

hama®

00062735



**Wireless LAN Router
MiMo 300 Express**

Inhaltsverzeichnis:

1.	Anschluß des Wireless LAN Routers.....	Seite 03
2.	Konfiguration von Betriebssystem und Computer	Seite 03
3.	Konfiguration des Wireless LAN Routers.....	Seite 05
3.1	Konfiguration der Internetverbindung mit Hilfe des Assistenten.....	Seite 05
3.2	Konfiguration des Wireless LAN.....	Seite 07
3.2.1	Basis Einstellungen für drahtlose Netzwerke	Seite 07
3.2.1.1	Betrieb als Accesspoint (AP)	Seite 07
3.2.1.2	Betrieb als AP Bridge-Point to Point.....	Seite 08
3.2.1.3	Betrieb als AP Bridge-Point to Multi-Point.....	Seite 08
3.2.1.4	Betrieb als AP Bridge WDS	Seite 09
3.2.2	Einstellung der Verschlüsselung für AP	Seite 09
3.2.2.1	WEP Verschlüsselung	Seite 10
3.2.2.2	WPA/WPA2 Verschlüsselung	Seite 11
3.2.3	Einstellung der Verschlüsselung für AP Bridge-Point to Point, Point to Multi-Point und WDS	Seite 12
3.2.3.1	WEP Verschlüsselung	Seite 13
3.2.3.2	WPA/WPA2 Verschlüsselung	Seite 13
3.3	Login-Daten ändern	Seite 14
3.4	LAN-Einstellungen.....	Seite 15
4.	Werkzeuge	Seite 15
4.1	Konfigurationswerkzeuge.....	Seite 16
4.2	Firmware-Aktualisierung.....	Seite 16
4.3	Neustart des Routers.....	Seite 16
5.	Statusinformationen.....	Seite 17
6.	Support- und Kontaktinformationen.....	Seite 17

Packungsinhalt:

- 1x** Hama Wireless LAN Router MiMo 300 Express
- 1x** Netzteil 12V
- 1x** gedruckte Bedienungsanleitung

Systemvoraussetzung:

- Betriebssystem mit installiertem TCP/IP Protokoll
- Java fähiger Webbrowser wie z. B. Mozilla Firefox oder Microsoft Internet Explorer

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.

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 „Verbindung bei Bedarf“ auszuwählen, damit der Internetzugang automatisch nach der eingestellten Zeit, unter der Option „Leerlaufzeit“, getrennt wird. 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 oder vom Modem trennen.

1. Anschluss des Wireless LAN Routers

1. 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). Der eingebaute Switch erkennt selbständig die Verbindungsgeschwindigkeit von 10 oder 100 Mbps, half/full Duplex Übertragungsmodus, sowie den verwendeten Kabeltyp.
2. Verbinden Sie den Ethernet-Port Ihres Modems mit dem Anschluss „WAN“ am Router. Je nach Modem wird ein 1:1 oder Cross-Over belegtes Kabel benötigt. In den meisten Fällen kann das bereits vorhandene Anschlusskabel verwendet werden.
3. Stecken Sie nun das mitgelieferte Netzgerät 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	Blinkt	Wireless LAN ist aktiviert / es werden Daten gesendet
	Aus	Wireless LAN ist deaktiviert
WAN	Leuchtet	Der WAN- Port hat eine korrekte Netzwerkverbindung hergestellt
	Blinkt	Datentransfer über WAN- Port
	Aus	Keine Verbindung
LAN1-4	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:
Start -> Einstellungen -> Systemsteuerung -> 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 6.0 und neuer oder Mozilla Firefox)



3. Konfiguration des Wireless LAN Routers

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 zu benutzen oder die Einrichtung manuell vorzunehmen. Nach der Konfiguration mit Hilfe des Assistenten ist das Gerät soweit eingerichtet, dass die angeschlossenen Computer Zugang zum Internet haben.

Hinweis !!! Zur Sicherheit sollten Sie Benutzername und Passwort auf jeden Fall ändern. Die Standardwerte sind bei vielen Geräten gleich und könnten fremden Personen Zugriff zur Routerkonfiguration gewähren. Informationen dazu finden Sie auf Seite 14.

3.1 Konfiguration der Internetverbindung mit Hilfe des Assistenten

Bitte starten Sie den Assistenten nach dem Einloggen indem Sie auf die Schaltfläche **Quick Setup** klicken.

Time Zone

Wählen Sie unter **Set Time Zone** die korrekte Zeitzone, z. B. für Deutschland „(GMT +01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna“. Die restlichen Einstellungen können ohne Änderung übernommen werden. Klicken Sie um fortzufahren auf **Next**.

Broadband 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**. In Österreich wird hingegen häufig PPTP verwendet. Die benutzerspezifischen Informationen erhalten Sie von ihrem Serviceprovider. Für die verschiedenen Verbindungstypen gibt es auf der Übersichtsseite eine Kurzbeschreibung. Auf Grund der weiten Verbreitung von DSL über **PPPoE** bezieht sich die weitere Beschreibung auf diesen Verbindungstyp. Für den Verbindungstyp **PPPoE** klicken Sie auf **PPPoE xDSL**.

IP-Adress Info

In der folgenden Ansicht müssen Sie die Zugangsdaten für Ihren Provider eingeben. Diese Informationen erhalten Sie entweder aus Ihren Unterlagen oder direkt vom Provider.

The screenshot shows the '3.P Address info' configuration page for PPPoE. The page title is '3.P Address info'. Below the title, there is a section for 'PPPoE' with instructions: 'Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a "Service Name" enter it in the Service Name field, otherwise, leave it blank.' The form contains the following fields:

User Name	Gerätezone
Password	*****
Service Name	
MTU	1392 (Standard Value: 1452)
Connection Type	Connect on Demand W Connect Disconnect
Idle Time Out	12 (0-100minutes)

At the bottom right of the form, there are 'Back' and 'Ok' buttons. The left sidebar shows a navigation menu with 'WAN' selected and sub-options like 'Dynamic IP', 'Static IP', 'PPPoE', 'LTP', 'Telstra Big Pond', 'DNS', and 'DMZ'. Other sections include 'LAN', 'Wireless', 'QoS', 'NAT', and 'Firewall'.

Bitte geben Sie ein: **User Name**
Password
Service Name (diese Angabe ist nicht immer erforderlich)

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-Suffix das Zeichen #.

AAAAAAAAAAAAATTTTTTTTTT#MMMM@t-online.de

Zusätzlich zu den Zugangsdaten können Sie noch folgende Angaben machen:

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 512 und 1492 möglich.

Mit der Angabe des **Connection Type** bestimmen Sie das Einwahlverhalten Ihres Routers. Sie haben die Wahl zwischen:

Continuous: Der Router ist immer mit dem Internet verbunden. Dieser Verbindungstyp ist zu empfehlen, wenn Sie z. B. eine Flatrate ohne Zeitbegrenzung haben.

Connect on Demand: Bei diesem Verbindungstyp wählt sich der Router erst bei einer Anforderung durch einen angeschlossenen Computer ein, z. B. wenn Sie an einem Computer den Browser öffnen. Die Verbindung besteht dann so lange, bis die unter **Idle Time Out** eingestellte Zeit, ohne Aktivität abgelaufen ist.

Manual: Entscheiden Sie sich für den Verbindungstyp **Manual**, können Sie die Verbindung über den Button **Connect** herstellen und über den Button **Disconnect** wieder beenden.

Hinweis !!! Bei Volumen- bzw. Zeittarifen ist es empfehlenswert die Auswahl „Verbindung bei Bedarf“ auszuwählen, damit der Internetzugang automatisch nach der eingestellten Zeit, unter der Option „Leerlaufzeit“, getrennt wird. 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 oder vom Modem trennen.

Idle Time Out: Legen Sie hier fest, nach wie vielen Minuten Inaktivität die Internetverbindung getrennt werden soll. Es sind Werte zwischen 1 und 1000 möglich.

Bestätigen Sie die Angaben mit Klick auf **OK**. Anschließend müssen Sie den Router neu starten, damit die Einstellungen wirksam werden. Drücken Sie dazu im nächsten Fenster auf **Apply** zum Übernehmen. Der Router benötigt nun ca. 30 Sekunden um neu zu starten. Nach dem Neustart ist der Router soweit konfiguriert, dass Sie mit den angebotenen Computern auf das Internet zugreifen können. Sie können diese Einstellungen auch manuell ändern, indem Sie im Menü links **WAN** und danach den entsprechenden Verbindungstyp wählen.

3.2 Konfiguration des Wireless LAN

Standardmäßig ist das Wireless LAN zu Ihrem Schutz deaktiviert. Möchten Sie die Funktion aktivieren, wählen Sie von der Startansicht ausgehend, die Sie durch Klick auf **Home** wieder erreichen, zuerst **General Setup** und anschließend in der Menüleiste links **Wireless**. Beachten Sie, dass eine Aktivierung des Wireless LAN ohne zusätzliche Einstellung einer Verschlüsselung ein Sicherheitsrisiko mit sich bringt. Markieren Sie jetzt **Enable** und klicken danach auf **Apply**. Fahren Sie fort mit Basis Einstellungen für drahtlose Netzwerke!

3.2.1 Basis Einstellungen für drahtlose Netzwerke (WLAN)

Wählen Sie im Menü links **Basic Settings**.

Unter dem Punkt **Mode** können Sie wählen, welche Aufgabe der Router im Netzwerk übernehmen soll.

Wählen Sie die Funktion Accesspoint **AP (3.2.1.1)**, wenn das Gerät der einzige Accesspoint in Ihrem Netzwerk ist oder keine Verbindung auf Bridge-Ebene zu anderen Accesspoints hergestellt werden soll.

Wählen Sie **AP Bridge-Point to Point (3.2.1.2)**, wenn Sie diesen Accesspoint mit einem zweitem Accesspoint drahtlos verbinden möchten. Clients haben in diesem Modus nicht die Möglichkeit sich über eine drahtlose Verbindung anzumelden.

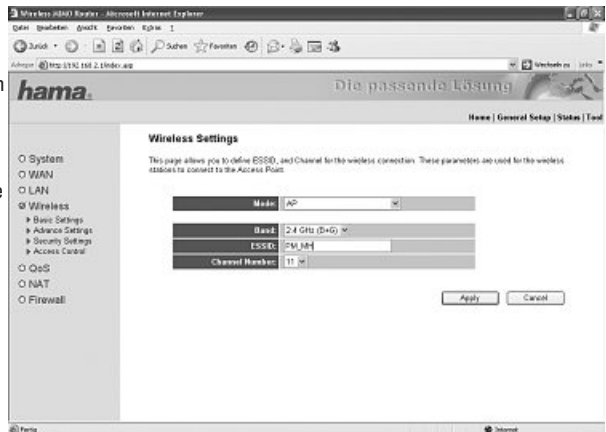
Wählen Sie **AP Bridge-Point to Multi-Point (3.2.1.3)**, wenn Sie diesen Accesspoint mit mehreren anderen Accesspoints drahtlos verbinden möchten. Clients haben in diesem Modus nicht die Möglichkeit sich über eine drahtlose Verbindung anzumelden.

Wählen Sie **AP Bridge WDS (3.2.1.4)**, wenn Sie diesen Accesspoint mit einem oder mehreren anderen Accesspoints drahtlos verbinden möchten und Clients weiterhin die drahtlose Anmeldung gewährt werden soll.

Setzen Sie die Konfiguration entsprechend ihrer Wahl fort.

3.2.1.1 Betrieb als Accesspoint (AP)

Mit der Auswahl unter **Band** legen Sie fest, ob das Gerät im 2,4 Ghz Band nach Standard 802.11b (11Mbps), 802.11g (54Mbps) oder kombiniert mit 802.11b und 802.11g arbeitet. Legen Sie anschließend die **ESSID** fest. Die Länge der **ESSID** kann bis zu 32 Zeichen betragen und muss für alle Geräte im Netzwerk identisch sein. Unter **Channel Number** legen Sie den Kanal fest, in dem die Daten übertragen werden sollen. Es stehen 13 Kanäle zur Verfügung.



Beispiel für eine ESSID : „WLAN_Router_54Mbps“

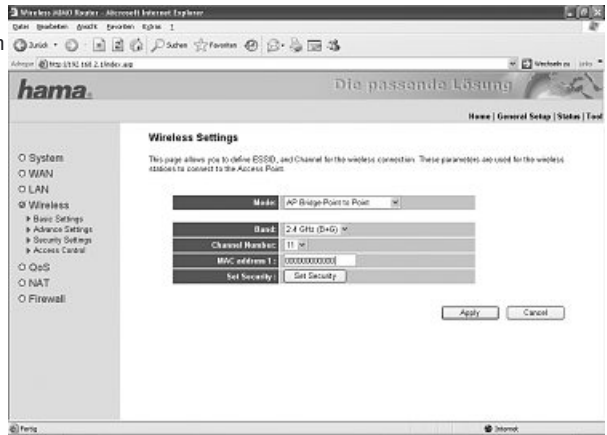
Übernehmen Sie Ihre Einstellungen durch Klick auf den **Apply** Button!

Um die Verschlüsselung für ihr drahtloses Netzwerk einzustellen, klicken Sie in der anschließenden Ansicht auf den Button **Continue** und danach auf **Security Settings** im Menü links. Für die Anleitung zur Einstellung der Wireless LAN Verschlüsselung lesen Sie auf Seite 09 weiter.

Möchten Sie ein drahtloses Netzwerk ohne Verschlüsselung betreiben, klicken Sie in der nächsten Ansicht auf **Apply**. Der Router wird anschließend neu gestartet. Nach dem Neustart steht das drahtlose Netzwerk zur Verfügung.

3.2.1.2 Betrieb als AP Bridge-Point to Point

Mit der Auswahl unter **Band** legen Sie fest, ob das Gerät im 2,4 Ghz Band nach Standard 802.11b (11Mbps), 802.11g (54Mbps) oder kombiniert mit 802.11b und 802.11g arbeitet. Unter **Channel Number** legen Sie den Kanal fest, in dem die Daten übertragen werden sollen. Es stehen 13 Kanäle zur Verfügung. Geben Sie im Feld **MAC address 1** die Adresse des Accesspoints ein zu dem die Bridge-Verbindung aufgebaut werden soll. Um die Verschlüsselung für ihr drahtloses Netzwerk einzustellen, klicken Sie anschließend auf den Button **Set Security**.

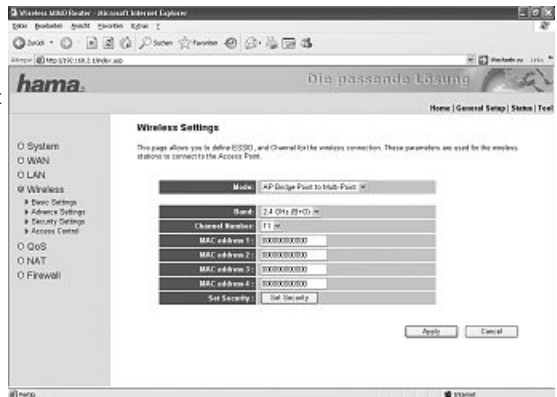


Für die Anleitung zur Einstellung der Wireless LAN Verschlüsselung lesen Sie auf Seite 12 weiter.

Möchten Sie ein drahtloses Netzwerk ohne Verschlüsselung betreiben, klicken Sie **Apply** und in der folgenden Ansicht auch **Apply**. Der Router wird anschließend neu gestartet. Nach dem Neustart steht das drahtlose Netzwerk zur Verfügung.

3.2.1.3 Betrieb als AP Bridge-Point to Multi-Point

Der Unterschied zum AP Bridge-Point to Point Betrieb ist, dass Sie in diesem Modus MAC-Adressen mehrerer Accesspoints eingeben können. Eine Bridge-Verbindung ist maximal zu 6 anderen Accesspoints möglich. Mit der Auswahl unter **Band** legen Sie fest, ob das Gerät im 2,4 Ghz Band nach Standard 802.11b (11Mbps), 802.11g (54Mbps) oder kombiniert mit 802.11b und 802.11g arbeitet. Unter **Channel Number** legen Sie den Kanal fest, in dem die Daten übertragen werden sollen. Es stehen 13 Kanäle zur Verfügung. Geben Sie in den Feldern **MAC address 1** bis **MAC address 6** die Adressen der Accesspoints ein zu denen die Bridge-Verbindung aufgebaut werden soll. Um die Verschlüsselung für ihr drahtloses Netzwerk einzustellen, klicken Sie anschließend auf den Button **Set Security**.



Für die Anleitung zur Einstellung der Wireless LAN Verschlüsselung lesen Sie auf Seite 12 weiter.

Möchten Sie ein drahtloses Netzwerk ohne Verschlüsselung betreiben, klicken Sie **Apply** und in der folgenden Ansicht auch **Apply**. Der Router wird anschließend neu gestartet. Nach dem Neustart steht das drahtlose Netzwerk zur Verfügung.

3.2.1.4 Betrieb als AP Bridge WDS

Was ist **WDS**? Wireless Distribution System bezeichnet die drahtlose Verbindung zwischen mehreren Access Points untereinander, und ermöglicht außerdem die Anmeldung von Clients, was andere Bridge Betriebsarten nicht zulassen. Dabei wird für jeden zusätzlichen Access Point die Bandbreite des Netzes halbiert, weil die Pakete doppelt übertragen werden müssen.

Es ergibt sich also eine Kombination der vorangegangenen Betriebsarten.

Mit der Auswahl unter **Band** legen Sie fest, ob das Gerät im 2,4 Ghz Band nach Standard 802.11b (11Mbps), 802.11g (54Mbps) oder kombiniert mit 802.11b und 802.11g arbeitet. Für das Client-Netzwerk wird die **ESSID** benötigt, die zur Identifikation im Netzwerk dient und somit für alle Teilnehmer des Client-Netzwerkes gleich sein muss. Die Länge der **ESSID** kann bis zu 32 Zeichen betragen.



Unter **Channel Number** legen Sie den Kanal fest, in dem die Daten übertragen werden sollen. Es stehen 13 Kanäle zur Verfügung. Geben Sie in den Feldern **MAC address 1** bis **MAC address 6** die Adressen der Accesspoints ein zu denen die Bridge-Verbindung aufgebaut werden soll. Um die Verschlüsselung für ihr drahtloses Netzwerk einzustellen, klicken Sie anschließend auf den Button **Set Security**.

Für die Anleitung zur Einstellung der Wireless LAN Verschlüsselung lesen Sie auf Seite 12 weiter.

Möchten Sie ein drahtloses Netzwerk ohne Verschlüsselung betreiben, klicken Sie **Apply** und in der folgenden Ansicht auch **Apply**. Der Router wird anschließend neu gestartet. Nach dem Neustart steht das drahtlose Netzwerk zur Verfügung.

