



ALL0277DSL B

**802.11g Wireless
ADSL VPN Router**

802.11g/802.11b Wireless Access Point

ADSL Modem

NAT Router

VPN Gateway

4-Port Switching Hub

Handbuch

HANDBUCH	1
<i>Internet-Zugangsmerkmale</i>	5
<i>Weiterführende Internetfunktionen</i>	6
<i>VPN Features</i>	6
<i>WLAN-Merkmale</i>	6
<i>LAN-Merkmale</i>	7
<i>Konfiguration & Management</i>	7
<i>Sicherheitsmerkmale</i>	7
PAKETINHALT	8
DAS GEHÄUSE	9
<i>Frontseite und Anzeige-LEDs</i>	9
<i>Rückseitige Ansicht</i>	10
KAPITEL 2	11
INSTALLATION	11
ANFORDERUNGEN	11
VERFAHREN	11
KAPITEL 3	13
EINRICHTUNG	13
ÜBERBLICK	13
KONFIGURATIONSPROGRAMM	14
<i>Vorbereitung</i>	14
SETUP HILFE	15
<i>Typische Verbindungsarten</i>	16
START-BILDSCHIRM	17
LAN-BILDSCHIRM	18
DHCP	19
WLAN BILDSCHIRM	20
WLAN SICHERHEIT	23
<i>WEP - WLAN Security Screen</i>	23
<i>WPA-PSK WLAN Sicherheit</i>	24
VERTRAUENSWÜRDIGE WLAN PORTS	25
KENNWORT-BILDSCHIRM	27
MODUS-BILDSCHIRM	28
KAPITEL 4	29
ÜBERBLICK	29
WINDOWS CLIENTS (PCs)	29
<i>TCP/IP Einrichtung - Überblick</i>	29
<i>Das Überprüfen der TCP/IP Einstellungen - Windows 9 x/ME- :</i>	30
<i>Checking TCP/IP Settings - Windows NT4.0</i>	32
<i>Das Überprüfen der TCP/IP Settings - Windows 2000 - :</i>	35
<i>Das Überprüfen der TCP/IP Settings - Windows XP</i>	37

<u>Internetzugang</u>	39
<u>MACINTOSH CLIENTS</u>	40
<u>LINUX CLIENTS</u>	40
<u>ANDERE UNIX-SYSTEME</u>	40
<u>WIRELESS LAN KONFIGURATION</u>	41
<u>WLAN KONFIGURATION AUF WINDOWS XP</u>	41
<u>Wenn WLAN Sicherheit ausgeschaltet ist</u>	42
<u>Wenn Sie WEP Datenverschlüsselung verwenden</u>	43
<u>Wenn WPA-PSK Datenverschlüsselung verwendet wird</u>	46
<u>Wenn SSID nicht aufgelistet wird</u>	48
<u>KAPITEL 5</u>	51
<u>OPERATION - ROUTERMODUS</u>	51
<u>STATUSBILDSCHIRM</u>	51
<u>VERBINDUNGSSTATUS - PPPoE & PPPoA</u>	54
<u>VERBINDUNGSDetails - DYNAMISCHE IP-ADRESSE</u>	55
<u>VERBINDUNGSDetails - FESTE IP-ADRESSE</u>	56
<u>ÜBERBLICK</u>	57
<u>INTERNET</u>	57
<u>DMZ ("De-Militarisierte Zone")</u>	57
<u>Spezielle Anwendungen</u>	58
<u>URL-Filter</u>	59
<u>DYNAMISCHE DNS (DOMÄNEN-NAMENSSERVER)</u>	61
<u>Dynamischer DNS Bildschirm</u>	61
<u>FIREWALLREGELN</u>	63
<u>Firewall-Regel-Bildschirm</u>	63
<u>Eingehende Regeln (einlaufende Dienste / Inbound Services)</u>	65
<u>Ausgehende Regeln (Outbound Services, ausgehende Dienste)</u>	66
<u>BENUTZERDEFINIERTER DIENSTE</u>	68
<u>Add/Edit Service</u>	69
<u>OPTIONEN</u>	70
<u>SCHEDULE</u>	71
<u>VIRTUELLE SERVER</u>	72
<u>Von Internetbenutzern gesehene IP-Adresse</u>	72
<u>Virtual Servers screen</u>	72
<u>Das Anschließen an virtuelle Server</u>	73
<u>VPN KONFIGURATION</u>	74
<u>VPN "Policies" / Regeln</u>	74
<u>VPN Policies Screen</u>	75
<u>VPN Auto Policy Bildschirm</u>	76
<u>VPN – Manual Policy Screen</u>	80
<u>VPN Status Bildschirm</u>	82
<u>ÜBERBLICK</u>	83
<u>PC-DATENBANK</u>	84
<u>PC-Datenbankbildschirm</u>	84
<u>Erweiterte PC-Datenbank</u>	86
<u>CONFIG DATEI</u>	88
<u>LOGS / LOGBÜCHER / PROTOKOLLE</u>	89
<u>E-MAIL</u>	91
<u>NETZWERKDIAGNOSE / FEHLERSUCHE</u>	93
<u>REMOTE / FERN-ADMINISTRATION</u>	94
<u>SICH VON EINEM ENTFERNTEN PC DURCH DAS INTERNET EINWÄHLEN</u>	95
<u>ROUTING</u>	96
<u>Überblick</u>	96
<u>Routingbildschirm</u>	96
<u>Benutzen dieses Bildschirms</u>	96
<u>Das Konfigurieren von anderen Routern in Ihrem LAN</u>	97

FIRMWARE UPDATE	100
ÜBERBLICK	101
LEITUNGSVERBINDUNGEN	101
HOME SCREEN	102
MODUSBILDSCHIRM	103
OPERATION / BETRIEB	103
STATUSBILDSCHIRM	104
ÜBERBLICK	106
ALLGEMEINE PROBLEME	106
INTERNETZUGANG	106
WLAN ZUGANG	107
MODI	108
BSS/ESS	108
KANÄLE	109
WEP	109
WPA-PSK	109
WLAN LAN-KONFIGURATION	110
ÜBERBLICK	111
IPSec	111
IKE	111
Policies	111
VPN Konfiguration	112
TYPISCHE VPN SITUATIONEN UND KONSTELLATIONEN	113
VPN Pass-through	113
Client PC mit VPN Gateway	113
Verbindung zweier LANs mit VPN Tunnel	114
VPN BEISPIEL	114
ANHANG D SPEZIFIKATIONEN	118
MULTI-FUNCTION WIRELESS ADSL ROUTER	118
WIRELESS INTERFACE	118
REGULATORY APPROVALS	119
FCC Statement	119
CE Approval	119

Copyright 2004, 2005. Alle Rechte vorbehalten.

Dokumentversion: 1.322.4

Alle Warenzeichen und Handelsnamen sind die Eigenschaften ihrer jeweiligen Eigentümer.

Kapitel I

Einführung

Dieses Kapitel liefert einen Überblick über die Merkmale und Fähigkeiten des WLAN ADSL Routers.

Herzliche Glückwünsche zum Kauf Ihres neuen WLAN ADSL Routers. Der WLAN ADSL Router ist ein multifunktionales Gerät, das die folgenden Dienste erbringt:

- ADSL Modem.
- Gemeinsamer Breitbandinternetzugang für alle LAN-Benutzer.
- WLAN Zugang für 802,11 b und 802,11 g mit WLAN Stationen.
- VPN Gateway zum Betrieb von sicheren VPN-Verbindungen über das Internet
- Switch mit 4 Anschlüssen für 10 BaseT oder 100 BaseT Verbindungen.

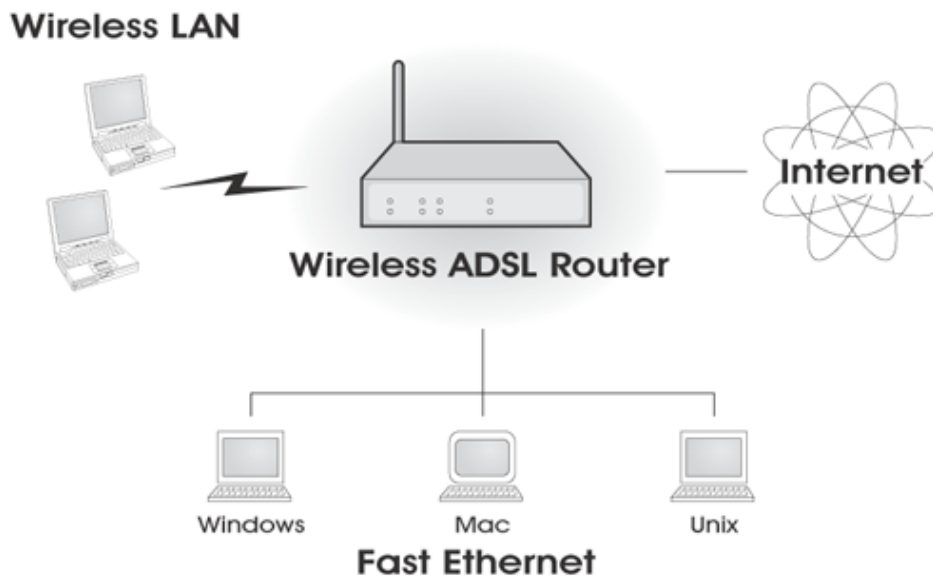


Abbildung 1: WLAN ADSL Router

Merkmale des WLAN ADSL Routers

Der WLAN ADSL Router integriert viele Merkmale, hoch entwickelte Funktionen, und ist dennoch leicht zu verwenden.

Internet-Zugangsmerkmale

- Gemeinsamer Internetzugang. Alle Benutzer auf dem LAN oder WLAN können auf das Internet durch den WLAN ADSL Router mit Hilfe nur einer einzelnen externen IP-Adresse zugreifen. Die lokalen IP-Adressen sind vor externen Quellen versteckt. Dieser Prozess wird NAT genannt.
- Eingebautes ADSL Modem. Der WLAN ADSL Router hat ein eingebautes ADSL Modem, das alle gemeinsamen ADSL Verbindungen unterstützt.
- IPoA, PPPoE, PPPoA Verbindungsunterstützung. Der WLAN ADSL Router unterstützt alle üblichen Verbindungsmethoden.
- Automatische Erkennung der Internetverbindungsmethode. In den meisten Situationen kann der WLAN ADSL Router Ihre ADSL- und Internetverbindung testen, um die von Ihrem ISP verwendete Verbindungsmethode zu bestimmen.

- Feste oder dynamische IP-Adresse. Auf der Internet (WAN Port) Verbindung unterstützt der WLAN ADSL Router sowohl eine dynamische IP-Adresse (IP-Adresse ist für die Verbindung vergeben) als auch eine feste IP-Adresse.

Weiterführende Internetfunktionen

- **Anwendungs-Gateways.** Anwendungen, die unübliche Verbindungen oder ungewöhnliche Port-Nummern verwenden, werden normalerweise von der Firewall blockiert. Es besteht die Möglichkeit, solche Anwendungen zu definieren, um die Ausführung zu ermöglichen.
- **Spezielle Anwendungen.** Dieses Merkmal, auch genannt Porttriggering, erlaubt Ihnen, Internetanwendungen zu verwenden, die normalerweise nicht funktionieren, wenn sie hinter einer Firewall verwendet werden.
- **Virtuelle Server.** Dieses Merkmal erlaubt Internetbenutzern, auf Internetserver in Ihrem LAN zuzugreifen. Die erforderliche Einrichtung ist schnell und einfach.
- **Unterstützung von Dynamischem DNS.** DDNS erlaubt es Benutzern, sich an Server in Ihrer Domain anzuschließen, auch wenn Sie keine statische IP-Adresse haben.
- **URL-Filter.** Benutzen Sie den URL-Filter, um Zugang zu unerwünschten Websites durch LAN-Benutzer zu blockieren.
- **Firewall.** Um Ihr LAN zu schützen, können Sie Firewallregeln definieren, um zu bestimmen, welcher eingehende und ausgehende Verkehr erlaubt sein sollte.
- **Zeitplanung.** Es kann festgesetzt werden, dass der URL-Filter und die Firewallregeln erst zu bestimmten Zeiten aktiv sind.
- **Protokolle.** Definieren Sie, welche Daten in den Protokollen aufgezeichnet werden sollen und senden Sie wahlweise Protokolldaten an einen Syslog Server. Protokolldaten können Ihnen auch per Email geschickt werden.
- **VPN Support.** PCs mit VPN-Software (Virtuelles Privates Netzwerk) werden transparent unterstützt, wenn Sie PPTP, L2TP oder IPSec verwenden. Es wird keine Konfiguration benötigt.

VPN Features

- **IPSec Support.** IPSec ist das am häufigsten verwendete Protokoll.
- **Einfache Konfiguration.** Die notwendige Konfigurationseinstellung, die benötigt wird, zwischen zwei WLAN ADSL Routern eine VPN Verbindung aufzubauen, ist schnell und einfach zu bewerkstelligen.

