PPPoE/PPPoA: (Breitbandverbindungsprotokoll)	12
6.4	Connection Setting (DSL Verbindungseinstellung)	13
6.5	IP Address (IP-Adressen Einstellung des Routers)	13
7	Advanced Setup: (Erweiterte Routereinstellung)	14
7.1	Firewall	14
7.2	NAT:	14
7.2.1	DMZ:	14
7.2.2	Virtual Server (Portweiterleitung)	15
8	Access Management (Zugangsmanagement)	15
8.1	ACL: (Zugangskontrolle für bestimmte Dienste)	15
8.2	Filter (Zugriffskontrolle über IP Adresse)	16
8.2.1	Application Filter:	17
8.2.2	URL Filter:	17
8.3	SNMP:	18
8.4	UPnP (Universal Plug and Play Einstellung):	18
8.5	DDNS: (Dyn. Domänen Namen System)	18
9	Maintenance: (Router Verwaltung)	18
9.1	Administration: (Verwaltung)	18
9.1.1	Passwort wiederherstellen:	19
9.2	Time Zone: (Zeitzone einrichten)	19
9.3	Firmware: (Firmware aktualisieren)	19
9.4	SysRestart: (Router Neustarten/Zurücksetzen)	20
9.5	Diagnostics: (Selbsttest des Routers)	20
10	Status: (Übersicht)	20
10.1	Device Info (Statusübersicht):	20
10.2	System Log: (Systemprotokollierung)	20
11	Help (Hilfe):	20
12	Glossar (Begriffserklärung):	21
13	Kontakt- und Supportinformationen:	21

Packungsinhalt:

- 1x Hama ADSL2+ Wireless LAN Modem Router, 54 Mbps
- 1x Netzteil 12V
- 1x gedruckte Bedienungsanleitung
- 1x Netzwerkkabel RJ45
- 1x DSL Verbindungskabel RJ11
- 1x Gutschein Kaspersky Internet Security (90 Tage Version)

Systemvoraussetzung:

- Computer mit eingebauter Netzwerkkarte oder WLAN Adapter
- Betriebssystem mit installiertem TCP/IP Protokoll
- Java fähiger Webbrowser wie z. B. Mozilla Firefox, Microsoft Internet Explorer, oder Opera.

Sicherheitshinweise:

Betreiben Sie das Gerät weder in feuchter, noch in extrem staubiger Umgebung, sowie auf Heizkörpern oder in der Nähe von Wärmequellen. Dieses Gerät ist nicht für den Einsatz im Freien bestimmt. Schützen Sie das Gerät vor Druck- und Stoßeinwirkung. Das Gerät darf während des Betriebes nicht geöffnet oder bewegt werden. Betreiben Sie das Gerät nicht ohne eine aufgeschraubte Antenne **Achtung!** Betreiben Sie den Router nur mit dem mitgelieferten Netzteil. Die Verwendung anderer Netzteile kann zur Zerstörung des Gerätes führen.

Hinweis: !! Bei Volumen- bzw. Zeittarifen ist es empfehlenswert die Auswahl „**Connect On-Demand**“ (**Verbindung bei Bedarf**) auszuwählen, damit der Internetzugang automatisch nach der eingestellten Zeit, unter der Option „**Idle**“ (**Leerlaufzeit**), getrennt wird (**siehe Punkt 6.4**). Bei permanenter Verbindung können ansonsten hohe Verbindungskosten entstehen. Beachten Sie aber auch, dass das Schließen des Browsers nicht zwingend die Abwahl aus dem Internet bedeutet. Sehr viele Programme senden Anfragen in das Internet oder empfangen Daten von dort, ohne das dies eindeutig erkennbar ist. Dies ist für den Router eine gleichwertige Anfrage, wie z.B. das Öffnen des Browsers. Möchten Sie sicher stellen, dass keine aktive Verbindung in das Internet besteht, sollten Sie das Gerät ausschalten.

Voraussetzung für die Installation des HAMA ADSL2+ WLAN Modem Routers, 54 Mbps:

Stellen Sie sicher, dass Sie folgende Voraussetzungen erfüllen, bevor Sie mit der Installation des Hama ADSL2+ WLAN Modem Routers beginnen!

1. Freigeschalteter ADSL oder ADSL2+ Anschluss
2. Von Ihrem DSL Anschluss Dienstleister haben Sie einen DSL Splitter erhalten und verbaut.
3. Sie haben die Benutzerdaten von Ihrem Internet Provider erhalten.
4. Computer mit fehlerfrei installierter Netzwerkkarte

1 Anschluss des ADSL2+ WLAN Modem Routers:

Schließen Sie die Computer und andere Netzwerkgeräte, wie zum Beispiel Hub/Switch, an die Buchsen 1-4 an. Verwenden Sie hierzu ein Crossover oder CAT5 Patchkabel (max. 100m lang). Der eingebaute Switch erkennt selbständig die Verbindungsgeschwindigkeit von 10 oder 100 Mbps, half/full Duplex Übertragungsmodus, sowie den verwendeten Kabel typ. Verbinden Sie den DSL Splitter mittels DSL-Verbindungskabel mit dem Anschluss „ADSL“ an der Rückseite des ADSL2+ WLAN Modem Routers. Stecken Sie nun das mitgelieferte Netzteil in eine freie Steckdose und verbinden es dann mit dem Router.

Vorsicht: Ein ungeeignetes Netzteil kann zu Beschädigungen führen!

Überprüfung der Installation:

An der Oberseite befinden sich verschiedene LEDs zur Statusanzeige:

LED	Zustand	Status
POWER	Leuchtet	Netzteil ist angeschlossen und liefert Strom
	Aus	Kein Netzteil angeschlossen, keine Stromversorgung des Geräts
WLAN-G	Blinkt	Wireless LAN ist aktiviert / es werden Daten gesendet
	Aus	Wireless LAN ist deaktiviert
SYNC	Leuchtet	Modem hat sich erfolgreich mit der Vermittlungsstelle synchronisiert
	Blinkt	Modem versucht sich mit der Vermittlungsstelle zu synchronisieren
LAN 1-4	Leuchtet	Der entsprechende LAN-Port hat eine korrekte Netzwerkverbindung hergestellt
	Blinkt	Datentransfer über jeweiligen LAN-Port
	Aus	Keine Verbindung

2 Konfiguration von Betriebssystem und Computer

Auf allen PC's, die das Internet nutzen sollen, muss das TCP/IP-Protokoll installiert sein. Standardmäßig ist für den Router die IP-Adresse 192.168.2.1 und ein aktivierter DHCP-Server vorkonfiguriert. Dadurch erhalten die angeschlossenen PC's automatisch passende Adressen und weitere Einstellungen. Wir empfehlen dies beizubehalten.

Um die Einstellungen an ihrem PC zu überprüfen gehen Sie folgendermaßen vor:

Klicken Sie auf Ihrem Windows XP Desktop auf **Start -> Systemsteuerung -> Netzwerk und Internetverbindungen -> Netzwerkverbindungen**

Bei Windows 9x/ME/2000 : **Start -> Einstellungen -> Netzwerk und DFÜ-Verbindungen**

Bei Windows Vista: **Start (Windows Logo) -> System-Steuerung -> Netzwerk und Internet -> Netzwerkverbindungen**

Wählen Sie hier die Verbindung (Netzwerkadapter) aus, über die ihr PC mit dem Router verbunden ist, zum Beispiel „**LAN Verbindung**“. Nach einem Rechtsklick auf die entsprechende Verbindung erhalten Sie ein Menü, in dem Sie **Eigenschaften** wählen.



Markieren Sie in der Liste den Eintrag **Internetprotokoll (TCP/IP)** und klicken Sie anschließend auf **Eigenschaften**.



Wählen Sie **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen**! Bestätigen Sie anschließend mit **OK** und im folgenden Fenster ebenfalls mit **OK**!

Ihr PC ist nun so konfiguriert, dass er seine IP-Adresse automatisch vom Router bezieht. Sie können jetzt den Router per Web-Browser einrichten. Der Browser muss Java-fähig sein und diese Funktion aktiviert haben (z. B. Internet Explorer 7.0 und neuer oder Mozilla Firefox / Opera).

3 Konfiguration des ADSL2+ WLAN Modem Router

Um die Konfiguration zu starten, öffnen Sie Ihren Browser und geben als Adresse <http://192.168.2.1> ein. Es erscheint danach das Login-Fenster. Als Standard ist der Benutzername: **admin** und das Kennwort: **1234** eingerichtet. Klicken Sie nach der Eingabe auf **OK**, um sich auf dem Router einzuloggen.

Sie haben die Möglichkeit zur Konfiguration des Routers den **integrierten Assistenten (Quick Start)** zu benutzen oder die Einrichtung manuell vorzunehmen. Nach der Konfiguration mit Hilfe des **Assistenten (Quick Start)** ist das Gerät soweit eingerichtet, dass die über LAN angeschlossenen Computer Zugang zum Internet haben.

Hinweis !!!

Zur Sicherheit sollten Sie das Passwort auf jeden Fall ändern. Die Standardwerte sind bei vielen Geräten gleich und könnten fremden Personen Zugriff zur Routerkonfiguration gewähren. Informationen dazu finden Sie bei Punkt 9.1.

3.1 Konfiguration der Internetverbindung mit Hilfe des Assistenten (Quick Start)

Bitte starten Sie den Assistenten nach dem Einloggen indem Sie auf das Navigationsmenü mit der Bezeichnung -> **Quick Start** klicken und anschließend auf -> **Run WIZARD** und -> **NEXT**.

3.1.1 Neues Router Passwort vergeben (Set Password):

Auf dieser Seite können Sie ein neues Passwort für den Router festlegen.

Geben Sie Ihr neues Passwort in die Zeile mit der Bezeichnung **New Password**: ein.

Bestätigen Sie ihre Eingabe indem Sie Ihr neues Passwort nochmals exakt gleich in die Zeile mit der Bezeichnung **Confirmed Password**: eingeben. Anschließend klicken Sie auf die Schaltfläche -> **Next**.

Hinweis: Bitte notieren Sie sich das neue Passwort an einer sicheren Stelle und vermeiden Sie leicht zu erratende Wörter.



3.1.2 Zeitzone Festlegen (Time Zone)

Wählen Sie im entsprechenden Menü Ihre korrekte Zeitzone, z. B. für Deutschland „(GMT +01:00) Berlin, Stockholm, Rome, Bern, Brussels, Vienna“ aus. Klicken Sie um Fortzufahren auf -> **Next**.



3.1.3 Breitbandverbindung auswählen (ISP Connection Type)

Im nächsten Schritt werden Sie aufgefordert den WAN-Verbindungstyp anzugeben.

In Deutschland ist dies in den meisten Fällen (z. B. T-Online, 1&1, AOL) PPPoE. Aufgrund der weiten Verbreitung von DSL über PPPoE bezieht sich die weitere Beschreibung auf diesen Verbindungstyp. Für den Verbindungstyp PPPoE wählen Sie die Option **PPPoE/PPPoA**. Anschließend klicken Sie auf die Schaltfläche -> **Next**.



3.1.4 PPPoE Benutzerdaten (PPPoE/PPPoA)

In der folgenden Ansicht müssen Sie die Zugangsdaten für Ihren Provider eingeben. Diese Informationen entnehmen Sie den Unterlagen Ihres Internetproviders.

Username (Benutzername): Diesen providerspezifischen Namen finden Sie in den Unterlagen Ihres Internetproviders.

Wichtiger Hinweis für T-Online Nutzer: Bitte tragen Sie ihre T-Online-Zugangsdaten in folgender Reihenfolge in das Feld Benutzername ein:

AAAAAAAAAAATTTTTTTTTTTTTMMMM@t-online.de

Dabei steht A für die 12 Ziffern Ihrer Anschlusskennung, das T für die zugehörige T-Online-Nummer und das M für den 4-stelligen Mitbenutzer-Suffix.

Dahinter folgt die Zeichenkette **@t-online.de**

Sollte Ihre T-Online-Nummer aus weniger als 12 Ziffern bestehen, folgt vor dem Mitbenutzer-Suffi x das Zeichen #. **AAAAAAAAAAATTTTTTTTTT#MMMM@t-online.de**

Zusätzlich zu den Zugangsdaten können Sie noch folgende Angaben machen:

Password (Passwort): Das providerspezifische Passwort finden Sie in Ihren Unterlagen Ihres Internetproviders.

VPI und VCI: Diese Werte können Sie bei Ihrem Internetprovider erfragen. Für die DSL Anschlüsse der deutschen Telekom und baugleiche, gelten zum Zeitpunkt der Handbucherstellung folgende Werte:

VPI: 1

VCI: 32.

Wie angedeutet, können die Werte je nach Land oder Provideranschluss abweichen!

Connection Type (Breitbandverbindungstyp):

Für den Verbindungstyp **PPPoE** wählen Sie die Option **PPPoE LLC**. Anschließend klicken Sie auf die Schaltfläche -> **Next**.

Im nächsten Fenster werden Sie darauf hingewiesen, dass die Konfiguration erfolgreich übernommen wurde und die Eingaben mit Klick auf die Schaltfläche -> **Next** gespeichert werden.

Damit ist die Konfiguration des Internetzugangs mit dem **Assistenten (Quick Start)** abgeschlossen.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf -> **CLOSE**.

Anschließend muss der Router neu gestartet werden, damit alle Einstellungen wirksam werden. Rufen Sie dazu das Menü -> **Maintenance** auf, wählen den Unterpunkt -> **SysRestart** und wählen danach die Option -> „**System Restart with: Current Settings**“. Klicken dann auf die Schaltfläche -> **RESTART**.



4 Konfiguration des Wireless LAN

Standardmäßig ist das Wireless LAN zu Ihrem Schutz deaktiviert. Möchten Sie die Funktion aktivieren, wählen Sie das Menü **Interface Setup** und dann den Unterpunkt **Wireless** aus. Nun erscheint das unten abgebildete Bild. Beachten Sie, dass eine Aktivierung des **Wireless LAN** ohne zusätzliche Einstellung einer Verschlüsselung ein hohes Sicherheitsrisiko birgt.



Access Point:

Hier schalten Sie das Wireless LAN an oder ab. Um das Wireless LAN einzuschalten, wählen Sie die Option **Activated** (eingeschaltet), um das Wireless LAN abzuschalten, die Option **Deactivated** (ausgeschaltet).

Channel (Kanal):

Hier wählen Sie den Kanal aus, über welchen Ihr Wireless LAN funken soll. In **Deutschland (GERMANY)** können Sie zwischen **Kanal 1 bis 13** oder **Auto** wählen.

Anmerkung: Je nach Standort kann es sein, dass nicht alle möglichen Kanäle auswählbar sind!

802.11 b/g:

Hier ist eigentlich nur die Option namens 802.11b+g relevant. Hier können Sie Ihren Wireless LAN Access Point so einstellen, dass dieser nur mit anderen Clients kommuniziert, die auf dem 802.11b (11 Mbps) oder 802.11g (54 Mbps) Standard basieren. Der Hama ADSL2+ WLAN Modem Router 54 Mbps unterstützt folgende Standards:

802.11b = nur WLAN Geräte basierend auf 11 Mbps werden unterstützt.

802.11g = nur WLAN Geräte basierend auf 54 Mbps Standard, werden unterstützt

802.11b+g = WLAN Geräte basierend auf 54 und 11 Mbps werden gleichzeitig unterstützt.

SSID:

Mit dieser Funktion können Sie einen eindeutigen Namen für Ihr Wireless LAN vergeben. Der Namen darf maximal 30 Buchstaben oder Ziffern beinhalten. Sonderzeichen werden nicht unterstützt!



Broadcast SSID (WLAN Netzwerkname anzeigen):

Hier können Sie bestimmen, ob Ihr Wireless LAN Name, für jeden im Netz sichtbar sein soll. Standardmäßig ist diese Option (eingeschaltet) **Yes**.