3.2.2 Einstellung der Verschlüsselung für AP

Als erstes ist es wichtig verschiedene Begriffe zu unterscheiden. Dazu eine kurze Erklärung der wichtigsten, hier verwendeten Begriffe:

Authentifizierung: Die Authentifizierung ist ein Vorgang, bei dem die Identität, zum Beispiel einer Person, an Hand eines bestimmten Merkmals festgestellt wird. Dies kann zum Beispiel mit einem Fingerabdruck, einem Passwort oder einem beliebigen anderen Berechtigungsnachweis geschehen.

Verschlüsselung: Die Verschlüsselung ist ein Vorgang, bei dem ein „Klartext“ mit Hilfe eines Verschlüsselungsverfahrens (Algorithmus) in einen „Geheimtext“ umgewandelt wird. Hierzu können einer oder auch mehrere Schlüssel verwendet werden. Weiterhin ist zu erwähnen, dass jedes einzelne Verschlüsselungsverfahren eine oder mehrere Möglichkeiten der Authentifizierung bietet.

Für diese Betriebsart stehen folgende Verschlüsselungen zur Verfügung:

- **WEP-Verschlüsselung mit 64 Bit und 128 Bit**
- **WPA und WPA2 Verschlüsselung**

Für die Betriebsart **AP**, können Sie die Einstellungen unter **Wireless/Security Settings** im Menü links vornehmen.

Standardmäßig ist die Verschlüsselung deaktiviert. Wir empfehlen Ihnen aber aus Sicherheitsgründen immer eine Verschlüsselung zu verwenden.

3.2.2.1 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 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. Wählen Sie als nächstes für das **Key Format** zwischen Hex (Sie können Zeichen von 0-9 und a-f verwenden) und ASCII aus (Sie dürfen jedes beliebige Zeichen verwenden), wodurch auch die Länge des Schlüssels bestimmt wird.

Unter **Default Tx Key** haben Sie die Möglichkeit, einen von vier voreingestellten Schlüsseln auszuwählen. 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) = 231074a6ef
64 bit ASCII (5 Zeichen) = j31n!

128 bit Hex (26 Zeichen) = 231074a6b9773ce43f91a5bef3
128 bit ASCII (13 Zeichen) = urlaub2006!+0

Um Ihre Einstellungen zu speichern klicken Sie bitte auf **Apply**. Anschließend muss der Router neu gestartet werden, damit alle Einstellungen wirksam werden. Klicken Sie dazu in der folgenden Ansicht auf **Apply**. Nach dem Neustart ist das drahtlose Netzwerk mit Verschlüsselung verfügbar.

3.2.2.2 WPA/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) oder Extensible Authentication Protocol (EAP) wofür jedoch ein Radius Server erforderlich ist. WPA2 ist die Weiterentwicklung von WPA und nutzt einen anderen Verschlüsselungsalgorithmus AES (Advanced Encryption Standard).

Bezüglich der Authentifizierung wird bei WPA zwischen **Pre-shared-key** und der Authentifizierung über spezielle **Authentifizierungsprotokolle**, bei denen es sich meist um Abwandlungen des EAP (Extensible Authentication Protocol) handelt, unterschieden. Für die zweite, im privaten Bereich doch eher seltene Authentifizierungsmethode wird ein so genannter Authentifizierungsserver (RADIUS-Server) verwendet. Die Angaben, die sie zur Konfiguration dieser Authentifizierungsmethode benötigen, erhalten Sie von ihrem Administrator.

WPA pre-shared-key (für die meisten Anwender empfohlen)

Wählen Sie als erstes, ob Sie **WPA mit TKIP** Verschlüsselungsalgorithmus, **WPA2 mit AES** Verschlüsselungsalgorithmus oder den **WPA Mixed** Modus verwenden möchten. Dieser Mixed Modus erlaubt Clients mit WPA oder WPA2 auf den Access-Point zuzugreifen. Die Mixtur ist sehr sinnvoll, da momentan nur wenige XP-Clients WPA2-fähig sind. Ist der Mixed Mode abgeschaltet, so lässt der AP nur Clients mit WPA2 zu und die große Zahl der WPA(TKIP)-Geräte bleibt draußen.

Als nächstes bestimmen Sie das Schlüsselformat (**Pre-shared Key Format**). Wählen Sie entweder **Passphrase** für einen Schlüssel mit einer Länge von mindestens 8 und höchstens 63 Zeichen, wobei Buchstaben (A-Z), Zahlen und Satzzeichen erlaubt sind oder **Hex** für einen Schlüssel mit einer Länge von 64 Zeichen, wobei nur Zeichen von 0-9 und a-f verwendet werden dürfen.

Der nächste Schritt ist die Eingabe des Schlüssels, des so genannten **Pre-shared-key** (PSK). Möchte ein Client auf den Access-Point zugreifen, muss er diese Zeichenfolge kennen.

Um Ihre Einstellungen zu speichern, klicken Sie bitte auf **Apply**. Anschließend muss der Router neu gestartet werden, damit alle Einstellungen wirksam werden. Klicken Sie dazu in der folgenden Ansicht auf **Apply**. Nach dem Neustart ist das drahtlose Netzwerk mit Verschlüsselung verfügbar.



WPA RADIUS (ein spezieller Authentifizierungs-Server ist erforderlich)

Wählen Sie als erstes, ob Sie **WPA mit TKIP** Verschlüsselungsalgorithmus, **WPA2 mit AES** Verschlüsselungsalgorithmus oder den **WPA Mixed** Modus verwenden möchten. Dieser Mixed Modus erlaubt Clients mit WPA oder WPA2 auf den Access-Point zuzugreifen. Die Mixtur ist sehr sinnvoll, da momentan nur wenige XP-Clients WPA2-fähig sind.

Wählen Sie nur **WPA2 (AES)**, so lässt der AP nur Clients mit WPA2 zu und die große Zahl der WPA(TKIP)-Geräte bleibt draußen.

Als nächstes geben Sie die **RADIUS Server IP address** an. Der **RADIUS Server Port** ist auf 1812 voreingestellt. Geben Sie jetzt noch das **Password** für den RADIUS Server ein.

Um Ihre Einstellungen zu speichern, klicken Sie bitte auf **Apply**. Anschließend muss der Router neu gestartet werden, damit alle Einstellungen wirksam werden. Klicken Sie dazu in der folgenden Ansicht auf **Apply**. Nach dem Neustart ist das drahtlose Netzwerk mit Verschlüsselung verfügbar.

3.2.3 Einstellung der Verschlüsselung für Bridge-Point to Point, Bridge-Point to Multi-Point und Bridge WDS

Als erstes ist es wichtig verschiedene Begriffe zu unterscheiden. Dazu eine kurze Erklärung der wichtigsten, hier verwendeten Begriffe:

Authentifizierung: Die Authentifizierung ist ein Vorgang, bei dem die Identität, zum Beispiel einer Person, an Hand eines bestimmten Merkmals festgestellt wird. Dies kann zum Beispiel mit einem Fingerabdruck, einem Passwort oder einem beliebigen anderen Berechtigungsnachweis geschehen.

Verschlüsselung: Die Verschlüsselung ist ein Vorgang, bei dem ein „Klartext“ mit Hilfe eines Verschlüsselungsverfahrens (Algorithmus) in einen „Geheimtext“ umgewandelt wird. Hierzu können einer oder auch mehrere Schlüssel verwendet werden. Weiterhin ist zu erwähnen, dass jedes einzelne Verschlüsselungsverfahren eine oder mehrere Möglichkeiten der Authentifizierung bietet.

Für die verschiedenen Betriebsarten stehen folgende Verschlüsselungen zur Verfügung:

- **WEP-Verschlüsselung mit 64 Bit und 128 Bit**
- **WPA(TKIP) und WPA2(AES) Verschlüsselung**

Für die Betriebsarten **Bridge-Point to Point, Bridge-Point to Multi-Point und Bridge WDS** können Sie die Einstellungen am Ende der jeweiligen Betriebsart-Einstellungen, durch Klick auf den Button **Set Security** vornehmen.

Für die Betriebsart **Bridge WDS** muss auch unter **Wireless/Security Settings** im Menü links eine Verschlüsselung für den Accesspoint eingestellt werden. Nur diese Verschlüsselung ist dann auch für WDS verfügbar.

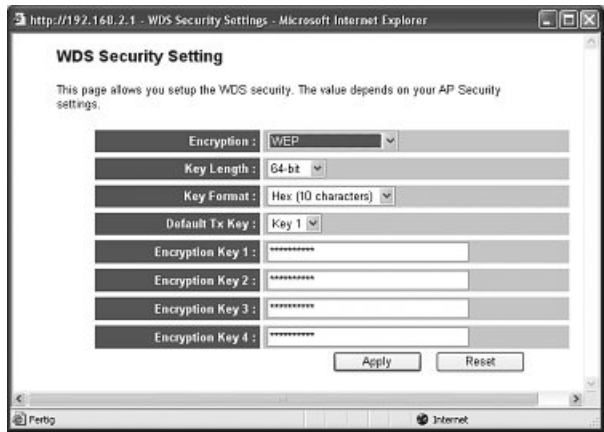
Sie haben die Wahl zwischen **WEP**-Verschlüsselung mit **64 Bit** und **128 Bit**, **WPA** mit **TKIP** Verschlüsselungsalgorithmus und **WPA2 mit AES** Verschlüsselungsalgorithmus.

3.2.3.1 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 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. Wählen Sie als nächstes für das **Key Format** zwischen Hex (Sie können Zeichen von 0-9 und a-f verwenden) und ASCII aus (Sie dürfen jedes beliebige Zeichen verwenden), wodurch auch die Länge des Schlüssels bestimmt wird.

Unter **Default Tx Key** haben Sie die Möglichkeit, einen von vier voreingestellten Schlüsseln auszuwählen. Wählen Sie dazu z. B. **Key 1** und geben in die darunter liegenden Felder Ihre Schlüssel mit der erforderlichen Länge ein.



Beispiele: 64 bit Hex (10 Zeichen) = 231074a6ef
 64 bit ASCII (5 Zeichen) = ¡31n!

128 bit Hex (26 Zeichen) = 231074a6b9773ce43f91a5bef3
 128 bit ASCII (13 Zeichen) = urlaub2006!+0

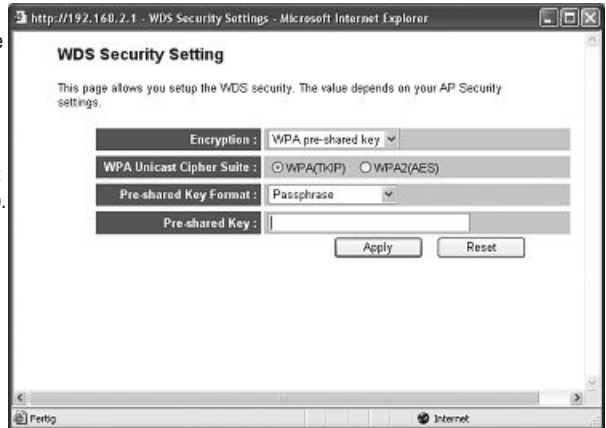
Um Ihre Einstellungen zu speichern, klicken Sie bitte auf **Apply**. Anschließend muss der Router neu gestartet werden, damit alle Einstellungen wirksam werden. Klicken Sie dazu in der folgenden Ansicht auf **Apply**. Nach dem Neustart ist das drahtlose Netzwerk mit Verschlüsselung verfügbar.

3.2.3.2 WPA/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) oder Extensible Authentication Protocol (EAP) wofür jedoch ein Radius Server erforderlich ist. WPA2 ist die Weiterentwicklung von WPA und nutzt einen anderen Verschlüsselungsalgorithmus AES (Advanced Encryption Standard).

Wählen Sie unter Encryption **WPA pre-shared Key**. Danach bestimmen Sie unter WPA Unicast Cipher Suite, ob Sie WPA (TKIP) oder WPA (AES) verwenden möchten.

Als nächstes bestimmen Sie das Format des Schlüssels (**Pre-shared Key Format**). Wählen Sie entweder **Passphrase** für einen Schlüssel mit einer Länge von mindestens 8 und höchstens 63 Zeichen, wobei Buchstaben (A-Z), Zahlen und Satzzeichen erlaubt sind oder **Hex** für einen Schlüssel mit einer Länge von 64 Zeichen, wobei nur Zeichen von 0-9 und a-f verwendet werden dürfen.



Der nächste Schritt ist die Eingabe des Schlüssels, des so genannten **Pre-shared-key** (PSK). Möchte ein Client auf den Access-Point zugreifen, muss er diese Zeichenfolge kennen.

Um Ihre Einstellungen zu speichern, klicken Sie bitte auf **Apply**. Anschließend muss der Router neu gestartet werden, damit alle Einstellungen wirksam werden. Klicken Sie dazu in der folgenden Ansicht auf **Apply**. Nach dem Neustart ist das drahtlose Netzwerk mit Verschlüsselung verfügbar.

3.3 Login-Daten ändern

Von der Startansicht ausgehend, die Sie durch Klick auf **Home** wieder erreichen, wählen Sie bitte **General Setup** und dann im Menü links **System => Password Settings**.

Auf dieser Seite können Sie ein neues Kennwort für den Router festlegen. Um ein neues Passwort vergeben zu können, muss zuerst das aktuelle Passwort in das Feld **Current Password** eingegeben werden. Das neue Passwort tragen Sie bitte im Feld **New Password** ein und Bestätigen die korrekte Schreibweise durch wiederholte Eingabe im Feld **Confirmed Password**. Bestätigen Sie ihre Eingaben mit **Apply**. Anschließend muss der Router neu gestartet werden, damit alle Einstellungen wirksam werden. Klicken Sie dazu in der folgenden Ansicht auf **Apply**. Nach dem Neustart ist das neue Kennwort gültig.

3.4 LAN Einstellungen

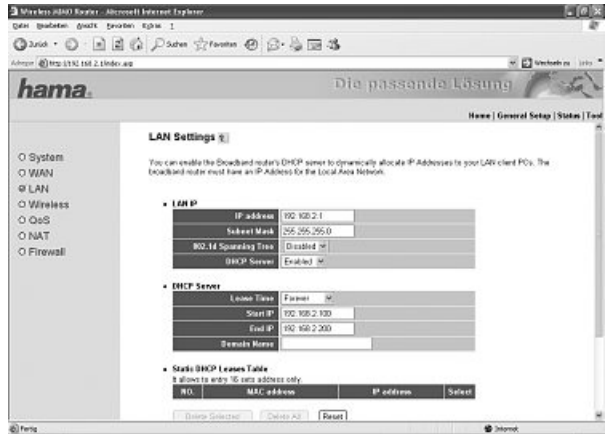
Von der Startansicht ausgehend, die Sie durch Klick auf **Home** wieder erreichen, wählen Sie bitte **General Setup** und dann im Menü links **LAN**.

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

LAN IP: Der Router ist auf die IP-Adresse 192.168.2.1 voreingestellt. Möchten Sie eine andere Adresse für den Router verwenden, können Sie diese in diesem Eingabefeld ändern. Im Eingabefeld direkt darunter wird die entsprechende **Subnet Mask** eingetragen.

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**. Möchten Sie den DHCP-Server verwenden, wählen Sie **Enabled** 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. In der unteren Tabelle haben Sie die Möglichkeit, eine bestimmte MAC-Adresse eine IP Adresse aus dem gültigen Bereich fest zu zuordnen. Meldet sich der Client am Router an bekommt er immer diese IP-Adresse zugewiesen. Markieren Sie hierzu **Enable Static DHCP Lease** und tragen in die leeren Felder der untersten Tabelle die MAC-Adress und IP Adresse ein. Nach einem Klick auf den **Add** Button wird der Eintrag in der Tabelle gespeichert. Bestätigen Sie ihre Eingaben mit **Apply**. Anschließend muss der Router neu gestartet werden, damit alle Einstellungen wirksam werden. Klicken Sie dazu in der folgenden Ansicht auf **Apply**.



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

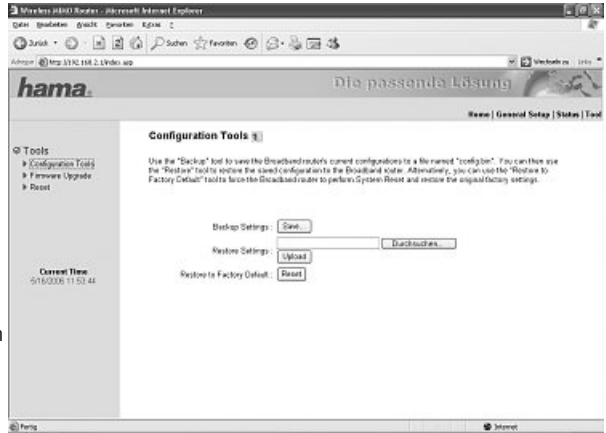
4. Werkzeuge

Der Hama Wireless LAN Router stellt Ihnen verschiedene Werkzeuge zur Verfügung, die Sie bei der Konfiguration und Handhabung des Gerätes unterstützen sollen.

4.1 Konfigurationswerkzeug

Von der Startansicht ausgehend, die Sie durch Klick auf **Home** wieder erreichen, wählen Sie bitte **Tools** im Menü oben rechts und danach **Konfiguration Tools** im Menü links!

Auf dieser Seite haben Sie die Möglichkeit, die gesamte Konfiguration des Routers zu speichern. Klicken Sie dazu auf den Button **Save**. Wählen Sie anschließend den Zielordner aus. Außerdem sollten Sie einen Dateinamen festlegen, der es ermöglicht, die Datei eindeutig zu identifizieren. Nach ihrer Auswahl klicken Sie auf **Save** und haben somit ihre Einstellungen gesichert. Möchten Sie zu einem späteren Zeitpunkt die gesicherten Einstellungen wiederherstellen, klicken Sie auf **Durchsuchen** und wählen danach die gewünschte Konfigurationsdatei aus. Um die Datei zu laden, klicken Sie auf **Upload**. Der Router benötigt nun einige Sekunden, die Datei zu laden und danach eine Neustart durchzuführen. Nach dem Neustart ist die ausgewählte Konfiguration gültig.



Möchten Sie ihren Router auf die werkseitigen Standardeinstellungen zurücksetzen, klicken Sie auf den Button **Reset (Restore to Factory Default)**. Bestätigen Sie die anschließende Abfrage mit **OK**, es erfolgt die Zurücksetzung aller Einstellungen auf Standardwerte.

4.2 Firmware-Aktualisierung

Von der Startansicht ausgehend, die Sie durch Klick auf **Home** wieder erreichen, wählen Sie bitte **Tools** im Menü oben rechts und danach **Firmware Upgrade** im Menü links! Klicken Sie in der nächsten Ansicht auf **Next**.

Um die neue Firmware-Datei auszuwählen, klicken Sie in der folgenden Ansicht auf **Durchsuchen**. Haben Sie die Datei gewählt, klicken Sie auf **Apply**. Die neue Firmware wird geladen und der Router neu gestartet.

Achtung!! Durch das Laden der neuen Firmware gehen vorher getroffene Einstellungen verloren.

4.3 Neustart des Routers

Von der Startansicht ausgehend, die Sie durch Klick auf **Home** wieder erreichen, wählen Sie bitte **Tools** im Menü oben rechts und danach **Reset** im Menü links!