WLAN-Merkmale

- **Übereinstimmung mit Standards.** Der WLAN ADSL Router entspricht den IEEE802.11g (DSSS) Spezifikationen für WLAN LANs.
- **Unterstützt 802,11 b und 802,11 g.** Der 802,11 g Standard ist mit dem 802,11 B Standard kompatibel. 802,11 b und 802,11 g Ports können simultan verwendet werden.
- **Geschwindigkeiten zu 54 Mbps.** Alle Geschwindigkeiten bis zum 802,11 g Maximum von 54 Mbps werden unterstützt.
- **WEP Unterstützung.** Unterstützung für WEP ist vorhanden. Schlüsselgrößen von 64 und 128 bit werden unterstützt. WEP verschlüsselt vor der Übertragung die Daten, um sie vor „Schnüfflern“ zu schützen.
- **WPA-PSK Unterstützung.** Wie WEP verschlüsselt WPA-PSK vor der Übertragung die Daten.. Das WPA-PSK ist ein erweiterter Standard als WEP und liefert sowohl leichtere Konfiguration als auch größere Sicherheit als WEP.
- **WLAN Mac-Adress-Zugangskontrolle.** Das WLAN Zugangskontrollmerkmal kann die Pakete (Hardware-Adresse) von WLAN Ports überprüfen und sicherstellen, dass nur vertrauenswürdige WLAN Teilnehmer auf Ihr LAN zugreifen können.
- **Einfache Konfiguration.** Wenn die Standardeinstellungen ungeeignet sind, können sie schnell und leicht den Gegebenheiten angepasst werden.

LAN-Merkmale

- **4-Port-Switch.** Der WLAN ADSL Router integriert einen 10/100 BaseT Switch mit 4 Anschlüssen, der es leicht macht, Ihr LAN aufzubauen oder zu erweitern.
- **DHCP Serverunterstützung.** Das DHCP- Protokoll liefert PCs und anderen Geräten eine dynamische IP-Adresse auf Anfrage. Der WLAN ADSL Router kann als ein DHCP Server für Geräte in Ihrem lokalen LAN und WLAN arbeiten.

Konfiguration & Management

- **Einfache Einrichtung.** Verwenden Sie Ihren Web-Browser von irgendwo auf dem LAN oder WLAN für die Konfiguration.
- **Konfigurationsdateien Hochladen / Herunterladen.** Retten Sie (Herunterladen) die Konfigurationsdaten vom WLAN ADSL Router auf Ihrem PC und die Wiederherstellung (Hochladen) einer zuvor gesicherten Konfigurationsdatei zum WLAN ADSL Router.
- **Remote Management.** Der WLAN ADSL Router kann von jedem PC auf Ihrem LAN oder WLAN LAN verwaltet werden. Und, wenn die Internetverbindung existiert, kann auch (wahlweise) über das Internet konfiguriert werden.
- **Netzwerkd Diagnose.** Sie können den WLAN ADSL Router verwenden, um eine PING- oder DNS-Suche auszuführen.

Sicherheitsmerkmale

- **Kennwort - geschützte Konfiguration.** Kennwortschutz wird gewährleistet, um unbefugte Benutzer daran zu hindern, die Konfigurationsfakten und Einrichten zu modifizieren.
- **WLAN-Sicherheit.** WPA-PSK, WEP und WLAN Zugangskontrolle von Pakete werden unterstützt. Das MAC-Adress-Zugangskontrollmerkmal kann verwendet werden, um unbekannte WLAN Ports daran zu hindern, auf Ihr LAN zuzugreifen.
- **NAT Schutz.** Eine wichtige Nebenwirkung der NAT (Netzadressübersetzung) Technik ist es, dass sie allen LAN-Benutzern erlaubt, eine einzelne IP-Adresse für den Standort zu verwenden, und damit sogar die Existenz jedes einzelnen PCs für das WAN zu verstecken. Unter dem externen Gesichtspunkt gibt es kein Netz, nur ein einzelnes Gerät - den WLAN ADSL Route.
- **Firewall.** Alle eingehenden Daten werden überwacht. Alle eingehenden Serveranfragen werden gefiltert. So wird Ihr Netz vor arglistigen Angriffen von Außen geschützt.
- **Schutz vor DoS Angriffen.** DoS (Denial of Service) Angriffe können Ihre Internetverbindung mit ungültigen Datenpaketen und Verbindungsanfragen überfluten, so viel Bandbreite und so viele Ressourcen verwenden, dass der Internetzugang für Sie nicht mehr verfügbar ist. Der WLAN ADSL Router integriert einen wirksamen Schutz vor DoS Angriffen.

Paketinhalt

Die folgenden Artikel sollten im Lieferumfang enthalten sein. Wenn etwas beschädigt ist oder fehlt, bitte wenden Sie sofort sich an Ihren Fachhändler.

- Die WLAN ADSL Routereinheit
- 1 CAT-5 Ethernet (LAN) Kabel
- 1 RJ -11 (ADSL) Kabel
- 1 RJ -11 auf RJ45 Kabel
- 230 V Steckeradapter
- Quick Installation Guide
- CD-ROM mit dem Handbuch.

Das Gehäuse

Frontseite und Anzeige-LEDs

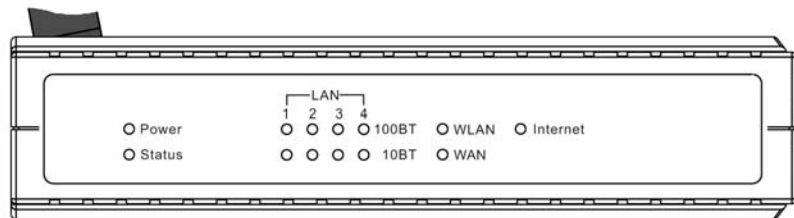


Abbildung 2: Frontseite

Power LED (grün)	Ein - Eingeschaltet. Aus – Kein Strom.
Status LED (gelb)	Aus - Normalbetrieb. Blinkt - Diese LED blinkt während des Starts und während eines Firmware Upgrades.
LAN	Jeder Port hat 2 LEDs, zum Anzeigen der Übertragungsgeschwindigkeit (10BaseT oder 100BaseT) 100BT – LED ist EIN wenn die LAN Verbindung 100BaseT verwendet. Sie blinkt, wenn über diesen Port Daten übertragen werden. 10BT - LED ist EIN wenn die LAN Verbindung 10BaseT verwendet. Sie blinkt, wenn über diesen Port Daten übertragen werden. Falls beide LEDs aus sind, wird dieser Port nicht verwendet
WLAN LED	Ein – WLAN wird verwendet. Aus – Keine Wireless WLAN Verbindung vorhanden.. Blinken - Daten werden über den WLAN Access Point gesendet oder empfangen.
WAN	Ein - ADSL Verbindung besteht. (Dies bedeutet nicht unbedingt, dass Internetzugang vorhanden ist.) Aus – Es besteht keine ADSL Verbindung. Blinken – Über die ADSL Leitung werden Daten übertragen.
Internet	Ein - Eine Internetverbindung besteht. Aus – Es besteht keine Internetverbindung.. Blinken – Über die ADSL Leitung werden Daten übertragen

Rückseitige Ansicht

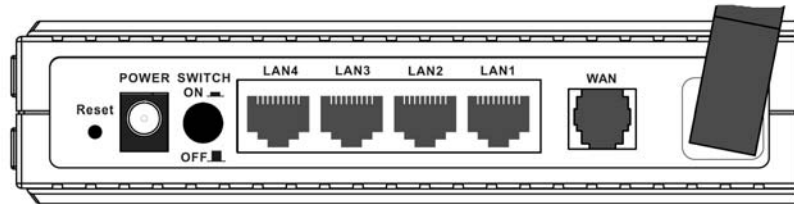


Abbildung 3: Rückansicht

Rückstellknopf (Reset to Defaults)	Mit diesem Knopf wird der ADSL Router auf den Auslieferungszustand zurückgesetzt. Dazu den Knopf drücken und ca. 5 Sekunden gedrückt halten. Wenn die STATUS-LED leuchtet, den Knopf loslassen. Der Router setzt sich automatisch zurück.
Netzteil Anschluss	Hier das mitgelieferte Netzteil anschließen
Ein/Aus Schalter	ON zum Einschalten, OFF zum Ausschalten drücken
10/100BaseT LAN Anschlussbuchsen	Standard LAN Kabel (RJ45) verwenden um PCs an diese Ports anzuschließen. Anmerkung: Ein jeder LAN Port des Wireless ADSL Routers kann automatisch als "Uplink" Port verwendet werden, wenn notwendig.
WAN Port (ADSL Port)	Hier wird das ADSL-Kabel angeschlossen.

Kapitel 2

Installation

Dieses Kapitel beschreibt die hardwareseitige Installation des WLAN ADSL Routers.

Anforderungen

- Verwenden Sie Standard 10/100 BaseT Netzwerkkabel mit RJ45 Anschlüssen.
- Das TCP/IP Protokoll muss auf allen PCs installiert sein.
- Für Internetzugang muß ein Internetzugangskonto bei einem ISP und eine DSL Verbindung bestehen.
- Um den WLAN Router zu verwenden, müssen alle WLAN Geräte kompatibel mit den Spezifikationen IEEE 802,11 g oder IEEE 802,11 b sein.

Verfahren

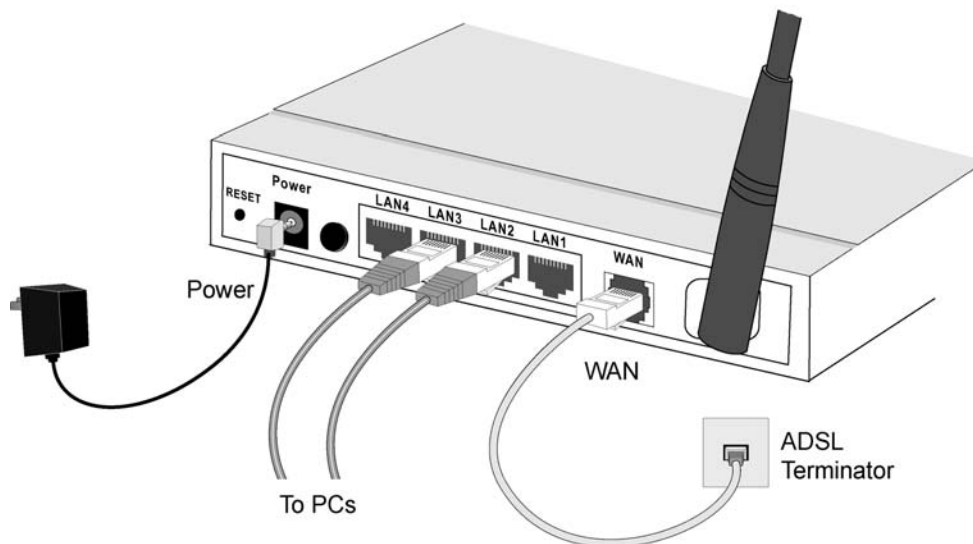


Abbildung 4: Installationsdiagramm

1. Wählen Sie einen Aufstellungsort

Wählen Sie eine geeignete Stelle im Netzwerk, um den WLAN ADSL Router zu installieren.

Für besten WLAN-Empfang und Leistung sollte der WLAN ADSL Router an einem zentralen Standort mit geringen Hindernissen zwischen dem WLAN ADSL Router und den PCs platziert werden. Auch sollten benachbarte Accesspoints beim Verwenden von mehreren Accesspoints verschiedene Kanäle verwenden.

2. Schließen Sie LAN-Kabel an

Verwenden Sie Standard-LAN-Kabel, um PCs mit dem Switch im WLAN ADSL Router zu verbinden. Beide 10 BaseT und 100 BaseT Verbindungen können simultan verwendet werden.

Falls erforderlich, schließen Sie einen beliebigen Port an einen normalen Port an einem anderen Switch mit Hilfe eines Standard-LAN-Kabels an. Jeder LAN-Port des WLAN ADSL Router dient automatisch als ein "Uplink" Port, wenn es erforderlich ist.

3. Schließen Sie das ADSL Kabel an

Verbinden Sie mit dem mitgelieferten ADSL Kabel den WAN Port auf dem WLAN ADSL Router (dem RJ11 Anschluss) mit dem von Ihrer Telefongesellschaft gelieferten ADSL Abschluss.

4. Fahren Sie den ADSL Router hoch

Verbinden Sie das mitgelieferte Netzteil mit dem WLAN ADSL Router. Benutzen Sie nur den gelieferten Adapter. Starten Sie durch Drücken des Ein-Schalters

5. Überprüfen Sie die LEDs

- Die Power-LED sollte an sein.
- Die Status-LED sollte blinken, dann ausschalten. Wenn sie nach 60 Sekunden weiter an bleibt oder blinkt, ist ein Hardwarefehler zu vermuten.
- Für jede LAN (PC) Verbindung sollte eine der LAN-LEDs an sein (dazu muß der PC auch eingeschaltet sein)
- Die WLAN LED sollte an sein.
- Die WAN LED sollte an sein, wenn auf ADSL Ebene verbunden.
- Es kann sein, dass die Internet-LED aus ist. Nach richtiger Konfiguration sollte sie angehen.

Zwecks weiterer Informationen beziehen Sie sich auf die LEDs in Kapitel 1.

Kapitel 3

Einrichtung

Dieses Kapitel enthält Einrichtungsdetails vom WLAN ADSL Router.

Überblick

Dieses Kapitel beschreibt das Einrichtungsverfahren für:

- Internetzugang
- LAN-Konfiguration
- WLAN Einrichtung
- Vergabe eines Kennworts, um die Konfigurationsdaten zu schützen.

Ggf. müssen PCs in Ihrem lokalen LAN auch konfiguriert werden.
Für Details siehe Kapitel 4 - PC-Konfiguration.

Weitere Konfiguration des WLAN ADSL Routers kann je nachden Merkmalen und Funktionen, die Sie verwenden möchten, erforderlich sein. Verwenden Sie die Tabelle unten, für detaillierte Anweisungen zu den erforderlichen Funktionen.