Authentication Type (Verschlüsselungsart einstellen):

Dieser Punkt ist äußerst wichtig für die Sicherheit Ihres Wireless LAN Netzwerkes. In dieser Option wählen Sie die **Verschlüsselungsart und -stärke** aus. Der Hama ADSL2+ WLAN Modem Router unterstützt augenblicklich folgende Verschlüsselungsstandards:

WEP (64 und 128-Bit)

WPA-PSK (TKIP)

WPA2-PSK (AES)

4.1 WEP Verschlüsselung:

Wired Equivalent Privacy (WEP) ist ein Standard-Verschlüsselungsalgorithmus für WLAN. Er soll sowohl den Zugang zum Netz regeln, als auch die Integrität der Daten sicherstellen. Aufgrund verschiedener Schwachstellen wird das Verfahren als unsicher/veraltet angesehen.

Wählen Sie als Erstes aus, ob Sie eine **64 bit oder 128 bit Verschlüsselung** verwenden möchten, wobei die **128 bit Verschlüsselung** die **höhere Sicherheit** bietet.

Geben Sie als Nächstes Ihren Sicherheitsschlüssel ein (Sie können Zeichen von 0-9 und a-f verwenden), wobei bei der 64bit Verschlüsselung die Länge des Sicherheitsschlüssels auf max. 10 bzw. bei 128 bit auf 26 Buchstaben/Ziffern beschränkt ist.

Unter **Key #1** bis **4** haben Sie die Möglichkeit, bis zu vier Schlüssel voreinzustellen. Wählen Sie dazu z. B. **Key #1** und geben Sie in die darunter liegenden Felder Ihre beliebigen Schlüssel mit der erforderlichen Länge ein.

Beispiele:

64 bit Hex (10 Zeichen) = 0x231074a6

128 bit Hex (26 Zeichen) = 2689x34ab368affb3476ab34ff

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unteren Ende des Fensters.



4.2 WPA und WPA2 Verschlüsselung:

Wi-Fi Protected Access (**WPA**) ist eine Verschlüsselungsmethode für WLAN. WPA enthält die Architektur von WEP, bietet jedoch zusätzlichen Schutz durch dynamische Schlüssel, die auf dem **Temporal Key Integrity Protocol (TKIP)** basieren, und bietet außerdem zur Authentifizierung von Nutzern **PSK (Pre-Shared-Keys)**. WPA2 ist die Weiterentwicklung von WPA und nutzt einen anderen Verschlüsselungsalgorithmus **AES (Advanced Encryption Standard)**.

Wählen Sie unter „**Authentication Type**“ zwischen **WPA-PSK (TKIP)** und **WPA2-PSK(AES)** aus.

Der nächste Schritt ist die Eingabe des Schlüssels (vorinstallierter Schlüssel), des so genannten **Pre-Shared-key (PSK)**. Der Schlüssel darf eine Länge von mindestens 8 und höchstens 63 beliebigen Zeichen haben, wobei Buchstaben (A-Z), Zahlen und Satzzeichen erlaubt sind. Möchte ein Client auf den Access-Point zugreifen, muss er diese Zeichenfolge kennen.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unteren Ende des Fensters.



4.3 WDS Settings: (Wireless Distributed System)

WDS (Wireless Distribution System) bezeichnet ein Funknetzwerk aus mehreren Basisstationen. Mittels WDS kann unter anderem eine größere Netzabdeckung erzielt werden, als dies mit nur einer Basisstation möglich wäre. Dazu werden mindestens zwei oder mehr WLAN Basisstationen benötigt, welche die WDS Funktion unterstützen, idealerweise sind diese vom selben Hersteller.

4.3.1 WDS mit WEP 64/128 Bit Verschlüsselung:

Wir empfehlen diese veraltete Verschlüsselungstechnik nicht mehr zu verwenden, es sei denn, Sie verwenden andere WLAN Geräte/Clients, welche die neueren Verschlüsselungsstandards wie WPA oder WPA2 nicht beherrschen.



WDS Mode:

Disabled: Die WDS Funktion ist abgeschaltet.

Bridge: Zwei per Kabel Netze (LAN) werden über eine (Richt-)Funkstecke miteinander verbunden. Beide WLAN Basisstationen müssen den gleichen WLAN Kanal, dürfen aber eine unterschiedliche SSID haben. Das Signal wird im Bridge Modus nicht verstärkt. Dieser Modus sollte gewählt werden, wenn Sie nur eine bestimmte Strecke per WLAN anstatt per Kabel überbrücken wollen. Sie müssen die jeweiligen Mac Adressen von der anderen WLAN Basisstation in den Feldern mit der Bezeichnung **Mac Address #1 bis #4** eingeben.

Repeater: Dieser Modus ist der Hauptanwendungsfall, wenn WDS genutzt werden soll, dabei wird die WLAN Netzabdeckung erhöht bzw. erweitert. Die beteiligten WLAN Basisstationen müssen den gleichen WLAN Kanal und die gleiche SSID haben. Sie müssen die jeweiligen Mac Adressen von der anderen WLAN Basisstationen in den Feldern mit der Bezeichnung **Mac Address #1 bis #4** eingeben.

Lazy: Wenn Sie diesen Modus aktivieren, brauchen Sie keine Mac Adressen in die oben abgebildeten Felder eingeben. Die WDS Router im Lazy Modus tauschen die Adressen automatisch aus, ohne manuelle Konfiguration. **Achtung! Ein nicht autorisierter Nutzer von Außen, könnten (falls das WLAN Verschlüsselungspasswort bekannt / gehackt wurde) zugreifen!**

Überprüfen Sie folgende Voreinstellungen:

Auf jedem WLAN Gerät, das Sie mittels WLAN ansprechen wollen, den gleichen WEP Standard 64 oder 128 bit eingestellt haben. Desweiteren ist bei den WDS fähigen Routern / Access Points (AP) oder WLAN Modem Router deren MAC Adresse zu notieren. Wo Sie die MAC Adresse finden können, entnehmen Sie bitte dem Handbuch Ihres Produktes. Die MAC Adresse dieses Produktes finden Sie im Hauptmenu unter den Punkt „**Status**“. Danach wählen Sie die Option „**Device Info**“ dort finden Sie im Absatz „**Device Info**“ die MAC Adresse.

Beachten Sie Bitte, dass Sie nur die in der unmittelbaren Umgebung aufgestellten WDS fähigen Routern / Access Points (AP) oder WLAN Modem deren MAC Adressen eintragen müssen. Stellen Sie überall den gleichen WDS Modus ein!

Beispiel:

Sie wollen mittels 3 WDS fähigen Geräten Ihr WLAN Netzwerk vergrößern. Wählen Sie den WDS Modus „**Repeater**“ aus geben Sie bei der ersten WLAN Basisstation nur die MAC Adresse des zweiten WLAN Basisstation unter „**Mac Address #1:**“ ein!

Bei dem 2ten WDS fähigen Gerät müssen Sie hingegen die MAC Adresse von der WLAN Basisstation Nr. 1 und Nr. 3 eintragen. Geben Sie dazu die Mac Adresse von Nr. 1 in das Feld mit der Bezeichnung „**Mac Address #1:** ein und von Nr. 3 in das Feld mit der Bezeichnung „**Mac Address #2:**“ ein.

Bei dem 3ten ist hingegen nur die Mac Adresse von Nr. 2 einzutragen, geben Sie dazu dessen Mac Adresse in das Feld mit der Bezeichnung „**Mac Address #1:**“ ein!

Hinweis:

Beachten Sie, dass bei Betrieb von zwei oder mehreren WLAN Basisstationen in einem Netzwerk nur an einem der DHCP Server aktiviert werden darf. Vergeben Sie für alle anderen WLAN Basisstationen eine entsprechende IP-Adresse.

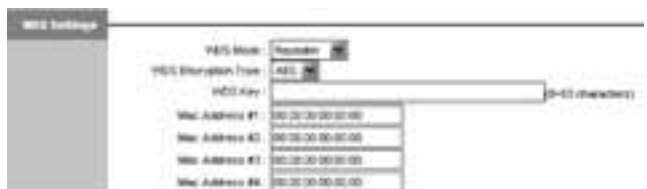
Zum Beispiel:

1. WLAN Basisstation (1) hat die IP Adresse 192.168.2.1 und die Subnetmask von 255.255.255.0 an diesem Gerät schalten Sie den DHCP Server ein.
2. WLAN Basisstation (2) hat die feste IP Adresse von 192.168.2.2 und die Subnetmask von 255.255.255.0 an diesem Gerät ist der integrierte DHCP Server ausgeschaltet!
3. WLAN Basisstation (3) hat die feste IP Adresse von 192.168.2.3 und die Subnetmask von 255.255.255.0 an diesem Gerät ist der integrierte DHCP Server ausgeschaltet!
4. usw.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unteren Ende des Fensters.

4.3.2 WDS mit WPA oder WPA2 Verschlüsselung.

Wi-Fi Protected Access (**WPA**) ist eine Verschlüsselungsmethode für WLAN. WPA enthält die Architektur von WEP, bietet jedoch zusätzlichen Schutz durch dynamische Schlüssel, die auf dem **Temporal Key Integrity Protocol (TKIP)** basieren, und bietet außerdem zur Authentifizierung von Nutzern **PSK (Pre-Shared-Keys)**. WPA2 ist die Weiterentwicklung von WPA und nutzt einen anderen Verschlüsselungsalgorithmus **AES (Advanced Encryption Standard)**.



WDS Mode:

Disabled: Die WDS Funktion ist abgeschaltet.

Bridge: Zwei per Kabel Netze (LAN) werden über eine (Richt-)Funkstecke miteinander verbunden. Beide WLAN Basisstationen müssen den gleichen WLAN Kanal, dürfen aber eine unterschiedliche SSID haben. Das Signal wird im Bridge Modus nicht verstärkt. Dieser Modus sollte gewählt werden, wenn Sie nur eine bestimmte Strecke per WLAN anstatt per Kabel überbrücken wollen. Sie müssen die jeweiligen Mac Adressen von der anderen WLAN Basisstation in den Feldern mit der Bezeichnung **Mac Address #1 bis #4** eingeben.

Repeater: Dieser Modus ist der Hauptanwendungsfall, wenn WDS genutzt werden soll, dabei wird die WLAN Netzabdeckung erhöht bzw. erweitert. Die beteiligten WLAN Basisstationen müssen den gleichen WLAN Kanal und die gleiche SSID haben. Sie müssen die jeweiligen Mac Adressen von der anderen WLAN Basisstationen in den Feldern mit der Bezeichnung **Mac Address #1 bis #4** eingeben.

Lazy: Wenn Sie diesen Modus aktivieren, brauchen Sie keine Mac Adressen in die oben abgebildeten Felder eingeben. Die WDS Router im Lazy Modus tauschen die Adressen automatisch aus, ohne manuelle Konfiguration. **Achtung! Ein nicht autorisierter Nutzer von Außen, könnten (falls das WLAN Verschlüsselungspasswort bekannt / gehackt wurde) zugreifen!**

Überprüfen Sie folgende Voreinstellungen:

Auf jedem WLAN Gerät, das Sie mittels WLAN ansprechen wollen, den gleichen WEP Standard 64 oder 128 Bit eingestellt haben. Desweiteren ist bei den WDS fähigen Routern / Access Points (AP) oder WLAN Modem Router deren MAC Adresse zu notieren. Wo Sie die MAC Adresse finden können, entnehmen Sie bitte dem Handbuch Ihres Produktes. Die MAC Adresse dieses Produktes finden Sie im Hauptmenu unter den Punkt „Status“. Danach wählen Sie die Option „Device Info“ dort finden Sie im Absatz „Device Info“ die MAC Adresse.

Beachten Sie Bitte, dass Sie nur die in der unmittelbaren Umgebung aufgestellten WDS fähigen Routern / Access Points (AP) oder WLAN Modem deren MAC Adressen eintragen müssen. Stellen Sie überall den gleichen WDS Modus ein!

Beispiel:

Sie wollen mittels 3 WDS fähigen Geräten Ihr WLAN Netzwerk vergrößern. Wählen Sie den WDS Modus „Repeater“ aus geben Sie bei der ersten WLAN Basisstation nur die MAC Adresse des zweiten WLAN Basisstation unter „Mac Address #1:“ ein!

Bei dem 2ten WDS fähigen Gerät müssen Sie hingegen die MAC Adresse von der WLAN Basisstation Nr. 1 und Nr. 3 eintragen. Geben Sie dazu die Mac Adresse von Nr. 1 in das Feld mit der Bezeichnung „Mac Address #1: ein und von Nr. 3 in das Feld mit der Bezeichnung „Mac Address #2:“ ein.

Bei dem 3ten ist hingegen nur die Mac Adresse von Nr. 2 einzutragen, geben Sie dazu dessen Mac Adresse in das Feld mit der Bezeichnung „Mac Address #1:“ ein!

Hinweis:

Beachten Sie, dass bei Betrieb von zwei oder mehreren WLAN Basisstationen in einem Netzwerk nur an einem der DHCP Server aktiviert werden darf. Vergeben Sie für alle anderen WLAN Basisstationen eine entsprechende IP-Adresse.

Zum Beispiel:

1. WLAN Basisstation (1) hat die IP Adresse 192.168.2.1 und die Subnetmask von 255.255.255.0 an diesem Gerät schalten Sie den DHCP Server ein.
2. WLAN Basisstation (2) hat die feste IP Adresse von 192.168.2.2 und die Subnetmask von 255.255.255.0 an diesem Gerät ist der integrierte DHCP Server ausgeschaltet!
3. WLAN Basisstation (3) hat die feste IP Adresse von 192.168.2.3 und die Subnetmask von 255.255.255.0 an diesem Gerät ist der integrierte DHCP Server ausgeschaltet!
4. usw.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unteren Ende des Fensters.

4.4 Wireless MAC Address Filtering: (WLAN Zugangskontrolle)

Mit dieser Funktion können Sie Notebooks/PC's mit Wireless LAN, anhand deren MAC Adressen, den Zugang zu Ihrem Netzwerk/ Internet erlauben oder verweigern.

Zuerst müssen Sie diese Funktion einschalten (**Activated**). Zu diesem Zweck wählen Sie die **Option Active**: -> **Activated** (eingeschaltet) aus. Jetzt müssen Sie danach bei der **Option Action**: zwischen **Allow Association** (erlauben) oder **Deny Association** (verweigern) für den jeweiligen Computer einstellen.

Allow Association: Nur den eingetragenen MAC-Adressen wird der Zugang gewährt **Deny Association:** Allen eingetragenen MAC-Adressen wird der Zugang verwehrt.

Jetzt geben die erste MAC Adresse Ihres gewünschten Rechners in die dafür vorbestimmte Maske **MAC Address #1:** ein. Bsp.: Ihr Notebook hat die MAC Adresse von 00:12:34:56:0A:0A, dann geben Sie diese Adresse genauso in das Feld mit der Bezeichnung **Mac Address #1:** ein.

Wie Sie die MAC Adresse Ihres Computers ausfindig machen können, entnehmen Sie bitte der Bedienungsanleitung Ihres Betriebssystems oder erfragen diese bei Ihrem Systemadministrator. Für weitere Rechner gehen Sie analog vor.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unteren Ende des Fensters.



5 Interface Setup: (LAN Einstellungen konfigurieren)

In dieser Ansicht können Sie die **Standard LAN Einstellungen** des Routers ändern.

Wählen Sie dazu im **Hauptmenü** den **Menüpunkt Interface Setup** und dann den **Unterpunkt LAN** aus. Nun erscheint das unten abgebildete Bild.



5.1 Router local IP: (IP Adresse des Routers ändern)

Der Router ist standardmäßig auf die **IP-Adresse**

192.168.2.1 eingestellt. Möchten Sie eine andere Adresse für den Router verwenden, können Sie diese hier entsprechend abändern. Im Eingabefeld direkt darunter wird die entsprechende **IP-Teilnetzmaske (Subnet Mask)** eingetragen. Alle anderen Optionen sind nur für sehr spezielle Anwendungsgebiete relevant, die an dieser Stelle aber nicht näher erläutert werden. Wir empfehlen die Standardvoreinstellungen zu belassen.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unteren Ende des Fensters.

Achtung!!: Nach dem Neustart ist die neue LAN-Konfiguration gültig. Um das Webinterface im Browser aufzurufen, müssen Sie also die neue IP-Adresse verwenden.