Klicken Sie in dieser Ansicht auf **Apply** und bestätigen den folgenden Hinweis mit **OK**, wird der Router neu gestartet. Ihre getroffenen Einstellungen gehen dabei nicht verloren.

5. Statusinformationen

Von der Startansicht ausgehend, die Sie durch Klick auf **Home** wieder erreichen, wählen Sie bitte **Status** im Menü oben rechts.

Im Menü auf der linken Seite können Sie sich in verschiedenen Untermenüs weitreichende Informationen, wie zum Beispiel **Internet Connection**, **Device Status** oder **Active DHCP-Clients** anzeigen lassen. Weiterhin ist unter dem Menüpunkt **Statistics** ein Packetzähler verfügbar.

6. 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, neue Treiber 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

Anmerkung:

Dieses Produkt darf nur in Deutschland, Österreich, Schweiz, England, Frankreich, Belgien, Spanien, Niederlande, Dänemark, Ungarn, Polen, Schweden, Luxemburg, Irland, Griechenland, Tschechische Republik, Slowakische Republik und Finnland betrieben werden!

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

Contents:

1.	Connecting the Wireless LAN Router	Page 03
2.	Configuring the operating system and computer.....	Page 03
3.	Configuring the Wireless LAN Router.....	Page 05
3.1	Configuring the Internet Connection using the Wizard.....	Page 05
3.2	Configuring the Wireless LAN.....	Page 06
3.2.1	Basic Settings for Wireless Networks.....	Page 06
3.2.1.1	Operation as an Access Point (AP)	Page 07
3.2.1.2	Operation as an AP Bridge Point to Point	Page 08
3.2.1.3	Operation as an AP Bridge Point to Multi-Point.....	Page 08
3.2.1.4	Operation as an AP Bridge WDS	Page 09
3.2.2	Setting the Encryption for AP	Page 09
3.2.2.1	WEP Encryption	Page 10
3.2.2.2	WPA/WPA2 encryption.....	Page 10
3.2.3	Setting the Encryption for AP Bridge-Point to Point, Point to Multi-Point and WDS.....	Page 11
3.2.3.1	WEP Encryption	Page 12
3.2.3.2	WPA/WPA2 Encryption.....	Page 13
3.3	Changing the Log-in Data.....	Page 13
3.4	LAN Settings.....	Page 13
4.	Tools.....	Page 14
4.1	Configuration Tools	Page 14
4.2	Firmware Update	Page 15
4.3	Re-starting the Router	Page 15
5.	Status Information	Page 15
6.	Support and Contact Information	Page 15

Packet contents:

- 1x Hama Wireless LAN Router MiMo 300 Express
- 1x 12V power supply
- 1x printed operating instructions

System requirements:

- Operating system with TCP/IP protocol installed
- Java-capable web browser such as Mozilla Firefox or Microsoft Internet Explorer

Safety instructions:

Do not use the device in moist or extremely dusty areas, on radiators or in the vicinity of 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.

Caution! 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 as required” setting is recommended for volume or timed rates, so that the internet connection is disconnected automatically after the period set in the „Idle time” option. Connection costs may be high if permanently connected. Please also note that closing the browser does not automatically disconnect from the internet. Many programs send queries to the internet or receive data from it without this being clearly visible. For the router, these queries 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 or disconnect it from the modem.

1. Connecting the Wireless LAN Router

1. Connect the computers and other network devices such as hubs/switches to sockets 1-4. Use a crossover or CAT5 patch cable (max. 100m). The integrated switch automatically identifies the connection speed of 10 or 100Mbps, half/full duplex transfer mode and the type of cable used.
2. Connect the Ethernet port of your modem to the WAN connection on the router. A 1:1 or crossover cable is required depending on the modem. In most cases, the existing connection cable can be used.
3. Plug the power unit supplied into an empty socket and connect it to the router. Caution: Unsuitable power supply units can cause damage!

Checking Installation

There are various status indicating LEDs on the top of the device:

LED	Condition	Status
Power	Illuminated	Power unit is connected and supplying electricity
	Off	No power unit connected, device not being supplied with electricity
WLAN	Flashing	Wireless LAN is activated / data is being sent
	Off	Wireless LAN is deactivated
WAN	Illuminated	The WAN port has generated a correct network connection
	Flashing	Data transfer via WAN port
	Off	No connection
LAN1-4	Illuminated	The corresponding LAN port has generated a correct network connection
	Flashing	Data transfer via respective LAN port
	Off	No connection

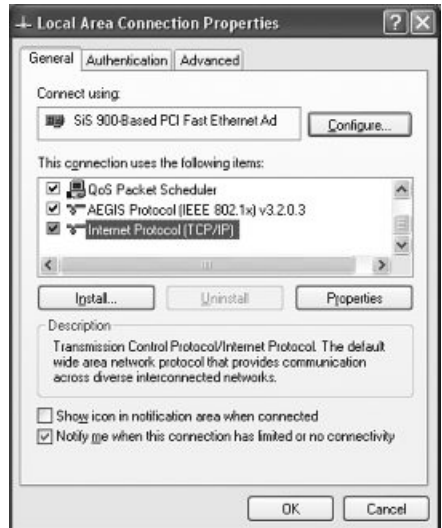
2. Configuring the operating system and computer

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

Proceed as follows to check the settings on your PC:
Start -> Settings -> Control panel -> Network connections

Select the connection (network adapter) via which your PC is connected to the router, e.g. "LAN connection". When you right-click the corresponding connection, a menu is displayed in which you select Properties.

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



Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**! Confirm by clicking **OK**, and again in the subsequent window.

Your PC is now configured such that the router assigns the IP address automatically. You can then configure the router using the web browser.

The browser must be Java-capable and the Java function must be activated (e.g. Internet Explorer 6.0 or better, or Mozilla Firefox).



3. Configuring the Wireless LAN Router

To start the configuration process, open your browser and enter “http://192.168.2.1” as the address. The login window is then displayed. By default, the user name is set to **admin** and the password is **1234**. After entering these, click **OK** to log on to the router.

You can configure the router via the integrated Setup Wizard or manually. After configuration using the Setup Wizard, the device is set so that the connected computers can access the internet.

Note! For security reasons, you must change your user name and password. The standard settings are identical for many devices and can allow others to access the router configuration. See Page 13 for information.

3.1 Configuring the Internet Connection using the Setup Wizard

Please start the Setup Wizard after logging in by clicking **Quick Setup**.

Time Zone

For **Set Time Zone** choose the appropriate time zone, e.g. **GMT sGreenwich Mean Time: Dublin, Edinburgh, Lisbon, London** for England. The remaining settings can be left as they are. Click => **Next** to continue.

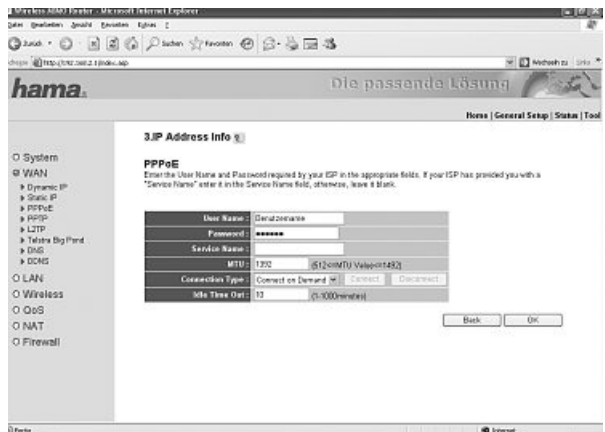
Broadband Type

Next, you are prompted to specify the WAN connection type. Your service provider will provide you with user-specific information. There is a brief description of the various connection types on the overview page. Due to the widespread use of DSL via **PPPoE**, the remainder of the description will refer to this type of connection.

For the **PPPoE** connection type, click **PPPoE xDSL**

IP Address Info

You must enter the access data for your provider in the next window. See your documents or contact the provider directly for this information.



Please enter the following details:

- User Name**
- Password**
- Service Name** (this must not always be entered)

In addition to the access data, you can make the following entries:

MTU stands for Maximal Transfer Unit and specifies the maximum packet size to be transferred. If you are not sure about this setting, we recommend leaving the standard value set. Values between 512 and 1492 can be set.

The **Connection Type** entry sets the dial-in action of your router. You can then select either:

Continuous: The router is always connected to the internet. This connection type is recommended if you have a flat-rate with no time limit, for example.

Connect on demand: With this connection type, the router does not dial in until it receives a request from a connected computer, e.g. if you open the internet browser on a computer. The connection is maintained until the period set under **Idle Time Out** has passed without activity.

Manual: If you choose the **Manual** connection type, you can make the connection by clicking **Connect**, and close it by clicking **Disconnect**.

Note! The “Connect as required” setting is recommended for volume or timed rates, so that the internet connection is disconnected automatically after the period set in the „idle time” option. Connection costs may be high if permanently connected. Please also note that closing the browser does not automatically disconnect from the internet. Many programs send queries to the internet or receive data from it without this being clearly visible. For the router, these queries 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 or disconnect it from the modem.

Idle Time Out: Enter the length of time you want to wait before internet connection is cut off when inactive. Values between 1 and 1000 can be set.

Click **OK** to confirm your entries. You must then restart the router for the settings to take effect. Click **Apply** in the next window to save the settings. The router takes approx. 30 seconds to restart. After the restart the router is configured so that you can access the internet via the connected computers. You can also edit these settings manually, by clicking **WAN** in the menu on the left and then selecting the corresponding connection type.

3.2 Configuring the Wireless LAN

Wireless LAN is deactivated by default for security reasons. To activate this function, from the start view which can be accessed by clicking **Home**, select **General Setup** and then **Wireless** in the menu on the left. Note that activating Wireless LAN without also setting encryption results in a security risk. Select **Enable** and then click **Apply**. Read Basic Settings for Wireless Networks for further instructions!

3.2.1 Basic Settings for Wireless Networks (WLAN)

Select **Basic Settings** in the menu on the left.

The **Mode** setting allows you can select the task the router is to perform in the network.

Select the **AP (3.2.1.1)** access point function if the device is the only access point in your network or if no bridge level connection is to be made to other access points.

Select **AP Bridge-Point to Point (3.2.1.2)** if you want to connect this access point wirelessly to a second access point. In this mode, clients cannot log-in via a wireless connection.

Select **AP Bridge-Point to Multi-Point (3.2.1.3)** if you want to connect this access point wirelessly to several other access points. In this mode, clients cannot log-in via a wireless connection.

Select **AP Bridge WDS (3.2.1.4)**, if you want to connect this access point to one or more other access points wirelessly and clients are to be allowed to log in wirelessly.

Continue configuration as required.

3.2.1.1 Operation as an Access Point (AP)

Selecting this under **Band** allows you to specify whether the device runs on the 2.4 GHz band in accordance with the 802.11b (11Mbps), 802.11g (54Mbps) standards or works in combination with 802.11b and 802.11g. Then set the **ESSID**. The **ESSID** can contain up to 32 characters and must be identical for all devices in the network. **Channel Number** allows you to select the channel in which the data is to be transferred. 13 channels are available.



Example of an ESSID : "WLAN_Router_54Mbps"

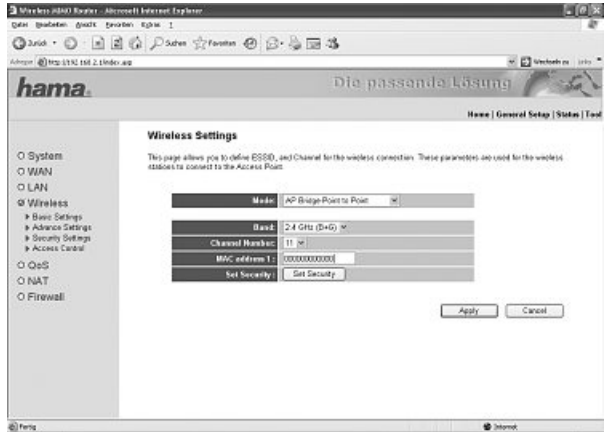
Click **Apply** to save your settings!

To set the encryption for your wireless network, click **Continue** in the next window and then **Security Settings** in the menu on the left. Continue reading on page 09 for instructions on setting Wireless LAN encryption.

Click **Apply** in the next window if you want to operate a wireless network without encryption. The router is then restarted. The wireless network is available after you restart.

3.2.1.2 Operation as an AP Bridge Point to Point

Selecting this under **Band** allows you to specify whether the device runs on the 2.4 GHz band in accordance with the 802.11b (11Mbps), 802.11g (54Mbps) standards or works in combination with 802.11b and 802.11g. **Channel Number** allows you to select the channel in which the data is to be transferred. 13 channels are available. Enter the address of the access point to which the bridge connection is to be made in **MAC address 1**. To set the encryption for your wireless network, click the **Set Security** button.

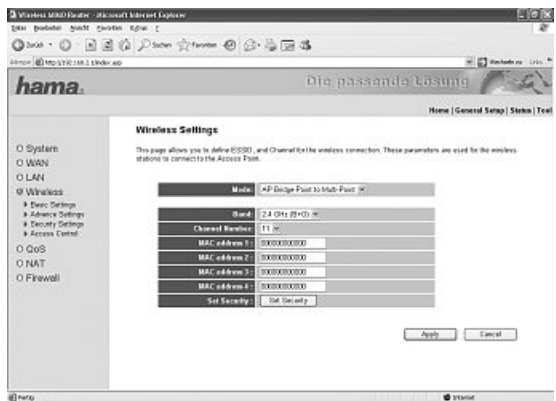


Continue reading on page 11 for instructions on setting Wireless LAN encryption.

Click **Apply** in the next window, and again in the window after that if you want to operate a wireless network without encryption. The router is then restarted. The wireless network is available after you restart.

3.2.1.3 Operation as an AP Bridge Point to Multi-Point

The difference to the AP Bridge Point to Point operation is that you can enter the MAC addresses of several access points in this mode. Bridge connections can be established to a maximum of 6 other access points. Selecting this under **Band** allows you to specify whether the device runs on the 2.4 GHz band in accordance with the 802.11b (11Mbps), 802.11g (54Mbps) standards or works in combination with 802.11b and 802.11g. **Channel Number** allows you to select the channel in which the data is to be transferred. 13 channels are available. Enter the addresses of the access points to which the bridge connection is to be made in **MAC address 1 to MAC address 6**.



To set the encryption for your wireless network, click the **Set Security** button.

Continue reading on page 11 for instructions on setting Wireless LAN encryption.

Click **Apply** in the next window, and again in the window after that if you want to operate a wireless network without encryption. The router is then restarted. The wireless network is available after you restart.

3.2.1.4 Operation as an AP Bridge WDS

What is **WDS**? Wireless Distribution System is the name for wireless connections between multiple access points, and also allows clients to log-in, which is not permitted by other bridge modes. The bandwidth of the network is halved for each additional access point as the packets have to be sent twice.

This makes it a combination of the previous modes.

Selecting this under **Band** allows you to specify whether the device runs on the 2.4 Ghz band in accordance with the 802.11b (11Mbps), 802.11g (54Mbps) standards or works in combination with 802.11b and 802.11g. The **ESSID** is required for the client network. It acts as identification in the network and must therefore be identical for all users in the client network. The **ESSID** can be up to 32 characters long.



Channel Number allows you to select the channel in which the data is to be transferred. 13 channels are available. Enter the addresses of the access points to which the bridge connection is to be made in **MAC address 1 to MAC address 6**. To set the encryption for your wireless network, click the **Set Security** button.

Continue reading on page 11 for instructions on setting Wireless LAN encryption.

Click **Apply** in the next window, and again in the window after that if you want to operate a wireless network without encryption. The router is then restarted. The wireless network is available after you restart.

3.2.2 Setting the Encryption for AP

First, it is important to understand a range of terms. The next section will explain the main terms used here:

Authentication: Authentication is a process in which the identity, e.g. of a person is determined based on a certain characteristic. This can be done by fingerprint, password or any other proof of authorisation.

Encryption: Encryption is a process in which plain text is transformed into a coded text via an encryption process (algorithm). One or more codes can be used for this. It must also be mentioned that each individual encryption process offers one or more authentication options.

The following encryption types are available for this mode:

- **64 Bit and 128 Bit WEP encryption**
- **WPA and WPA2 encryption**

You can make the settings under **Wireless/Security Settings** in the menu on the left for the **AP** mode.

Encryption is deactivated by default. However, for security reasons, we recommend that you always use encryption.

3.2.2.1 WEP encryption

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

First select whether you want to use 64 bit or 128 bit encryption. 128 bit encryption offers greater security. Then select either Hex (characters from 0-9 and a-f) or ASCII (any character) for the **Key Format**. This also determines the length of the key.

Default Tx Key allows you to select one of four preset keys. Select **Key 1**, for example, and enter your key of choice with the required length.



Examples: 64 bit Hex (10 characters) = 231074a6ef
 64 bit ASCII (5 characters) = j31n.

 128 bit Hex (26 characters) = 231074a6b9773ce43f91a5bef3
 128 bit ASCII (13 characters) = urlaub2006.-0

Click **Apply** to save your settings. You must then restart the router for the settings to take effect. To do so, click **Apply** in the next window. The wireless network with encryption is available after you restart.

3.2.2.2 WPA/WPA2 Encryption

Wi-Fi Protected Access (**WPA**) is an encryption method for WLAN. WPA contains the WEP architecture, but offers additional protection via dynamic codes, which are based on the Temporal Key Integrity Protocol (TKIP), and also offers pre-shared keys (PSK) or extensible authentication protocol (EAP) for user authentication. However, a radius server is required for this. WPA2 is a development of WPA and uses a different encryption algorithm, advanced encryption standard (AES).

WPA offers two types of authentication, either **pre-shared key** or authentication via special **authentication protocols**, which are generally variations of EAP (Extensible Authentication Protocol). An authentication server (RADIUS server) is used for the latter authentication method, which is rarely used for private applications. Your administrator can give you the information you require to configure this authentication method.

WPA pre-shared-key (recommended for most users)

First select whether you want to use **WPA with TKIP** encryption algorithm, **WPA2 with AES** encryption algorithm or the **WPA Mixed** mode. The mixed mode allows clients using WPA or WPA2 to access the access point. The mixture is very practical as presently few XP clients are WPA2 compatible. If the mixed mode is switched off, the AP only allows WPA2 clients, and the large number of WPA (TKIP) devices cannot connect.

Then you must select the key format (**Pre-shared Key Format**). Select either **Pass phrase** for a key with a length of at least 8 and max. 63 characters, whereby letters (A-Z), numbers and punctuation marks can be used, or **Hex** for a 64 character key, in which only numbers from 0-9 and letters from a-f can be used.



The next step is entering a key, called a **pre-shared-key (PSK)**. All clients which are to access the access point must know this character string.

Click **Apply** to save your settings. You must then restart the router for the settings to take effect. To do so, click **Apply** in the next window. The wireless network with encryption is available after you restart.