Aktion	Informationen
Konfigurieren Sie PCs auf Ihrem LAN	Kapitel 4: PC-Konfiguration
Überprüfen Sie WLAN ADSL Routeroperation und Status.	Kapitel 5: Operation and Status
Verwenden Sie einige der folgenden erweiterten Merkmale: <ul style="list-style-type: none">• Internet (DMZ, spezielle Anwendungen, URL-Filter)• Dynamische DNS• Firewall Regeln und• Firewalldienste• Scheduling• URL-Filter• Virtuelle Server• VPN	Kapitel 6: Erweiterte Merkmale
Verwenden Sie einige der folgenden Verwaltungskonfigurationseinrichten oder Merkmale: <ul style="list-style-type: none">• PC-Datenbank• Config Dateiabladen/Hochladen• Logging• Protokolle und Alarme per Email schicken• Netzdiagnose (PING, DNS Suche)• PC-Datenbank• Remote Management/ Admin• Routing (RIP und statisches Routing)• Firmware-Update	Kapitel 7 Weiterführende Administration

Konfigurationsprogramm

Der WLAN ADSL Router enthält einen HTTP-Server. Dies ermöglicht Ihnen, ihn mit Hilfe Ihres Web-Browsers daran anzuschließen und zu konfigurieren. Ihr Browser muss JavaScript unterstützen. Das Konfigurationsprogramm ist auf den folgenden Browsern getestet worden:

- Netscape V4.08 oder später
- Netscape 7
- Internet Explorer V5.01 oder später

Vorbereitung

Bevor Sie Versuchen, den WLAN ADSL Router zu konfigurieren, stellen Sie bitte folgendes sicher:

- Ihr PC kann eine physische Verbindung zum WLAN ADSL Router herstellen. Der PC und der WLAN ADSL Router müssen direkt verbunden (über die Ports auf dem WLAN ADSL Router) oder in demselben LAN-Segment sein.
- Der WLAN ADSL Router muss installiert und eingeschaltet werden.
- Wenn die voreingestellte IP-Adresse des WLAN ADSL Routers (192.168.0.1) schon von einem anderen Gerät verwendet wird, muss das andere Gerät ausgeschaltet werden, bis an dem WLAN ADSL Router eine neue IP-Adresse (während Konfiguration) vergeben wird.

Das Verwenden Ihres Web-Browsers

1. Eine Verbindung von Ihrem PC zum WLAN ADSL Router herstellen:
2. Nach dem Installieren des WLAN ADSL Routers in Ihrem LAN starten Sie Ihren PC. Wenn Ihr PC schon läuft, starten Sie ihn neu.
3. Starten Sie Ihren Web-Browser.
4. Im Adresskasten schreiben Sie "HTTP: //" und die IP-Adresse des WLAN ADSL Routers. In diesem Beispiel die Default IP-Adresse des WLAN ADSL Routers: HTTP: // 192.168.0.1
5. Wenn Sie zum Eingeben von Benutzernamen und Kennwort aufgefordert werden, geben Sie die Werte wie folgt ein:
 - User name: admin
 - Password: password

Wenn die Verbindung nicht klappt

Wenn der WLAN ADSL Router nicht antwortet, überprüfen Sie Folgendes:

- Ist der WLAN ADSL Router richtig installiert, LAN-Verbindung ist in Ordnung, und sie ist eingeschaltet? Sie können die Verbindung durch Verwenden des "PING" Befehls testen:
- Öffnen Sie das MS-DOS Fenster.
- Geben Sie den Befehl ein:
- PING 192.168.0.1
- Wenn keine Antwort empfangen wird, funktioniert die Verbindung nicht, oder die IP-Adresse Ihres PCs ist nicht mit der IP-Adresse des WLAN ADSL Routers kompatibel.
- Wenn Ihr PC eine feste IP-Adresse verwendet, muss seine IP-Adresse innerhalb des Bereichs 192.168.0.2 bis 192.168.0.254 sein, um mit der voreingestellten IP-Adresse des WLAN ADSL Routers von 192.168.0.1 kompatibel zu sein. Auch muss die Netzmaske auf 255.255.255.0 gesetzt werden. Siehe Kapitel 4 - PC-Konfiguration, für Details.
- Stellen Sie sicher, dass Ihr PC und der WLAN ADSL Router auf demselben Netzsegment sind. (Wenn Sie keinen Router haben, muss dies der Fall sein.)
- Stellen Sie sicher, dass Sie die Kabel-LAN-Schnittstelle verwenden. Die WLAN Schnittstelle kann nur verwendet werden, wenn ihre Konfiguration zur WLAN Einstellung Ihres PCs passt.

Setup Hilfe

Das erste Mal, wenn Sie sich an den WLAN ADSL Router anschließen, läuft der Setup Wizard automatisch. (Der Wizard läuft auch, wenn die Standardeinstellungen des WLAN ADSL Routers wiederhergestellt werden.)

1. Gehe Sie schritt für Schritt vor, bis zum Ende.
2. Sie brauchen die Daten, die Ihnen vom Ihrem ISP geliefert worden sind. Die meisten Verbindungsmethoden erfordern eine Dateneingabe.
3. Die gebräuchlichsten Verbindungsarten werden in den folgenden Tabellen erklärt.
4. Auf dem letzten Bildschirm des Wizards führen Sie den Test durch und überprüfen, ob eine Internetverbindung hergestellt werden kann.
5. Wenn der Verbindungstest fehlschlägt:
6. Überprüfen Sie alle Verbindungen und die Front-LEDs.
7. Überprüfen Sie, ob Sie alle Daten richtig eingegeben haben.

Typische Verbindungsarten

Typ	Details	Benötigte ISP Daten
Dynamic IP Address	Ihre IP-Adresse wird automatisch vergeben, wenn Sie an Sie ISP anschließen	a) es kann sein, dass ADSL Parameter (VPI und VCI) erforderlich sind, wenn sie nicht automatisch ermittelt werden können. b) Einige ISP verlangen, dass Sie einen besonderen Hostname- oder Domännennamen oder eine besondere Pakete verwenden.
Statische (Fixed) IP Address	Ihr ISP vergibt eine permanente IP-Adresse. Normalerweise ist die Verbindung an.	a) es kann sein, dass ADSL Parameter (VPI und VCI) erforderlich sind, wenn sie nicht automatisch erkannt werden können. b) IP-Adresse, die Ihnen zugeordnet wurde, Netzmaske, Gateway-IP-Adresse und DNS Adresse.
PPPoE, PPPoA	Sie verbinden sich nur mit dem ISP, wenn erforderlich. Die IP-Adresse wird normalerweise automatisch vergeben.	a)Es kann sein, dass ADSL Parameter (VPI und VCI) erforderlich sind, wenn sie nicht automatisch erkannt werden können. b) Benutzername und Kennwort sind immer erforderlich. c) beim Verwenden einer (festen) statischen IP-Adresse, brauchen Sie die IP-Adresse und verwandte Information (Netzwerk-Maske, Gateway-IP-Adresse und DNS Adresse)
IPoA (IP over ATM)	Normalerweise ist die Verbindung an	a) es kann sein, dass ADSL Parameter (VPI und VCI) erforderlich sind, wenn sie nicht automatisch ermittelt werden können. b) IP-Adresse, die Ihnen zugewiesen wurde, Information wie Netzmaske, Gateway-IP-Adresse und DNS Adresse.

Start-Bildschirm

Nach dem Beenden des Einrichtungszauberers sehen Sie den Start-Bildschirm. Wenn Sie sich in Zukunft verbinden, sehen Sie diesen Bildschirm. Ein Beispielbildschirm wird unten gezeigt.

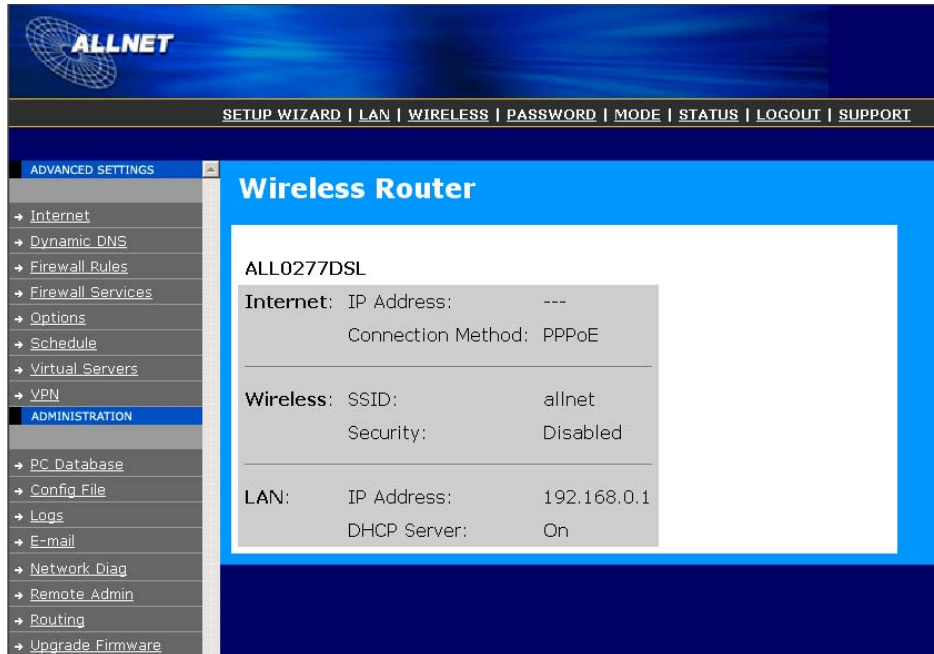


Abbildung 5: Start-Bildschirm

Hauptmenü

Das Hauptmenü enthält auf der linken Seite Links zu den am häufigsten gebrauchten Bildschirmen. Um die anderen verfügbaren Bildschirme zu sehen. Klicken Sie auf "Advanced" oder "Administration".

Navigation & Dateneingabe

- Verwenden Sie das Menü auf der linken Seite des Bildschirms und den "Back" Knopf auf Ihrem Browser für die Navigation.
- Um zu einem anderen Bildschirm zu wechseln, ohne "save" zu klicken, sichert keine der Änderungen, die Sie vorgenommen haben. Sie müssen "Save" anklicken, oder Ihre Änderungen werden ignoriert.



Note!

Auf jedem Bildschirm können Sie den "Hilfe" Knopf anklicken, um Hilfe für genau diesen Bildschirm zu erhalten

LAN-Bildschirm

Verwenden Sie die LAN-Verbindung im Hauptmenü, um den LAN-Bildschirm zu erreichen. Ein Beispielbildschirm wird unten gezeigt.

Abbildung 6: LAN-Bildschirm

TCP/IP	
IP Address	IP-Adresse für den WLAN ADSL Router wie vom LAN aus gesehen. Verwenden Sie den Standardwert, es sei denn, die Adresse ist schon in Verwendung oder Ihr LAN verwendet einen anderen IP-Adressbereich. Im letzteren Fall verwenden Sie eine ungenutzte IP-Adresse von innerhalb des von Ihrem LAN verwendeten Bereichs.
Subnet Mask	Der Standardwert 255.255.255.0 ist für kleine (Klasse "C") Netze normal. Für andere Netze verwenden Sie die Unternetzmaske für das LAN-Segment, woran der WLAN ADSL Router angeschlossen ist, (denselben Wert wie die PCs auf diesem LAN-Segment).
DHCP Server	<ul style="list-style-type: none"> • Wenn aktiviert, vergibt der WLAN ADSL Router IP-Adressen an PCs (DHCP Clientn) in Ihrem LAN. Der voreingestellte (und empfohlene) Wert ist ENABLED. • Wenn Sie schon einen DHCP Server benutzen, muss das Setting DISABLED sein, und der vorhandene DHCP Server muss so konfiguriert werden, das der WLAN ADSL Router als das Default Gateway verwendet wird. Siehe den folgenden Abschnitt für weitere Details. • Die Anfangs-IP-Adressen- und End-IP-Adressen-Felder beinhalten die vom DHCP Server verwendeten Werte, wenn sie IP-Adressen an DHCP Clients vergeben. Dieser Bereich bestimmt auch die Anzahl von unterstützten DHCP Clients. • Siehe den folgenden Abschnitt für weitere Details darüber, wie Sie DHCP verwenden.

DHCP

Was macht DHCP

Ein DHCP (Dynamic Host Configuration Protocol) Server vergibt eine gültige IP-Adresse an einen DHCP Client (PC oder Gerät) auf Anfrage.

- Die Client-Anfrage wird erzeugt, wenn der Client startet (bootet).
- Der DHCP Server liefert dem Client sowohl die IP-Adresse als auch die Gateway- und DNS-Adressen.
- Der WLAN ADSL Router kann als DHCP Server wirken.
- Windows 95/98/ME, und andere Nicht-Serverversionen von Windows wirken als ein DHCP Client. Dies ist das default Setup bei Windows für das IP Netzwerkprotokoll. Jedoch, Windows verwendet den Ausdruck *Obtain an IP Address automatically* statt "DHCP Client".
- Sie dürfen keine zwei (2) oder mehr DHCP Server auf demselben LAN-Segment haben. (Wenn Ihr LAN keine anderen Router hat, bedeutet dies, dass es nur einen (1) DHCP Server auf Ihrem LAN gibt.)

Verwenden des DHCP Server des WLAN ADSL Routers

Dies ist die Standardeinstellung. Die DHCP Servereinstellungen sind auf dem LAN-Bildschirm. Auf diesem Bildschirm können Sie:

- Den WLAN DHCP Server des ADSL Routers Funktion ein- bzw. ausschalten.
- Einstellen des IP-Adressen-Bereichs des DHCP Servers.



Note! Sie können einigen Geräten feste IP-Adressen zuteilen, während Sie DHCP verwenden, vorausgesetzt, dass die festen IP-Adressen nicht innerhalb des vom DHCP Server verwendeten Bereichs sind.