5.2 DHCP-Server:

Der integrierte DHCP-Server ermöglicht die automatische Vergabe von IP-Adressen für angeschlossene Clients. Vergeben Sie in ihrem Netzwerk die IP-Adressen manuell und benötigen somit keinen DHCP-Server, wählen Sie **Disabled** (ausgeschaltet). Möchten Sie den DHCP-Server verwenden, wählen Sie **Enabled** (eingeschaltet) aus. Die Einstellung für die Lease Time gibt an, wie lange die zugewiesene IP-Adresse für den Client gültig ist. Der IP-Adressenbereich, aus dem der DHCP-Server IP-Adressen an die Clients verteilen darf, wird durch die Start-IP-Adresse und die End-IP-Adresse begrenzt.

Starting IP Address:

Hier können Sie die IP-Adresse eingeben, bei dem der DHCP Server anfängt aufsteigend die Nr. an die angeschlossenen Computer zu verteilen.

Hinweis:

Die IP-Adresse muss im selben Adressraum befinden, wie Sie bei der Option „**Router Local IP**“ eingegeben haben! Anderenfalls, kommen Sie nicht mehr auf Ihren Router drauf.

Beispiel:

Ihre Router IP Adresse lautet: 192.168.2.1, dann muss die IP-Adresse des DHCP Server auch mit 192.168.2. angehen, die letzte Ziffer kann zwischen 2 und 254 sein, wobei wir empfehlen die Standardeinstellung zu lassen.

IP Pool Count:

Hier stellen Sie die Anzahl der max. zu Vergebenen IP-Adressen ein.

Lease Time:

Bezeichnet die Gültigkeitsdauer einer dynamisch vergebenen IP-Adresse, die ein Client von dem integrierten DHCP Server erhalten hat.

Um Ihre Einstellungen zu speichern, klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.

6 Interface Setup:

(Einstellungen für Modem und Internetzugang)

In dieser Ansicht können Sie die **Parameter des integrierten ADSL+ Modems** und die Zugangsdaten für den Internet-zuganges ändern. Wählen Sie dazu im **Hauptmenu** den **Menüpunkt Interface Setup** und dann den **Unterpunkt Internet** aus. Nachfolgend, werden Ihnen die wichtigsten Einstellungen davon erläutert:

6.1 ATM VC: (DSL-Modem Einstellung)

Asynchronous Transfer Mode (ATM) ist eine Technik der Datenübertragung, bei der der Datenverkehr in kleine Pakete, codiert und asynchron übertragen wird. Je nach DSL Anschluss müssen folgende Werte eingetragen werden.

Virtual Circuit: Standardmäßig ist PVC0 ausgewählt.

Status: Activated (eingeschaltet) muss ausgewählt sein!

VPI: 1

VCI: 32



Anmerkung: Diese Werte 1 und 32 sind Beispielsweise nur für den DSL Anschluss der deutschen Telekom gültig. Falls Sie einen Anschluss von einer anderen Firma besitzen oder sich außerhalb Deutschlands befinden, erfragen Sie bitte diese Werte bei Ihrem DSL Anschluss Provider.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.

6.2 Encapsulation: (DSL- Protokoll)

Encapsulation dient dazu, andere Protokolle einzukapseln und so in Form von IP-Tunneln zu transportieren.

Für Deutschland wird beinahe ausschließlich das PPPoE Protokoll benutzt, deswegen wird auch im Rahmen dieses Handbuches nur darauf näher eingegangen. Für Benutzer anderer Protokolle konsultieren Sie bitte Ihren Internet Dienstleister, dieser stellt Ihnen die entsprechenden Einstellungsdaten zur Verfügung.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.



6.3 PPPoE/PPPoA: (Breitbandverbindungsprotokoll)

Das **PPP over Ethernet (PPPoE)** ist die Verwendung des Netzwerkprotokolls Point-to-Point Protocol (PPP) über eine Ethernet-Verbindung. Das PPPoE wird heute bei ADSL- Anschlüssen in Deutschland verwendet.

Servicename: Hier können Sie einen beliebigen Namen eingeben. Diese Eingabe ist optional.

Übename: Geben Sie hier den Benutzernamen ein, den Sie von Ihren Internet Provider erhalten haben.

Password: Geben Sie hier das Passwort ein, das Sie von Ihrem Internet Provider erhalten haben.



Wichtiger Hinweis für T-Online Nutzer:

Bitte tragen Sie ihre T-Online-Zugangsdaten in folgender Reihenfolge in das Feld Benutzername ein:

AAAAAAAAAAAAATTTTTTTTTTTTMMMM@t-online.de

Dabei steht A für die 12 Ziffern Ihrer Anschlusskennung, das T für die zugehörige T-Online-Nummer und das M für den 4-stelligen Mitbenutzer-Suffix. Dahinter folgt die Zeichenkette **@t-online.de**

Sollte Ihre T-Online-Nummer aus weniger als 12 Ziffern bestehen, folgt vor dem Mitbenutzer-Suffi x das Zeichen #.

AAAAAAAAAAAAATTTTTTTTTT#MMMM@t-online.de

Encapsulation: PPPoE LLC für T-COM DSL Anschlüsse in Deutschland

Der Hama ADSL+ WLAN Modem Router unterstützt folgende Encapsulation Protokolle: PPPoE LLC, PPPoE VC-Mux, PPPoA LLC and PPPoA VC-Mux. Sollten Sie sich nicht sicher sein, welches Protokoll Sie für Ihren Internet-Anschluss benötigen, konsultieren Sie bitte Ihren DSL-Provider.

Bridge Interface: Deactivated (ausgeschaltet)

Diese Funktion muss nur Activated (eingeschaltet) werden, wenn Sie den ADSL+ WLAN Modem Router nur als ADSL Modem benutzen wollen und die Routerfunktion abschalten müssen oder wollen.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.

6.4 Connection Setting (DSL Verbindungseinstellung)

Hier können Sie unter folgenden Einstellungen (Conection) wählen, Always On und Connect On-Demand.



Always On: Die Internetverbindung wird permanent aufrecht erhalten. Beachten Sie, dass durch die permanente Verbindung bei Zeittarifen hohe Verbindungskosten entstehen.

Connect On-Demand: Bei Volumen- bzw. Zeittarifen ist es empfehlenswert die Auswahl „**Connect On-Demand**“ (Verbindung bei Bedarf) auszuwählen, damit der Internetzugang automatisch nach der eingestellten Leerlaufzeit, unter der Option „**Close if idle for XY minutes**“ getrennt wird.

Connect Manually: Bei dieser Option verbindet sich der Modem Router nur nach manueller Aktivierung der Verbindung über die oben abgebildeten Benutzeroberfläche.

Wichtiger Hinweis:

Beachten Sie aber auch, dass das Schließen des Browsers nicht zwingend die Beendigung des Internetzugangs bedeutet. Sehr viele Programme senden Anfragen in das Internet oder empfangen Daten von dort, ohne das dies eindeutig für den Benutzer erkennbar ist. Dies ist für den Router eine gleichwertige Anfrage, wie z.B. das Öffnen des Browsers. Möchten Sie sicher stellen, dass keine aktive Verbindung in das Internet besteht, sollten Sie das Gerät ausschalten.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.

6.5 IP Address (IP-Adressen Einstellung des Routers)

Eine IP-Adresse (Internet-Protocol- Adresse) ist eine Nummer, die Adressierung von Computern und anderen Geräten in einem IP-Netzwerk erlaubt.

Sollten Sie von Ihrem Internetprovider eine festgelegte IP Adresse benutzen müssen sind folgende Einstellungen abändern:



Get IP Address: Static (statisch) bedeutet, dass Sie eine von Ihren Internetprovider festgelegte IP Adresse benutzen müssen. Dynamic (dynamisch) ist für die meisten deutschen DSL Anbieter standardmäßig vorgesehen und deshalb hier so voreingestellt.

Static IP Address: Geben Sie hier die festgelegte IP Adresse ein, falls benötigt.

IP Subnet Mask: Geben Sie hier die festgelegte Subnetz IP Adresse ein, falls benötigt.

Gateway: Geben Sie hier die festgelegte Standardgateway IP Adresse ein, falls benötigt.

NAT: Sollte immer enabled (eingeschaltet) sein!

TCP MTU Option: MTU steht für Maximal Transfer Unit und gibt die maximal zu übertragende Paketgröße an. Sollten Sie sich bei dieser Einstellung nicht sicher sein, empfehlen wir den standardmäßig eingestellten Wert zu belassen. Es sind Werte zwischen 0 und 1492 möglich.

Alle anderen Einstellungen sind zu sehr speziell und werden daher nicht näher erläutert.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.

7 Advanced Setup: (Erweiterte RouterEinstellung)

In dieser Übersicht können Sie den Router Ihren Bedürfnissen entsprechend anpassen. Wählen Sie dazu im **Hauptmenu den Menüpunkt Advanced Setup** aus.

7.1 Firewall

Eine **Firewall** ist eine Netzwerk-Sicherheitskomponente in der Computertechnik, die Netzwerkverkehr anhand eines definierten Firewall-Regelwerks erlaubt oder verbietet. Das Ziel einer Firewall ist, den Übergang zwischen einem lokalen Netzwerk (LAN) (hohes Vertrauen) und dem Internet (kein Vertrauen) zu kontrollieren.



Firewall: **Enabled**, bedeutet das die integrierte Firewall eingeschaltet ist.
Disabled, bedeutet, dass die integrierte Firewall ausgeschaltet ist.

SPI: **Enabled**, bedeutet die integrierte Paketfiltertechnik ist eingeschaltet.
Disabled, bedeutet die integrierte Paketfiltertechnik ist ausgeschaltet.

Nähere Hinweise zu der Funktionsweise von SPI finden Sie im Glossar!

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.

7.2 NAT:

Network Address Translation (NAT) ist in Computernetzwerken der Sammelbegriff für Verfahren, um automatisiert Adressinformationen in Datenpaketen durch andere zu ersetzen. Diese kommen typischerweise auf Routern und Firewalls zum Einsatz.

NAT Status: **Activated**, bedeutet das NAT eingeschaltet ist. Dies ist zwingend notwendig, um den Routerbetrieb überhaupt zu ermöglichen!
Disabled, bedeutet das NAT ausgeschaltet ist. Ein Routerbetrieb ist nicht möglich, um diesen zu aktivieren, lesen Sie bitte Punkt 6.5!



Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.

7.2.1 DMZ:

Eine Demilitarized Zone (DMZ, auch ent- oder demilitarisierte Zone) bezeichnet ein Computernetzwerk mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server. Die in der DMZ aufgestellten Systeme wird durch Firewalls gegen andere Netze (z. B. Internet, LAN) abgeschirmt. Durch diese Trennung kann der Zugriff auf öffentlich erreichbare Dienste gestattet und gleichzeitig das interne Netz (LAN) vor unberechtigten Zugriffen geschützt werden.

DMZ: **Enabled**, bedeutet das DMZ eingeschaltet ist.
Disabled, bedeutet das DMZ ausgeschaltet ist.

DMZ Host IP Address: Geben Sie hier die IP Adresse für Ihren Computer ein, auf den ein Server/Programm läuft, das DMZ benötigt.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.



7.2.2 Virtual Server (Portweiterleitung)

Die Portweiterleitung wird z.B. benötigt um einen Spieleserver für ein Internetmatch bereit zu stellen oder für P2P Netzwerke.

Rule Index: 1 bis 16 auswählbar, d.h. es sind bis zu 16 verschiedene Portweiterleitungen möglich.

Application: Hier können Sie den Namen Ihres Programmes eingeben, mit für das Sie die Port weiterleiten wollen.

Im hinteren Pull-Down-Menu können Sie zusätzlich bereits Vordefinierte Protokolle/Programme angeben, falls Ihr gewünschtes Programm darunter fallen sollte.

Im darunterliegenden Pull-Down-Menu können Sie zwischen den beiden Protokollen UDP/TCP und All aus.

Start Port Number: Hier im oberen Bild angegeben ist der erste Port 21

End Port Number: Hier ist der letzte Port anzugeben in unserem Fall ist das ebenfalls 21.

Hinweis: Es sind auch mehrere nachfolgende Ports auf einmal einzustellen, geben Sie dazu lediglich den ersten Port z. B. 3000 bei **Start Port Number** und den letzten z.B. 3005 bei **End Port Number** ein.

Local IP Address: Geben Sie hier die IP Adresse des Rechners ein, auf dem Ihr Programm installiert ist, welches Portweiterleitung benötigt.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.



8 Access Management (Zugangsmanagement)

In dieser Übersicht können Sie detaillierte Zugriffseinstellung Ihren Bedürfnissen entsprechend anpassen. Wählen Sie dazu im **Hauptmenu** den **Menüpunkt Access Management** aus.

8.1 ACL: (Zugangskontrolle für bestimmte Dienste)

Wählen Sie dazu im **Hauptmenu** den **Menüpunkt Access Management** und den Unterpunkt **ACL** aus.

Die Access Control List (ACL), zu Deutsch Zugangskontrollliste, wird verwendet, um zu kontrollieren, welcher Benutzer auf welche Dienste und Dateien (Dateien, Netzwerkdienste) Zugriff hat.

ACL: Activated, bedeutet dass ACL eingeschaltet ist.
Deactivated, bedeutet das ACL ausgeschaltet ist.

ACL Rule Index: Es sind 1 bis 16 auswählbar, d.h. bis zu 16 verschiedene ACL sind konfigurierbar.

Active: Yes, bedeutet das z.B. Regel (Rule) 1 eingeschaltet ist.
No, bedeutet dass z.B. Regel (Rule) 1 ausgeschaltet ist.
Es ist also möglich, je nach Bedarf einzelne Regeln (Rules) ein- oder auszuschalten.

Secure IP Address: Geben Sie dort die IP Adresse des Computers ein, wenn z.B. Regel (Rule) 1 für diesen ausschließlich gelten soll. Soll die Regel (Rule) für alle am Router angeschlossenen Computer gelten geben Sie 0.0.0.0 ein.

Application: Geben Sie an, für welches Protokoll/Anwendung die Regel (Rule) gelten soll. Folgende Möglichkeiten zur Auswahl werden Ihnen zur Verfügung gestellt: Web, FTP, Telnet, SNMP, Ping oder ALL (alles).

Interface: Wählen Sie Übergabestelle aus, für das die Regel (Rule) gelten soll. Folgende Möglichkeiten stehen zur Auswahl: WAN, LAN und Both (beide).



Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.

8.2 Filter (Zugriffskontrolle über IP Adresse)

Wählen Sie dazu im **Hauptmenu** den **Menüpunkt Access Management** und den Unterpunkt **Filter** aus.

Ein Paketfilter ist eine Anwendung, die den ein- und ausgehenden Datenverkehr in einem Computernetz filtert. Dies dient in der Regel dem Schutz des Netzes vor Angreifern. Ebenso wichtig wie der Schutz gegen Angreifer von Außen ist der Schutz gegen ungewollt ausgehende Pakete; damit kann man z. B. erschweren, dass der eigene Rechner ungewollt und unbemerkt Viren im Internet verbreitet.

Filter Type: Hier können Sie zwischen zwei verschiedene Filter auswählen, zwar den **Application Filter** und den **URL Filter**.

IP/MAC Filter Set Editing:

IP/MAC Filter Set Index: Es sind 1 bis 12 auswählbar

Interface: Gleiche Einstellung, wie unter Interface Setup/Virtual Circuit übernehmen.

Direction: **Incoming:** Eingehende Pakete werden gefiltert
Outgoing: Ausgehende Pakete werden gefiltert
Both: Ein- und Ausgehende Pakete werden anhand der voreingestellten Regel (Rule) gefiltert (überprüft)



IP/MAC Filter Rule Editing:

IP Rule Index: Es sind 1 bis 6 Regeln (Rules) einstellbar

Rule Type: Mit dieser Option können Sie wählen zwischen **IP** und **MAC**. Das bedeutet, wenn Sie **IP** auswählen gilt der Filter für eine **spezielle IP-Adresse**, bei **MAC**, müssen Sie die MAC Adresse der Netzwerkkarte oder WLAN Adapter eintragen, des Computers, für den der Filter gelten soll.