WPA RADIUS (requires a special authentication server)

First select whether you want to use **WPA with TKIP** encryption algorithm, **WPA2 with AES** encryption algorithm or the **WPA Mixed** mode. The mixed mode allows clients using WPA or WPA2 to access the access point. The mixture is very practical as presently few XP clients are WPA2 compatible.

Select **WPA2 (AES)** only. The AP only allows WPA2 clients, and the large number of WPA (TKIP) devices cannot connect.

Next enter the **RADIUS server IP address**. The **RADIUS Server Port** is preset to 1812. Enter the **password** for the RADIUS Server.

Click **Apply** to save your settings. You must then restart the router for the settings to take effect. To do so, click **Apply** in the next window. The wireless network with encryption is available after you restart.

3.2.3 Setting the Encryption for Bridge-Point to Point, Bridge Point to Multi-Point and Bridge WDS

First, it is important to understand a range of terms. The next section will explain the main terms used here:

Authentication: Authentication is a process in which the identity, e.g. of a person is determined based on a certain characteristic. This can be done by fingerprint, password or any other proof of authorisation.

Encryption: Encryption is a process in which plain text is transformed into a coded text via an encryption process (algorithm). One or more codes can be used for this. It must also be mentioned that each individual encryption process offers one or more authentication options.

The following encryption types are available for the various modes:

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

Click the **Set Security** button to make the settings for the **Bridge-Point to Point, Bridge-Point to Multi-Point and Bridge WDS** modes after setting the mode.

For the **Bridge WDS** mode, encryption must be set for the access point under **Wireless/Security Settings** in the menu on the left. This is the only encryption available for WDS.

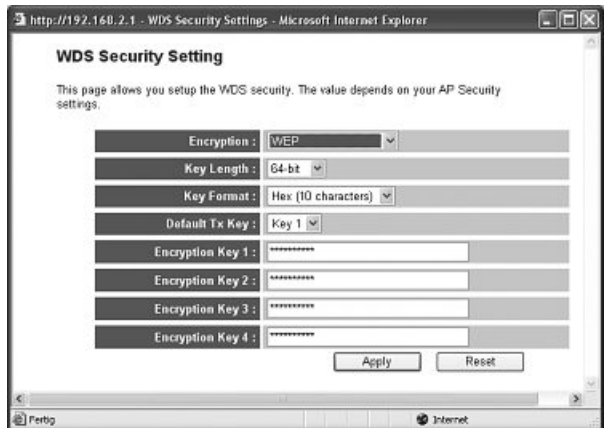
You can choose either **WEP** encryption with **64 Bit and 128 Bit, WPA with TKIP** encryption algorithm and **WPA2 with AES** encryption algorithm.

3.2.3.1 WEP Encryption

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

First select whether you want to use 64 bit or 128 bit encryption. 128 bit encryption offers greater security. Then select either Hex (characters from 0-9 and a-f) or ASCII (any character) for the **Key Format**. This also determines the length of the key.

Default Tx Key allows you to select one of four preset keys. Select **Key 1**, for example, and enter your key of choice with the required length.



Examples: 64 bit Hex (10 characters) = 231074a6ef
 64 bit ASCII (5 characters) = j31n.

 128 bit Hex (26 characters) = 231074a6b9773ce43f91a5bef3
 128 bit ASCII (13 characters) = urlaub2006.+0

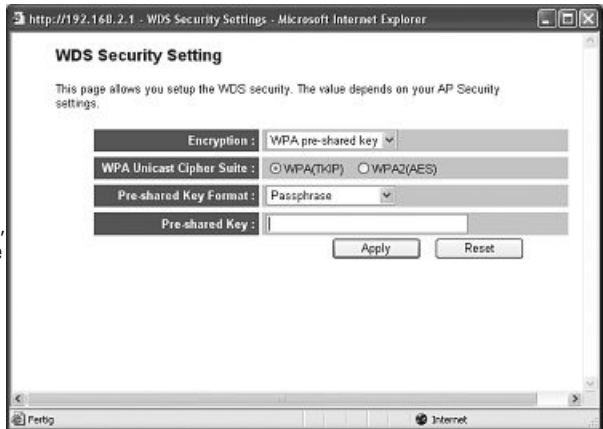
Click **Apply** to save your settings. You must then restart the router for the settings to take effect. To do so, click **Apply** in the next window. The wireless network with encryption is available after you restart.

3.2.3.2 WPA/WPA2 Encryption

Wi-Fi Protected Access (**WPA**) is an encryption method for WLAN. WPA contains the WEP architecture, but offers additional protection via dynamic codes, which are based on the Temporal Key Integrity Protocol (TKIP), and also offers pre-shared keys (PSK) or extensible authentication protocol (EAP) for user authentication. However, a radius server is required for this. WPA2 is a development of WPA and uses a different encryption algorithm, advanced encryption standard (AES).

Select **WPA Pre-shared Key** under Encryption. Then, under WPA Unicast Cipher Suite, select WPA (TKIP) or WPA (AES).

Then you must select the **Pre-shared Key Format**. Select either **Pass phrase** for a key with a length of at least 8 and max. 63 characters, whereby letters (A-Z), numbers and punctuation marks can be used, or **Hex** for a 64 character key, in which only numbers from 0-9 and letters from a-f can be used. The next step is entering a key, called a **pre-shared-key** (PSK). All clients which are to access the access point must know this character string.



Click **Apply** to save your settings. You must then restart the router for the settings to take effect. To do so, click **Apply** in the next window. The wireless network with encryption is available after you restart.

3.3 Changing the Log-in Data

From the start view which can be accessed by clicking **Home**, select **General Setup** and then **System => Password Settings** in the menu on the left.

This page allows you to enter a new password for the router. To assign a new password, you must first enter the current password in the Current Password field. Enter the new password in the **New Password** field and again in the **Confirmed Password** field to confirm that it was typed correctly. Click **Apply** to confirm your entries. You must then restart the router for the settings to take effect. To do so, click **Apply** in the next window. The new password applies after restarting.

3.4 LAN Settings

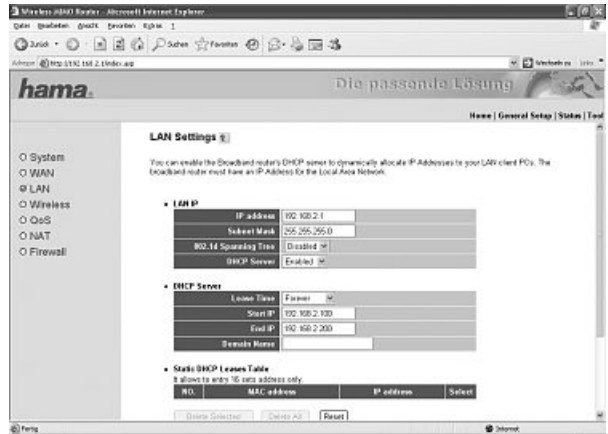
From the start view which can be accessed by clicking **Home**, select **General Setup** and then LAN in the menu on the left.

This allows you to change the standard LAN settings of the router.

LAN IP: The router is preset to the IP address 192.168.2.1. If you want to use a different address for the router, you can change it in this entry field. The corresponding **Subnet Mask** is entered in the field directly below this.

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 to apply for the client.



The IP address range from which the DHCP server can assign IP address to the clients is restricted by the **Start-IP Address** and the **End-IP Address**. The table below allows you to permanently assign a certain MAC address to an IP address from the valid range. When the client logs in on the router, it is always given this IP address. To do so, select **Enable Static DHCP Lease** and enter the MAC address and the IP address in the empty fields of the table at the bottom.. The entry is saved in the table when you click **Add**.

Click **Apply** to confirm your entries. You must then restart the router for the settings to take effect. To do so, click **Apply** in the next window.

Warning! The new LAN configuration is valid after restarting. Therefore, you have to use the new IP address to open the web interface in the browser.

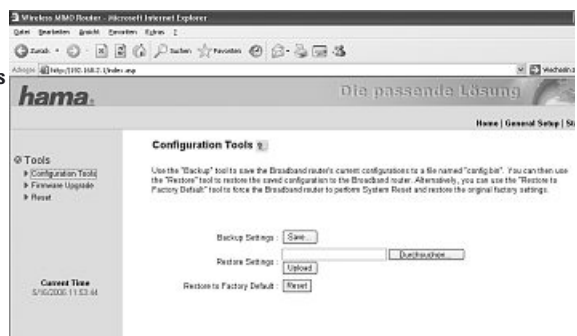
4. Tools

The Hama Wireless LAN router provides you with various tools to help you configure and use the device.

4.1 Configuration Tools

From the start view which can be accessed by clicking **Home**, select **Tools** in the menu at the top right, and then **Configuration Tools** in the menu on the left.

This page allows you to save all configuration options of the router. Click **Save** to do so. Then select the target folder. You should also set a file name which allows you to identify the file clearly. Click **Save** after your selection. The settings are now saved. If you want



to restore the saved settings at a later time, click **Browse** and then select the configuration file required. Click **Upload** to load the file. The router takes a few seconds to load the file and then to restart. The selected LAN configuration is valid after restarting. To reset the router to the default settings, click **Reset (Restore to Factory Default)**. Click **OK** at the next prompt. All settings are reset to the default settings.

4.2 Firmware Update

From the start view which can be accessed by clicking **Home**, select **Tools** in the menu at the top right, and then **Firmware Upgrade** in the menu on the left. To do so, click **Next** in the next window.

Click **Browse** to select the new firmware file in the next window. Click **Apply** after you select the file. The new firmware is loaded and the router is restarted.

Warning! Earlier settings are lost when new firmware is loaded.

4.3 Re-starting the Router

From the start view which can be accessed by clicking **Home**, select **Tools** in the menu at the top right and then **Reset** in the menu on the left.

The router is restarted when you click **Apply** in this window and confirm the subsequent prompt by clicking **OK**. Settings you have made are not lost.

5. Status Information

From the start view which can be accessed by clicking **Home**, select **Status** in the menu at the top right.

The menu on the left contains various sub-menus via which you can view detailed information, such as **Internet Connection, Device Status or Active DHCP Clients**. The **Statistics** menu item also provides a packet counter.

6. Support and Contact Information

If products are defective:

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

Internet / World Wide Web:

Product support, new drivers 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

Note:

This product may only be used in Germany, Austria, Switzerland, France, England, Belgium, Spain, Holland, Denmark, Hungary, Poland, Sweden, Luxemburg, Ireland, Greece, the Czech Republic, Slovakia and Finland.

See www.hama.com for the declaration of conformity with R&TTE Directive 99/5/EC.



Sommaire:

1.	Connexion du routeur pour réseau local sans fil	page 03
2.	Configuration du système d'exploitation et de l'ordinateur	page 03
3.	Configuration du routeur pour réseau local sans fil.....	page 05
3.1	Configuration de la connexion internet à l'aide de l'assistant	page 05
3.2	Configuration du réseau local sans fil	page 06
3.2.1	Réglages de base des réseaux sans fil	page 07
3.2.1.1	Mode de fonctionnement point d'accès (AP)	page 07
3.2.1.2	Mode de fonctionnement point d'accès AP pont point à point	page 08
3.2.1.3	Mode de fonctionnement point d'accès AP pont point à multipoint	page 08
3.2.1.4	Mode de fonctionnement AP pont WDS	page 09
3.2.2	Réglage du chiffrement pour AP.....	page 09
3.2.2.1	Chiffrement WEP	page 10
3.2.2.2	Chiffrement WPA/WPA2	page 11
3.2.3	Réglage du chiffrement pour AP pont point à point, point à multipoint et WDS	page 12
3.2.3.1	Chiffrement WEP	page 13
3.2.3.2	Chiffrement WPA/WPA2	page 13
3.3	Modification des données d'identifiant	page 14
3.4	Réglages du réseau local	page 15
4.	Outils.....	page 15
4.1	Outils de configuration	page 16
4.2	Actualisation du micrologiciel	page 16
4.3	Redémarrage du routeur	page 16
5.	Informations d'état	page 17
6.	Support technique et contact.....	page 17

Contenu de l'emballage :

- 1x routeur pour réseau local sans fil MiMo 300 Express
- 1x bloc secteur 12 V
- 1x mode d'emploi imprimé

Exigences minimales du système :

- Système d'exploitation avec protocole TCP/IP installé
- Navigateur compatible Java comme Mozilla Firefox ou Microsoft Internet Explorer

Consignes de sécurité :

N'utilisez pas l'appareil dans des environnements poussiéreux ou humides ainsi qu'à proximité de radiateurs ou d'autres sources de chaleur. Cet appareil n'est pas conçu pour une utilisation en plein air. Protégez l'appareil de pression et des chocs. L'appareil ne doit être ni ouvert, ni transporté pendant son fonctionnement.

Attention ! Utilisez exclusivement le bloc secteur fourni avec le routeur. L'utilisation d'un autre bloc secteur est susceptible de détruire l'appareil..

Remarque !!! En présence de tarifs au volume ou de tarifs temporaires, il est recommandé de sélectionner « Connexion à la demande » (« Dial up on Demand ») pour que l'accès à internet soit automatiquement interrompu après la durée réglée sous l'option « Temps d'attente » (« PPPoE Timeout »). Une connexion permanente serait sinon susceptible d'occasionner des frais élevés. Veuillez également noter que la fermeture du navigateur n'implique pas forcément la déconnexion à internet. De nombreux programmes envoient des demandes ou reçoivent des données par internet, sans que cela ne soit clairement identifiable. Ces demandes seront perçues par le routeur comme des actions volontaires, comme l'ouverture de votre navigateur. Vous devriez mettre votre appareil hors tension ou désactiver le modem dans le cas où vous voulez être sûr(e) qu'aucune connexion à internet n'est active.

1. Connexion du routeur pour réseau local sans fil

1. Connectez les ordinateurs et les autres appareils de réseau (concentrateur, commutateur, etc.) aux ports 1 à 4. Utilisez un câble patch croisé ou un câble patch CAT5 (100 m au maximum). Le commutateur intégré détecte automatiquement la vitesse de la connexion (10 ou 100 Mbits/s), le mode de transfert (half/full duplex) ainsi que le type de câble utilisé.
2. Connectez le port ethernet de votre modem au port « WAN » du routeur. Selon le type de votre modem, vous aurez besoin d'un câble 1:1 ou d'un câble croisé. Dans la plupart des cas, vous pouvez utiliser le câble de raccordement fourni. Branchez alors le bloc d'alimentation fourni à une prise de courant et raccordez-le au routeur. Attention : Un bloc d'alimentation inadapté est susceptible d'endommager l'appareil !

Contrôle de l'installation

Différentes DEL d'état sont placées sur la face supérieure de l'appareil :

DEL	Etat	Statut
Power	Allumée	Le bloc d'alimentation est connecté et alimente l'appareil
	Eteinte	Pas de bloc d'alimentation connecté, l'appareil n'est pas alimenté
WLAN	Clignote	Le réseau local sans fil est activé / des données sont en train d'être envoyées
	Eteinte	Le réseau local sans fil est désactivé
WAN	Allumée	Le port WAN a établi une connexion réseau correcte
	Clignote	Transfert de données via le port WAN
	Eteinte	Pas de connexion
LAN1-4	Allumée	Le port LAN correspondant a établi une connexion réseau correcte
	Clignote	Transfert de données via le port LAN correspondant
	Eteinte	Pas de connexion

2. Configuration du système d'exploitation et de l'ordinateur

Le protocole TCP/IP doit être installé sur tous les ordinateurs censés utiliser internet. Par défaut, l'adresse IP 192.168.2.1 et un serveur DHCP sont préconfigurés pour le routeur. Les ordinateurs connectés obtiennent ainsi automatiquement les adresses adéquates et d'autres paramètres. Nous vous recommandons de conserver ces réglages.

Procédez comme suit afin de vérifier les paramètres de votre ordinateur :
Démarrer -> Paramètres -> Panneau de configuration -> Connexions réseau

Sélectionnez la connexion (adaptateur de réseau) par laquelle votre ordinateur est connecté au routeur, « Connexion LAN » par exemple. Vous pouvez ouvrir un menu contenant les propriétés de la connexion en cliquant avec le bouton droit de votre souris sur la connexion correspondante.

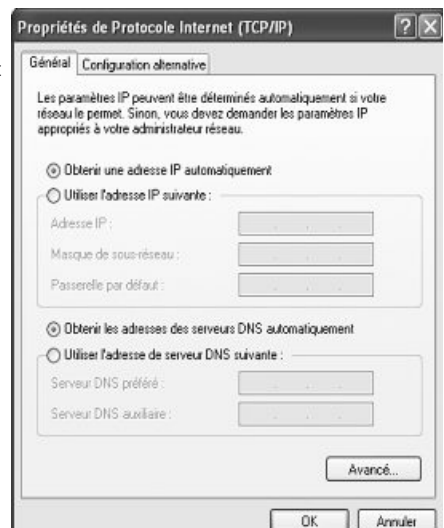
Sélectionnez l'entrée **Protocole internet (TCP/IP)** dans la liste, puis cliquez sur **Propriétés**.



Sélectionnez « **Obtenir une adresse IP automatiquement** » et « **Obtenir les adresse des serveurs DNS automatiquement** ». Confirmez votre saisie en cliquant sur **OK**, puis de nouveau sur **OK** dans la fenêtre suivante.

Votre ordinateur est alors configuré pour pouvoir obtenir automatiquement son adresse IP à partir du serveur. Vous pouvez maintenant configurer votre routeur à l'aide d'un navigateur web.

Le navigateur doit prendre Java en charge (Internet Explorer 6.0 et versions ultérieures ou Mozilla Firefox, etc.) et cette fonction doit être activée.



3. Configuration du routeur pour réseau local sans fil

Ouvrez votre navigateur et saisissez l'adresse « <http://192.168.2.1> » afin de lancer la configuration. La fenêtre d'identification apparaît. Le nom d'utilisateur **admin** et le mot de passe **1234** sont des réglages par défaut. Après la saisie, cliquez sur **OK** afin de vous enregistrer dans le routeur.

Pour la configuration du routeur, vous pouvez soit utiliser l'assistant intégré, soit réaliser les réglages manuellement. A la fin de la configuration à l'aide de l'assistant intégré, l'appareil sera configuré de telle sorte que les ordinateurs connectés aient accès à internet.

Remarque !!! Pour votre propre sécurité, nous vous recommandons instamment de modifier le nom d'utilisateur et le mot de passe. Les valeurs standard sont identiques pour de nombreux appareils et pourraient permettre l'accès au routeur de personnes non autorisées. Vous trouverez de plus amples informations à ce sujet à la page 14.

3.1 Configuration de la connexion internet à l'aide de l'assistant

Après vous être identifié, lancez l'assistant en cliquant sur le bouton **Quick Setup**.

Time Zone (fuseau horaire)

Sélectionnez votre fuseau horaire sous **Time Zone**, par exemple **GMT (+01:00) Amsterdam, Berlin, Berne, Rome, Stockholm, Vienne** pour l'France. Vous pouvez adopter les autres paramètres sans modifications. Cliquez sur **Next** afin de continuer.