Das Benutzen eines anderen DHCP Servers

Sie können nur einen (1) DHCP Server pro LAN-Segment benutzen. Wenn Sie einen anderen DHCP Server anstatt dem WLAN ADSL Router benutzen möchten, ist das folgende Verfahren erforderlich.

- Schalten Sie das DHCP Serverfeature im WLAN ADSL Router aus. Einstellungen sind auf dem LAN-Bildschirm.
- Konfigurieren Sie den DHCP Server, um die IP-Adresse des WLAN ADSL Routers als das default Gateway zu liefern.
-

Konfigurieren Sie Ihre PCs, um DHCP zu verwenden

Dies ist die Standardeinstellung für IP für alle Nicht-Serverversionen von Windows. Siehe Kapitel 4 – Client-Konfiguration,.

WLAN Bildschirm

Die Einstellungen des WLAN ADSL Routers müssen zu den anderen WLAN Ports passen.

Beachten Sie, dass der WLAN ADSL Router automatisch beide 802,11 b und 802,11 g Verbindungen akzeptiert, und für dieses Merkmal keine Konfiguration benötigt wird.

Um die Standardeinstellungen des WLAN ADSL Routers für das WLAN Accesspoint-Merkmal zu ändern, verwenden Sie den Link Wireless auf dem Hauptmenü. Ein Beispielsbildschirm wird unten gezeigt.

Abbildung 7: WLAN Bildschirm

Daten - WLAN Bildschirm

Identifikation	
Region	Wählen Sie die richtige Domäne für Ihren Standort. Es ist Ihre Aufgabe sicherzustellen: <ul style="list-style-type: none"> • Dass der WLAN ADSL Router nur bei Domänen für welche er lizenziert ist, verwendet wird. • Dass Sie die richtige Domäne wählen, so dass nur die legalen Kanäle für diese Domäne gewählt werden können.
Station name	Dies ist das Gleiche wie der "Gerätename" für den WLAN ADSL Router
SSID	Dies wird auch der "Netzname" genannt. <ul style="list-style-type: none"> • Beim Verwenden eines ESS (mehrfache Accesspointe) wird diese Kennung ESSID (erweiterte Dienstsatzkennzeichnung) genannt. • WLAN Ports müssen dieselben SSID/ESSID verwenden.

Optionen	
Mode	<p>Wählen Sie die gewünschte Option.</p> <ul style="list-style-type: none"> 802,11 G Plus (TI) Dies ist die Standardeinstellung und erlaubt Clients, einige der folgenden Modi zu verwenden: <ul style="list-style-type: none"> Standard802,11 b 802,11 B+ (Texas Instruments verbesserter Modus) Standard802,11 g 802,11 G Plus (Texas Instruments verbesserter Modus). Dieser Modus kann Durchsatz um bis zu 50% steigern, aber arbeitet nur zwischen kompatiblen TI WLAN Ports. 802,11 g & 802,11 b Beide 802,11 g und 802,11 B Ports sind in der Lage, sich zu verbinden. 802,11 g Wenn gewählt, stellt dies sicher, dass 802,11 g Modus, WLAN Ports mit hoher Geschwindigkeit verbunden werden, aber 802,11 B Modus ausgeschlossen sind. 802,11 b Wenn gewählt, ist der 802,11 g Modus nicht verfügbar. 802,11 g WLAN Ports können sich nur verbinden, wenn sie auch im Standard802,11 b Modus laufen können.
Channel No.	<ul style="list-style-type: none"> Wählen Sie den Kanal, den Sie in Ihrem WLAN LAN verwenden möchten. Wenn Sie Übertragungsstörungen feststellen, kann es sein, dass Sie mit verschiedenen Kanälen experimentieren müssen, um zu sehen, welcher der Beste ist..
Broadcast SSID	<p>Wenn aktiviert, sendet das SSID seinen Namen an alle WLAN Ports. Ports, die kein SSID haben, (oder einen "null" Wert) können dann das richtige SSID zu diesem Accesspoint übernehmen</p>
WLAN Sicherheit	
Current Setting	<p>Die gegenwärtige WLAN Sicherheitsstufe wird angezeigt. Der Standardwert ist „Disabled“</p>
Configure Button	<p>Klicken Sie diesen Knopf, um auf den WLAN Sicherheitsunterbildschirm zuzugreifen und die so erforderlichen Sicherheitseinrichtung zu modifizieren</p>
Access Point	
Enable Wireless Access Point	<p>Enable bedeutet, dass Sie den WLAN Accesspoint verwenden wollen. Disable bedeutet, dass Sie kein WLAN verwenden und alle Verbindungen über das Kabel-LAN hergestellt werden.</p>

Allow access by ...	Hiermit legen Sie fest, welche WLAN Station den Access Point nutzen darf. <ul style="list-style-type: none">• Die Optionen sind: All Wireless Stations – Alle WLAN Stationen können den Accesspoint verwenden, vorausgesetzt, sie verwenden die richtigen Sicherheitseinstellungen und SSID.• Trusted Wireless stations only – Nur als vertrauenswürdig eingestufte Stationen haben Zugang, auch wenn sie die richtigen Sicherheitseinstellungen und SSID verwenden. Dieses Feature verwendet die MAC Adresse, um die WLAN Stationen zu identifizieren. Die MAC Adresse ist eine Netzwerk Identifikation, die eindeutige Kennnummern verwendet. Um festzulegen, welche WLAN Stationen vertrauenswürdig sind, benutzen Sie den "Set Stations" Knopf.
Set Stations Button	Klicken Sie diesen Knopf, um die PC-Datenbank der vertrauenswürdigen PCs zu verwalten

WLAN Sicherheit

Auf diesen Bildschirm wird durch Klicken des "Configure" Knopfs auf den Wireless Bildschirm zugegriffen. Es gibt 3 Optionen für WLAN Sicherheit:

- **Disable** - keine Datenverschlüsselung.
- **WEP** - Daten werden mit Hilfe des WEP Standards verschlüsselt.
- **WPA-PSK** - Daten werden mit Hilfe des WPA-PSK Standards verschlüsselt. Diese sind ein neuerer Standard als WEP und ist sicherer als WEP. Wenn all Ihre WLAN Stationen WPA-PSK unterstützen, sollten Sie WPA-PSK statt WEP verwenden.

WEP - WLAN Security Screen

Abbildung 8: WEP Bildschirm

Daten - WEP Bildschirm

WEP Daten-Verschlüsselung	
Authentication	Normalerweise kann der Standardwert "Automatic" gelassen werden. Wenn das fehlschlägt, wählen Sie den entsprechenden Wert - "Open System" oder "Shared Key". Überprüfen Sie die Dokumentation Ihrer WLAN Karte welche Methode zu verwenden ist.
Data Key Size	Wählen Sie die WEP Verschlüsselungsebene: <ul style="list-style-type: none"> • 64-Bit (manchmal 40-Bit genannt) Verschlüsselung • 128-Bit Verschlüsselung
Key Value	Enter the key value or values you wish to use. The Default Key is required, the other keys are optional. Other stations must have the same key.
Passphrase	Wenn die Verschlüsselungsstärke auf 64 bit gestellt wird, dann wird jeder der vier Schlüsselfelder mit Schlüsselwerten gefüllt. Wenn die Verschlüsselungsstärke auf 128 bit eingestellt wird, dann wird nur das gewählte WEP Schlüsselfeld mit einem Schlüssel gefüllt.

WPA-PSK WLAN Sicherheit

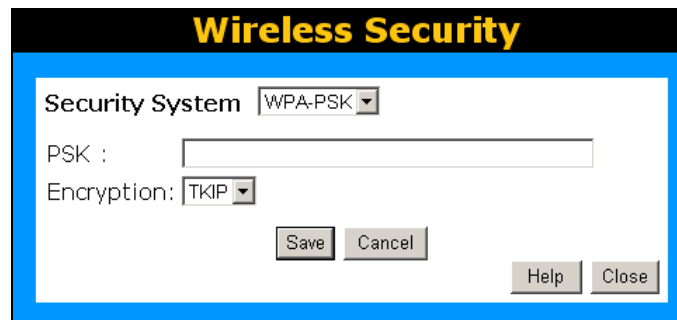


Abbildung 9: WPA-PSK

Daten - WPA-PSK Bildschirm

Security System	WPA-PSK Wie bei WEP werden die Daten vor der Übertragung verschlüsselt. WPA ist sicherer als WEP und sollte wenn möglich verwendet werden. WPA-PSK ist die Version von WPA, das keinen RADIUS-Server in Ihrem LAN erfordert.
PSK	Geben Sie den PSK Network Key ein. Die Daten werden mit Hilfe eines vom Netzschlüssel abgeleiteten Schlüssels verschlüsselt. Andere WLAN Ports müssen denselben Network Key benutzen. Das PSK muss zwischen 8 und 63 Zeichen lang sein.
WPA Encryption	Der WPA-PSK Standard ermöglicht verschiedene Verschlüsselungsmethoden. Wählen Sie die gewünschte Option. WLAN Ports müssen immer dieselbe Verschlüsselungsmethode verwenden.

Vertrauenswürdige WLAN Ports

Dieses Merkmal kann verwendet werden, um unbekannte WLAN Ports daran zu hindern, den Accesspoint zu verwenden. Diese Liste hat so lange keine Wirkung bis die Einstellung [Allow access by trusted stations only](#) eingeschaltet ist.

Um die Liste von vertrauenswürdigen WLAN Ports zu ändern, verwendet Listenknopf *Modify* auf dem Bildschirm [Access Control](#). Sie sehen einen Bildschirm wie die hier unten.

Abbildung 10: Vertrauenswürdige WLAN Ports

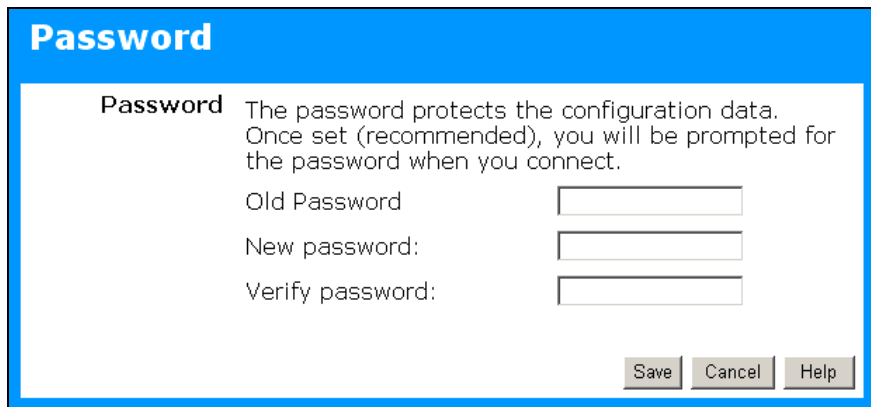
Daten - vertrauenswürdige WLAN Ports

Trusted Wireless Stations	Dies listet WLAN Ports auf, die Sie als "vertrauenswürdig" bestimmt haben
Other Wireless Stations	Diese Liste zeigt die WLAN Ports, die der Accesspoint entdeckt hat, die Sie nicht als "vertrauenswürdig" eingestuft haben. ..Mit "All" wählen Sie alle Stations in der Liste aus, mit "None" entfernen Sie diese.
Name	Der Name des vertrauenswürdigen WLAN Station. Verwenden Sie diesen, wenn Sie eine vertrauenswürdige Station hinzufügen oder ändern wollen.
Address	Die MAC (physicalische) Adresse der vertrauenswürdigen WLAN Station.
Buttons	
<<	Fügen Sie eine vertrauenswürdige WLAN Station der Liste zu (von der Liste "Other Stations"). <ul style="list-style-type: none"> Wählen Sie ein Station in der Liste "Other Stations" aus und klicken Sie auf " << " . Geben Sie die Adresse (MAC oder physikalische Adresse) der WLAN Station ein und klick Sie auf "Add " .

>>	<p>Löschen Sie einen vertrauenswürdigen WLAN Port von der Liste (Bewegung zur Liste "Other Stations").</p> <ul style="list-style-type: none"> • Wählen Sie einen Eintrag (oder Einträge) in der "Trusted Stations" Liste. • Klicken Sie den ">>" Knopf.
Edit	<p>Verwenden Sie dieses, um einen vorhandenen Eintrag in der "Trusted Stations" Liste zu ändern:</p> <ol style="list-style-type: none"> 1. Wählen Sie die WLAN Station in der Liste der vertrauenswürdigen Stationen. 2. Klicken Sie den Editierknopf. Die Adresse wird zum "Adresse" Feld kopiert. Aus dem ADD-Knopf wird der UPDATE Knopf. 3. Editieren Sie die Adresse (MAC Adresse) 4. Klicken Sie auf Update, um Ihre Änderungen zu sichern.
Add (Update)	<p>Um eine vertrauenswürdige Station hinzuzufügen, die nicht in der "Other Wireless Stations" Liste ist, geben Sie die erforderlichen Daten ein und klicken Sie diesen Knopf.</p>
Clear	<p>Löscht Namens- und Adressfelder</p>

Kennwort-Bildschirm

Der Kennwortbildschirm erlaubt Ihnen, dem WLAN ADSL Router ein Kennwort zuzuteilen.



Password

The password protects the configuration data. Once set (recommended), you will be prompted for the password when you connect.