Active: **Yes**, bedeutet das z.B. Regel (Rule) 1 eingeschaltet ist.

No, bedeutet dass z.B. Regel (Rule) 1 ausgeschaltet ist. Es ist also möglich je nach Notwendigkeit einzelne Regeln (Rules) ein- oder auszuschalten.

Source IP Add: IP Adresse des Rechners, der als Quelle fungiert. Wenn Sie 0.0.0.0 eingeben wird diese Einstellung ignoriert.

Subnet Mask: Subnetz Maske des Rechners, der als Quelle fungiert.

Port: Nummer des Ports eingeben, für den die Regel (Rule) gelten soll. Falls Sie 0 eingeben, wird diese Einstellung ignoriert.

Destination IP Add: IP Adresse des Rechners, der als Ziel fungiert. Wenn Sie 0.0.0.0 eingeben wird diese Einstellung ignoriert.

Subnet Mask: Subnetz Maske des Rechners, der als Ziel fungiert.

Port: Nummer des Ports eingeben, für den die Regel (Rule) gelten soll. Falls Sie 0 eingeben, wird diese Einstellung ignoriert.

Protocol: Hier können Sie das IP Protokoll eingeben. z.B. TCP, UDP oder ICMP auswählen.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.

8.2.1 Application Filter:

Hier können Sie vordefinierte Programme für das Internet sperren oder freigeben

Zuerst müssen Sie den Filter anschalten, wählen Sie dazu den Menü-Punkt „**Application Filter**“ -> **Activated** (eingeschaltet). Erst jetzt haben die weiteren Einstellungen Auswirkung. Wählen Sie als nächstes das Programm/Protokoll aus, welches Sie dem Zugang verweigern wollen.

Beispielsweise MSN:

Wenn Sie **Allow (erlauben)** auswählen, dürfen alle angeschlossenen Computer mit dem MSN Netzwerk Daten austauschen, wenn Sie **Deny (verweigern)** auswählen, ist das Programm / Protokoll MSN für jeden angeschlossenen Computer gesperrt.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.



8.2.2 URL Filter:

Mit diesem Filter können Sie bestimmte Webadressen sperren.

Als erstes schalten Sie den Filter an, indem Sie die Option **Active** im Menu **URL Filter Editing** aktivieren (siehe Bild oben).

Beispiel:

Sie möchten für alle an diesem Router angeschlossenen Computer die Webseite www.playboy.com sperren.

Gehen Sie wie folgt vor:

Wählen Sie im Pull-Down Menu **URL Index**: die Nr. aus. (Es können maximal 16 Webseiten gesperrt werden). Geben Sie in dem Feld mit der Bezeichnung **URL**: nun die exakte Webseitenadresse ein, in unserem Fall hier www.playboy.com. Klicken Sie nun am unteren Ende der Oberfläche auf die Schaltfläche **SAVE**, um die Einstellung zu speichern. Jetzt erscheint in der **Tabelle** unter **Index 1** Ihr Eintrag www.playboy.com. Damit ist die Einstellung abgeschlossen, fahren Sie nun mit der zweiten Webseite fort, falls notwendig.



8.3 SNMP:

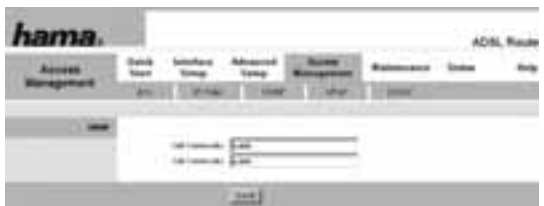
Wählen Sie dazu im **Hauptmenu** den **Menüpunkt Access Management** und den Unterpunkt **SNMP** aus.

Das **Simple Network Management Protocol** (englisch für „einfache Netzwerkverwaltungsprotokoll“, kurz **SNMP**), ist ein Netzwerkprotokoll, das entwickelt wurde, um Netzwerkelemente (z. B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Station aus überwachen und steuern zu können.

Get Community: Geben Sie den Namen Ihres Netzwerks ein.

Set Community: Geben Sie den Namen Ihres Netzwerkes ein.

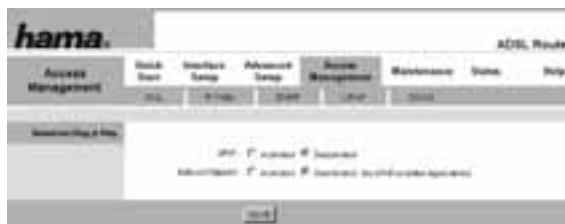
Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.



8.4 UPnP (Universal Plug and Play Einstellung):

Wählen Sie dazu im **Hauptmenu** den **Menüpunkt Access Management** und den **Unterpunkt UPnP** aus.

Universal Plug and Play (UPnP) dient zur herstellerübergreifenden Ansteuerung von Geräten (Media-Center, Router, Drucker) über ein IP-basierendes Netzwerk, mit oder ohne zentrale Kontrolle. Es basiert auf einer Reihe von standardisierten Netzwerkprotokollen und Datenformaten.



UPnP: Activated bedeutet, dass UPnP eingeschaltet ist.
Deactivated bedeutet, dass UPnP ausgeschaltet ist.

Auto-configured: Activated bedeutet, dass das automatische UPnP eingeschaltet ist.
Deactivated bedeutet, dass das automatische UPnP ausgeschaltet ist.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.

8.5 DDNS: (Dyn. Domänen Namen System)

Wählen Sie dazu im **Hauptmenu** den **Menüpunkt Access Management** und den **Unterpunkt DDNS** aus.

DynDNS oder **dynamischer Domain-Name-System-Eintrag** ist ein Internetdienst, der es ermöglicht,

einen festen Hostnamen als Pseudonym für eine sich dynamisch ändernde IP-

Adresse einzurichten. Das sorgt dafür, dass ein Rechner immer über denselben Domainnamen angesprochen werden kann.



Dynamic DNS: **Activated** bedeutet, dynamisches DNS ist eingeschaltet.
Deactivated bedeutet, dynamisches DNS ist ausgeschaltet.

My Host Name: Hostname den Sie z.B. von DynDNS.org erhalten haben.
Bitte geben Sie den gesamten Namen an, inkl. @DynDns.org

E-Mail Address: Geben Sie Ihre E-Mail Adresse an, den Sie im Zuge der DynDNS Registrierung angegeben haben.

Username: Geben Sie Ihren Benutzernamen an, den Sie im Zuge der DynDNS Registrierung angegeben haben.

Password: Geben Sie Ihr Passwort ein, das Sie im Zuge der DynDNS Registrierung angegeben haben.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.

9 Maintenance: (Router Verwaltung)

In dieser Übersicht können Sie detaillierte Zugriffseinstellung Ihren Bedürfnissen entsprechend anpassen.

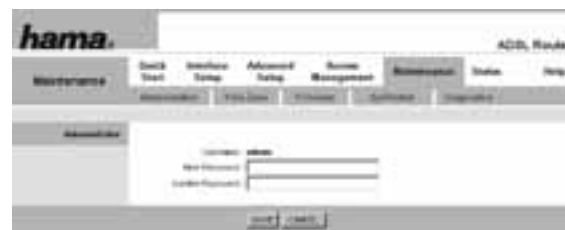
9.1 Administration: (Verwaltung)

Wählen Sie dazu im **Hauptmenu** den Menüpunkt **Maintenance** und den Unterpunkt **Administration** aus.

Hier können Sie gegebenenfalls Ihr Administrator Passwort für den Hama ADSL2+ WLAN Modem Router 54Mbps ändern.

Geben Sie deshalb in der Zeile mit der Bezeichnung **New Password**, Ihr neues Passwort ein und nochmals exakt das gleiche in die Zeile mit der Bezeichnung **Confirm Password**.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.



9.1.1 Passwort wiederherstellen:

Anmerkung:

Sollten Sie aus Versehen Ihr Passwort vergessen haben, können Sie den Hama ADSL 2+ WLAN Modem Router auf die Grundeinstellung zurücksetzen um wieder das Standardpasswort 1234 benutzen zu können. Um den Router zurückzusetzen, benutzen Sie einen Kugelschreiber oder ähnliches und halten den schwarzen Druckpunkt mit der Bezeichnung Reset auf der Rückseite des Routers ca. 5 Sekunden gedrückt. Danach startet der Router wieder im Auslieferungszustand.

9.2 Time Zone: (Zeitzone einrichten)

Wählen Sie dazu im **Hauptmenu** den **Menüpunkt Maintenance** und den **Unterpunkt Time Zone** aus.

Hier können Sie die Zeitzone, die Uhrzeit und das Datum einstellen.

NTP Server automatically: Der Router gleicht die Uhrzeit und Datum mit den Server ab, den Sie bei der Option NTP Server Address eingegeben haben.

PC's clock: Der Router gleicht die Uhrzeit und Datum mit Ihrem Computer ab.

Manually: Manuell, d.h. nach Ihren Eingaben hin, wird die Zeit und das Datum eingestellt.

Time Zone: Zeitzone Ihres Standortes auswählen.

Daylight Saving: Sommer und Winterzeit einschalten.

NTP Server Address: Meist öffentlicher Server, der automatisch die Zeit und das Datum angleicht.

Um Ihre Einstellungen zu speichern klicken Sie bitte auf die Schaltfläche -> **SAVE** am unterem Ende des Fensters.



9.3 Firmware: (Firmware aktualisieren)

Wählen Sie dazu im **Hauptmenu** den **Menüpunkt Maintenance** und den **Unterpunkt Firmware** aus.

Bei dieser Option können Sie, falls Verfügbar ein neues Firmwareupdate einspielen. Ob ein neues Firmwareupdate vorliegt, können Sie auf unserer Homepage www.hama.com oder über die Hama Produktberatung in Erfahrung bringen.

Wenn Sie die neue Firmware heruntergeladen haben, entpacken Sie diese und speichern Sie die Datei auf Ihrem Desktop ab. Klicken Sie nun auf die Schaltfläche -> **Durchsuchen** und wählen die eben entpackte Datei aus und klicken anschließend auf -> **UPGRADE**. Nun wird die Firmware auf den Router überspielt und anschließend neu gestartet:

Anmerkung:

Führen Sie nur ein Firmware Upgrade aus, wenn Sie Probleme mit dem Router haben. Ansonsten raten wir dringendst davon ab, ein Update auszuführen. Es werden auch alle vorher von Ihnen vorgenommenen Änderungen im Zuge des Updates gelöscht! Es ist daher nach dem Upgrade des Routers notwendig, diesen neu einzurichten. Weiterhin weisen wir darauf hin, dass nur von uns autorisierte und freigegebene Firmwareupdates auf den Router überspielt werden dürfen, anderenfalls erlischt Ihr Garantieanspruch gegenüber der Firma Hama GmbH & Co.KG.



9.4 SysRestart: (Router Neustarten/Zurücksetzen)

Wählen Sie dazu im **Hauptmenu** den Menüpunkt **Maintenance** und den **Unterpunkt SysRestart** aus. Hier können Sie den Router bei Bedarf mit den **aktuellen Einstellung Neustarten** oder in den Auslieferungszustand zurücksetzen.

Wollen Sie den Router mit den **aktuellen Einstellung neu starten**, wählen Sie die Option **Current Settings** und klicken dann auf -> **RESTART**.

Wollen Sie den Router auf den Auslieferungszustand zurücksetzen, wählen Sie die Option **Factory Default Settings** und klicken dann auf -> **RESTART**.



9.5 Diagnostics: (Selbsttest des Routers)

Wählen Sie dazu im Hauptmenu den Menüpunkt **Main-tenance** und den **Unterpunkt Diagnostics** aus.

Hier können Sie den ADSL+ WLAN Modem Router eines Selbsttestes unterziehen.

Virtual Circuit: Wenn Sie die Standardeinstellung beibehalten haben, müssen Sie hier **PVCO** auswählen.

PASS = Test bestanden

FAIL = Fehler oder falsche Konfiguration

SKIPPED = Test wurde übersprungen.



10 Status: (Übersicht)

In dieser Übersicht finden Sie detaillierte Information über Ihre aktuellen Routereinstellungen. Wählen Sie dazu im **Hauptmenu** den **Menüpunkt Status** aus.

10.1 Device Info (Statusübersicht):

In diesem Fenster haben Sie den Überblick über den derzeitigen Betriebsstatus Ihres ADSL+ Modem Routers.

Bitte halten Sie einen Ausdruck oder Screenshot des Statusübersicht bereit, falls Sie die Hama Produktberatung anrufen/kontaktieren.

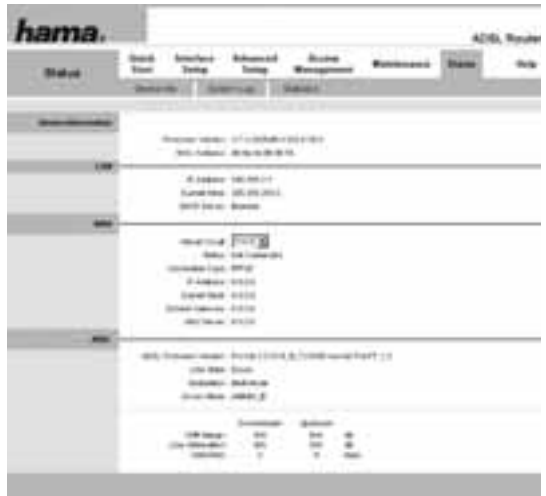
10.2 System Log: (Systemprotokollierung)

Wählen Sie dazu im **Hauptmenu** den **Menüpunkt Status** und den **Unterpunkt System Log** aus.

Hier können Sie die detaillierten Fehlermeldungen des Routers überprüfen. Bitte halten Sie einen Ausdruck des System Logs bereit, falls Sie die Hama Produktberatung anrufen/kontaktieren.

CLEAR LOG: System Log, löschen.

SAVE LOG: System Log in eine Datei speichern.



12 Glossar (Begriffserklärung):

- Clients:** Ist ein Computer der mit einem Server Daten austauscht, aber selbst keine Daten anbietet.
- MAC Adresse:** Die MAC-Adresse (Media Access Control, Ethernet-ID oder bei Apple Airport-ID und Ethernet-ID genannt) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifikation des Geräts im Netzwerk dient. Die MAC-Adresse steht häufig bereits, zum Teil in die Seriennummer integriert, auf der Netzwerkkarte. Daneben kann man sie per Software auslesen, je nach Betriebssystem sind hierzu verschiedene Kommandos nötig.
- SPI:** Unter **Stateful Packet Inspection (SPI)** versteht man eine dynamische Paketfiltertechnik, bei der jedes Datenpaket einer bestimmten aktiven Sitzung zugeordnet wird. Die Datenpakete werden untersucht und der Verbindungsstatus wird in die Entscheidung einbezogen. Bei dieser Technik, die in Firewall eingesetzt wird, werden die Datenpakete während der Übertragung untersucht und in Tabellen gespeichert. Auf Basis des Vergleichs von mehreren Datenpaketen und der Tabelle werden die Entscheidungen für die Weiterleitung der Datenpakete getroffen. Datenpakete, die nicht bestimmten Kriterien zugeordnet werden können werden verworfen. Firewalls mit SPI-Technik sind daher in sicherheitsrelevanten Anwendungen den reinen Paketfilter-Firewalls überlegen.
- Web:** Das **World Wide Web (kurz Web, WWW oder deutsch: Weltweites Netzwerk)** ist ein über das Internet abrufbares Hypertext -System. Hierzu benötigt man einen Webbrowser, um die Daten vom Webserver zu holen und z. B. auf dem Bildschirm anzuzeigen. Der Benutzer kann den Hyperlinks im Dokument folgen, die auf andere Dokumente verweisen, gleichgültig ob sie auf demselben Webserver oder einem anderen gespeichert sind.
- FTP:** Das **File Transfer Protocol (engl. für „Dateiübertragungsverfahren“, kurz FTP)**, ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke. Es wird benutzt, um Dateien vom Server zum Client (Download), vom Client zum Server (Upload) oder clientgesteuert zwischen zwei Servern zu übertragen. Außerdem können mit FTP Verzeichnisse angelegt und ausgelesen, sowie Verzeichnisse und Dateien umbenannt oder gelöscht werden.
- Telnet:** **Telnet (Telecommunication Network)** ist der Name eines im Internet weit verbreiteten Netzwerkprotokolls. Es wird üblicherweise dazu verwendet, Benutzern den Zugang zu Internetrechnern über die Kommandozeile zu bieten.
- SNMP:** Das **Simple Network Management Protocol (englisch für „einfaches Netzwerkverwaltungsprotokoll“, kurz SNMP)**, ist ein Netzwerkprotokoll, das entwickelt wurde, um Netzwerkelemente (z. B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Station aus überwachen und steuern zu können.
- Ping:** **ping** ist ein Programm, mit dem überprüft werden kann, ob ein bestimmter Host/Computer in einem Netzwerk erreichbar ist und welche Antwortzeit er besitzt.
- WAN:** Ein **Weitverkehrsnetz** (engl. wide area network, daher auch oft abgekürzt WAN), auch Weitbereichsnetz, ist ein Rechnernetz, das sich im Gegensatz zu einem LAN über einen sehr großen geografischen Bereich erstreckt.
- LAN:** Ein **Lokales Netz** (engl. local area network, daher oft abgekürzt LAN) ist ein Netz, das mittels Netzwerkkabel oder per Wireless LAN mit anderen Rechnern/Clients verbunden ist.
- TCP:** Das **Transmission Control Protocol (TCP)** ist eine Vereinbarung (Protokoll) darüber, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen. Alle Betriebssysteme moderner Computer beherrschen TCP und nutzen es für den Datenaustausch mit anderen Rechnern. Es ist Teil der Internetprotokollfamilie, der Grundlage des Internets.
- UDP:** Das **User Datagram Protocol (Abk. UDP)** ist ein minimales, verbindungsloses Netzprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört. Aufgabe von UDP ist es, Daten, die über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen.
- ICMP:** Das **Internet Control Message Protocol (ICMP)** benutzt wie TCP und UDP das Internet Protocol (IP), ist also ein Teil der Internetprotokoll-familie. Es dient in Netzwerken zum Austausch von Fehler- und Informationsmeldungen.