Broadband Type (type de connexion à large bande)

Votre fournisseur d'accès vous communiquera toutes informations spécifiques. Vous trouverez une brève explication des différents types de connexion à la page de récapitulation. En raison du degré de diffusion de DSL via **PPPoE**, la description suivante se base sur ce type de connexion.

Cliquez sur **PPPoE xDSL** afin de sélectionner le type de connexion **PPPoE**

IP Address Info (Informations relatives à l'adresse IP)

La fenêtre suivante vous invite à saisir les données d'accès de votre fournisseur. Vous trouverez ces informations dans les documents que votre fournisseur vous a transmis.

Microsoft Internet Explorer
Date: Wednesday, 25 April 2008 12:00:00
Zurück Suchen Favoriten Webhost 22 Links
http://192.168.2.1/3pindex.asp
hama Die passende Lösung
Home | General Setup | Status | Tools

3.P Address Info

PPPoE
Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a "Service Name" enter it in the Service Name field, otherwise, leave it blank.

User Name	Genarbenname
Password	*****
Service Name	
MTU	1392 (512=MTU Value-45)
Connection Type	Connect on Demand <input type="checkbox"/> Connect <input type="checkbox"/> Disconnect <input type="checkbox"/>
Idle Time Out	12 (0-100minutes)

Back OK

IP Info Internet

Veillez saisir : **User Name (Nom d'utilisateur)**
Password (Mot de passe)
Service Name (Nom de service) (cette indication n'est pas nécessaire dans tous les cas)

En plus des données d'accès, vous pouvez aussi saisir les précisions suivantes :

MTU est l'abréviation de « Maximal Transfer Unit » et indique la taille maximale des paquets à transmettre. Nous vous conseillons de conserver ce réglage par défaut dans le cas où vous n'êtes pas sûr(e) de la configuration à adopter. Les valeurs entre 512 et 1492 peuvent être saisies. Vous pouvez déterminer le type d'accès à internet à l'aide de **Connection Type (Type de connexion)**. Vous pouvez choisir entre :

Continuous (Continu) : Le routeur est connecté à internet en permanence. Ce type de connexion est conseillé lorsque vous utilisez un tarif forfaitaire sans limitation de temps.

Connect on Demand (Connexion à la demande) : Avec ce type de connexion, le routeur se connecte uniquement lorsqu'un ordinateur l'exige, par exemple lorsque vous lancez le navigateur internet d'un ordinateur. La connexion reste active jusqu'à ce que la période définie sous **Idle Time Out (Compteur de temps mort)** soit écoulée consécutivement à une période de non-activité.

Manual (Connexion manuelle) : En sélectionnant **Manual** (Connexion manuelle), vous pouvez établir la connexion à l'aide du bouton **Connect** et l'interrompre à l'aide du bouton **Disconnect**.

Remarque !!! En présence de tarifs au volume ou de tarifs temporaires, il est recommandé de sélectionner « Connexion à la demande » (« Dial up on Demand ») pour que l'accès à internet soit automatiquement interrompu après la durée réglée sous l'option « Temps d'attente » (« PPPoE Timeout »). Une connexion permanente serait sinon susceptible d'occasionner des frais élevés. Veuillez également noter que la fermeture du navigateur n'implique pas forcément la déconnexion à internet. De nombreux programmes envoient des demandes ou reçoivent des données par internet, sans que cela ne soit clairement identifiable. Ces demandes seront perçues par le routeur comme des actions volontaires, comme l'ouverture de votre navigateur par exemple. Vous devriez mettre votre appareil hors tension ou désactiver le modem dans le cas où vous voulez être sûr(e) qu'aucune connexion à internet n'est active.

Idle Time Out (Compteur de temps mort) : Vous pouvez déterminer ici la durée d'inactivité (en minutes) désirée avant que la connexion à internet ne soit automatiquement interrompue. Les valeurs entre 1 et 1000 peuvent être saisies. Confirmez votre saisie en cliquant sur **OK**. Vous devrez redémarrer votre ordinateur afin d'appliquer les réglages. Appuyez sur **Apply**. Le routeur prend environ 30 secondes pour redémarrer. Après le redémarrage, votre routeur est configuré de telle sorte que les ordinateurs connectés aient accès à internet. Vous pouvez également modifier ces paramètres manuellement en sélectionnant **WAN** dans le menu de gauche, puis en sélectionnant le type de connexion correspondant.

3.2 Configuration du réseau local sans fil

Pour votre sécurité, le réseau local sans fil est désactivé par défaut. Dans le cas où vous désirez activer le fonctionnement, sélectionnez **General Setup**, puis **Wireless** dans la barre de menu gauche à partir de la fenêtre de démarrage que vous pouvez ouvrir en retournant à **Home**. Veuillez noter qu'il n'est pas sans danger d'activer le réseau local sans fil sans avoir effectué le réglage du chiffrement. Sélectionnez **Enable**, puis cliquez sur **Apply**. Vous pouvez continuer à configurer les réglages de base des réseaux sans fil !

3.2.1 Réglages de base des réseaux sans fil (WLAN)

Sélectionnez le menu de gauche **Basic Settings (Réglages de base)**.

Vous pouvez sélectionner, au point **Mode**, quelles tâches le routeur doit accomplir au sein du réseau.

Sélectionnez la fonction point d'accès **AP (3.2.1.1)**, dans le cas où l'appareil est le seul point d'accès dans votre réseau ou aucune connexion ne doit être établie vers d'autres points d'accès au niveau du pont.

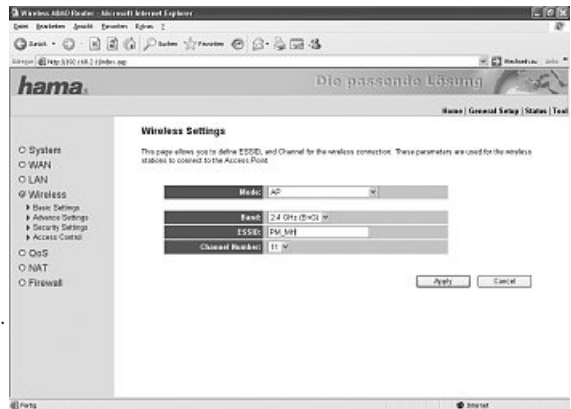
Sélectionnez le point d'accès **AP Bridge-Point to Point (pont point à point) (3.2.1.2)**, dans le cas où vous désirez établir une connexion sans fil entre ce point d'accès et un autre point d'accès. Dans ce mode, les clients ne peuvent pas s'enregistrer par connexion sans fil.

Sélectionnez le point d'accès **AP Bridge-Point to Multi-Point (pont point à multipoint) (3.2.1.3)**, dans le cas où vous désirez établir une connexion sans fil entre ce point d'accès et plusieurs autres points d'accès. Dans ce mode, les clients ne peuvent pas s'enregistrer par connexion sans fil.

Sélectionnez la fonction point d'accès **AP Bridge WDS (3.2.1.4)**, dans le cas où vous désirez établir une connexion sans fil entre ce point d'accès et plusieurs autres points d'accès, et que les clients puissent s'enregistrer sans fil. Veuillez continuer la configuration conformément à votre sélection.

3.2.1.1 Mode de fonctionnement point d'accès (AP)

Vous pouvez définir sous **Band** si vous désirez que votre appareil fonctionne sur une bande de fréquence de 2,4 Ghz au standard 802.11b (11 Mbit/s), 802.11g (54 Mbit/s) ou en combinaison avec 802.11b et 802.11g. Définissez ensuite l'**ESSID** (« Identifiant Electronic Switching System »). L'identifiant **ESSID** peut compter jusqu'à 32 caractères et doit être identique pour tous les appareils du réseau. Définissez sous **Channel Number (Numéro de canal)** quel canal doit être utilisé pour la transmission des données. 13 canaux sont disponibles.



Exemple d'identifiant ESSID : « WLAN_Router_54Mbps »

Cliquez sur **Apply** afin d'appliquer vos réglages ! Cliquez dans la fenêtre suivante sur le bouton **Continue**, puis sur l'option **Security Settings (réglages de sécurité)** du menu de gauche afin de configurer le chiffrement de votre réseau sans fil. Pour de plus amples informations relatives à la configuration du chiffrement de votre réseau local sans fil, veuillez consulter la page 9.

Dans la fenêtre suivante, cliquez sur **Apply** dans le cas où vous désirez faire fonctionner votre réseau sans chiffrement. Le routeur doit ensuite être redémarré. Votre réseau sans fil sera disponible après le redémarrage.

3.2.1.2 Mode de fonctionnement point d'accès pont point à point (AP Bridge-Point to Point)

Vous pouvez définir sous **Band** si vous désirez que votre appareil fonctionne sur une bande de fréquence de 2,4 Ghz au standard 802.11b (11 Mbit/s), 802.11g (54 Mbit/s) ou en combinaison avec 802.11b et 802.11g. Définissez sous **Channel Number (Numéro de canal)** quel canal doit être utilisé pour la transmission des données. 13 canaux sont disponibles. Saisissez, sous **MAC address 1**, l'adresse du point d'accès vers laquelle la connexion pont doit être établie. Cliquez sur le bouton **Set Security** afin de régler le chiffrement de votre réseau sans fil.

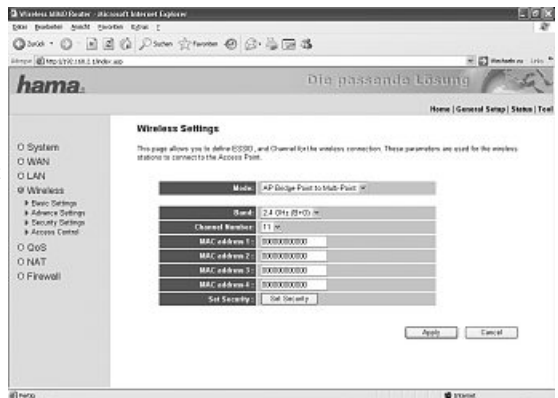


Pour de plus amples information relatives à la configuration du chiffrement de votre réseau local sans fil, veuillez consulter la page 12.

Dans la fenêtre suivante, cliquez sur **Apply**, puis à nouveau sur **Apply** dans la fenêtre suivante, dans le cas où vous désirez faire fonctionner votre réseau sans fil sans chiffrement. Le routeur doit ensuite être redémarré. Votre réseau sans fil sera disponible après le redémarrage.

3.2.1.3 Mode de fonctionnement point d'accès AP pont point à multipoint (AP Bridge-Point to Multi-Point)

Ce mode de fonctionnement diffère du mode de fonctionnement AP pont point à point dans le sens qu'il vous permet de saisir les adresses MAC de plusieurs points d'accès. Une connexion pont est possible vers un maximum de 6 autres points d'accès. Vous pouvez déterminer sous **Band** si vous désirez que votre appareil fonctionne sur une bande de fréquence de 2,4 Ghz au standard 802.11b (11 Mbit/s), 802.11g (54 Mbit/s) ou en combinaison avec 802.11b et 802.11g. Définissez sous **Channel Number (Numéro de canal)** quel canal doit être utilisé pour la transmission des données. 13 canaux sont disponibles. Saisissez, sous **MAC address 1 jusqu'à MAC address 6**, les adresses des points d'accès vers lesquelles la connexion pont doit être établie. Cliquez sur le bouton **Set Security** afin de régler le chiffrement de votre réseau sans fil. Pour de plus amples information relatives à la configuration du chiffrement de votre réseau local sans fil, veuillez consulter la page 12.



Dans la fenêtre suivante, cliquez sur **Apply**, puis à nouveau sur **Apply** dans la fenêtre suivante, dans le cas où

vous désirez faire fonctionner votre réseau sans fil sans chiffrement. Le routeur doit ensuite être redémarré. Votre réseau sans fil sera disponible après le redémarrage.

3.2.1.4 Bridge WDS (Mode de fonctionnement AP pont WDS)

Que signifie **WDS**? On appelle Wireless Distribution System (système de distribution sans fil) la connexion sans fil entre plusieurs points d'accès entre eux ; ce système permet l'enregistrement des clients, une fonctionnalité impossible dans les autres modes de fonctionnement par pont. Pour chaque point d'accès supplémentaire, la bande passante du réseau est séparée en deux car les paquets doivent être transmis à double.

Il en résulte donc une combinaison des modes de fonctionnement précédents.

Vous pouvez définir sous **Band** si vous désirez que votre appareil fonctionne sur une bande de fréquence de 2,4 Ghz au standard 802.11b (11 Mbit/s), 802.11g (54 Mbit/s) ou en combinaison avec 802.11b et 802.11g. L'**ESSID** est nécessaire pour le client réseau ; l'**ESSID** sert à l'identification dans le réseau et doit donc être identique pour tous les participants au client réseau. La longueur de l'**ESSID** peut compter jusqu'à 32 caractères.



Définissez sous **Channel Number (Numéro de canal)** quel canal doit être utilisé pour la transmission des données. 13 canaux sont disponibles. Saisissez, sous **MAC address 1 jusqu'à MAC address 6**, les adresses des points d'accès vers lesquelles la connexion pont doit être établie. Cliquez sur le bouton **Set Security** afin de régler le chiffrement de votre réseau sans fil.

Pour de plus amples information relatives à la configuration du chiffrement de votre réseau local sans fil, veuillez consulter la page 12.

Dans la fenêtre suivante, cliquez sur **Apply**, puis à nouveau sur **Apply** dans la fenêtre suivante, dans le cas où vous désirez faire fonctionner votre réseau sans fil sans chiffrement. Le routeur doit ensuite être redémarré. Votre réseau sans fil sera disponible après le redémarrage.

3.2.2 Réglage du chiffrement pour le point d'accès

Dans un premier temps, il importe de distinguer les différentes notions. Petit glossaire des termes les plus importants utilisés ici :

Authentification : L'authentification est une procédure au cours de laquelle l'identité, d'une personne par exemple, est déterminée à l'aide d'une caractéristique particulière. Cette caractéristique peut être une empreinte digitale, un mot de passe ou tout autre justificatif.

Chiffrement : Le chiffrement est une procédure au cours de laquelle un « texte en langage clair » est transformé en « texte codé » à l'aide d'un processus de chiffrement (algorithme). Un ou plusieurs codes

peuvent être utilisés à cet effet. Il convient également de relever que chaque procédé de chiffrement offre une ou plusieurs possibilités d'authentification.

Les types de chiffrements suivants sont disponibles pour ce mode de fonctionnement :

- **Chiffrement WEP 64 bits et 128 bits**
- **Chiffrement WPA et WPA2**

Pour le mode de fonctionnement **AP**, vous pouvez effectuer les réglages sous **Wireless / Security Settings** dans le menu de gauche.

Le chiffrement est désactivé par défaut. Par mesure de sécurité, nous vous conseillons cependant d'utiliser un chiffrement en permanence.

3.2.2.1 Chiffrement WEP

Le standard **WEP** (Wired Equivalent Privacy) est un algorithme de chiffrement standard pour réseaux locaux sans fil. Il est censé régler l'accès au réseau aussi bien que garantir l'intégrité des données, mais ce procédé est considéré comme peu sûr en raison de différents maillons faibles.

Sélectionnez premièrement le type de chiffrement (64 bits ou 128 bits) que vous désirez utiliser ; veuillez noter que le chiffrement à 128 bits offre davantage de sécurité. Sélectionnez ensuite la méthode que vous désirez utiliser pour le **format de la clé (Key Format)** : Hex vous permettant l'utilisation des caractères 0-9 et a-f, ou ASCII vous permettant l'utilisation de tous les caractères et ainsi de déterminer la longueur de la clé.

Vous pouvez définir un des quatre codes pré-configurés sous **Default Tx Key (clé de transmission par défaut)**.

Sélectionnez par exemple **Key 1** puis saisissez votre clé personnelle de la longueur requise dans un des champs.



Exemples : 64 bits Hex (10 caractères) = 231074a6ef
 64 bits ASCII (5 caractères) = j31n!

128 bits Hex (26 caractères) = 231074a6b9773ce43f91a5bef3
 128 bits ASCII (13 caractères) = conges2006!+0

Cliquez sur **Apply** afin d'enregistrer vos réglages ! Vous devrez redémarrer votre routeur afin d'appliquer les réglages en cliquant sur **Apply** dans la fenêtre suivante. Votre réseau sans fil sera disponible avec son chiffrement après le redémarrage.

3.2.2.2 Chiffrement WPA/WPA2

L'accès protégé WiFi **WPA** (WiFi Protected Access) est une méthode de chiffrement pour WiFi (WLAN). WPA comprend l'architecture de WEP mais offre une protection supplémentaire grâce à un encodage dynamique basé sur le protocole Temporal Key Integrity Protocol (TKIP) qui offre en outre des « clés pré-partagées » (PSK Pre-Shared-Keys) ou un « protocole d'authentification extensible » (EAP, Extensible Authentication Protocol) pour lequel cependant un serveur radius est nécessaire. WPA2 est un post-développement de WPA et utilise AES (Advanced Encryption Standard), un autre algorithme de chiffrement.

Une distinction est faite entre « **Authentification par clé partagée (Pre-Shared-Key)** » et une authentification via des **protocoles d'authentification** spéciaux, souvent des variations du protocole EAP (Extensible Authentication Protocol). La deuxième méthode d'authentification citée, utilisée rarement dans le domaine privé, nécessite un serveur d'authentification (serveur RADIUS). Vous pouvez vous procurer les informations requises pour la configuration de cette méthode d'authentification chez votre administrateur.

WPA pre-shared-key / clé partagée WPA (position est recommandée pour la plupart des utilisateurs)

Sélectionnez premièrement l'algorithme de chiffrement vous désirez utiliser : **WPA avec TKIP**, **WPA2 avec AES** ou encore le mode **WPA mixed**. Ce mode mixte permet aux clients WPA ou WPA2 de se connecter au point d'accès. Le mode mixte est très utile car, actuellement, peu de clients XP sont compatibles avec WPA2. Lorsque le mode mixte n'est pas actif, le point d'accès autorise l'accès uniquement aux clients avec WPA2 et la plupart des appareils WPA (TKIP) sont rejetés.



Déterminez ensuite le format de la clé (**Pre-shared Key Format/ Format de clé pré-partagée**). Choisissez entre **phrase de passe / Passphrase** pour une clé

comportant au moins 8 caractères et au plus 63 (les lettres (A-Z), chiffres et signe de ponctuation sont admissibles) ou **Hex** pour une clé d'une longueur de 64 signes (uniquement les caractères 0-9 et a-f peuvent être utilisés).

L'étape suivante est la saisie de la clé, la **clé pré-partagée / Pre-shared Key (PSK)**. Chaque client désirant accéder au point d'accès doit connaître cette clé.

Cliquez sur **Apply** afin d'enregistrer vos réglages. Vous devrez redémarrer votre routeur afin d'appliquer les réglages en cliquant sur **Apply** dans la fenêtre suivante. Votre réseau sans fil sera disponible avec son chiffrement après le redémarrage.