Old Password

New password:

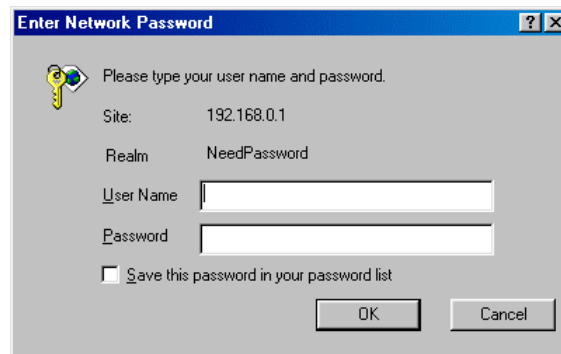
Verify password:

Save Cancel Help

Abbildung 11: Kennwortbildschirm

Old Password	Geben Sie das vorhandene Kennwort in diesem Feld ein.
New Password	Geben Sie das neue Kennwort hier ein.
Verify Password	Geben Sie das neue Kennwort hier noch einmal ein.

Sie werden aufgefordert das Passwort einzugeben, wenn Sie sich anmelden, wie unterhalb gezeigt.



Enter Network Password

Please type your user name and password.

Site: 192.168.0.1

Realm: NeedPassword

User Name

Password

Save this password in your password list

OK Cancel

Abbildung 12: Kennwortdialog

- Der "Benutzername" ist immer admin
- Geben Sie das Kennwort für den WLAN ADSL Router ein, wie auf dem Kennwortbildschirm oben gesetzt.

Modus-Bildschirm

Benutzen Sie diesen Bildschirm, um den Modus zwischen **Routermodus** und **Modem (Brücke) Modus** zu ändern.

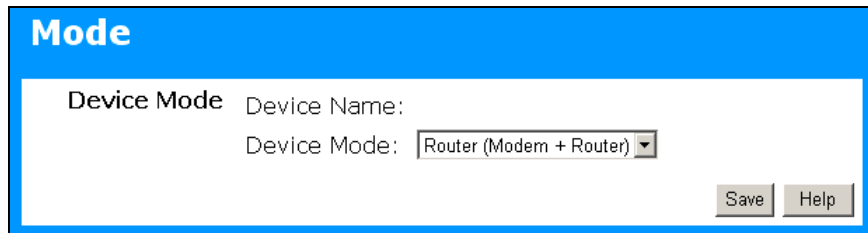


Abbildung 13: Modusbildschirm

Wählen Sie die gewünschte Option und klicken Sie "Save".

Device Name	Feld zeigt den gegenwärtigen Namen dieses Geräts an
Device Mode	<p>Wählen Sie den gewünschten Gerätemodus für den Router:</p> <ul style="list-style-type: none">• Router - sowohl der ADSL Modem als auch die Routermerkmale sind betriebsbereit. In diesem Modus haben alle WLAN / LAN Benutzer einen gemeinsamen Zugang zum Internet.• Modem - nur der ADSL Modembestandteil ist betriebsbereit. Alle Routermerkmale sind ausgeschaltet. Dieses Gerät ist "transparent" - es führt keine Operationen aus und beeinflusst den Netzverkehr nicht.. Sie müssen einen DHCP Server in Ihrem LAN haben, um denn WLAN Clients IP-Adressen mit Hilfe des Accesspoints zu liefern. <p>Nach dem Ändern des Modus startet dieses Gerät neu. Das kann einige Sekunden dauern. Das Menü ändert sich je nach dem Modus, in dem Sie gerade sind.</p>

Hinweise:

- Im Allgemeinen sollten Sie keinen Modemmodus verwenden. Wählen Sie nur diesen Modus, wenn Sie sicher sind, dass dies das ist, was Sie tatsächlich wollen.
- Der WLAN Accesspoint kann entweder im Router- oder Modemmodus arbeiten. Aber es ist im Allgemeinen keine gute Idee, ein Modem mit einem Accesspoint zu verbinden, weil alle Daten von den WLAN Ports über die Modemverbindung geschickt werden. (Da das Modem „transparent“ ist, prüft er den Datenverkehr nicht, um zu ermitteln, ob die Daten für das LAN oder das WAN sind)
- Für Details über den Modemmodus siehe Kapitel 8.

Kapitel 4

PC-Konfiguration

Dieses Kapitel beschreibt die PC-Konfiguration für das LAN.

Überblick

Folgendes muss u.U. für jeden PC konfiguriert werden:

- TCP/IP Netzwerkeinrichtung
- Internetzugangskonfiguration
- WLAN Konfiguration

Windows Clients (PCs)

Dieser Abschnitt beschreibt, wie Windows-Clients für den Internetzugang durch den WLAN ADSL Router zu konfigurieren sind.

Zuerst sollte die TCP/IP des PCs überprüft werden.

Der WLAN ADSL Router verwendet das TCP/IP Netzwerkprotokoll für alle Funktionen, so dass es wesentlich ist das das TCP/IP Protokoll auf jedem PC installiert und richtig konfiguriert ist.

TCP/IP Einrichtung - Überblick

Beim Verwenden der Default WLAN ADSL Routereinstellungen und der default Windows TCP/IP Einstellungen sind keine Änderungen notwendig.

- Standardmäßig wirkt der WLAN ADSL Router als ein DHCP Server und liefert automatisch jedem PC eine geeignete IP-Adresse (und verwandte Information), wenn der PC bootet.
- Für alle Nicht-Serverversionen von Windows soll TCP/IP als DHCP Client eingerichtet werden.
- Beim Verwenden einer festen (angegebenen) IP-Adresse sind die folgenden Änderungen erforderlich:
- Das Gateway muss auf die IP-Adresse des WLAN ADSL Routers gestellt werden
- Die DNS sollte auf die von Ihrem ISP gelieferte Adresse gestellt werden.



Note! Wenn Ihr LAN einen Router hat, muss der LAN-Administrator den Router selbst wieder konfigurieren. Siehe Kapitel 8 - fortschrittliche Einrichtung für Details.

Das Überprüfen der TCP/IP Einstellungen - Windows 9 x/ME- :

Wählen Sie Control Panel - Netzwerk. Sie sollten einen Bildschirm wie das Folgende sehen:

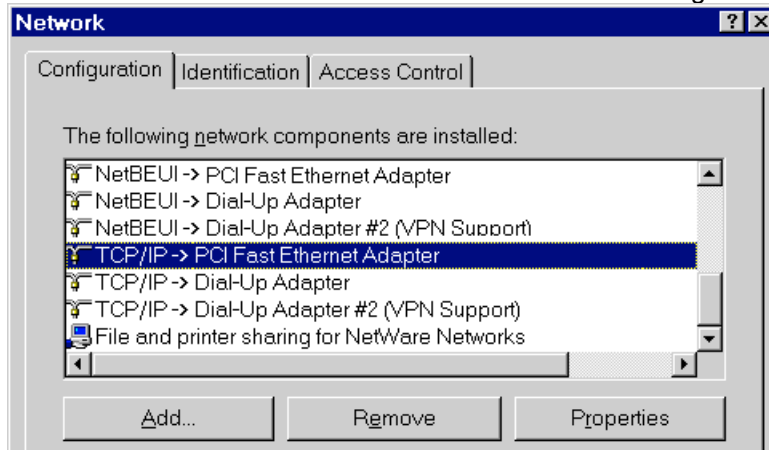


Abbildung 14: Netzkonfiguration

Wählen Sie das TCP/ IP Protokoll für Ihre Netzwerkkarte.

Klicken Sie auf Eigenschaften / Properties. Sie sollten einen Bildschirm wie den Folgenden sehen.

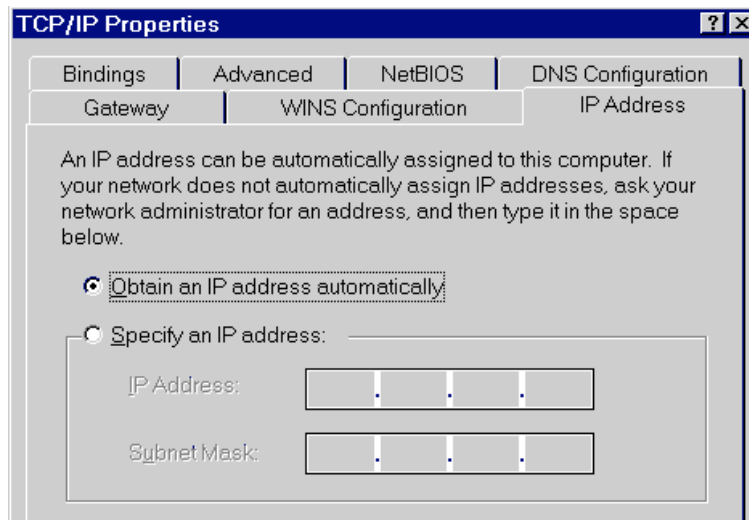


Abbildung 15: IP-Adresse (Windows 95)

Stellen Sie sicher, dass Ihre TCP/IP Einrichten wie folgt richtig sind:

Verwenden von DHCP

Um DHCP zu verwenden, wählen Sie den Radioknopf „Obtain an IP-Adress automatically“. Dies ist die Standardeinstellung und empfohlen. Standardmäßig wirkt der WLAN ADSL Router als ein DHCP Server. Starten Sie Ihren PC neu, um sicherzustellen, dass er eine IP-Adresse vom WLAN ADSL Router erhält.

"Specify an IP-Adress" (eine IP Adresse vorgeben)

Wenn Ihr PC schon konfiguriert wird, fragen Sie bei Ihrem Netzverwalter bevor sie folgenden Änderungen vornehmen:

- Im Gateway Fenster tragen Sie die IP-Adresse des WLAN ADSL Routers ins Feld „New Gateway“ ein. Klicken Sie auf „Add“ hinzufügen, wie unterhalb gezeigt. Ihr LAN-Verwalter kann Ihnen die IP-Adresse mitteilen, die sie dem WLAN ADSL Router eingeben müssen.

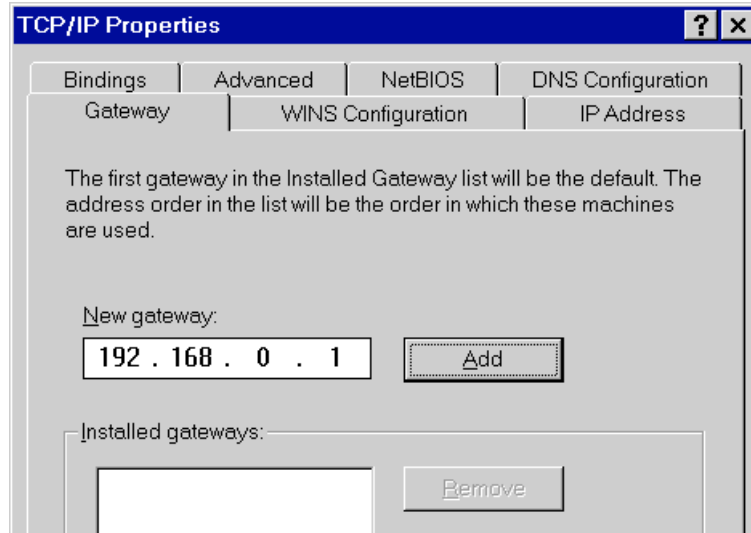


Abbildung 16: Gateway Fenster (Windows 95/98)

- Im DNS-Konfigurationsfenster stellen Sie sicher, das Enable DNS gewählt ist. Wenn die DNS-Serversuchliste leer ist, tragen Sie die von Ihrem ISP gelieferte DNS Adresse in die Felder ein und bestätigen mit dem ADD Knopf.

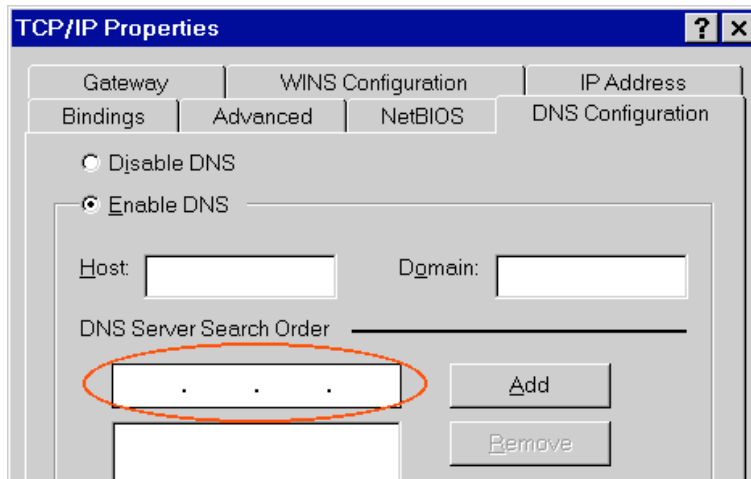


Abbildung 17: DNS Server Eintragen (Windows 95/98)