13 Kontakt- und Supportinformationen:

Bei defekten Produkten:

Bitte wenden Sie sich bei Produktreklamationen an Ihren Händler oder an die Hama Produktberatung

Internet/World Wide Web:

Produktunterstützung, Updates oder Produktinformationen bekommen Sie unter www.hama.com

Support Hotline – Hama Produktberatung:

Tel. +49 (0) 9091 / 502-115

Fax +49 (0) 9091 / 502-272

e-mail: produktberatung@hama.de

Dieses Gerät darf nur in den folgenden Ländern betrieben werden: (D)

Die Konformitätserklärungen nach der R&TTE-Richtlinie 99/5/EG finden Sie unter www.hama.com



Contents:

1	Connecting the ADSL2+ WLAN Modem Router	23
2	Configuring the Operating System and Computer	24
3	Configuring the ADSL2+ WLAN Modem Router	25
3.1	Configuring the Internet connection using the wizard (Quick Start)	25
3.1.1	Setting a new router password	25
3.1.2	Setting the time zone	25
3.1.3	Selecting the ISP connection type	25
3.1.4	PPPoE user data (PPPoE/PPPoA)	26
4	Configuring the Wireless LAN	26
4.1	WEP encryption:	27
4.2	WPA and WPA2 encryption:	27
4.3	Wireless distributed system settings	28
4.3.1	WDS with WEP 64/128 bit encryption	28
4.3.2	WDS with WPA or WPA2 encryption.	29
4.4	Wireless MAC address filtering	30
5	Interface Setup (Configuring LAN Settings)	30
5.1	Router local IP (changing the router IP address)	30
5.2	DHCP server	30
6	Interface Setup (Modem and Internet Access Settings)	31
6.1	ATM VC (DSL modem setting)	31
6.2	Encapsulation (DSL protocol)	31
6.3	PPPoE/PPPoA (broadband connection protocol)	31
6.4	Connection setting (DSL connection setting)	32
6.5	IP address (router IP address settings)	32
7	Advanced Setup	33
7.1	Firewall	33
7.2	NAT	33
7.2.1	DMZ	33
7.2.2	Virtual servers (port forwarding)	34
8	Access Management	34
8.1	ACL (access control for certain services)	34
8.2	Filters (access control using IP address)	35
8.2.1	Application filters	35
8.2.2	URL filters	36
8.3	SNMP	36
8.4	UPnP (Universal Plug and Play setting)	37
8.5	DDNS (Dynamic Domain Name System)	37
9	Maintenance	37
9.1	Administration	37
9.1.1	Resetting the password	37
9.2	Time zone (setting the time zone)	38
9.3	Firmware (updating the firmware)	38
9.4	SysRestart (restarting/resetting the router)	38
9.5	Diagnostics (router self-test)	38
10	Status (Overview)	38
10.1	Device info (status overview)	39
10.2	System log	39
11	Help	39
12	Glossary	39
13	Contact and Support Information:	40

Package contents:

- 1x Hama ADSL2+ Wireless LAN Modem Router, 54 Mbps
- 1x 12 V power supply unit
- 1x Printed operating instructions
- 1x RJ45 network cable
- 1x RJ11 DSL connecting cable
- 1x Voucher Kaspersky Internet Security (90 days version)

System requirements:

- Computer with built-in network card or WLAN adapter
- Operating system with TCP/IP protocol installed
- Java-capable Web browser such as Mozilla Firefox, Microsoft Internet Explorer or Opera.

Safety notes:

Do not use the device in moist or extremely dusty areas, on radiators or near heat sources. This device is not designed for use outdoors. Protect the device from pressure and impact. The device may not be opened or moved during operation. Do not use the device without an antenna attached.

Warning: Use the router with the enclosed power supply unit only. Using other power supply units can cause irreparable damage to the product.

Note: !! The “Connect On-Demand” setting is recommended if you have a **pay-as-you-go payment plan (if you pay according to volume or time)**. This means that the Internet connection is disconnected automatically after the period set in the “Idle” field (see section 6.4). Connection costs may be high if you are permanently connected to the Internet. Please also note that closing the browser does not automatically disconnect you from the Internet. A number of programs send requests to the Internet or receive data without this being clearly indicated. For the router, these requests are just as valid as opening a browser, for example. If you want to ensure that there is no active connection to the Internet, you should switch off the device.

Requirements for installing the HAMA ADSL2+ WLAN Modem Router, 54 Mbps:

Ensure that you have the following before installing the Hama ADSL2+ WLAN Modem Router:

1. Enabled ADSL or ADSL2+ connection
2. Installed DSL splitter provided by your DSL connection service provider
3. User information from your Internet provider
4. Computer with installed (and error-free) network card

1 Connecting the ADSL2+ WLAN Modem Router

Connect the computers and other network devices such as hubs/switches to ports 1-4. Use a crossover or CAT5 patch cable (max. 100 m). The integrated switch automatically detects the connection speed of 10 or 100 Mbps, half/full duplex transfer mode and the type of cable used.

Connect the DSL splitter to the “ADSL” connection on the rear of the ADSL2+ WLAN modem router using the DSL connecting cable. Plug the provided power supply unit into an empty socket and connect it to the router.

Caution: Unsuitable power supply units can cause damage.

Checking the installation:

There are different LEDs for indicating the status on the top of the device:

LED	State	Status
POWER	Illuminated	Power supply unit is connected and supplying power
	Off	No power unit connected, device not being supplied with power
WLAN-G	Flashing	Wireless LAN is activated/data is being sent
	Off	Wireless LAN is deactivated
SYNC	Illuminated	Modem has successfully synchronised with the switching centre
	Flashing	Modem is attempting to synchronise with the switching centre
LAN 1-4	Illuminated	The corresponding LAN port has established a correct network connection
	Flashing	Data transfer via respective LAN port
	Off	No connection

2 Configuring the Operating System and Computer

The TCP/IP protocol must be installed on all PCs that will be using the Internet. By default, the IP address is set to 192.168.2.1 and the DHCP server is activated for the router. This means that the connected PCs are automatically given suitable addresses and other settings. We recommend that you keep these settings.

Proceed as follows to check the settings on your PC:

On your Windows XP Desktop click **Start -> Control Panel -> Network and Internet Connections -> Network Connections** or

with Windows 9x/ME/2000 **Start -> Settings -> Network and Dial-up Connections**

with Windows Vista:

Start (Windows logo) -> Control Panel -> Network and Internet -> Network Connections

Select the connection (network adapter) via which your PC is connected to the router, e.g. **"Local Area Connection"**.

When you right-click the appropriate connection, a menu is displayed; select Properties.

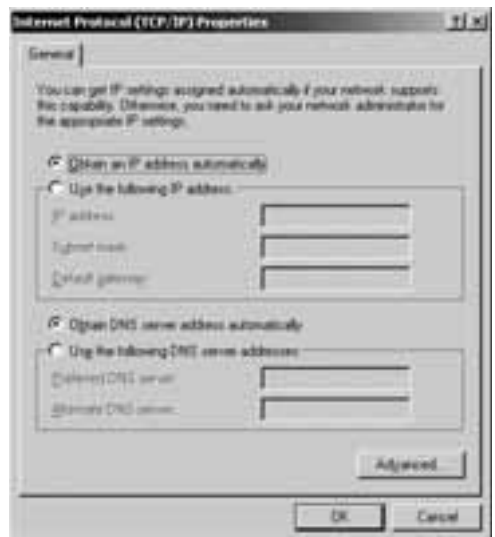


Select the Internet Protocol (TCP/IP) entry in the list and then click Properties.

Ensure that the check boxes **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected. Confirm by clicking **OK**, and again in the following window.

Your PC is now configured so that it now obtains its IP address from the router automatically. You can then configure the router using the Web browser.

The browser must be Java-capable and the Java function must be activated (Internet Explorer 7.0 or above, or Mozilla Firefox/Opera, for example).



3 Configuring the ADSL2+ WLAN Modem Router

To start the configuration process, open your browser and enter **http://192.168.2.1** as the address. The login window appears.

By default, the user name is: **admin** and the password is: **1234**. After entering these, click **OK** to log into the router.

You can configure the router manually or using the integrated **wizard (Quick Start)**. After configuration using the **wizard (Quick Start)**, the device is set so that the computers connected via LAN can access the Internet.

Note:
For security reasons, you must change the password. The standard settings are identical for many devices and can allow others to access the router configuration. For more information, see section 9.1.

3.1 Configuring the Internet connection using the wizard (Quick Start)

After you have logged in, start **the wizard** by clicking on the navigation menu called -> **Quick Start**, then -> **Run WIZARD** and -> **NEXT**.

3.1.1 Setting a new router password

Enter a new password for the router on this page.

Enter your new password in the **New Password**: field. Confirm by accurately entering your new password again in the **Confirmed Password**: field. Then click -> **Next**.

Note: You must keep your password in a safe place and avoid using words that others may guess easily.



3.1.2 Setting the time zone

Choose the appropriate time zone in the menu, e.g. "(GMT +01:00) Berlin, Stockholm, Rome, Bern, Brussels, Vienna" for Germany. Click -> **Next** to continue.



3.1.3 Selecting the ISP connection type

In the following step, you are asked to specify the WAN connection type. In Germany, this is generally PPPoE (e.g. T-Online, 1&1, AOL). Due to the widespread use of DSL over PPPoE, the remainder of the description will refer to this type of connection. For the PPPoE connection type, select **PPPoE/PPPoA**. Then click -> **Next**.



3.1.4 PPPoE user data (PPPoE/PPPoA)

You must enter the access data for your provider in the next window. Refer to the documents from your Internet provider for this information.

Username:

Refer to the documents from your Internet provider for this name, which is specific to the provider.

Important note for T-Online users:

Please enter your T-Online access data in the following order in the **Username** field:

AAAAAAAAAAAAATTTTTTTTTTTTTMMMM@t-online.de

“A” represents the 12 characters of your connection ID, “T” is the corresponding T-Online number and “M” stands for the 4-digit user suffix. This is followed by the character string: **@t-online.de**.

If your T-Online number contains fewer than 12 characters, enter the # symbol before the user suffix.

AAAAAAAAAAAAATTTTTTTTTT#MMMM@t-online.de

Password:

Refer to the documents from your Internet provider for the provider-specific password.

VPI and VCI:

Consult your Internet provider for these values. When this manual was printed, the following values were applicable for DSL connections with Deutsche Telekom and similar companies:

VPI: 1

VCI: 32.

As is implied, the values can vary according to the country or provider.

Connection Type:

For the PPPoE connection type, select the **PPPoE LLC** option. Then click -> **Next**. In the next window you will be notified that the configuration has been successful. Save your entries by clicking -> **Next**.

Configuring your Internet connection using the **wizard (Quick Start)** is then complete.

Click -> **CLOSE** to save your settings. You must then restart the router for the settings to take effect. To do so, call the **Maintenance** menu, select the **SysRestart** sub-item and then choose **System Restart with: Current Settings**. Then click **RESTART**.

4 Configuring the Wireless LAN

Wireless LAN is deactivated by default for security reasons. If you want to activate the function, go to the **Interface Setup** menu and select the **Wireless** sub-item. You will now see the screen depicted below.

Note that activating wireless LAN without enabling encryption poses a serious security risk.

Access Point:

Switches wireless LAN on or off. To switch on wireless LAN, select **Activated**; to switch it off, select **Deactivated**.

Channel:

Select the channel you wish to use for your wireless LAN. In Germany you can choose channels 1 to 13, or Auto. Note: Depending on your location, you may not be able to select all available channels.

802.11 b/g:

Only the 802.11b/g: option is relevant here. Here you can set your wireless LAN access point so that it only communicates with other clients that work with the 802.11b (11 Mbps) or 802.11g (54 Mbps) standards. The Hama ADSL+ WLAN Modem Router 54 Mbps supports the following standards:



- 802.11b = only WLAN devices using the 11 Mbps standard are supported.
- 802.11g = only WLAN devices using the 54 Mbps standard are supported.
- 802.11b+g = WLAN devices using both the 54 and 11 Mbps standards are supported at the same time.

SSID:
 You can enter a clearly identifiable name for your wireless LAN in this field. The name can have a maximum of 30 characters. Special characters are not supported.



Broadcast SSID:
 Here, you can stipulate whether or not your wireless LAN name should be visible to everyone in the network. The default setting is **Yes (activated)**.

Authentication Type:
 This field is extremely important for the security of your wireless LAN. Select the **encryption type** and **strength**. The Hama ADSL2+ WLAN Modem Router currently supports the following encryption standards:

- WEP (64 and 128 Bit)
- WPA-PSK (TKIP)
- WPA2-PSK (AES)

4.1 WEP encryption:

Wired Equivalent Privacy (WEP) is a standard encryption algorithm for WLAN. It controls access to the network and guarantees the integrity of the data. This method is considered unsafe and outdated due to a number of weaknesses.

First select whether you want to use **64 bit** or **128 bit** encryption. The latter offers greater security. Next, enter your security key (you can use characters ranging from 0-9 and a-f). The length of the key is limited to 10 letters/numbers for 64 bit encryption, and 21 letters/numbers for 128 bit encryption.

You can preset up to four keys in the **Key #1** to **#4** fields. Select **Key #1**, for example, and enter your key of choice with the required length.

Examples:

- 64 bit hex (10 characters) = 0x231074a6
- 128 bit hex (26 characters) = 2689x34ab368affb3476ab34ff

Click -> **SAVE** at the bottom of the window to save your settings.



4.2 WPA and WPA2 encryption:

Wi-Fi Protected Access (WPA) is an encryption method for WLAN. WPA contains the WEP architecture, but offers additional protection using dynamic codes that are based on the **Temporal Key Integrity Protocol (TKIP)**. WPA also offers **pre-shared keys (PSK)** for user authentication. WPA2 is a development of WPA and uses a different encryption algorithm, the **Advanced Encryption Standard (AES)**.



Choose between **WPA-PSK (TKIP)** and **WPA2-PSK (AES)** in the **Authentication Type** field.