WPA RADIUS (un serveur d'authentification spécial est indispensable)

Sélectionnez premièrement l'algorithme de chiffrement vous désirez utiliser : **WPA avec TKIP, WPA2 avec AES** ou encore le mode **WPA mixed**. Ce mode mixte permet aux clients WPA ou WPA2 de se connecter au point d'accès. Le mode mixte est très utile car, actuellement, peu de clients XP sont compatibles avec WPA2.

Dans le cas où vous ne sélectionnez que **WPA2 (AES)**, le point d'accès n'autoriserait l'accès qu'aux clients WPA2 et la plupart des appareils WPA (TKIP) seraient rejetés.

Sélectionnez ensuite **l'adresse IP du serveur RADIUS / RADIUS Server IP address**. Le **port du serveur Radius (RADIUS Server Port)** est préconfiguré sur 1812. Saisissez encore le **Password** du serveur RADIUS.

Cliquez sur **Apply** afin d'enregistrer vos réglages. Vous devrez redémarrer votre routeur afin d'appliquer les réglages en cliquant sur **Apply** dans le fenêtre suivante. Votre réseau sans fil sera disponible avec son chiffrement après le redémarrage.

3.2.3 Réglage du chiffrement pour les fonctions pont point à point, pont point à multipoint et pont WDS

Dans un premier temps, il importe de distinguer les différentes notions. Petit glossaire des termes les plus importants utilisés ici :

Authentification : L'authentification est une procédure au cours de laquelle l'identité, d'une personne par exemple, est déterminée à l'aide d'une caractéristique particulière. Cette caractéristique peut être une empreinte digitale, un mot de passe ou tout autre justificatif.

Chiffrement : Le chiffrement est une procédure au cours de laquelle un « texte en langage clair » est transformé en « texte codé » à l'aide d'un processus de chiffrement (algorithme). Un ou plusieurs codes peuvent être utilisés à cet effet. Il convient également de relever que chaque procédé de chiffrement offre une ou plusieurs possibilités d'authentification.

Les types de chiffrements suivants sont disponibles pour les différents modes de fonctionnement :

- **Chiffrement WEP 64 bits et 128 bits**
- **Chiffrement WPA (TKIP) et WPA2 (AES)**

Vous pouvez régler la configuration des modes de fonctionnement **Bridge point to point, Bridge point to multipoint et Bridge WDS** en cliquant sur le bouton **Set Security** à la fin des réglages du mode de fonctionnement correspondant.

Dans le cas du mode de fonctionnement **Bridge WDS (pont WDS)**, un chiffrement pour le point d'accès doit aussi être configuré sous **Wireless/Security Settings (réglages de sécurité sans fil)** dans le menu de gauche. Seul ce chiffrement est disponible pour WDS.

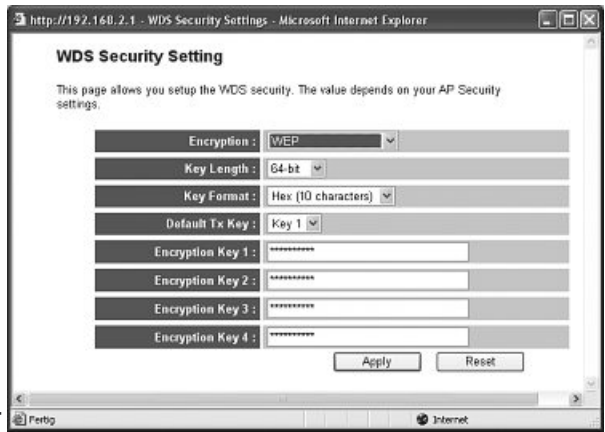
Vous pouvez choisir entre le chiffrement **WEP à 64 bits et 128 bits, WPA** avec l'algorithme de chiffrement **TKIP et WPA2** avec l'algorithme de chiffrement **AES**.

3.2.3.1 Chiffrement WEP

Le standard **WEP** (Wired Equivalent Privacy) est un algorithme de chiffrement standard pour WiFi. Il est censé régler l'accès au réseau aussi bien que garantir l'intégrité des données, mais ce procédé est considéré comme peu sûr en raison de différents maillons faibles.

Sélectionnez premièrement le type de chiffrement (64 bits ou 128 bits) que vous désirez utiliser ; veuillez noter que le chiffrement à 128 bits offre davantage de sécurité. Sélectionnez ensuite la méthode que vous désirez utiliser pour le **format de la clé (Key Format)** : Hex vous permettant l'utilisation des caractères 0-9 et a-f, ou ASCII vous permettant l'utilisation de tous les caractères et ainsi de déterminer la longueur de la clé.

Vous pouvez sélectionner une des quatre clés pré-configurées sous **Default Tx Key (clé de transmission par défaut)**. Sélectionnez par exemple **Key 1** puis saisissez votre clé personnelle de la longueur requise dans les champs situés plus bas.



Exemples : 64 bits Hex (10 caractères) = 231074a6ef
 64 bits ASCII (5 caractères) = j31n!

 128 bits Hex (26 caractères) = 231074a6b9773ce43f91a5bef3
 128 bits ASCII (13 caractères) = conges2006!+0

Cliquez sur **Apply** afin d'enregistrer vos réglages. Vous devrez redémarrer votre routeur afin d'appliquer les réglages en cliquant sur **Apply** dans le fenêtre suivante. Votre réseau sans fil sera disponible avec son chiffrement après le redémarrage.

3.2.3.2 Chiffrement WPA/WPA2

L'accès protégé WiFi **WPA** (WiFi Protected Access) est une méthode de chiffrement pour WiFi (WLAN). WPA comprend l'architecture de WEP mais offre une protection supplémentaire grâce à un encodage dynamique basé sur le protocole Temporal Key Integrity Protocol (TKIP) qui offre en outre des « clés pré-partagées » (PSK Pre-Shared-Keys) ou un « protocole d'authentification extensible » (EAP, Extensible Authentication Protocol) pour lequel cependant un serveur radius est nécessaire. WPA2 est un post-développement de WPA et utilise AES (Advanced Encryption Standard), un autre algorithme de chiffrement.

Sélectionnez **WPA pre-shared-key (clé partagée WPA) Encryption**. Définissez ensuite, sous WPA Unicast Cipher Suite, le type de chiffrement - WPA (TKIP) ou WPA (AES) – que vous désirez utiliser.

Déterminez alors le **format de la clé pré-partagée (Pre-shared Key Format)**. Choisissez entre (**phrase de passe**) **Passphrase** pour une clé comportant au moins 8 caractères et au plus 63 (les lettres (A-Z), chiffres et signe de ponctuation sont admissibles) et **Hex** pour une clé d'une longueur de 64 signes (uniquement les caractères 0-9 et a-f peuvent être utilisés).



L'étape suivante est la saisie de la clé, la (**clé pré-partagée**) **Pre-shared Key (PSK)**. Chaque client désirant accéder au point d'accès doit connaître cette clé.

Cliquez sur **Apply** afin d'enregistrer vos réglages. Vous devrez redémarrer votre routeur afin d'appliquer les réglages en cliquant sur **Apply** dans le fenêtre suivante. Votre réseau sans fil sera disponible avec son chiffrement après le redémarrage.

3.3 Modification des données d'identifiant

Sélectionnez **General Setup**, puis **System => Password Settings** dans le menu de gauche à partir de la fenêtre de démarrage que vous pouvez ouvrir en cliquant sur **Home**.

Vous pouvez saisir un nouveau mot de passe pour votre routeur dans cette page. Pour définir un nouveau mot de passe, saisissez premièrement le mot de passe actuel dans le champ **Current password**. Saisissez ensuite votre nouveau mot de passe dans le champ **New Password**, puis confirmez ce mot de passe en le tapant à nouveau dans **Confirmed Password**. Confirmez votre saisie en cliquant sur **Apply**. Vous devrez redémarrer votre routeur afin d'appliquer les réglages en cliquant sur **Apply** dans le fenêtre suivante. Votre nouveau mot de passe est valide après le redémarrage.

3.4 Réglages de réseau local

Sélectionnez **General Setup**, puis **Réseau local (LAN)** dans le menu de gauche à partir de la fenêtre de démarrage que vous pouvez ouvrir en cliquant sur **Home**.

Vous pouvez modifier les réglages réseau local standards de votre routeur dans cette fenêtre.

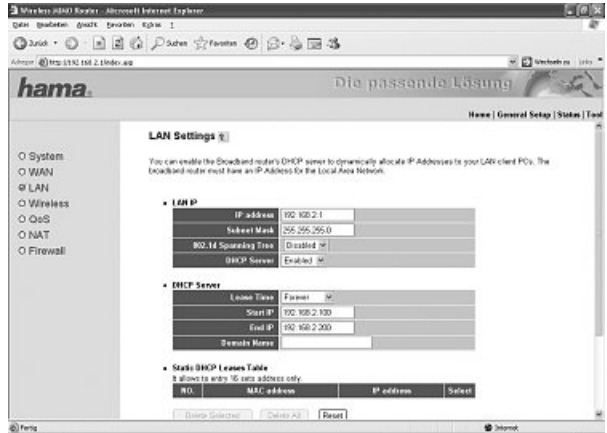
LAN IP (Adresse IP de réseau local) :

Votre routeur est préconfiguré sur l'adresse IP 192.168.2.1. Vous pouvez modifier cette adresse dans le cas où vous désirez en utiliser une autre. Le **masque de sous-réseau (Subnet mask)** correspondant est saisi dans le champ situé directement dessous l'adresse.

Serveur DHCP :

Le serveur **DHCP** intégré vous permet d'attribuer automatiquement des adresses IP aux clients connectés.

Choisissez **Disabled (Bloqué)** dans le cas où vous avez décidé d'attribuer les adresses IP manuellement et n'avez donc pas besoin du serveur DHCP. Sélectionnez **Enable (Activé)** dans le cas où vous décidez d'utiliser le serveur DHCP. Le réglage du **Lease Time (Période de bail)** vous indique la période de validité de l'adresse IP du client.



La zone d'adresses IP à partir de laquelle le serveur DHCP attribue les adresses IP aux clients est délimitée par **Start-IP-Address (Première adresse IP)** et **End-IP-Address (Dernière adresse IP)**. Vous pouvez attribuer une adresse MAC ou une adresse IP à partir de la zone valide dans le tableau situé en bas. Un client recevra toujours cette même adresse IP lorsqu'il s'annonce au routeur. Marquez, à cet effet, **Enable Static DHCP Lease (Activer bail DHCP)** et saisissez l'adresse MAC ainsi que l'adresse IP dans les champs vides du bas du tableau. Votre saisie sera enregistrée dans le tableau dès que vous cliquez sur le bouton **Add**.

Confirmez votre saisie en cliquant sur **Apply**. Vous devrez redémarrer votre routeur afin d'appliquer les réglages en cliquant sur **Apply** dans la fenêtre suivante.

Attention : Votre nouvelle configuration de réseau local est valide après le redémarrage. Vous devrez donc utiliser la nouvelle adresse IP lorsque vous désirez ouvrir l'interface web dans votre navigateur.

4. Outils

Le routeur pour réseau local sans fil de Hama vous propose plusieurs outils, utiles lors de la configuration et de la manipulation de votre appareil.

4.1 Outil de configuration

Sélectionnez **Tools (Outils)** dans le menu supérieur droit, puis **Configuration Tools (Outils de configuration)** à partir de la fenêtre de démarrage que vous pouvez ouvrir en cliquant sur **Home**.

Vous pouvez enregistrer toute la configuration de votre routeur dans cette page. Pour ce faire, cliquez sur le bouton **Save**. Sélectionnez ensuite un dossier cible. Vous devriez également définir un nom de fichier vous permettant d'identifier le fichier sans équivoque. Cliquez sur **Save** afin d'enregistrer vos réglages. Dans le cas où vous désirez reconstituer ultérieurement les réglages enregistrés, cliquez sur **Parcourir**, puis sélectionnez le fichier de configuration recherché. Cliquez sur **charger (Upload)** afin de charger le fichier. Votre routeur prendra quelques secondes à charger le fichier, puis à redémarrer. La configuration sélectionnée est valide après le redémarrage.



Dans le cas où vous désirez réinitialiser votre routeur à ses réglages d'origine, cliquez sur le bouton **Reset (Restore to Factory Default)**. Répondez à la question posée en cliquant sur **OK** ; votre routeur sera remis à ses réglages d'origine.

4.2 Actualisation du micrologiciel

Sélectionnez **Tools (Outils)** dans le menu supérieur droit, puis **Firmware Upgrade (Actualisation du micrologiciel)** à partir de la fenêtre de démarrage que vous pouvez ouvrir en cliquant sur **Home**. Cliquez sur **Next** dans la fenêtre suivante.

Cliquez sur **Parcourir**, dans la fenêtre suivante, afin de sélectionner le nouveau fichier de micrologiciel. Cliquez sur **Apply** dès que vous avez sélectionné le fichier. Le nouveau micrologiciel est chargé et le routeur redémarre automatiquement.

Attention : Le chargement d'un nouveau micrologiciel efface tous les réglages que vous avez effectués.

4.3 Redémarrage du routeur

Sélectionnez **Tools (Outils)** dans le menu supérieur droit, puis **Reset (Réinitialisation)** dans le menu de gauche à partir de la fenêtre de démarrage que vous pouvez ouvrir en cliquant sur **Home**.

Cliquez sur **Apply** dans cette fenêtre, puis confirmez la remarque suivante à l'aide de **OK** ; votre routeur redémarrera automatiquement. Tous les réglages que vous avez effectués seront effacés.

5. Informations d'état

Sélectionnez **Status (Etat)** dans le menu supérieur droit à partir de la fenêtre de démarrage que vous pouvez ouvrir en cliquant sur **Home**.

Vous pouvez afficher les informations supplémentaires de différents sous-menus comme **Internet connection (Connexion internet)**, **Device Status (Etat de l'appareil)** ou **Active DHCP Clients (Clients DHCP actifs)**. Un compte de paquets est également disponible sous l'item de menu **Statistiques (Statistics)**.

6. Support technique et contact

En cas d'appareil défectueux :

En cas de réclamation concernant le produit, veuillez vous adresser à votre revendeur ou au département conseil produits de Hama.

Internet / World Wide Web

Notre support technique, les nouveaux pilotes et les informations produits sont disponibles sous : www.hama.com

Ligne téléphonique directe d'assistance – Conseil produits Hama :

Tél. +49 (0) 9091 / 502-115

Fax +49 (0) 9091 / 502-272

e-mail : produktberatung@hama.de

Remarque :

Cet appareil peut être utilisé uniquement en Allemagne, Autriche, Suisse, Angleterre, France, Belgique, Espagne, aux Pays-Bas, au Danemark, en Hongrie, Pologne, Suède, Luxembourg, en Irlande, Grèce, République Tchèque, Slovaquie et Finlande.

La déclaration de conformité à la directive R&TTE 99/5/EC se trouve sur www.hama.com

Indholdsfortegnelse:

1.	Tilslutning af Wireless LAN router	side 03
2.	Konfiguration af styresystem og computer	side 03
3.	Konfiguration af Wireless LAN router	side 05
3.1	Konfiguration af Internetforbindelse med hjælp af assistenten	side 05
3.2	Konfiguration af Wireless LAN	side 06
3.2.1	Basisindstillinger for trådløse netværk	side 07
3.2.1.1	Drift som accesspoint (AP)	side 07
3.2.1.2	Drift som AP Bridge-Point to Point	side 08
3.2.1.3	Drift som AP Bridge-Point to Multi-Point	side 08
3.2.1.4	Drift som AP Bridge WDS	side 09
3.2.2	Indstilling af kryptering for AP	side 09
3.2.2.1	WEP kryptering	side 10
3.2.2.2	WPA/WPA2 kryptering	side 11
3.2.3	Indstilling af kryptering for AP Bridge-Point to Point, Point to Multi-Point og WDS	side 12
3.2.3.1	WEP kryptering	side 13
3.2.3.2	WPA/WPA2 kryptering	side 13
3.3	Ændring af log-in data	side 14
3.4	LAN indstillinger	side 15
4.	Værktøj.....	side 15
4.1	Konfigurationsværktøjer.....	side 16
4.2	Firmware opdatering	side 16
4.3	Genstart af routeren	side 16
5.	Statusoplysninger.....	side 17
6.	Support- og kontaktoplysninger	side 17

Pakningens indhold:

- 1x Hama Wireless LAN Router MiMo 300 Express
- 1x netdel 12 V
- 1x trykt betjeningsvejledning

Systemforudsætning:

- Styresystem med installeret TCP/IP protokol
- Java-egnet webbrowser som fx Mozilla Firefox eller Microsoft Internet Explorer

Sikkerhedsanvisninger:

Brug aldrig apparatet hverken i fugtige eller i meget støvede omgivelser, ej heller på radiatorer eller i nærheden af andre varmekilder. Denne enhed er ikke beregnet til udendørs brug. Beskyt enheden mod tryk- og stødpåvirkninger. Enheden må ikke åbnes eller flyttes under brug.

Bemærk! Benyt kun routeren med den medfølgende netdel. Anvendelse af andre netdele kan medføre ødelæggelser i apparatet.

Et tips!!!

Ved volumen- eller tidstariffer anbefales det at vælge "Forbindelse ved behov", hvorved Internetadgangen automatisk afbrydes efter den indstillede tid under muligheden "Tomgangstid". Ved permanent forbindelse kan der ellers opstå høje forbindelsesomkostninger. Men læg også mærke til, at lukning af browseren ikke betyder fravalg af Internetforbindelsen. Rigtig mange programmer sender forespørgsler på Internettet eller modtager data herfra uden at dette entydigt kan registreres. Dette er for routeren et lige så vigtigt spørgsmål som fx åbning af browseren. Hvis du skal være sikker på, at der ingen aktiv forbindelse består til Internettet, skal du slukke for apparatet eller adskille det fra modemmet.

1. Tilslutning af Wireless LAN router

1. Tilslut computeren og andre netværksenheder som fx hub/switch til bøsningerne 1-4. Anvend hertil et cross-over eller CAT5 patchkabel (max. 100 m). Den indbyggede switch registrerer selv forbindelseshastigheden på 10 eller 100 Mbps, halv/fuld duplex overførselsfunktion samt den benyttede kabeltype.
2. Forbind dit modems Ethernet-port med tilslutningen "WAN" på routeren. Alt efter modemmet er et 1:1 eller cross-over konfigureret kabel nødvendigt. I de fleste tilfælde kan det allerede foreliggende tilslutningskabel benyttes.
3. Sæt nu den medfølgende netadapter i en ledig stikkontakt og forbind den med routeren. Forsigtig: en uegnet neddel kan medføre beskadigelser!