Checking TCP/IP Settings - Windows NT4.0

1. Wählen Sie Control-Panel –Network. Im Netzwerk-Fenster wählen Sie das TCP/IP Protokoll, wie unterhalb gezeigt.

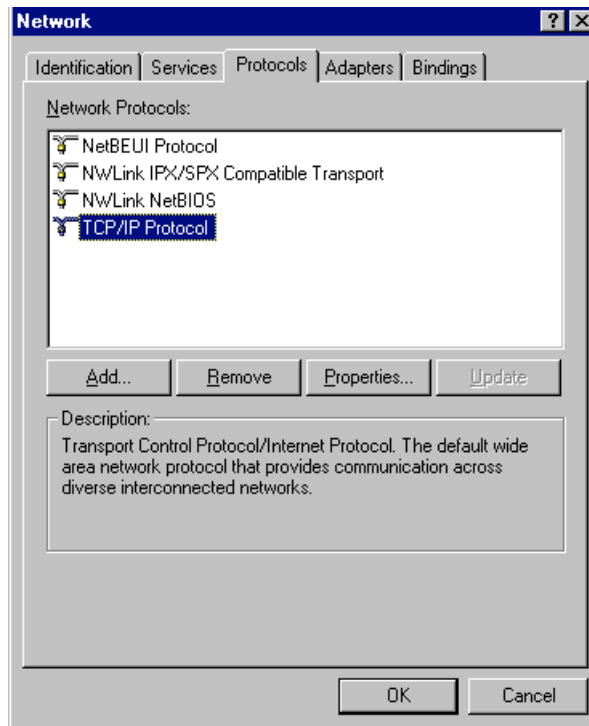


Abbildung 18: Fenster NT4.0 – IP

2. Klicken Sie Properties (Eigenschaften).

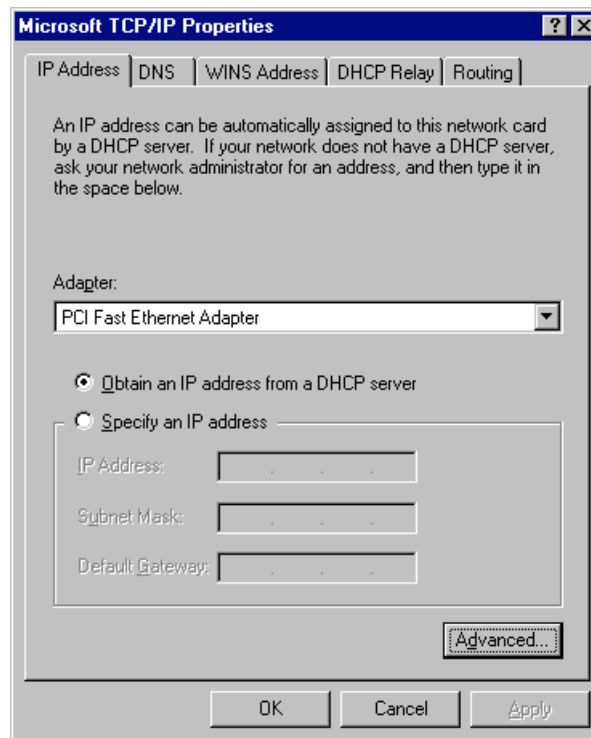


Abbildung 19 Windows NT4.0 - IP-Adresse

3. Wählen Sie die Netzwerkkarte für Ihr LAN.
4. Wählen Sie den entsprechenden Radioknopf - *Obtain an IP address from a DHCP Server* or *Specify an IP Address*,

„Obtain an IP address from a DHCP Server“

Dies ist die Standard Windows-Einstellung und es ist empfohlen, diese zu verwenden. Standardmäßig wirkt der WLAN ADSL Router als ein DHCP Server.

Starten Sie Ihren PC neu, um sicherzustellen, dass er eine IP-Adresse vom WLAN ADSL Router erhält.

Specify an IP Address

Wenn Ihr PC schon konfiguriert ist, fragen Sie bei Ihrem Netzwerkverwalter bevor sie folgende Änderungen vornehmen.

1. Das default Gateway muss auf die IP-Adresse vom WLAN ADSL Router gestellt werden.
 - Klicken Sie den Advanced Knopf auf den Bildschirm oben.
 - Auf dem folgenden Bildschirm klicken Sie den Knopf Add im Fenster Gateway und geben Sie die IP-Adresse des WLAN ADSL Routers ein, wie in Abbildung 20 gezeigt.
 - Wenn notwendig, verwenden Sie den Up Knopf, um den WLAN ADSL Router zum ersten Eintrag in der Gateway-Liste zu machen.

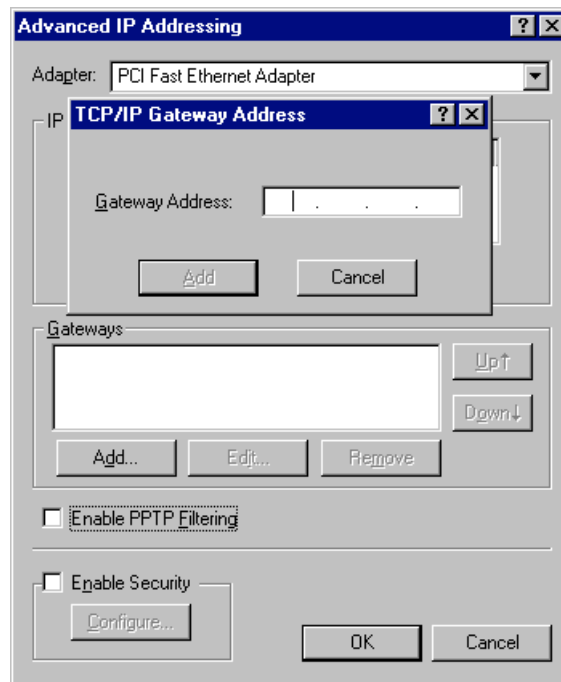


Abbildung 20 - Windows NT4.0 Gateway hinzufügen

2. Die DNS sollte auf die von Ihrem ISP gelieferte Adresse gestellt werden, wie folgt:
- Klicken Sie den DNS Tab.
 - In dem unten gezeigten DNS Bildschirm auf den Knopf ADD klicken (unter DNS Service Search) und die von Ihrem ISP gelieferten DNS eingeben.

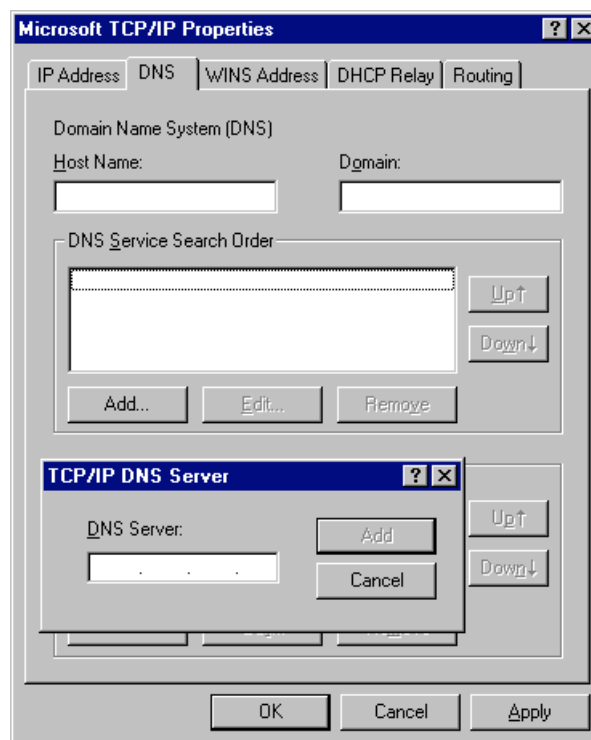


Abbildung 21: Windows NT4.0 - DNS

Das Überprüfen der TCP/IP Settings - Windows 2000 - :

1. Wählen Sie Control Panel - *Network and Dial-up Connection*.
2. Rechts klicken auf *Local Area Connection* und dann Properties (Eigenschaften) auswählen. Sie sollten einen Bildschirm wie den Folgenden sehen:

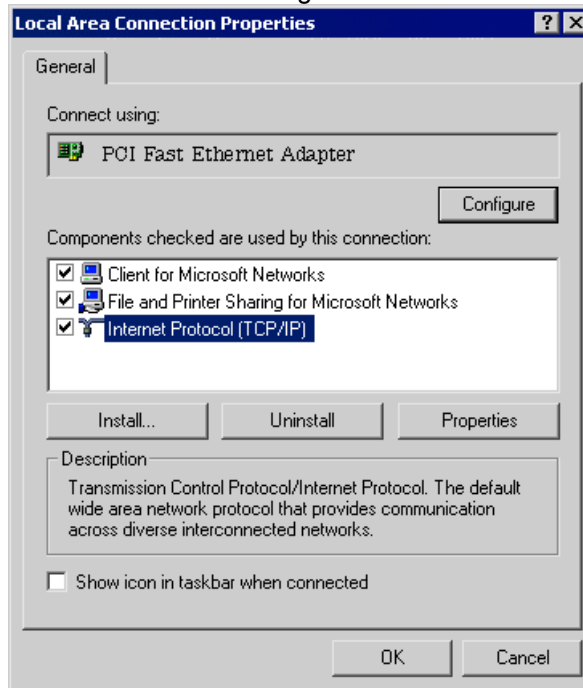


Abbildung 22: Netzwerkkonfiguration (Windows 2000)

3. Wählen Sie das TCP/IP Protokoll für Ihre Netzwerkkarte.
4. Klicken Sie auf den Knopf Properties/ Eigenschaften. Sie sollten einen Bildschirm wie den Folgenden sehen.

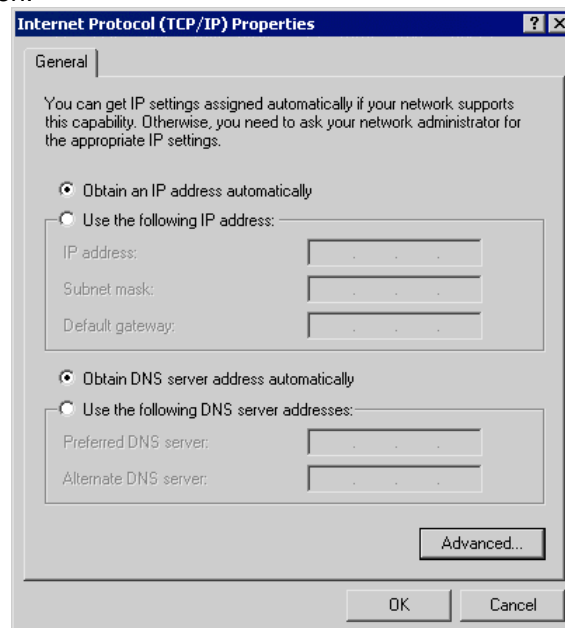


Abbildung 23: IP Eigenschaften (WIN 2000)

5. Stellen Sie sicher, dass Ihre TCP/IP Einstellungen wie unterhalb beschrieben richtig sind..

Die Verwendung von DHCP

Um DHCP zu verwenden, mit dem Radioknopf *Obtain an IP Address automatically* auswählen. Dies ist die default Windows-Einstellung und empfohlen. Standardmäßig wirkt der WLAN ADSL Router als ein DHCP Server.

Starten Sie Ihren PC neu, um sicherzustellen, dass er eine IP-Adresse vom WLAN ADSL Router erhält.

Das Verwenden einer festen IP-Adresse ("die folgende IP-Adresse verwenden")

Wenn Ihr PC schon konfiguriert ist, fragen Sie bei Ihrem Netzverwalter vor dem Vornehmen der folgenden Änderungen nach.

- Tragen Sie die IP-Adresse des WLAN ADSL Routers in das Feld default Gateway ein und klicken Sie auf ok . (Ihr LAN-Verwalter kann Ihnen die IP-Adresse mitteilen, die sie dem WLAN ADSL Router zuordnen müssen.)
- Wenn die DNS-Serverfelder leer sind, wählen Sie *Use the following DNS server addresses* und geben Sie die DNS Adresse ein, die von Ihrem ISP geliefert wurden, dann klicken Sie ok.

Das Überprüfen der TCP/IP Settings - Windows XP

1. Wählen Sie Control Panel – Network Connection.
2. Klicken Sie rechts auf *Local Area Connection* und dann auf *Properties*. Sie sollten einen Bildschirm wie das Folgende sehen:



Abbildung 24: Netzkonfiguration (Windows XP)

3. Wählen Sie das TCO/IP Protokoll für Ihre Netzwerkkarte.
4. Klicken Sie auf den Properties / Eigenschaftsknopf. Sie sollten dann einen Bildschirm wie den Folgenden sehen.

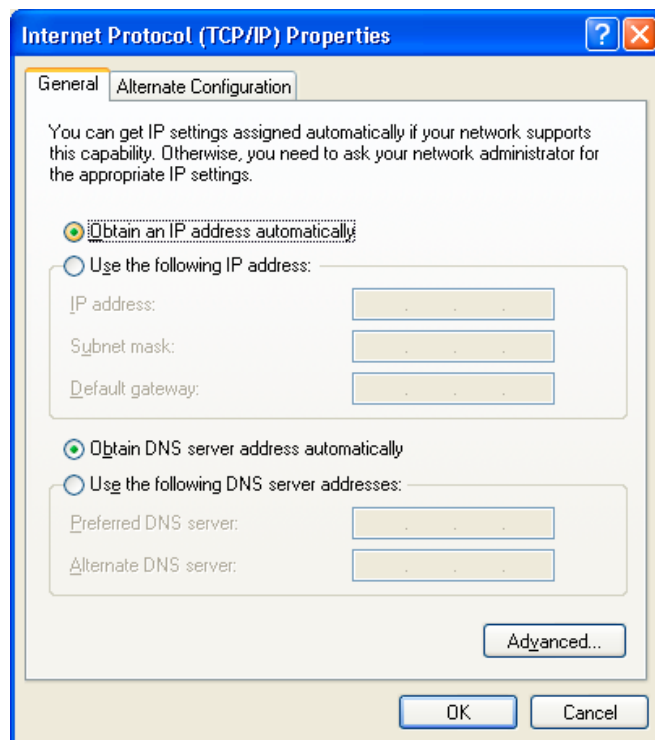


Abbildung 25: IP Eigenschaften (Windows XP)

3. Stellen Sie sicher, dass Ihre TCP/IP Einrichten richtig sind.

Das Verwenden von DHCP

Um DHCP zu verwenden, wählen Sie mit dem Radioknopf *Obtain an IP Address automatically* (IP-Adresse automatisch beziehen). Dies ist die default Einstellung und empfohlen. Standardmäßig wirkt der WLAN ADSL Router als ein DHCP Server.