The next step is entering a key called a **Pre-Shared Key (PSK)**. The key must be between 8 and 63 random characters; letters (A-Z), numbers and punctuation marks are permitted. Any client wanting to access the access point must know this character string.

Click -> **SAVE** at the bottom of the window to save your settings.

4.3 Wireless distributed system settings

WDS (Wireless Distribution System) refers to a wireless network consisting of multiple base stations. With WDS you can achieve a wider network coverage than would be possible with just one base station. To do so, you need at least two (or more) WLAN base stations which support the WDS function (ideally, from the same manufacturer).

4.3.1 WDS with WEP 64/128 bit encryption

We recommend that you no longer use it, unless you have other WLAN devices/clients that cannot handle newer encryption standards such as WPA or WPA2.

WDS Mode:

Disabled: The WDS function is deactivated.

Bridge: Two cable-based networks (LAN) are connected to one another using a (directional) wireless link. Both WLAN base stations have to use the same WLAN channel, but their SSIDs can be different. In bridge mode the signal is not strengthened. You should choose this mode when you just want to bridge a specific path via WLAN instead of by cable. You have to enter the respective MAC addresses from the other WLAN base stations in the fields labelled **Mac Address #1 to #4**.

Repeater: This mode is mainly used when you want WDS with increased/extended WLAN coverage. The participating WLAN base stations have to use the same WLAN channel and the same SSID. You have to enter the respective MAC addresses from the other WLAN base stations in the fields labelled **Mac Address #1 to #4**.

Lazy: When you use this mode, you do not have to enter any MAC addresses in the fields shown above. In lazy mode, the WDS routers automatically change addresses without manual configuration. **Warning:** Unauthorised users could gain access from outside (if the WLAN encryption password becomes public or is hacked).

Check the following settings:

Every WLAN device that is to be addressed via WLAN should have the same WEP standard 64/128 bit setting. In addition, you should make a note of the MAC addresses for WDS-capable routers/access points (AP) or WLAN modem routers. To find out where to get the MAC address, check the product manual. You can find the MAC address for this product in the Main Menu under **Status**. Then choose the **Device Info** option, and there you will find the MAC address in the **Device Info** paragraph.

Please note that you only have to enter the MAC addresses for the WDS-capable routers/access points (AP) or WLAN modems that are located in the immediate vicinity. Use the same WDS mode for all devices.

Example:

You want to expand your WLAN using 3 WDS-capable devices. Select the WDS mode **"Repeater"** and for the first WLAN base station only enter the MAC address of the second WLAN base station under **"Mac Address #1"**.

For the second WDS-capable device, however, you have to enter the MAC address from WLAN base stations #1 and #3. To do so, enter the MAC address from #1 in the field labelled **„Mac Address #1:“** and the MAC address from #3 in the field labelled **„Mac Address #2:“**.

For the 3rd device, however, you only need the MAC address from #2, which you should enter in the field labelled **„Mac Address #1:“**.


Note:

Please note that when operating two or more WLAN base stations on a single network, the DHCP server can be activated on only one of them. Assign an appropriate IP address for all other WLAN base stations.

For example:

1. WLAN base station (1) has IP address 192.168.2.1 and subnet mask 255.255.255.0 – activate the DHCP server on this device.
2. WLAN base station (2) has the static IP address 192.168.2.2 and subnet mask 255.255.255.0 – the integrated DHCP server is deactivated on this device.
3. WLAN base station (3) has the static IP address 192.168.2.3 and subnet mask 255.255.255.0 – the integrated DHCP server is deactivated on this device.
4. etc.

Click -> **SAVE** at the bottom of the window to save your settings

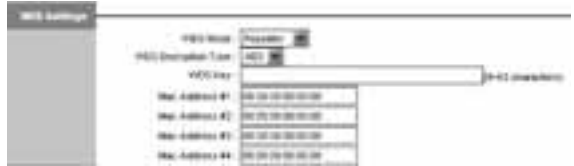


The screenshot shows the 'WDS Settings' window. At the top, 'WDS Mode' is set to 'Repeater'. Below it are four fields for 'Mac Address #1' through '#4', each containing the hexadecimal value '00:00:00:00:00:00'.

WDS Mode:	Repeater
Mac Address #1:	00:00:00:00:00:00
Mac Address #2:	00:00:00:00:00:00
Mac Address #3:	00:00:00:00:00:00
Mac Address #4:	00:00:00:00:00:00

4.3.2 WDS with WPA or WPA2 encryption.

Wi-Fi Protected Access (**WPA**) is an encryption method for WLAN. WPA contains the WEP architecture, but offers additional protection using dynamic codes that are based on the **Temporal Key Integrity Protocol (TKIP)**. WPA also offers **pre-shared keys (PSK)** for user authentication. WPA2 is a development of WPA and uses a different encryption algorithm, the **Advanced Encryption Standard (AES)**.



WDS Mode:

Disabled: The WDS function is deactivated.

Bridge: Two cable-based networks (LAN) are connected to one another using a (directional) wireless link. Both WLAN base stations have to use the same WLAN channel, but their SSIDs can be different. In bridge mode the signal is not strengthened. You should choose this mode when you just want to bridge a specific path via WLAN instead of by cable. You have to enter the respective MAC addresses from the other WLAN base stations in the fields labelled **Mac Address #1 to #4**.

Repeater: This mode is mainly used when you want WDS with increased/extended WLAN coverage. The participating WLAN base stations have to use the same WLAN channel and the same SSID. You have to enter the respective MAC addresses from the other WLAN base stations in the fields labelled **Mac Address #1 to #4**.

Lazy: When you use this mode, you do not have to enter any MAC addresses in the fields shown above. In lazy mode, the WDS routers automatically change addresses without manual configuration. **Warning:** Unauthorised users could gain access from outside (if the WLAN encryption password becomes public or is hacked).

Check the following settings:

Every WLAN device that is to be addressed via WLAN should have the same WEP standard 64/128 bit setting.

In addition, you should make a note of the MAC addresses for WDS-capable routers/access points (AP) or WLAN modem routers. To find out where to get the MAC address, check the product manual. You can find the MAC address for this product in the Main Menu under **Status**. Then choose the **Device Info** option, and there you will find the MAC address in the **Device Info** paragraph.

Please note that you only have to enter the MAC addresses for the WDS-capable routers/access points (AP) or WLAN modems that are located in the immediate vicinity.

Use the same WDS mode for all devices.

Example:

You want to expand your WLAN using 3 WDS-capable devices. Select the WDS mode "**Repeater**" and for the first WLAN base station only enter the MAC address of the second WLAN base station under "**Mac Address #1**".

For the second WDS-capable device, however, you have to enter the MAC address from WLAN base stations #1 and #3. To do so, enter the MAC address from #1 in the field labelled „**Mac Address #1:**“ and the MAC address from #3 in the field labelled „**Mac Address #2:**“.

For the 3rd device, however, you only need the MAC address from #2, which you should enter in the field labelled "**Mac Address #1:**".

Note: Please note that when operating two or more WLAN base stations on a single network, the DHCP server can be activated on only one of them. Assign an appropriate IP address for all other WLAN base stations.

For example:

1. WLAN base station (1) has IP address 192.168.2.1 and subnet mask 255.255.255.0 – activate the DHCP server on this device.
2. WLAN base station (2) has the static IP address 192.168.2.2 and subnet mask 255.255.255.0 – the integrated DHCP server is deactivated on this device.
3. WLAN base station (3) has the static IP address 192.168.2.3 and subnet mask 255.255.255.0 – the integrated DHCP server is deactivated on this device.
4. etc.

Click -> **SAVE** at the bottom of the window to save your settings.

4.4 Wireless MAC address filtering

With this function, you can stipulate which notebooks and PCs with wireless LAN are allowed/denied access to your network/Internet by entering their MAC addresses.

First, this function needs to be activated. To do so, select the Active: -> **Activated option**. Then choose either **Allow Association** or **Deny Association** in the Action field for the respective computer.

Allow Association: Only the MAC addresses that you have entered are given access.

Deny Association: None of the MAC addresses that you have entered are given access.

Now enter the first MAC address of your chosen computer in the **Mac Address #1: field**.

Example:

The MAC address of your notebook computer is 00:12:34:56:0A:0A, so you enter this address in the Mac Address #1: field, exactly as it is written.

To find out the MAC address of your computer, refer to the operating instructions for your operating system, or ask your system administrator. For additional computers, proceed as same as before.

Click -> **SAVE** at the bottom of the window to save your settings.



5 Interface Setup (Configuring LAN Settings)

On this screen, you can change the standard LAN settings of the router.

To do so, select **Interface Setup** from the **Main Menu** and then select the **LAN** sub-item. You will now see the screen depicted below.

5.1 Router local IP (changing the router IP address)

The IP address of the router is set to **192.168.2.1** by default. If you want to use a different address for the router, you can make the necessary changes here.

The corresponding IP subnet mask is entered in the field directly below this. All other fields are only relevant for specialised application areas, which cannot be explained in depth here.

We recommend that you keep the default settings.

Click -> **SAVE** at the bottom of the window to save your settings.

Note: The new LAN configuration takes effect after restarting. You must therefore use the new IP address to open the Web interface in the browser.



5.2 DHCP server

The integrated DHCP server allows IP addresses to be assigned to connected clients automatically.

Select **Disabled** if you assign the IP addresses manually in your network, and therefore do not need a DHCP server.

Select **Enabled** if you want to use the DHCP server.

The Lease Time setting specifies how long the assigned IP address is valid for the client. The IP address range from which the DHCP server can assign IP addresses to clients is restricted by the Start-IP address and the End-IP address.

Starting IP Address:

Here you can enter the IP address at which the DHCP server starts to assign ascending numbers to the connected computers.

Note:
The IP address has to be in the same address space as the one entered in the "Router Local IP" field. Otherwise, you will no longer be able to reach your router.

Example:
If your router IP address is 192.168.2.1, then the IP address for the DHCP Server should also begin with 192.168.2., and the last digits can be between 2 and 254, although we do recommend that you keep the default setting.

IP Pool Count:
Here you enter the maximum number of IP addresses to be assigned.

Lease Time:
Indicates the validity period of a dynamically assigned IP address that a client received from the integrated DHCP server.
Click -> **SAVE** at the bottom of the window to save your settings.

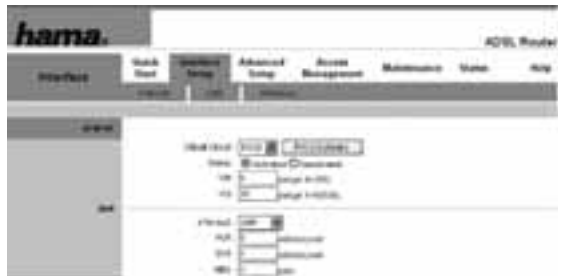
6 Interface Setup (Modem and Internet Access Settings)

On this screen, you can change the parameters for the integrated ADSL2+ modem and the access data for Internet access. To do so, select **Interface Setup** from the **Main Menu** and then select the **Internet** sub-item. The most important settings in this area are explained below:

6.1 ATM VC (DSL modem setting)

Asynchronous Transfer Mode (ATM) is a method of transferring data whereby the data traffic is transferred in small packets, and the transfer is coded and asynchronous. You must enter the following values, which differ according to the DSL connection. (See screenshot below)

Virtual Circuit: PVC0 is selected by default.
Status: Activated must be selected.
VPI: 1
VCI: 32



Note: The values 1 and 32 are only valid for a Deutsche Telekom DSL connection. If your connection is through a different company or you are not resident in Germany, ask your DSL connection provider for these values.

Click -> **SAVE** at the bottom of the window to save your settings.

6.2 Encapsulation (DSL protocol)

The purpose of encapsulation is to encapsulate other protocols and to transport these in the form of IP tunnels.

In Germany, the PPPoE protocol is used almost exclusively; this manual will therefore cover this protocol only. Users with different protocols should consult their Internet service provider, which will provide the relevant setting information.

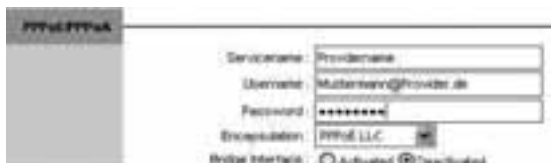
Click -> **SAVE** at the bottom of the window to save your settings.



6.3 PPPoE/PPPoA (broadband connection protocol)

PPP over Ethernet (PPPoE) is the use of the Point-to-Point Protocol (PPP) with an Ethernet connection. PPPoE is currently used for ADSL connections in Germany.

Service name: You can enter a name of your choosing here. This is optional.
Username: Enter the user name that you received from your Internet provider in this field.
Password: Enter the user password that you received from your Internet provider in this field.



Important note for T-Online users:

Please enter your T-Online access data in the following order in the **Username field**:

AAAAAAAAAAAAATTTTTTTTTTTTTMMMM@t-online.de

“A” represents the 12 characters of your connection ID, “T” is the corresponding T-Online number and “M” stands for the 4-digit user suffix. This is followed by the character string: **@t-online.de**.

If your T-Online number contains fewer than 12 characters, enter the # symbol before the user suffix.

AAAAAAAAAAAAATTTTTTTTT#MMMM@t-online.de

Encapsulation: PPPoE LLC for T-COM DSL connections in Germany

The Hama ADSL2+ WLAN Modem Router supports the following encapsulation protocols: PPPoE LLC, PPPoE VC-Mux, PPPoA LLC and PPPoA VC-Mux. If you are not sure which protocol you need for your Internet connection, consult your DSL provider.

Bridge Interface: Deactivated

This function should only be activated if you want to use the ADSL2+ WLAN Modem Router as an ADSL modem only, and you want/ have to switch off the router function.

Click -> **SAVE** at the bottom of the window to save your settings.

6.4 Connection setting (DSL connection setting)

In the following settings (Connection), you can choose between Always On and Connect On-Demand.



Always On: The Internet is permanently connected. Connection costs may be high if you are permanently connected to the Internet and have a pay-as-you-go payment plan.

Connect On-Demand: The “**Connect On-Demand**” setting is recommended if you have a pay-as-you-go payment plan (if you pay according to volume or time). This means that the Internet connection is disconnected automatically after the period set in the “**Close if idle for XY minutes**” field.

Connect Manually: With this option, the modem router connects only after manually activating the connection via the user interface shown above.

Important:

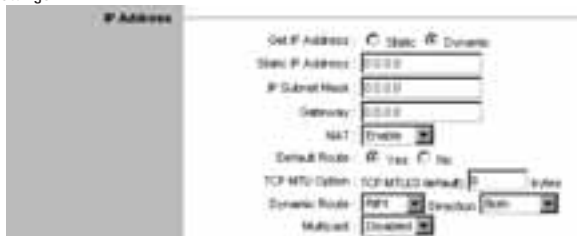
Please also note that closing the browser does not automatically disconnect you from the Internet. A number of programs send queries to the Internet or receive data without it being clearly visible to the user. For the router, these requests are just as valid as opening a browser, for example. If you want to ensure that there is no active connection to the Internet, you should switch off the device.

Click -> **SAVE** at the bottom of the window to save your settings.

6.5 IP address (router IP address settings)

An IP address (Internet Protocol address) is a number that facilitates the addressing of computers and other devices in an IP network.

If you need to use a specific IP address from your Internet provider, carry out the following settings:



Get IP Address:

Static means that you must use an IP address that has been set by your Internet provider. Dynamic is set as default for most German DSL providers, and is therefore set as default here, too.

Static IP Address: If required, enter the specified IP address.

IP Subnet Mask: If required, enter the specified subnet IP address.

Gateway: If required, enter the specified standard gateway IP address.

NAT: This field should always be enabled.

TCP MTU Option: MTU stands for Maximal Transfer Unit and specifies the maximum packet size to be transferred. If you are unsure about this setting, we recommend that you keep the default value. You can set values between 0 and 1492.

All other settings are too specialised and are therefore not covered in this manual.

Click -> **SAVE** at the bottom of the window to save your settings.

7 Advanced Setup

In this overview, you can customise the router to suit your individual requirements. To do so, select **Advanced Setup** from the **Main Menu**.