Afprøvning af installationen

På oversiden befinder der sig forskellige lysdioder til visning af status:

Lysdiode	Tilstand	Status
Power	Lyser	Netdel er tilsluttet og leverer strøm
	Slukket	Ingen netdel tilsluttet, ingen strømforsyning til enheden
WLAN	Blinker	Wireless LAN er aktiveret/der afsendes data
	Slukket	Wireless LAN er deaktiveret
WAN	Lyser	WAN porten har oprettet en korrekt netværksforbindelse
	Blinker	Dataoverførsel via WAN porten
	Slukket	Ingen forbindelse
LAN1-4	Lyser	Den pågældende LAN port har oprettet en korrekt netværksforbindelse
	Blinker	Dataoverførsel via den pågældende LAN port
	Slukket	Ingen forbindelse

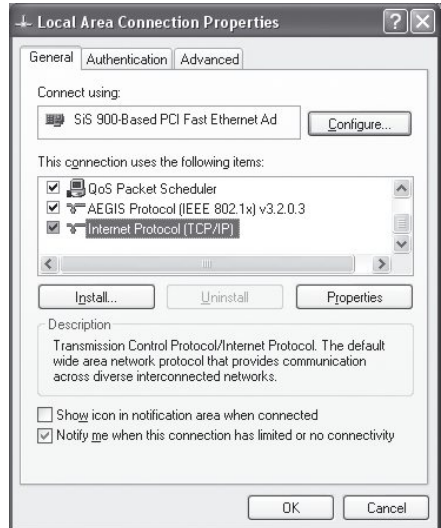
2. Konfiguration af styresystem og computer

På alle PC'er der skal benytte Internettet skal der være installeret en TCP/IP protokol. Standardmæssigt er der for routeren konfigureret en IP-adresse 192.168.2.1 og en aktiveret DHCP server. Derved får den tilsluttede PC automatisk tildelt passende adresser og yderligere indstillinger. Vi anbefaler at bibeholde dette.

For at kontrollere indstillingerne på din PC skal du gå således frem:
Start -> Indstillinger -> Systemindstillinger -> Netværksforbindelser

Udvælg her den forbindelse (netværksadapter), til hvilken din router er forbundet, fx "LAN forbindelse". Efter et højreklik på den pågældende forbindelse kommer der en menu frem, i hvilken du kan vælge egenskaber.

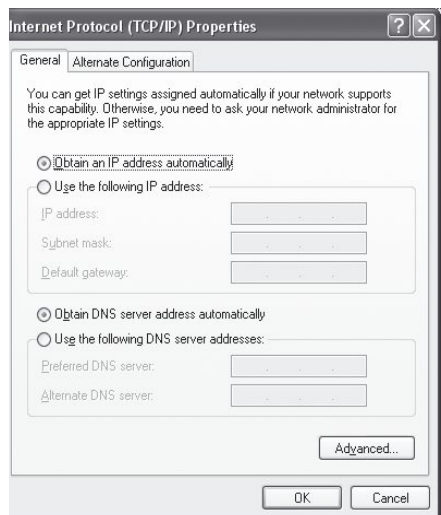
Marker her på listen **Internet Protocol (TCP/IP)** og klik derefter på **Properties**.



Vælg **Obtain an IP address automatically** og **Obtain DNS Server address automatically!** Bekræft herefter med **OK** og i det følgende vindue ligeledes med **OK!**

Din PC er nu således konfigureret, at den automatisk får tildelt sin IP-adresse fra routeren. Du kan nu installere routeren pr. web-browser.

Browseren skal være Java-egnet og have denne funktion aktiveret (fx Internet Explorer 6.0 og nyere eller Mozilla Firefox)



3. Konfiguration af Wireless LAN router

For at starte konfigurationen skal du åbne din browser og indtaste adressen "http://192.168.2.1". Derefter ses log-in vinduet. Som standard er brugernavnet: **admin** og kendeordet: **1234** installeret. Klik efter indtastningen på **OK** for at logge på routeren.

Til konfiguration af routeren har du mulighed for at benytte den integrerede assistent eller at foretage installationen manuelt. Efter konfiguration med hjælp fra assistenten er apparatet så vidt installeret, at den tilsluttede computer har adgang til Internettet.

Et tips!!!

For sikkerhedens skyld skal du i hvert fald ændre brugernavn og password. Standardværdierne er ens på mange apparater og kan dermed give fremmede personer adgang til routerkonfigurationen. Oplysninger vedrørende dette finder du på side 14.

3.1 Konfiguration af Internetforbindelsen med hjælp af assistenten

Efter at være logget på skal du starte assistenten ved at klikke på feltet **Quick Setup**.

Time Zone

Vælg under **Set Time Zone** den korrekte tidszone, fx for Danmark "(GMT+1.00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien". De resterende indstillinger kan overtages uden ændringer. Klik på **Next** for at komme videre.

Broadband Type

I næste trin bliver du opfordret til at angive WAN forbindelsestype. De brugerspecificerede oplysninger får du fra din netudbyder. Til de forskellige forbindelsestyper findes der på oversigtssiden en kort beskrivelse. På grund af den store udbredelse af DSL over **PPPoE** drejer den videre beskrivelse sig om denne forbindelsestype.

For forbindelsestypen **PPPoE** skal du klikke på **PPPoE xDSL**.

IP adresse info

I det følgende skærmbillede skal du indtaste adgangsdata for din udbyder. Disse oplysninger får du enten fra dine papirer eller direkte fra udbyderen.

3.PP Address Info

PPPoE
Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a "Service Name" enter it in the Service Name field, otherwise, leave it blank.

User Name	Genzebra/nt
Password	*****
Service Name	
MTU	1392 (Standard Value:1452)
Connection Type	Connect on Demand W
Idle Time Out	12 (0-100minutes)

Back Ok

Indtast følgende: **User Name**
 Password
 Service Name (dette er ikke altid nødvendigt)

Ud over adgangsdata kan du give de efterfølgende oplysninger:

MTU står for Maximal Transfer Unit og angiver den maksimale datapakkestørrelse, der kan overføres. Hvis du ikke er sikker på denne indstilling, anbefaler vi den standardmæssigt indstillede værdi. Værdier mellem 512 og 1492 er mulige.

Med oplysningen **Connection Type** bestemmer du din routers valgforhold. Du har valget mellem:

Continuous: Routeren er altid forbundet med nettet. Denne forbindelsestype anbefales, hvis du fx har en flatrate uden tidsbegrænsning.

Connect on Demand: Ved denne forbindelsestype tilslutter routeren sig først på opfordring gennem en tilsluttet computer, fx når du åbner computerens browser. Forbindelsen består i så fald så længe som den indstillede tid under **Idle Time Out** er forløbet uden aktivitet.

Manual: Hvis du bestemmer dig for forbindelsestypen **Manual**, kan du med button **Connect** oprette forbindelse og med button **Disconnect** atter afbryde forbindelsen.

Et tips!!! Ved volumen- eller tidstariffer anbefales det at vælge "Forbindelse ved behov", hvorved Internetadgangen automatisk afbrydes efter den indstillede tid under muligheden "Tomgangstid". Ved permanent forbindelse kan der ellers opstå høje forbindelsesomkostninger. Men læg også mærke til, at lukning af browseren ikke betyder fravalg af Internetforbin-del-sen. Rigtig mange programmer sender forespørgsler på Inter nettet eller modtager data herfra uden at dette entydigt kan registreres. Dette er for routeren et lige så vigtigt spørgsmål som fx åbning af browseren. Hvis du skal være sikker på, at der ingen aktiv forbindelse består til Internettet, skal du slukke for apparatet eller adskille det fra modemmet.

Idle Time Out: Fastlæg her efter hvor mange minutters inaktivitet Internetforbindelsen skal afbrydes. Værdier mellem 1 og 1000 er mulige.

Bekræft indtastningerne med **OK**. Derefter skal du starte routeren på ny, for at få indstillingerne virksomme. Tryk derfor på **Apply** for at udføre. Routeren behøver ca. 30 sekunder for at starte på ny. Efter genstarten er routeren så vidt konfigureret, at du med tilsluttet computer kan få adgang til Internettet. Du kan også manuelt ændre disse indstillinger, idet du i menuen til venstre vælger **WAN** og derefter den pågældende forbindelsestype.

3.2 Konfiguration af Wireless LAN

Standardmæssigt er Wireless LAN deaktiveret for at beskytte dig. Hvis du vil aktivere denne funktion, vælger du fra startskærmbilledet, som du atter når ved klik på **Home**, først **General Setup** og derefter i menulisten til venstre **Wireless**. Bemærk at en aktivering af Wireless LAN uden ekstra indstilling af kryptering medfører en sikkerhedsrisiko. Marker nu **Enable** og klik derefter på **Apply**. Gå videre med basisindstillinger for trådløse netværk!

3.2.1 Basisindstillinger for trådløse netværk (WLAN)

Vælg i menuen til venstre **Basic Settings**.

Under punktet **Mode** kan du vælge, hvilke opgaver routeren skal overtage i netværket. Vælg funktionen **Accesspoint AP (3.2.1.1)**, når apparatet er det eneste accesspoint i dit netværk eller ingen forbindelse skal oprettes på Bridge-niveau til andre netværk.

Vælg **AP Bridge-Point to Point (3.2.1.2)**, når du trådløst skal forbinde dette accesspoint til et andet accesspoint. Klienter har i denne funktion ikke mulighed for at tilmelde sig over en trådløs forbindelse.

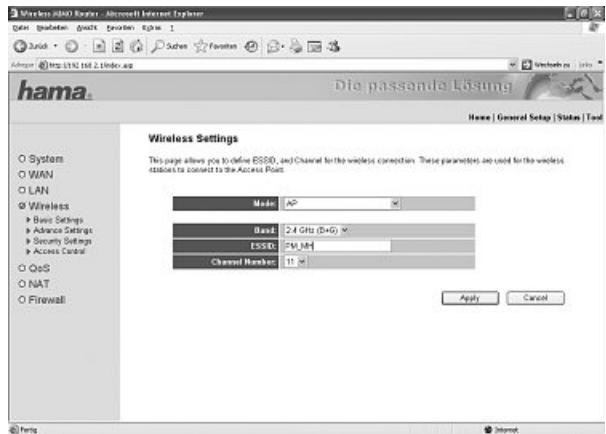
Vælg **AP Bridge-Point to Multi-Point (3.2.1.3)**, når du trådløst skal forbinde dette accesspoint til flere andre accesspoints. Klienter har i denne funktion ikke mulighed for at tilmelde sig over en trådløs forbindelse.

Vælg **AP Bridge-WDS (3.2.1.4)**, når du trådløst skal forbinde dette accesspoint til et eller flere andre accesspoints og klienter yderligere skal kunne tilmelde sig over en trådløs forbindelse.

Fortsæt konfigurationen i henhold til dine valg.

3.2.1.1 Drift som accesspoint (AP)

Med valget under **Band** fastlægger du om apparatet skal arbejde i 2,4 GHz båndet ifølge standard 802.11b (11 Mbps), 802.11g (54 Mbps) eller kombineret med 802.11b og 802.11g. Fastlæg desuden **ESSID**. Længden af **ESSID** kan være op til 32 tegn og skal være identisk for alle enheder i netværket. Under **Channel Number** fastlægger du kanalen, i hvilken data skal overføres. Der er 13 kanaler til rådighed.



Eksempel på en ESSID: "WLAN_Router_54Mbps"

Bekræft dine indstillinger ved klik på **Apply** button!

For at indstille krypteringen for et trådløst netværk klikker du i skærbilledet i tilslutning hertil på button **Continue** og derefter på **Security Settings** i menuen til venstre. Vejledning om indstilling af Wireless LAN kryptering kan du læse om på side 9.

Hvis du ønsker at bruge et trådløst netværk uden kryptering klikker du i næste skærbillede på **Apply**. Routeren bliver herefter genstartet. Efter genstarten er det trådløse netværk klar til brug.

3.2.1.2 Drift som AP Bridge-Point to Point

Med valget under **Band** fastlægger du om apparatet skal arbejde i 2,4 GHz båndet ifølge standard 802.11b (11 Mbps), 802.11g (54 Mbps) eller kombineret med 802.11b og 802.11g. Under **Channel Number** fastlægger du kanalen, i hvilken data skal overføres. Der er 13 kanaler til rådighed. Indtast i feltet **MAC address 1** det accesspoints adresse, til hvilket Bridge-forbindelsen skal opbygges. For at indstille krypteringen for dit trådløse netværk klikker du derefter på **Set Security** button.



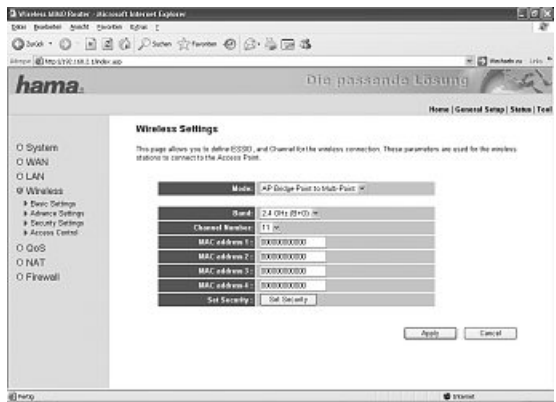
Vejledning om indstilling af Wireless LAN kryptering kan du læse om på side 12.

Hvis du ønsker at bruge et trådløst netværk uden kryptering klikker du på **Apply** og i det følgende skærmbillede også på **Apply**. Routeren bliver herefter genstartet. Efter genstarten er det trådløse netværk klar til brug.

3.2.1.3 Drift som AP Bridge-Point to Multi-Point

Forskellen til AP Bridge-Point to Point drift er, at du i denne funktion MAC-adresser kan indtaste flere accesspoints. En Bridge-forbindelse er maksimalt mulig til 6 andre accesspoints. Med valget under **Band** fastlægger du om apparatet skal arbejde i 2,4 GHz båndet ifølge standard 802.11b (11 Mbps), 802.11g (54 Mbps) eller kombineret med 802.11b og 802.11g. Under **Channel Number** fastlægger du kanalen, i hvilken data skal overføres. Der er 13 kanaler til rådighed.

Indtast i felterne **MAC address 1 til MAC Address 6** de accesspoints adresser, til hvilke Bridge-forbindelsen skal opbygges. For at indstille krypteringen for dit trådløse netværk klikker du derefter på **Set Security** button.



Vejledning om indstilling af Wireless LAN kryptering kan du læse om på side 12.

Hvis du ønsker at bruge et trådløst netværk uden kryptering klikker du på **Apply** og i det følgende skærmbillede også på **Apply**. Routeren bliver herefter genstartet. Efter genstarten er det trådløse netværk klar til brug.

3.2.1.4 Drift som AP Bridge WDS

Hvad er **WDS**? Wireless Distribution System betegner den trådløse forbindelse mellem flere accesspoints under hinanden og muliggør desuden tilmelding af klienter, hvilket andre Bridge driftsformer ikke tillader. Derved bliver for hvert ekstra accesspoint nettets båndbredde halveret, fordi datapakken skal overføres dobbelt.

Det fremstår altså som en kombination af de foregående driftsformer.

Med valget under **Band** fastlægger du om apparatet skal arbejde i 2,4 GHz båndet ifølge standard 802.11b (11 Mbps), 802.11g (54 Mbps) eller kombineret med 802.11b og 802.11g. Til Client-netværk er **ESSID** påkrævet. Det tjener til identifikation i netværket, og skal dermed være ens for alle deltagere i Client-netværket. Længden af **ESSID** kan udgøre op til 32 tegn.



Under **Channel Number** fastlægger du kanalen, i hvilken data skal overføres. Der er 13 kanaler til rådighed. Indtast i felterne **MAC address 1 til MAC Address 6** de accesspoints adresser, til hvilke Bridge-forbindelsen skal opbygges. For at indstille krypteringen for dit trådløse netværk klikker du derefter på **Set Security** button.

Vejledning om indstilling af Wireless LAN kryptering kan du læse om på side 12.

Hvis du ønsker at bruge et trådløst netværk uden kryptering klikker du på **Apply** og i det følgende skærmbillede også på **Apply**. Routeren bliver herefter genstartet. Efter genstarten er det trådløse netværk klar til brug.

3.2.2 Indstilling af kryptering for AP

Først er det vigtigt at skelne mellem forskellige begreber. Derfor en kort forklaring om de vigtigste her anvendte begreber:

Autentifikation: Autentificeringen er et forløb, ved hvilket fx en persons identitet fastlægges med et bestemt kendetegn. Dette kan fx ske med et fingeraftryk, et password eller en hvilket som helst anden berettigelsesidentifikation.

Kryptering: Krypteringen er en proces, ved hvilken en "klartekst" ved hjælp af en krypteringsmetode (algoritme) forvandles til en "hemmelig tekst". Til dette formål kan anvendes en eller flere krypteringsnøgler. Yderligere skal det nævnes, at hver enkelt krypteringsmetode byder på en eller flere muligheder for autentifikation.

Til denne driftstype er der følgende krypteringer til rådighed:

- **WEP-kryptering med 64 bit og 128 bit**
- **WPA og WPA2 kryptering**

For driftstypen **AP** kan du foretage indstillingerne under **Wireless/Security Settings** i menuen til venstre.

Standardmæssigt er kryptering deaktiveret. Men vi anbefaler dig at sikkerhedsgrunde altid at benytte kryptering.

3.2.2.1 WEP kryptering

Wired Equivalent Privacy (**WEP**) er en standard krypteringsalgoritme til WLAN. Den skal såvel regulere adgangen til nettet som sikre dataenes integritet. På grund af forskellige svagheder anses metoden for usikker.

Først skal du vælge om du vil anvende en 64 bit eller en 128 bit kryptering, hvor 128 bit krypteringen tilbyder en højere sikkerhed. Som det næste skal du vælge **Key Format** mellem Hex (du kan benytte tegn fra 0-9 og a-f) og ASCII (du kan benytte ethvert ønsket tegn), hvorved også krypteringsnøglens længde bestemmes.

Under **Default Tx Key** har du muligheden for at vælge en forud indstillet kryptering. Vælg fx **Key 1** og indtast i de herunder liggende felter din ønskede krypteringsnøgle med den påkrævede længde.



Eksempel: 64 bit Hex (10 tegn) = 231074a6ef
64 bit ASCII (5 tegn) = j31n!

128 bit (26 tegn) = 231074a6b9773ce43f91a5bef3
128 bit ASCII (13 tegn) = urlaub2006!+0

For at gemme dine indstillinger skal du klikke på **Apply**. Derefter skal routeren genstartes for at aktivere alle indstillinger. Klik dertil i det følgende vindue på **Apply**. Efter genstart er det trådløse netværk klar med kryptering.

3.2.2.2 WPA/WPA2 kryptering

WiFi Protected Access (**WPA**) er en krypteringsmetode til WLAN. WPA indeholder arkitekturen fra WEP, men tilbyder dog yderligere beskyttelse med dynamisk krypteringsnøgle, der er baseret på Temporal Key Integrity Protocol (TKIP), og desuden til autentifikation af brugere tilbyder PSK (Pre-Shared Keys) eller Extensible Authentication Protocol (EAP), til hvilket dog en Radius Server er nødvendig. WPA2 er videreudviklingen af WPA og udnytter en anden krypteringsalgoritme AES (Advanced Encryption Standard).