Starten Sie Ihren PC neu, um sicherzustellen, dass er eine IP-Adresse vom WLAN ADSL Router erhält.

Das Verwenden einer festen IP-Adresse ("die folgende IP-Adresse verwenden")

Wenn Ihr PC schon konfiguriert wurde, fragen Sie bei Ihrem Netzverwalter vor dem Vornehmen der folgenden Änderungen nach.

- Im Feld Default Gateway geben Sie die IP-Adresse des WLAN ADSL Routers ein und Klicken Sie auf ok. Ihr LAN-Verwalter kann Ihnen die IP-Adresse mitteilen, die sie dem WLAN ADSL Router zuteilen müssen.
- Wenn die DNS-Serverfelder leer sind, wählen Sie *Use the following DNS server addresses* und geben Sie die DNS Adresse ein, die von Ihrem ISP geliefert wurden, dann klicken Sie ok.

Internetzugang

Um Ihre PCs zu konfigurieren und um den WLAN ADSL Router für den Internetzugang zu verwenden:

- Stellen Sie sicher, dass das DSL Modem, das Kabelmodem oder die andere permanente Verbindung funktioniert.
- Verwenden Sie das folgende Verfahren, um Ihren Browser zu konfigurieren, um auf das Internet über das LAN statt über eine Wähl-Verbindung zuzugreifen.
-

Für Windows 9 x/ME/2000

1. Wählen *Start Menu - Settings - Control Panel - Internet Options*.
2. Wählen Sie den *Connection /Verbindungen und Setup*.
3. Wählen Sie, "ich will meine Internetverbindung manuell aufstellen, oder ich will mich durch ein lokales Netz (LAN) verbinden", und klicken Sie auf weiter
4. Wählen Sie, "ich verbinde mich durch ein lokales Netz (LAN)", und klicken Sie auf weiter.
5. Stellen Sie sicher, dass alle Kästen auf dem folgenden lokalen LAN-Konfigurations-Bildschirm nicht markiert sind.
6. Überprüfen Sie die "Nein" Option, wenn sie aufgefordert werden, "wollen Sie jetzt ein Internetkonto einrichten"?
7. Klick Sie auf Beenden, um den Internet-Wizard zu schließen.

Die Einrichtung ist jetzt beendet.

Für Windows XP

1. Wählen Sie *Start Menu – Einstellungen, Netzwerkverbindungen, Assistent für neue Verbindungen*. Klicken Sie auf weiter
2. Wählen Sie, *Verbindung mit dem Internet herstellen* und dann weiter
3. Wählen Sie *Manuell einrichten*.
4. Wählen Sie *Verbindung über eine beständige aktive Breitbandverbindung herstellen*
5. Klicken Sie auf *Fertig stellen*, um den Assistenten zu schließen.

Die Einrichtung ist jetzt beendet.

Macintosh Clients

Von Ihrem Macintosh aus können Sie auf das Internet über den WLAN ADSL Router zugreifen. Das Verfahren ist wie folgt.

1. Öffnen Sie das TCP/IP Control Panel.
2. Wählen Sie *Ethernet* im *Connect via* Pop-Up Menü.
3. Wählen Sie *Using DHCP Server* im Configure Pop-Up Menü. Das DHCP Client-ID-Feld kann frei gelassen werden.
4. Schließen Sie das Fenster TCP/ IP Tafel und sichern Sie Ihre Einstellungen.

Hinweis:

Beim Verwenden von manuell zugeteilten IP-Adressen statt DHCP sind die erforderlichen Änderungen:

- Stellen Sie das Routeradressfeld auf die IP-Adresse des WLAN ADSL Routers.
- Stellen Sie sicher, dass Ihre DNS Einrichten richtig sind.

Linux Clients

Um auf das Internet über den WLAN ADSL Router zuzugreifen, ist es nur notwendig, den WLAN ADSL Router zum "Gateway" zu machen.

Stellen Sie sicher, dass Sie als „Root“ angemeldet sind.

Feste IP-Adresse

Standardmäßig verwenden die meisten Unix-Installationen eine feste IP-Adresse. Wenn Sie auch weiterhin eine feste IP-Adresse verwenden möchten, nehmen Sie die folgenden Änderungen an Ihrer Konfiguration vor.

- Setzen Sie Ihr "default Gateway" auf die IP-Adresse des WLAN ADSL Routers.
- Stellen Sie sicher, dass Ihre DNS (Namen Server) Einrichten richtig sind.
-

Als DHCP Client arbeiten (empfohlen)

Das Verfahren unten kann entsprechend Ihrer Version von Linux und Ihren X Windows Shell variieren.

1. Starten Sie Ihren X WindowsClient.
2. Wählen Sie Control Panel - Netzwerk
3. Wählen Sie den Eintrag "Schnittstelle" für Ihre Netzwerkkarte. Normalerweise wird dies "eth0" genannt.
4. Klicken Sie den Editierknopf, stellen Sie das "Protokoll" auf "DHCP" und sichern Sie.
5. Um die Änderungen zu aktivieren
 - Verwenden Sie die "inaktiviert" und "aktiviert" Knöpfe, wenn verfügbar.
 - Oder, starten Ihr System neu.
 -

Andere Unix-Systeme

Um auf das Internet über den WLAN ADSL Router zugreifen:

- Stellen Sie sicher, dass das "Gateway" Feld für Ihre Netzwerkkarte auf die IP-Adresse vom WLAN ADSL Router gestellt ist.
- Stellen Sie sicher, dass Ihre DNS (Namensserver) Einrichten richtig sind.

Wireless LAN Konfiguration

Dieser Abschnitt gilt für alle WLAN Ports, die den Accesspoint des WLAN ADSL Routers ohne Rücksicht auf das Client-Betriebssystem verwenden wollen.

Um den WLAN Accesspoint im WLAN ADSL Router zu verwenden, muss jeder WLAN Station kompatibel wie folgt eingerichtet sein:

Mode	Der Modus muss auf Infrastruktur (anstatt Ad-hoc) gesetzt werden)- Accesspoints arbeiten nur im Infrastructure mode.
SSID (ESSID)	Dies muss zu dem auf dem WLAN ADSL Router verwendeten Wert passen. Der Standardwert ist wireless. Hinweis! Das SSID unterscheidet Groß-/Kleinschreibung.
Wireless Security	Standardmäßig ist die WLAN Sicherheit auf dem WLAN ADSL Router ausgeschaltet <ul style="list-style-type: none">• Wenn WLAN Sicherheit auf dem WLAN ADSL Router ausgeschaltet bleibt, müssen alle Ports WLAN Sicherheit ebenfalls ausgeschaltet haben.• Wenn WLAN Sicherheit auf dem WLAN Router aktiviert ist (entweder WEP oder WPA-PSK) muss jede Station dieselben Einstellungen wie der WLAN ADSL Router verwenden

WLAN Konfiguration auf Windows XP

Wenn Sie Windows XP verwenden, um die WLAN Schnittstelle auf Ihrem PC zu konfigurieren, ist das Konfigurationsverfahren wie folgt:

1. Öffnen Sie den Netzwerkverbindungsordner. (Start - Einstellungen - Netzwerkverbindungen).

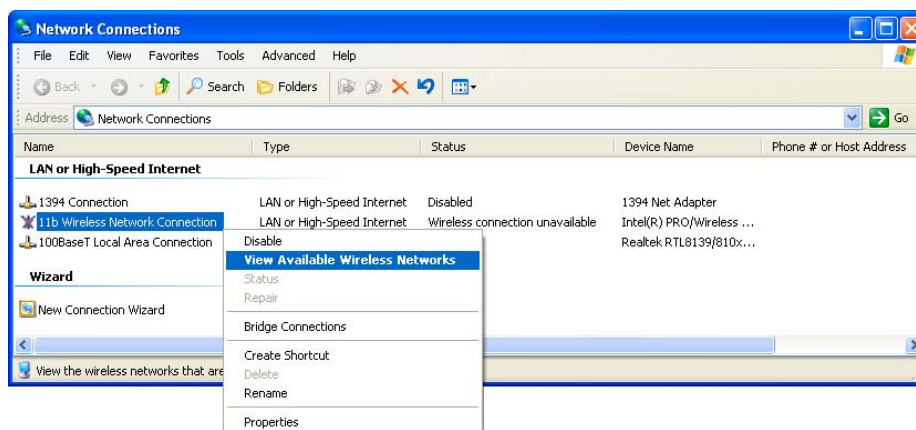


Abbildung 26: Netzverbindungen (Windows XP)

2. Mit rechts auf drahtlose Netzwerkverbindung klicken. Überprüfen Sie, dass sie aktiviert ist und dann wählen Sie das Funknetzwerk.
3. Sie sehen dann eine Liste von Drahtlosnetzwerken.

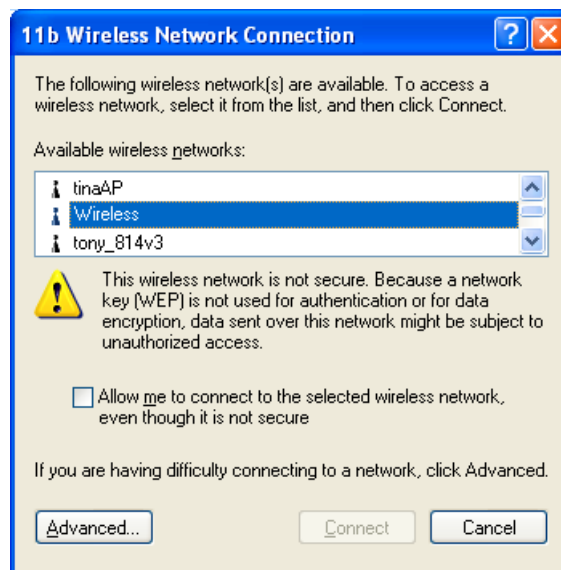


Abbildung 27 WLAN-Netze (Windows XP)



Note!

Wenn das "senden SSID" Einrichten auf dem WLAN ADSL Router ausgeschaltet worden ist, wird sein SSID nicht aufgelistet. Siehe den folgenden Abschnitt "wenn das SSID nicht aufgelistet wird" für Details.

4. Der nächste Schritt hängt davon ab, ob WLAN Sicherheit auf dem WLAN ADSL Router eingeschaltet worden ist.

Wenn WLAN Sicherheit ausgeschaltet ist

Wenn WLAN Sicherheit auf dem WLAN ADSL Router ausgeschaltet ist, wird Windows Sie warnen, dass das Funknetzwerk nicht sicher ist.

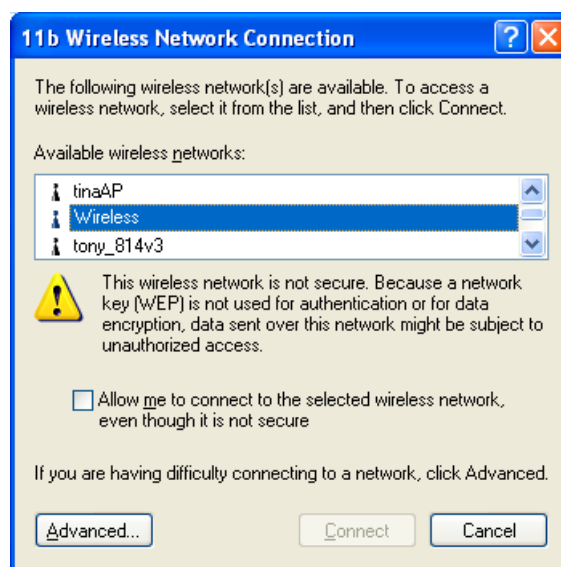


Abbildung 28 unsicheres Funknetzwerk (Windows XP)

- **Verbindung herstellen:**
- Markieren Sie *Mit dem unsicheren Funknetzwerk verbinden*.
- Den Knopf *Verbinden* anklicken. Warten Sie einige Sekunden, damit die Verbindung hergestellt wird.

Wenn Sie WEP Datenverschlüsselung verwenden

Wenn WEP Datenverschlüsselung auf dem WLAN ADSL Router eingeschaltet ist, erkennt Windows dies und zeigt einen Bildschirm wie den Folgenden.

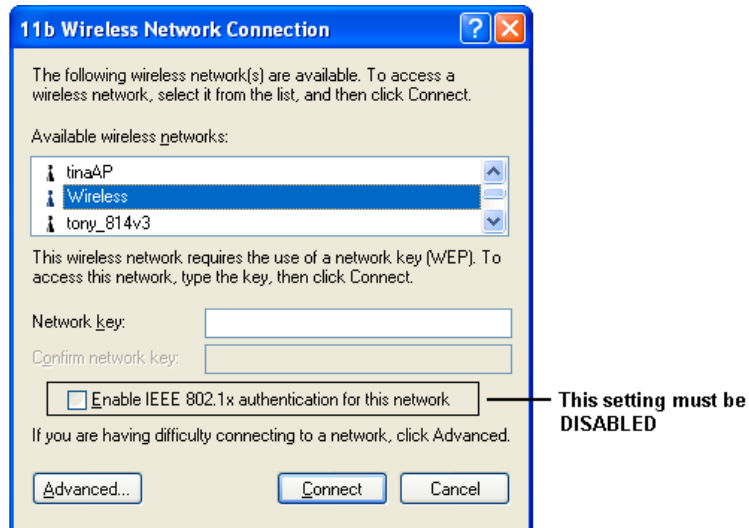


Abbildung 29: WEP (Windows XP)

Verbindung herstellen

- Geben Sie den WEP Schlüssel exakt so ein, wie im WLAN ADSL Router .
- Geben Sie den WEP Schlüssel zur Bestätigung noch einmal ein.
- Schalten Sie IEEE 802,1 aus.
- Klicken den Knopf *Verbinden*.