7.1 Firewall

A firewall is a network security component in computer technology that permits or denies network traffic using a predefined firewall security policy. The aim of a firewall is to control the transfer between a local network (LAN) (high trust) and the Internet (low trust).



Firewall: **Enabled** means that the integrated firewall is switched on.
Disabled means that the integrated firewall is switched off.

SPI: **Enabled** means that the integrated packet filter is switched on.
Disabled means that the integrated packet filter is switched off.

You can find more information about SPI in the glossary.

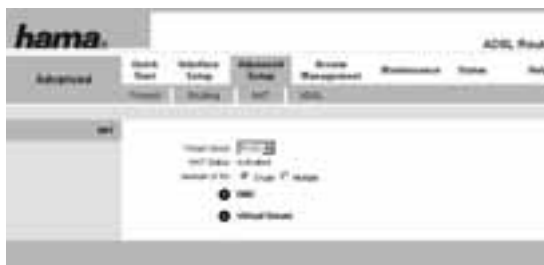
Click -> **SAVE** at the bottom of the window to save your settings.

7.2 NAT

In computer networking, **Network Address Translation (NAT)** is the collective term for the process of automatically changing the address information of data packets. The most common application areas are in routers and firewalls.

NAT Status: **Activated** means that NAT is switched on. This setting is imperative for router operation of any kind.
Disabled means that NAT is switched off. The router will not operate; to activate it, see section 6.5.

Click -> **SAVE** at the bottom of the window to save your settings.



7.2.1 DMZ

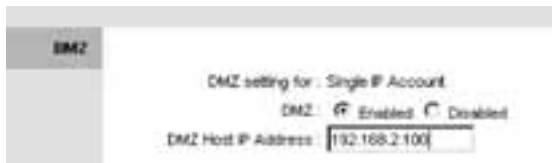
A Demilitarized Zone (DMZ) denotes a computer network where access to its connected servers is controlled via security checks.

The systems set up within the DMZ are protected against other networks (Internet, LAN, for example) using firewalls. This separation allows access to services that are publicly accessible whilst protecting the internal network (LAN) against unauthorised access.

DMZ: **Enabled** means that DMZ is switched on.
Disabled means that DMZ is switched off.

DMZ Host IP Address: In this field enter the IP address of the computer that has a server/program requiring DMZ.

Click -> **SAVE** at the bottom of the window to save your settings.



7.2.2 Virtual servers (port forwarding)

You will need port forwarding if you wish to set up a game server for online gaming or for P2P networks.

Rule Index: You can choose from 1 to 16; up to 16 different port forwardings are possible.

Application: In this field you enter the name of the program for which you want to forward the port.

In the following pull-down menu you can also specify predefined protocols/programs, if your program falls into one of the categories.

In the pull-down menu below it, you can choose UDP/TCP or ALL.

Start Port Number: Port 21 is specified as the first port in the above screenshot.

End Port Number: Here you enter the last port; in our example, it is also 21.

Note: To enter many consecutive ports in one go, simply enter the first port 3000 (for example) as the **Start Port Number**, and 3005 (for example) as the **End Port Number**.

Local IP address: In this field, enter the IP address of the computer on which the program requiring port forwarding is installed.

Click -> **SAVE** at the bottom of the window to save your settings.



8 Access Management

In this overview, you can adjust the access settings comprehensively to suit your individual requirements.

To do so, select **Access Management** from the **Main Menu**.

8.1 ACL (access control for certain services)

From the Main Menu, select the **Access Management** menu item, and then the **ACL** sub-item.

You use the Access Control List (ACL) to control which users can access which files and services (computer files, network services).

ACL: **Activated** means that ACL is switched on. **Deactivated** means that ACL is switched off.

ACL Rule Index: You can choose from 1 to 16, which means that you can configure up to 16 different ACLs.

Active: **Yes** means that Rule 1, for example, is switched on.

No means that Rule 1, for example, is switched off. You can also switch individual rules on or off if required.

Secure IP Address: In this field, enter the computer's IP address if you want the rule to be valid for this computer exclusively. If you want the rule to be valid for all computers connected to the router, enter 0.0.0.0.

Application: Enter the protocol/application to which the rule should apply. You can choose from the following options: Web, FTP, Telnet, SNMP, Ping or ALL.

Interface: Select the exchange point for which the rule is valid. **You can choose from the following options:** WAN, LAN and Both.

Click -> **SAVE** at the bottom of the window to save your settings.



8.2 Filters (access control using IP address)

From the Main Menu, select the **Access Management** menu item, and then the **Filter** sub-item.

A packet filter is an application for filtering the incoming and outgoing data traffic in a computer network. This is generally used to protect the network from attackers, however the filter also protects against unwanted outgoing packets. This means, for example, that you can prevent your own computer from spreading unwanted and undetected viruses on the Internet.

Filter Type: In this field you can choose between two different filters – the **Application Filter** and the **URL Filter**.

IP/MAC Filter Set Editing:

IP/MAC Filter Set Index: You can choose a setting from 1 to 12.

Interface: Use the same setting as entered in the Virtual Circuit field on the Interface Setup page.

Direction: **Incoming:** Incoming packets are filtered
Outgoing: Outgoing packets are filtered
Both: Incoming and outgoing packets are filtered using the preset rule.

IP/MAC Filter Rule Editing:

IP Rule Index: You can set from 1 to 6 rules

Rule Type: With this option you can choose between **IP** and **MAC**. This means that when you choose **IP** the filter applies to a specific **IP address**, and for **MAC**, you have to enter the **MAC address** of the network card or WLAN adapter of the computer to which the filter should apply.

Active: **Yes** means that Rule 1, for example, is switched on.
No means that Rule 1, for example, is switched off. You can thus switch individual rules on or off, if required.

Source IP Add: IP address of the source computer. If you enter 0.0.0.0 this setting is ignored.

Subnet Mask: Subnet mask of the source computer.

Port: Enter the number of the port to which the rule is to apply. If you enter 0, this setting is ignored.

Destination IP Add: IP address of the destination computer. If you enter 0.0.0.0 this setting is ignored.

Subnet Mask: Subnet mask of the destination computer.

Port: Enter the number of the port to which the rule is to apply. If you enter 0, this setting is ignored.

Protocol: Enter the IP protocol in this field, e.g. TCP, UDP or ICMP.

Click -> **SAVE** at the bottom of the window to save your settings.

8.2.1 Application filters

You use this option to block/allow Internet access for predefined programs.

You have to activate the filter first. To do so, select the menu item Application Filter -> **Activated**. Only then will the additional settings take effect.

Now select the program/protocol for which you want to block/allow access.



For example, MSN:

When you select **Allow**, all connected computers are allowed to exchange data with the MSN network, and when you select **Deny**, the MSN program/protocol is blocked for all connected computers.

Click -> **SAVE** at the bottom of the window to save your settings.

8.2.2 URL filters

You use this filter to block specific Web addresses.

First, turn the filter on by activating the **Active** option in the **URL Filter Editing** menu (see screenshot above).

Example:

You want to block the Website www.playboy.com for all computers that are connected to this router.

Proceed as follows:

Select the number in the URL Index: pull-down menu. (You can block a maximum of 16 Websites). Now enter the exact Website address in the field labelled URL:, which in our case is www.playboy.com. Click on **SAVE** at the bottom of the window to save your settings. The entry www.playboy.com now appears in the table under Index 1. You have now made your first setting and can continue to add more Websites, if necessary.



8.3 SNMP

From the Main Menu, select the Access Management menu item, and then the SNMP sub-item.

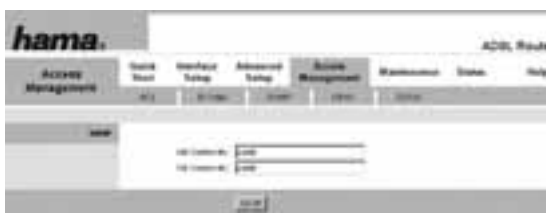
Simple Network Management Protocol

is a network protocol that was designed to monitor and control network elements (e.g. routers, servers, switches, printers, computers, etc.) from a central station.

Get Community: Enter the name of your network.

Set Community: Enter the name of your network.

Click -> **SAVE** at the bottom of the window to save your settings.



8.4 UPnP (Universal Plug and Play setting)

From the **Main Menu**, select the **Access Management** menu item, and then the **UPnP** sub-item.

Universal Plug and Play (UPnP) allows you to control devices made by any manufacturer (media centres, routers, printers), using an IP-based network, with or without central control. It is based on a series of standardised network protocols and data formats.

UPnP: **Activated** means that UPnP is switched on.

Deactivated means that the UPnP is switched off.

Auto-configured: **Activated** means that automatic UPnP is switched on.
Deactivated means that automatic UPnP is switched off.

Click -> **SAVE** at the bottom of the window to save your settings.



8.5 DDNS (Dynamic Domain Name System)

From the **Main Menu**, select the **Access Management** menu item, and then the **DDNS** sub-item.

DynDNS or **Dynamic Domain Name System** is an Internet service that allows you to establish a fixed host name as a pseudonym for a dynamically changing IP address. This ensures that you can always access a computer at the same domain name.

Dynamic DNS: Activated means that dynamic DNS is switched on.

Deactivated means that dynamic DNS is switched off.

My Host Name: Host name that you have received from DynDNS.org, for example. Please enter the entire name, including @DynDns.org

E-Mail Address: Enter the e-mail address that you specified during DynDNS registration.

Username Enter the username that you specified during DynDNS registration.

Password: Enter the password that you specified during DynDNS registration.

Click -> **SAVE** at the bottom of the window to save your settings.



9 Maintenance

In this overview, you can adjust the access settings comprehensively to suit your individual requirements.

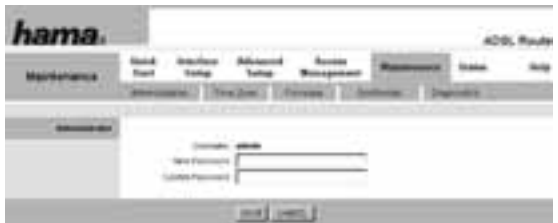
9.1 Administration

From the **Main Menu**, select the **Maintenance** menu item, and then the **Administration** sub-item.

On this page, you can change your administrator password for the Hama ADSL2+ WLAN Modem Router 54Mbps.

To do so, enter your new password in the New Password field and then enter it again (in exactly the same way) in the Confirmed Password field.

Click -> **SAVE** at the bottom of the window to save your settings.



9.1.1 Resetting the password

Note:

If you accidentally forget your password, you can reset the Hama ADSL2+ WLAN Modem Router back to the default setting and use the default password, 1234. To reset the router, use a pen or similarly shaped item to press down on the black pressure point labeled Reset on the back of the router for approx. 5 seconds. The router will then default to the original factory settings.

9.2 Time zone (setting the time zone)

From the **Main Menu**, select the **Maintenance** menu item, and then the **Time Zone** sub-item.

This is where you can set the time zone, time and the date.

NTP Server automatically: The router adjusts the time and date to the server specified in the NTP Server Address field.

PC's clock: The router adjusts the time and date to your computer.

Manually: You set the time and date manually.

Time Zone: Select the time zone of your location.



Daylight Saving: Enable or disable daylight saving time.
NTP Server Address: Usually a public server that automatically adjusts the time and date.
 Click -> **SAVE** at the bottom of the window to save your settings.

9.3 Firmware (updating the firmware)

From the **Main Menu**, select the **Maintenance menu** item, and then the **Firmware** sub-item.

This is where you can install a new firmware update if there is one available. Check our homepage www.hama.com or Hama Product Consulting to learn about firmware updates.

Once you have downloaded the new firmware, extract it and save it to your desktop. Then click -> **Browse**, select the extracted file, and click -> **UPGRADE**. The firmware is then copied to the router, which then performs a restart.



Note:
 Only upgrade the firmware if you are experiencing problems with the router. Otherwise, we strongly recommend against performing an update. The update deletes any changes that you have made previously and so you will need to carry out these settings again once the upgrade is complete. Please note that only firmware updates authorised and released by Hama may be loaded onto the router; otherwise any warranty claims against Hama GmbH & Co. KG are void.

9.4 SysRestart (restarting/resetting the router)

From the **Main Menu**, select the **Maintenance menu** item, and then the **SysRestart** sub-item.

Here, you can restart the router with the current settings or reset it to the factory default settings.

If you want to restart the router with the current settings, select **Current Settings** and click -> **RESTART**.

If you want to reset the factory default settings, select **Factory Default Settings** and click -> **RESTART**.



9.5 Diagnostics (router self-test)

From the **Main Menu**, select the **Maintenance menu** item, and then the **Diagnostics** sub-item.

You can run a diagnostics test for the ADSL2+ WLAN Modem Router here.

Virtual Circuit: If you have retained the default settings, you must select **PVC0** in this field.

- PASS** = Passed the test
- FAIL** = Error or incorrect configuration
- SKIPPED** = Test was skipped



10 Status (Overview)

This overview provides detailed information about your current router settings. From the **Main Menu**, select the **Status menu** item.

10.1 Device info (status overview)

This window provides an overview of the current operating status of your ADSL2+ Modem Router.

If you contact or call Hama Product Consulting, please have a printout or screen shot of the status overview to hand.



10.2 System log

From the **Main Menu**, select the **Status menu** item, and then the **System Log** sub-item.

You can check the detailed error messages for the router in this view. If you contact or call Hama Product Consulting, please have a printout of the system log to hand.

- CLEAR LOG:** Delete system log.
- SAVE LOG:** Save the system log to a file.

11 Help

From the Main Menu, select the Help menu item.

This view provides an overview of the router in addition to detailed explanations of the different functions. This is currently only available in English.

12 Glossary

Client: A computer that exchanges data with a server, but does not offer any data itself.

MAC address: The MAC address (Media Access Control, Ethernet ID or, with Apple, Airport ID and Ethernet ID) is the hardware address of every individual network adapter, and is used as a unique identifier for devices in a computer network. The MAC address is often found on the network card, integrated into the serial number. You can also locate the address using software; various commands are required depending on the operating system.

SPI: Stateful Packet Inspection (SPI) refers to a dynamic packet filter whereby every data packet is assigned to a specific active session. The data packets are inspected and the connection state is included in the decision. With this method, which is implemented in the firewall, the data packets are inspected and entered into tables during the transfer. A data packet comparison and the table determine whether the data packet is passed through. Data packets that cannot be assigned to certain criteria are not allowed through. In security applications, firewalls that use the SPI procedure are therefore superior to the standard packet filter firewalls.

Web: The World Wide Web (shortened to Web or www) is a system of hypertext documents that is retrievable over the Internet. The user needs a Web browser to retrieve the data from the Web server or to display the information on a screen, for example. In the document, the user can navigate the hyperlinks (which refer to other documents) regardless of the Web server on which the hyperlinks are saved.

Ping: Ping is a program used to test whether a particular host or computer is reachable in a network and for determining its response rate.

WAN: A Wide Area Network is a computer network that, in contrast to a LAN, covers a very large geographical area.

LAN: A Local Area Network is a network in which computers or clients are connected using network cables or wireless LAN.

TCP: Transmission Control Protocol (TCP) is a protocol that determines the way in which data should be exchanged between computers. All modern computer operating systems have TCP and employ it for exchanging data with other computers. It is a component of the Internet protocol suite, the core basis of the Internet.

UDP: The User Datagram Protocol (UDP) is a minimal, connectionless network protocol that belongs to the transport layer of the Internet protocol family. The task of UDP is to ensure that data transferred over the Internet arrives at the correct application.

ICMP: As with TCP and UDP, the Internet Control Message Protocol (ICMP) uses the Internet Protocol (IP) and is a core protocol in the Internet protocol family. Its purpose in networks is to send error and information messages.

13 Contact and Support Information:

If the product is defective:

Please contact your dealer or Hama Product Consulting if you have any product claims.

Internet/World Wide Web

Product support, updates or product information can be found at www.hama.com

Support hotline – Hama Product Consulting:

Tel. +49 (0) 9091 / 502-115

Fax +49 (0) 9091 / 502-272

E-mail: produktberatung@hama.de

This operation of this device is only allowed in the following countries: (D)

See www.hama.com for the declarations of conformity with R&TTE Directive 1999/5/EC.