Vedrørende autentificeringen er forskellen ved WPA mellem **Pre-Shared Key** og autentificeringen via særlige **autentifikationsprotokoller**, ved hvilke det mest handler om varianter af EAP (Extensible Authentication Protocol). For dem begge, på det private område temmelig sjældne autentifikationsmetoder, benyttes en såkaldt autentifikationsserver (RADIUS-Server). De oplysninger som du behøver til denne autentifikationsmetode får du fra din administrator.

WPA pre.shared key (anbefales til de fleste anvendelser)

Vælg først om du vil benytte **WPA med TKIP** krypteringsalgoritme, **WPA2 med AES** krypteringsalgoritme eller **WPA Mixed Modus**. Denne Mixed Modus tillader klienter med WPA eller WPA2 at koble sig på accesspointet. Denne blanding er meget fornuftig, da kun få XP-klienter for øjeblikket er WPA2 egnede. Hvis Mixed Modus er afbrudt, så lader AP kun klienter med WPA2 og det store antal WPA(TKIP)-enheder blive udenfor.



Som det næste bestemmer du krypteringsformatet (**Pre-Shared Key Format**). Vælg enten **Passphrase** til en nøgle med en længde på mindst 8 og højst 63 tegn, hvorved bogstaver (A-Z), tal og sætningstegn er tilladt, eller **Hex** til en nøgle med en længde på 64 tegn, hvorved kun tegn fra 0-9 og a-f kan benyttes.

Det næste trin er indtastning af nøglen, den såkaldte **Pre-Shared-Key** (PSK). Hvis en klient skal tilslutte sig accesspointet, skal han kende denne tegnække.

For at gemme dine indstillinger skal du klikke på **Apply**. Derefter skal routeren genstartes for at aktivere alle indstillinger. Klik dertil i det følgende vindue på **Apply**. Efter genstart er det trådløse netværk klar med kryptering.

WPA RADIUS (en særlig autentifikations-server er nødvendig)

Vælg først om du vil benytte **WPA med TKIP** krypteringsalgoritme, **WPA2 med AES** krypteringsalgoritme eller **WPA Mixed Modus**. Denne Mixed Modus tillader klienter med WPA eller WPA2 at koble sig på accesspointet. Denne blanding er meget fornuftig, da kun få XP-klienter for øjeblikket er WPA2 egnede.

Vælger du kun **WPA2 (AES)** så lader AP kun klienter med WPA2 og det store antal WPA(TKIP)-enheder blive udenfor.

Som det næste indtaster du **RADIUS Server IP address**. **RADIUS Server Port** er forudindstillet til 1812. Indtast nu **password** for RADIUS serveren.

For at gemme dine indstillinger skal du klikke på **Apply**. Derefter skal routeren genstartes for at aktivere alle indstillinger. Klik dertil i det følgende vindue på **Apply**. Efter genstart er det trådløse netværk klar med kryptering.

3.2.3 Indstilling af kryptering for Bridge-Point to Point, Bridge-Point to Multi-Point og Bridge WDS

Først er det vigtigt at skelne mellem forskellige begreber. Derfor en kort forklaring om de vigtigste her anvendte begreber:

Autentifikation: Autentificeringen er et forløb, ved hvilket fx en persons identitet fastlægges med et bestemt kendetegn. Dette kan fx ske med et fingeraftryk, et password eller en hvilket som helst anden berettigelsesidentifikation.

Kryptering: Krypteringen er en proces, ved hvilken en "klartekst" ved hjælp af en krypteringsmetode (algoritme) forvandles til en "hemmelig tekst". Til dette formål kan anvendes en eller flere krypteringsnøgler. Yderligere skal det nævnes, at hver enkelt krypteringsmetode byder på en eller flere muligheder for autentifikation.

Til de forskellige driftsformer er der følgende krypteringer til rådighed:

- **WEP-kryptering med 64 bit og 128 bit**
- **WPA(TKIP) og WPA2(AES) kryptering**

For driftsformerne **Bridge-Point to Point**, **Bridge-Point to Multi-Point** og **Bridge WDS** kan du foretage indstillingerne ved slutningen af de pågældende driftsform-indstillinger ved klik på **Set Security** button. For driftstypen **Bridge WDS** skal der også under **Wireless/Security Settings** i menuen til venstre indstilles en kryptering for accesspointet. Kun denne kryptering er så også til rådighed for WDS.

Du har valget mellem **WEP** kryptering med **64 bit og 128 bit**, **WPA med TKIP** krypteringsalgoritme og **WPA2** med **AES** krypteringsalgoritme

3.2.3.1 WEP-kryptering

Wired Equivalent Privacy (**WEP**) er en standard krypteringsalgoritme til WLAN. Den skal såvel regulere adgangen til nettet som sikre dataenes integritet. På grund af forskellige svagheder anses metoden for usikker.

Først skal du vælge om du vil anvende en 64 bit eller en 128 bit kryptering, hvor 128 bit krypteringen tilbyder en højere sikkerhed. Som det næste skal du vælge **Key Format** mellem Hex (du kan benytte tegn fra 0-9 og a-f) og ASCII (du kan benytte ethvert ønsket tegn), hvorved også krypteringsnøglenes længde bestemmes.

Under **Default Tx Key** har du muligheden for at vælge en forud indstillet kryptering. Vælg fx **Key 1** og indtast i de herunder liggende felter din ønskede krypteringsnøgle med den påkrævede længde.



Eksempel: 64 bit Hex (10 tegn) = 231074a6ef
64 bit ASCII (5 tegn) = j31n!

128 bit (26 tegn) = 231074a6b9773ce43f91a5bef3
128 bit ASCII (13 tegn) = urlaub2006!+0

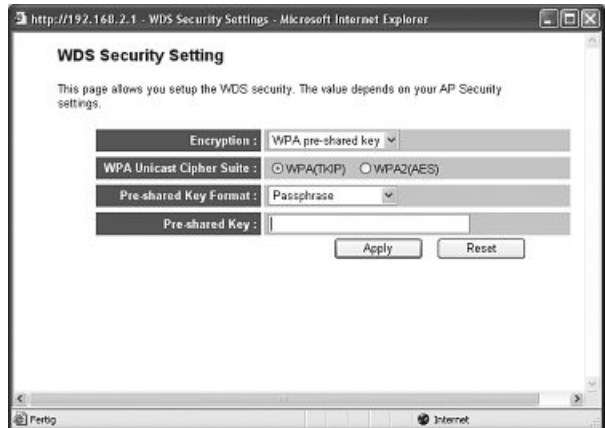
For at gemme dine indstillinger skal du klikke på **Apply**. Derefter skal routeren genstartes for at aktivere alle indstillinger. Klik dertil i det følgende vindue på **Apply**. Efter genstart er det trådløse netværk klar med kryptering.

3.2.3.2 WPA/WPA2 kryptering

WiFi Protected Access (**WPA**) er en krypteringsmetode til WLAN. WPA indeholder arkitekturen fra WEP, men tilbyder dog yderligere beskyttelse med dynamisk krypteringsnøgle, der er baseret på Temporal Key Integrity Protocol (TKIP), og desuden til autentifikation af brugere tilbyder PSK (Pre-Shared Keys) eller Extensible Authentication Protocol (EAP), til hvilket dog en Radius Server er nødvendig. WPA2 er videreudviklingen af WPA og udnytter en anden krypteringsalgoritme AES (Advanced Encryption Standard).

Vælg nu under Encryption **WPA Pre-Shared Key**. Derefter bestemmer du under WPA Unicast Cipher Suite, om du vil anvende WPA(TKIP) eller WPA (AES).

Som det næste bestemmer du krypteringsformatet (**Pre-Shared Key Format**). Vælg enten **Passphrase** til en nøgle med en længde på mindst 8 og højst 63 tegn, hvorved bogstaver (A-Z), tal og sætningstegn er tilladt, eller **Hex** til en nøgle med en længde på 64 tegn, hvorved kun tegn fra 0-9 og a-f kan benyttes.



Det næste trin er indtastning af nøglen, den såkaldte **Pre-Shared-Key** (PSK). Hvis en klient skal tilslutte sig accesspointet, skal han kende denne tegnække.

For at gemme dine indstillinger skal du klikke på **Apply**. Derefter skal routeren genstartes for at aktivere alle indstillinger. Klik dertil i det følgende vindue på **Apply**. Efter genstart er det trådløse netværk klar med kryptering.

3.3 Ændring af log-in data

Vælg fra startskærmbilledet, som du atter når ved klik på **Home**, først **General Setup** og derefter i menulisten til venstre **System => Password Settings**.

På denne side kan du fastlægge et nyt password for routeren. For at kunne indtaste et nyt password skal først det aktuelle password indtastes i feltet **Current Password**. Det nye password indsætter du i feltet **New Password** og bekræfter den korrekte skrivemåde med gentagen indtastning i feltet **Confirmed Password**. Bekræft dine indtastninger med **Apply**. Derefter skal routeren genstartes for at aktivere alle indstillinger. Klik dertil i det følgende vindue på **Apply**. Efter genstart er det nye password gyldigt.

3.4 LAN indstillinger

Vælg fra startskærm-billedet, som du atter når ved klik på **Home**, først **General Setup** og derefter i menulisten til venstre **LAN**.

I dette vindue kan du ændre LAN indstillingerne for din router.

LAN IP: Routeren er forudindstillet til IP-adresse 192.168.2.1. Hvis du skal anvende en anden adresse til din router, kan du ændre dette i indtastningsfeltet direkte derunder registreres den tilsvarende **Subnet Mask**.

DHCP-Server:

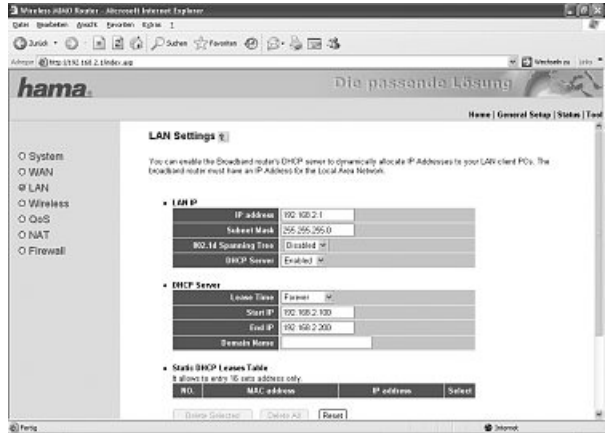
Den integrerede DHCP-Server muliggør automatisk tildeling af IP-adresser for tilsluttede klienter.

Hvis du tildeler IP-adresser manuelt i dit netværk og derfor ikke behøver DHCP-Server, skal du vælge **Disabled**.

Hvis du vil bruge DHCP-Serveren, vælger du **Enabled**. Indstillingen for **Lease Time** viser, hvor længe den tildelte IP-adresse er gyldig for klienten.

IP-adresseområdet fra hvilket DHCP-Serveren skal fordele IP-adresser til klienter, bliver gennem **Start-IP-Address** og **End_IP-Address** begrænset. I den nederste tabel har du muligheden for fast at tilordne en bestemt MAC-adresse en IP-adresse fra det gyldige område. Hvis en klient melder sig på routeren, får han altid tildelt denne IP-adresse. Marker hertil **Enable Static DHCP Lease** og sæt i det tomme felt i den underste tabel MAC-adressen og IP-adressen ind. Efter et klik på **Add** button gemmes indtastningen i tabellen.

For at bekræfte dine indstillinger skal du klikke på **Apply**. Derefter skal routeren genstartes for at aktivere alle indstillinger. Klik dertil i det følgende vindue på **Apply**.



Bemærk!! Efter genstart er den nye LAN-konfiguration gyldig. For at kalde dit Webinterface i browseren frem, skal du altså benytte den nye IP-adresse.

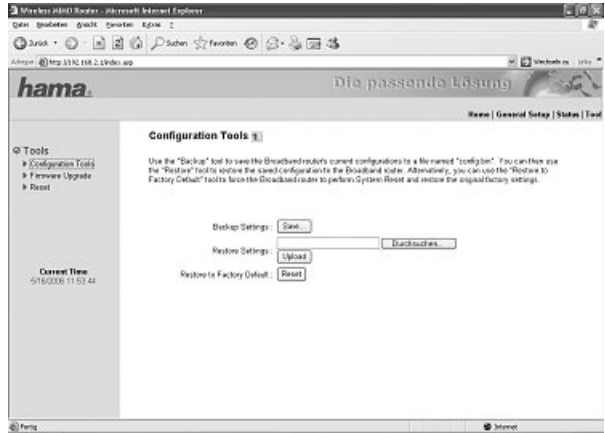
4. Værktøj

Hama Wireless LAN routeren giver dig forskellige værktøjer til rådighed, der skal hjælpe dig med konfigurationen og brugen af apparatet.

4.1 Konfigurationsværktøj

Vælg fra startskærbilledet, som du atter når ved klik på **Home**, først **Tools** i menuen øverst til højre og derefter **Configuration Tools** i menuen til venstre!

På denne side har du muligheden for at gemme den samlede konfiguration af routeren. Klik dertil på button **Save**. Vælg i tilslutning hertil destinationen. Desuden skal du fastlægge et filnavn der gør det muligt entydigt at identificere filen. Efter dit valg klikker du på **Save** og har dermed sikret dine indstillinger. Hvis du på et senere tidspunkt ønsker at få de sikrede indstillinger frem igen skal du klikke på **Browse** og dernæst udvælge de ønskede konfigurationsdata. For at sende filen klikker du på **Upload**. Routeren har nu brug for nogle sekunder til at sende filen og derefter gennemføre en genstart. Efter genstart er den valgte konfiguration gyldig.



Hvis du skal tilbagestille din router til fabriksstandardindstillingen skal du klikke på button **Reset (Restore to Factory Default)**. Bekræft spørgsmålet i tilslutning hertil med **OK**, og nu følger tilbagesætningen til standardværdierne.

4.2 Firmware-aktualisering

Vælg fra startskærbilledet, som du atter når ved klik på **Home**, først **Tools** i menuen øverst til højre og derefter **Firmware Upgrade** i menuen til venstre! Klik i det næste vindue på **Next**.

For at udvælge den nye Firmware-fil skal du klikke på **Browse** i det følgende vindue. Når du har valgt en fil, skal du klikke på **Apply**. Den nye firmware bliver registreret og routeren genstartet.

Bemærk!! Ved registrering af den nye firmware går tidligere foretagne indstillinger tabt.

4.3 Genstart af routeren

Vælg fra startskærbilledet, som du atter når ved klik på **Home**, først **Tools** i menuen øverst til højre og derefter **Reset** i menuen til venstre!

Klik i dette vindue på **Apply** og bekræft den følgende henvisning med **OK** for at genstarte routeren. De trufne indstillinger går derved ikke tabt.

5. Statusoplysninger

Vælg fra startskærbilledet, som du atter når ved klik på **Home**, først **Status** i menuen øverst til højre.

I menuen på venstre side kan du i de forskellige undermenuer få vist omfattende informationer, fx **Internet Connection**, **Device Status** eller **active DHCP-Clients**. Desuden er under menupunktet **Statistics** en datapakketæller til rådighed.

6. Support- og kontaktoplysninger

Ved defekte produkter:

Ved produktreklamationer skal du henvende dig til forhandleren eller til Hama produktrådgivning.

Internet/World Wide Web

Produktsupport, nye drivere eller produktinformationer fås under www.hama.com

Support Hotline – Hama produktrådgivning:

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

Fax +49 (0) 9091 / 502-272

e-mail: produktberatung@hama.de

Bemærkning:

Dette produkt må kun anvendes i Tyskland, Østrig, Schweiz, England, Frankrig, Belgien, Spanien, Nederlandene, Danmark, Ungarn, Polen, Sverige, Luxemburg, Irland, Grækenland, Tjekkiet, Slovakiet og Finland!

Overensstemmelseserklæringen iht R&TTE-direktivet 99/5/EF finder du under www.hama.com

Die Konformitätserklärung nach der R&TTE-Richtlinie (D)
99/5/EG finden Sie unter www.hama.de

See www.hama.de for the declaration of conformity (GB)
with R&TTE Directive 99/5/EC

La déclaration de conformité á la directive (F)
R&TTE 99/5/EC se trouve sur www.hama.de

La declaración de conformidad según la directiva (E)
R&TTE 99/5/EC la encontrará en www.hama.de

La dichiarazione di conformità secondo la direttiva (I)
R&TTE 99/5/EC é disponibile sul sito www.hama.de

De verklaring van overeenstemming conform de (NL)
R&TTE-richtlijn 99/5/EC vindt u onder www.hama.de

Konformitetserklæringen iflg. (DK)
R & TTE-retningslinierne 99/5/EC finder du under www.hama.de

Treść Deklaracji Zgodności na podstawie dyrektywy (PL)
R&TTE 99/5/EC można znaleźć na stronach www.hama.de

A megfelelőségi nyilatkozat a 99/5/EC R&TTE-irányelv (H)
Szerinti, amely megtalálható a www.hama.de honlapon.

Prohlášení, o shodě podle směrnice R&TTE 99/5/EG, (CZ)
naleznete na www.hama.de

Prehlásenie o zhode podľa R&TTE smernice 99/5/EG (SK)
nájdete na www.hama.de

Radio- ja telepäätelaitteita koskevan direktiivin 99/5/EY (FIN)
mukainen vaatimustenmukaisuusvakuutus löytyy osoitteesta
www.hama.de.

Konformitetserklæringen R&TTE-retningslinierne 99/5/EC (S)
finder du under www.hama.de

Τη δήλωση συμμόρφωσης σύμφωνα με την Οδηγία R&TTE 99/5/ΕΟΚ (GR)
θα τη βρείτε στη διεύθυνση www.hama.de

Software: (GB)

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

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

(F) Cet appareil ne peut être utilisé que dans les pays suivants:

(E) Este aparato se puede utilizar sólo en los países siguientes:

(I) L'uso di questo apparecchio é ammesso soltanto nei seguenti Paesi:

(NL) Dit apparaat mag alleen gebruikt worden in de volgende landen:

(DK) Dette apparat må kun benyttes i følgende lande:

(PL) Urządzenie sprzedawane jest tylko w następujących krajach:

(H) Ez a készülék a következő országokban üzemeltethető:

(CZ) Tento přístroj se smí používat pouze v následujících zemích:

(SK) Toto zariadenie sa môže používať len v týchto krajinách:

(S) Denna apparat får endast användas i följande länder:

(FIN) Tätä laitetta saa käyttää vain.

(GR) Η λειτουργία αυτής της σύνδεσης επιτρέπεται στις παρακάτω χώρες:

(D) (A) (CH) (GB) (F) (B) (NL) (E) (DK) (S) (H) (PL) (CZ) (SK) (GR) (FIN) (L) (IRL)

www.hama.de

hama®

Hama GmbH & Co KG
Postfach 80
86651 Monheim/Germany
Tel. +49 (0)9091/502-0
Fax +49 (0)9091/502-274
hama@hama.de
www.hama.de