(D) Hinweis zum Umweltschutz:



Ab dem Zeitpunkt der Umsetzung der europäischen Richtlinien 2002/96/EG und 2006/66/EG in nationales Recht gilt folgendes:
Elektrische und elektronische Geräte sowie Batterien dürfen nicht mit dem Hausmüll entsorgt werden. Der Verbraucher ist gesetzlich verpflichtet, elektrische und elektronische Geräte sowie Batterien am Ende ihrer Lebensdauer an den dafür eingerichteten, öffentlichen Sammelstellen oder an die Verkaufsstelle zurückzugeben. Einzelheiten dazu regelt das jeweilige Landesrecht. Das Symbol auf dem Produkt, der Gebrauchsanleitung oder der Verpackung weist auf diese Bestimmungen hin. Mit der Wiederverwertung, der stofflichen Verwertung oder anderen Formen der Verwertung von Altgeräten/Batterien leisten Sie einen wichtigen Beitrag zum Schutz unserer Umwelt.

(GB) Note on environmental protection:



After the implementation of the European Directive 2002/96/EU and 2006/66/EU in the national legal system, the following applies:
Electric and electronic devices as well as batteries must not be disposed of with household waste. Consumers are obliged by law to return electrical and electronic devices as well as batteries at the end of their service lives to the public collecting points set up for this purpose or point of sale. Details to this are defined by the national law of the respective country.
This symbol on the product, the instruction manual or the package indicates that a product is subject to these regulations.
By recycling, reusing the materials or other forms of utilising old devices/Batteries, you are making an important contribution to protecting our environment.

(F) Remarques concernant la protection de l'environnement:



Conformément à la directive européenne 2002/96/CE et 2006/66/CE, et afin d'atteindre un certain nombre d'objectifs en matière de protection de l'environnement, les règles suivantes doivent être appliquées:
Les appareils électriques et électroniques ainsi que les batteries ne doivent pas être éliminés avec les déchets ménagers. Le pictogramme "picto" présent sur le produit, son manuel d'utilisation ou son emballage indique que le produit est soumis à cette réglementation. Le consommateur doit retourner le produit/la batterie usagée aux points de collecte prévus à cet effet. Il peut aussi le remettre à un revendeur. En permettant enfin le recyclage des produits ainsi que les batteries, le consommateur contribuera à la protection de notre environnement. C'est un acte écologique.

(E) Nota sobre la protección medioambiental:



Después de la puesta en marcha de la directiva Europea 2002/96/EU y 2006/66/EU en el sistema legislativo nacional, se aplicara lo siguiente:
Los aparatos eléctricos y electrónicos, así como las baterías, no se deben evacuar en la basura doméstica. El usuario está legalmente obligado a llevar los aparatos eléctricos y electrónicos, así como pilas y pilas recargables, al final de su vida útil a los puntos de recogida comunales o a devolverlos al lugar donde los adquirió. Los detalles quedan definidos por la ley de cada país. El símbolo en el producto, en las instrucciones de uso o en el embalaje hace referencia a ello. Gracias al reciclar, al reciclaje del material o a otras formas de reciclaje de aparatos/pilas usados, contribuye Usted de forma importante a la protección de nuestro medio ambiente.

(NL) Notitie aangaande de bescherming van het milieu:



Ten gevolge van de invoering van de Europese Richtlijn 2002/96/EU en 2006/66/EU in het nationale juridisch systeem, is het volgende van toepassing:
Elektrische en elektronische apparatuur, zoals batterijen mag niet met het huisvuil weggegooid worden. Consumenten zijn wettelijk verplicht om elektrische en elektronische apparaten zoals batterijen op het einde van gebruik in te dienen bij openbare verzamelplaatsen speciaal opgezet voor dit doel of bij een verkooppunt. Verdere specificaties aangaande dit onderwerp zijn omschreven door de nationale wet van het betreffende land. Dit symbool op het product, de gebruiksaanwijzing of de verpakking duidt erop dat het product onderworpen is aan deze richtlijnen. Door te recycleren, hergebruiken van materialen of andere vormen van hergebruiken van oude toestellen/batterijen, levert u een grote bijdrage aan de bescherming van het milieu.

(I) Informazioni per protezione ambientale:



Dopo l'implementazione della Direttiva Europea 2002/96/EU e 2006/66/EU nel sistema legale nazionale, ci sono le seguenti applicazioni:
Le apparecchiature elettriche ed elettroniche e le batterie non devono essere smaltite con i rifiuti domestici. I consumatori sono obbligati dalla legge a restituire i dispositivi elettrici ed elettronici e le batterie alla fine della loro vita utile ai punti di raccolta pubblici preposti per questo scopo o nei punti vendita. Dettagli di quanto riportato sono definiti dalle leggi nazionali di ogni stato. Questo simbolo sul prodotto, sul manuale d'istruzioni o sull'imballaggio indicano che questo prodotto è soggetto a queste regole. Riciclando, ri-utilizzando i materiali o utilizzando sotto altra forma i vecchi prodotti/le batterie, darete un importante contributo alla protezione dell'ambiente.

(GR) Υπόδειξη σχετικά με την προστασία περιβάλλοντος:



Από τη στιγμή που η Ευρωπαϊκή Οδηγία 2002/96/ΕΕ και 2006/66/ΕΕ ενσωματώνεται στο εθνικό δίκαιο ισχύουν τα εξής:
Οι ηλεκτρικές και οι ηλεκτρονικές συσκευές καθώς και οι μπαταρίες δεν επιτρέπεται να πετιούνται στα οικιακά απορρίμματα. Οι καταναλωτές υποχρεούνται από τον νόμο να επιστρέφουν τις ηλεκτρικές και ηλεκτρονικές συσκευές καθώς και τις μπαταρίες στο τέλος της ζωής τους στα δημόσια σημεία περισυλλογής που έχουν δημιουργηθεί γι' αυτό το σκοπό ή στα σημεία πώλησης. Οι λεπτομέρειες ρυθμίζονται στη σχετική νομοθεσία. Το σύμβολο πάνω στο προϊόν, στο εγχειρίδιο χρήσης ή στη συσκευασία παραμένει σε αυτές τις διατάξεις. Με την ανακύκλωση, επαναχρησιμοποίηση των υλικών ή με άλλες μορφές χρησιμοποίησης παλιών συσκευών / Μπαταριών συνεισφέρετε σημαντικά στην προστασία του περιβάλλοντος. Στη Γερμανία ισχύουν αντίστοιχοι οι παραπάνω κανόνες απόρριψης σύμφωνα με τον κανονισμό για μπαταρίες και συσσωρευτές.

(S) Not om miljöskydd:



Efter implementeringen av EU direktiv 2002/96/EU och 2006/66/EU i den nationella lagstiftningen, gäller följande:
Elektriska och elektroniska apparater samt batterier får inte kastas i hushållssoporna. Konsumenter är skyldiga att återlämna elektriska och elektroniska apparater samt batterier vid slutet av dess livslängd till, för detta ändamål, offentliga samlingsplatser. Detaljer för detta definieras via den nationella lagstiftningen i respektive land. Denna symbol på produkten, instruktionsmanualen eller på förpackningen indikerar att produkten innefattas av denna bestämmelse. Genom återvinning och återanvändning av material/batterier bidrar du till att skydda miljön och din omgivning.

(FIN) Ympäristönsuojelua koskeva ohje:



Siitä lähtien, kun Euroopan unionin direktiivi 2002/96/EU ja 2006/66/EU otetaan käyttöön kansallisessa lainsäädännössä, pätevät seuraavat määräykset:
Sähkö- ja elektroniikkalaitteita ja paristoja ei saa hävittää talousjätteen mukana. Kuluttajalla on lain mukaan velvollisuus toimittaa sähkö- ja elektroniikkalaitteet niiden käyttöäin päätyttyä niille varattuun julkisiin keräyspisteisiin tai palauttaa ne myyntipaikkaan. Tähän liittyvästä yksityiskohdistaa säädetään kulloisenkin osavaltion laissa. Näistä määräyksistä mainitaan myös tuotteen symbolissa, käyttöohjeessa tai pakkaussessa. Uudelleenkäytöllä, materiaalien/paristojen uudelleenkäytöllä tai muilla vanhojen laitteiden uudelleenkäyttövoilla on tärkeä vaikutus yhteisen ympäristömme suojelussa.

PL Wskazówki dotyczące ochrony środowiska:



Od czasu wprowadzenia europejskiej dyrektywy 2002/96/EU i 2006/66/EU do prawa narodowego obowiązują następujące ustalenia: Urządzeni elektrycznych, elektronicznych oraz baterii jednorazowych nie należy wyrzucać razem z codziennymi odpadami domowymi! Użytkownik zobowiązany prawnie do odniesienia zepsutych, zniszczonych lub niepotrzebnych urządzeń elektrycznych i elektronicznych do punktu zbiórki lub do sortowawcy. Szczegółowe kwestie regulują przepisy prawne danego kraju. Informuje o tym symbol przekreślonego kosza umieszczony na opakowaniu. Segregując odpady pomagasz chronić środowisko!

H Környezetvédelmi tudnivalók:



Az európai irányelvek 2002/96/EU és 2006/66/EU ajánlása szerint, a megjelölt időponttól kezdve, minden EU-s tagállamban érvényesek a következők: Az elektromos és elektronikai készülékeket és az elemeket nem szabad a háztartási szemétkébe dobni! A leselejtezett elektromos és elektronikus készülékeket és elemeket, akkumulátorokat nem szabad a háztartási szemétkébe dobni. Az elhasznált és működésképtelen elektromos és elektronikus készülékek gyűjtésére törvényi előírás kötelez mindenkit, ezért azokat el kell szállítani egy kijelölt gyűjtő helyre vagy visszavinni a vásárlás helyére. A termék csomagolásán feltüntetett szimbólum egyértelmű jelzést ad erre vonatkozóan a felhasználónak. A régi készülékek begyűjtése, visszaváltása vagy bármilyen formában történő újra hasznosítása közös hozzájárulás környezetünk védelméhez.

CZ Ochrana životního prostředí:



Evropská směrnice 2002/96/EG a 2006/66/EU ustanovuje následující: Elektrická a elektronická zařízení stejně jako baterie nepatří do domovního odpadu. Spotřebitel se zavazuje odevzdat všechna zařízení a baterie po uplynutí jejich životnosti do příslušných sběrů. Podrobnosti stanoví zákon příslušné země. Symbol na produktu, návod k obsluze nebo balení na toto poukazuje. Recyklaci a jinými způsoby užití přispíváte k ochraně životního prostředí.

SK Ochrana životného prostredia:



Európska smernica 2002/96/EU a 2006/66/EU stanovuje: Elektrické a elektronické zariadenia, rovnako ako batérie sa nesmú vyhadzovať do domáceho odpadu. Spotrebiteľ je zo zákona povinný zlikvidovať elektrické a elektronické zariadenia, rovnako ako batérie na miesta k tomu určené. Symbolizuje to obrázok v návode na použitie, alebo na balení výrobku. Opätovným užitkovanim alebo inou formou recyklácie starých zariadení/batérií prispievate k ochrane životného prostredia.

P Nota em Protecção Ambiental:



Após a implementação da directiva comunitária 2002/96/EU e 2006/66/EU no sistema legal nacional, o seguinte aplica-se: Os aparelhos eléctricos e electrónicos, bem como baterias, não podem ser eliminados juntamente com o lixo doméstico. Consumidores estão obrigados por lei a colocar os aparelhos eléctricos e electrónicos, bem como baterias, sem uso em locais públicos específicos para este efeito ou no ponto de venda. Os detalhes para este processo são definidos por lei pelos respectivos países. Este símbolo no produto, o manual de instruções ou a embalagem indicam que o produto está sujeito a estes regulamentos. Reciclando, reutilizando os materiais dos seus velhos aparelhos/baterias, esta a fazer uma enorme contribuição para a protecção do ambiente.

RU Охрана окружающей среды:



С момента перехода национального законодательства на европейские нормы 2002/96/EU и 2006/66/EU действительно следующее: Электрические и электронные приборы, а также батареи запрещается утилизировать с обычным мусором. Потребитель, согласно закону, обязан утилизировать электрические и электронные приборы, а также батареи и аккумуляторы после их использования в специально предназначенных для этого пунктах сбора, либо в пунктах продажи. Детальная регламентация этих требований осуществляется соответствующим местным законодательством. Необходимо соблюдение данных предписаний обозначается особым значком на изделии, инструкции по эксплуатации или упаковке. При переработке, повторном использовании материалов или при другой форме утилизации бывших в употреблении приборов Вы помогаете охране окружающей среды. В соответствии с предписаниями по обращению с батареями, в Германии вышеназванные нормы действуют для утилизации батарей и аккумуляторов.

TR Çevre koruma uyarısı:



Avrupa Birliği Direktifi 2002/96/EU ve 2006/66/EU ulusal yasal uygulamalar için de geçerli olduğu tarihten itibaren: Elektrikli ve elektronik cihazlarla piller normal evsel çöpe atılmamalıdır. Tüketiciler için, artık çalışmayan elektrikli ve elektronik cihazlar piller, kamuya ait toplama yerlerine götürülme veya satın alınımları yerlere geri verme yasal bir zorunluluktur. Bu konu ile ilgili ayrıntılar ulusal yasalarla düzenlenmektedir. Ürün üzerinde, kullandığınız cihazınızda veya ambalajında bulunan bu sembol tüketicileri bu konuda uyarır. Eski cihazların geri kazanımı, yapıldıkları malzemelerin değerlendirilmesi veya diğer değerlendirme şekilleri ile, çevre korumasına önemli bir katkıda bulunursunuz. Yukarıda adı geçen atık toplama kuralları Almanya'da piller ve aküler için de geçerlidir.

RO Instrucțiuni pentru protecția mediului înconjurător:



Din momentul aplicării directivelor europene 2002/96/UE în dreptul național sunt valabile următoarele: Aparatele electrice și electronice nu pot fi salubritate cu gunoii menajer. Consumatorul este obligat conform legii să predea aparatele electrice și electronice la sfârșitul duratei de utilizare la locurile de colectare publice sau înapoți de unde au fost cumpărate. Detaliile sunt reglementate de către legislația țării respective. Simbolul de pe produs, în instrucțiunile de utilizare sau pe ambalaj indică aceste reglementări. Prin reciclarea, revalorificarea materialelor sau alte forme de valorificare a aparatelor scoase din uz aduceți o contribuție importantă la protecția mediului nostru înconjurător.

DK Anvisninger til beskyttelse af miljøet:



Fra og med indførelsen af EU-direktiverne 2002/96/EF og 2006/66/EF i national ret gælder følgende: Elektrisk og elektronisk udstyr samt batterier må ikke bortskaffes sammen med almindeligt husholdningsaffald. Forbrugeren er lovmæssigt forpligtet til at aflevere udtjent elektrisk og elektronisk udstyr samt batterier til dertil indrettede, offentlige indsamlingssteder eller til forhandleren. De nærmere bestemmelser vedr. dette fastlægges af lovgivningen i det pågældende land. Symbolet på produktet, brugsvejledningen eller emballagen henviser til disse bestemmelser. Ved genbrug, genvinding eller andre former for nyttiggørelse af udtjent udstyr/batterier giver du et vigtigt bidrag til beskyttelse af miljøet.

N Informasjon om beskyttelse av miljøet:



Fra tidspunktet for omsetning av de europeiske direktivene 2002/96/EF og 2006/66/EF i nasjonal rett gjelder følgende: Elektriske og elektroniske apparater og batterier må ikke deponeres sammen med husholdningsaffald. Forbrukeren er lovmessig forpliktet til å levere elektriske og elektroniske apparater og batterier til de offentlige samlestedene eller tilbake til stedet hvor produktene ble kjøpt. Detaljer angående dette reguleres av hvert land. Symbolet på produktet, bruksanvisningen eller emballasjen henviser om disse bestemmelsene. Med resirkulering, gjenbruk av stoffer eller andre former av gjenbruk av gamle apparater/batterier bidrar du betydelig til å beskytte miljøet vårt.