Falls dies fehlschlägt, klicken Sie auf *Erweiterte Einstellungen*.

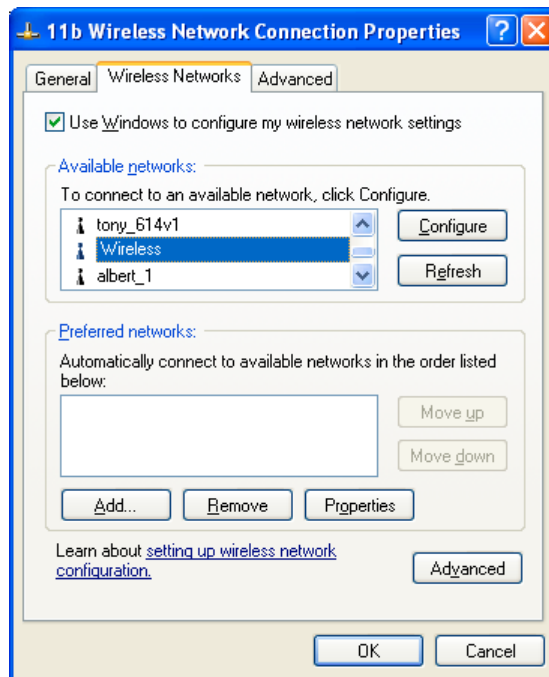


Abbildung 30: Weitere Einstellungen

Wählen die SSID für den WLAN ADSL Router und Klicken Sie auf *Konfiguration*. Sie sehen dann einen Bildschirm wie den Folgenden:

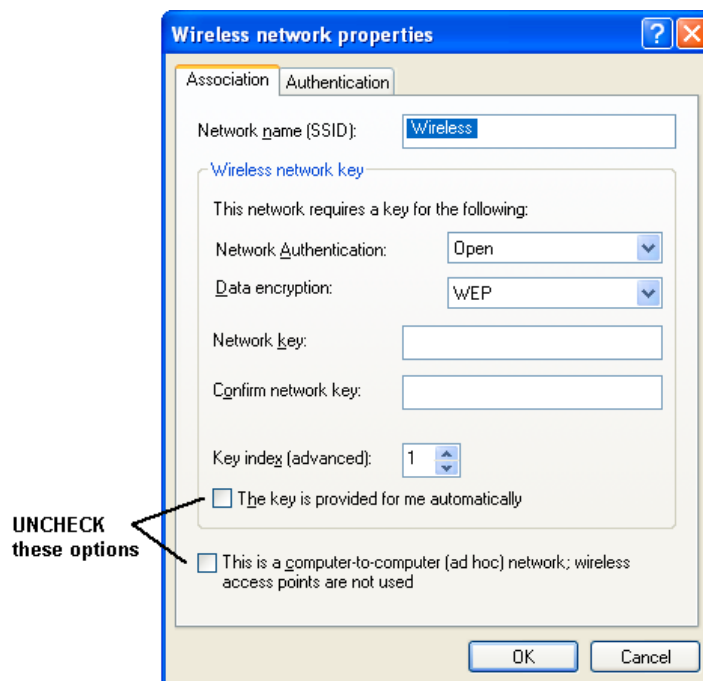


Abbildung 31: WLAN Netzwerkeinstellungen - WEP

Konfigurieren Sie diesen Bildschirm wie folgt:

- Setzen Sie Netzwerkauthentikation so, dass sie zum WLAN ADSL Router zu passt (wenn die Einstellung auf dem WLAN ADSL Router "Auto" ist, dann geht sowohl OPEN als auch SHARED.).
- Für Datenverschlüsselung wählen Sie WEP.

- Als Netzwerk-Schlüssel geben Sie den Default Key ein, wie im WLAN ADSL Router. (Windows wird selbst entscheiden, ob 64 Bit oder 128 Bit Verschlüsselung verwendet wird.)
- Der Schlüsselindex muss zum default Schlüsselindex auf dem WLAN ADSL Router passen. Der Standardwert ist 1.
- Stellen Sie sicher, dass die Optionen, *der Schlüssel wird automatisch bereitgestellt*, und *dies ist ein Computer-zu-Computer (ad hoc) Netzwerk* ausgeschaltet sind.
- Klicken Sie OK, um diesen Vorgang abzuschließen.
- Dieses Drahtlosnetzwerk wird jetzt in „bevorzugte Netze“ auf dem Bildschirm unten aufgeführt.

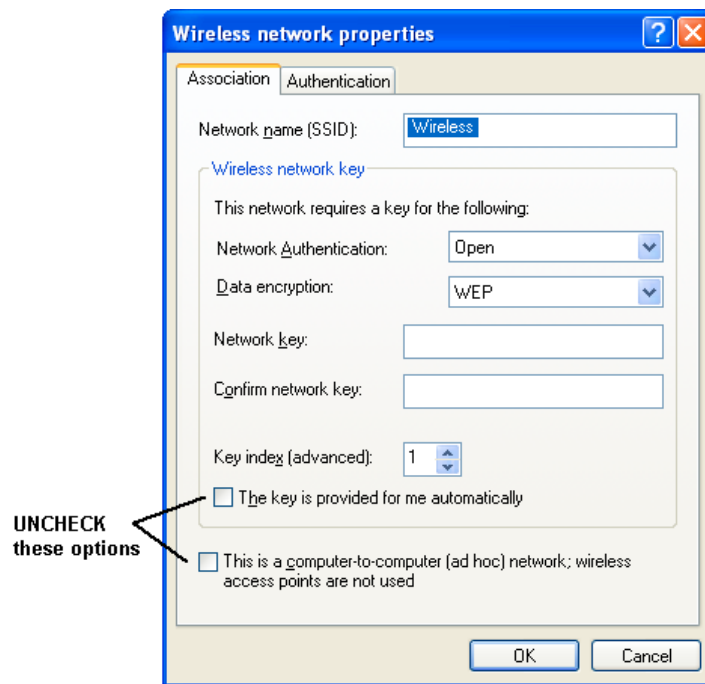


Abbildung 32: Bevorzugte Netze

Klicken Sie auf OK, um eine Verbindung zum WLAN ADSL Router herzustellen.

Wenn WPA-PSK Datenverschlüsselung verwendet wird

Wenn WPA-PSK Datenverschlüsselung auf dem WLAN ADSL Router eingestellt worden ist, ist sie nicht wichtig welches Netzwerk auf dem Bildschirm unten gewählt wurde. Klicken Sie den Knopf *Advanced*.

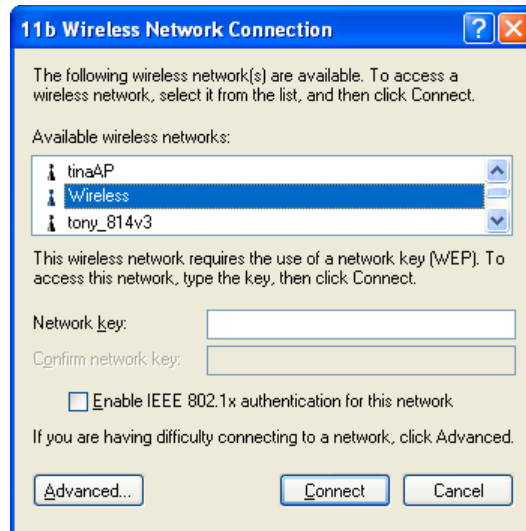


Abbildung 33: Drahtlosnetzwerk (Windows XP)

Sie sehen dann einen Bildschirm wie das Beispiel unten.

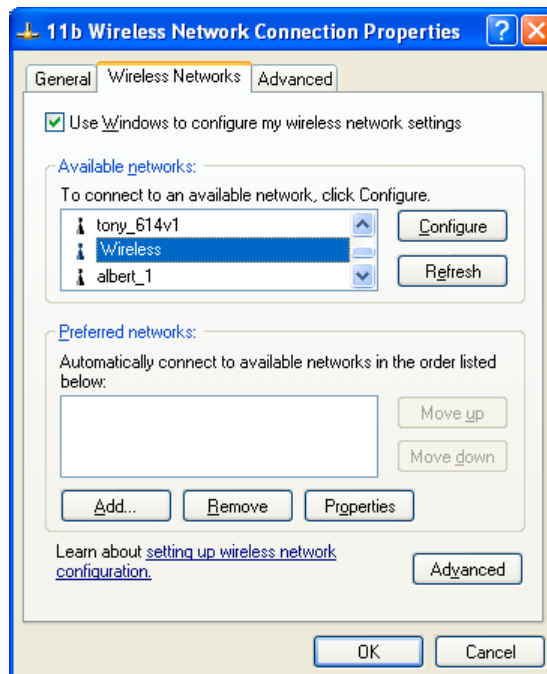


Abbildung 34: WLAN-Netze

Wählen die SSID am WLAN ADSL Router und Klicken Sie auf Konfiguration, um einen Bildschirm wie den Folgenden zu sehen:

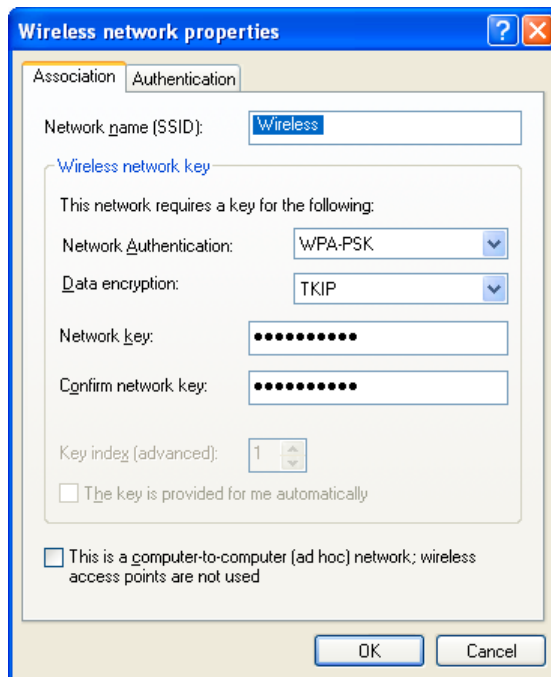


Abbildung 35: Eigenschaften WPA-PSK

Konfigurieren Sie diesen Bildschirm wie folgt:

- Stellen Sie Netzwerk Authentifikation auf WPA-PSK.
- Als Datenverschlüsselung wählen Sie TKIP.
- Für das Netz geben Sie den Schlüssel ein und bestätigen Sie ihn, (Den gleichen, wie den auf dem WLAN ADSL Router benutzten Schlüssel (PSK)).
- Deaktivieren Sie die Option, dass dies ein Computer zu Computer (Ad-hoc--) Netz ist.
- Klicken Sie auf und schließen Sie den Dialog ab.
- Dieses Drahtlosnetzwerk wird jetzt in *bevorzugten Netze* auf dem Bildschirm unten aufgeführt.

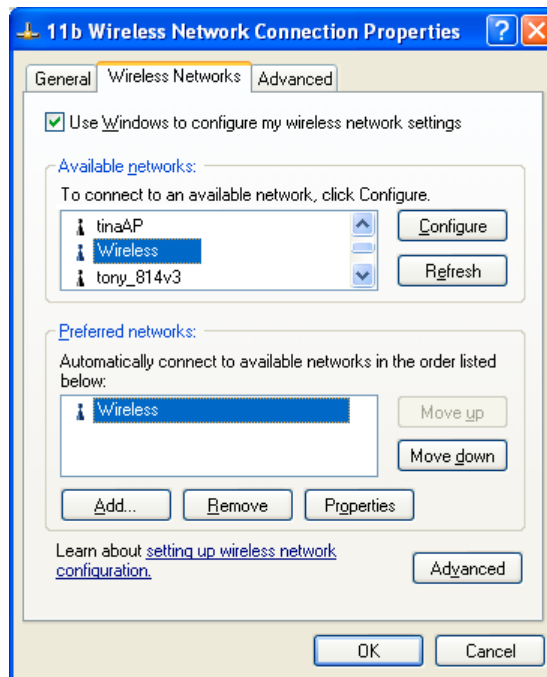


Abbildung 36: Bevorzugte Netze

Klicken Sie auf OK, um eine Verbindung zum WLAN ADSL Router herzustellen.

Wenn SSID nicht aufgelistet wird

Wenn das "Broadcast SSID" im WLAN ADSL Router ausgeschaltet worden ist, wird sein SSID nicht im Bildschirm unten aufgeführt.

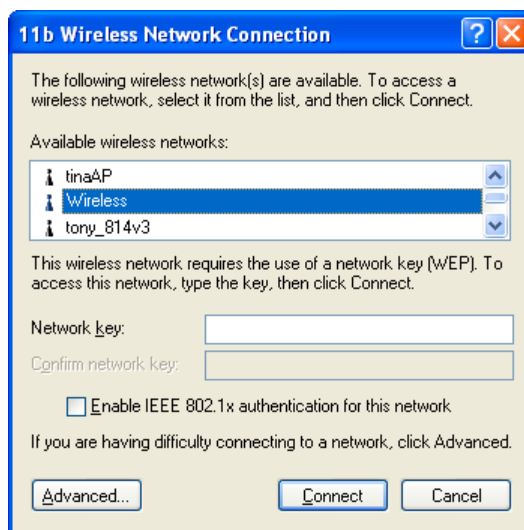


Abbildung 37: Drahtlosnetzwerk (Windows XP)

In dieser Situation müssen Sie das SSID bei Ihrem Netzverwalter erfragen, dann folgen Sie diesem Verfahren:

1. Klicken Sie den Knopf *Advanced*, um einen Bildschirm wie das Beispiel unten zu sehen.

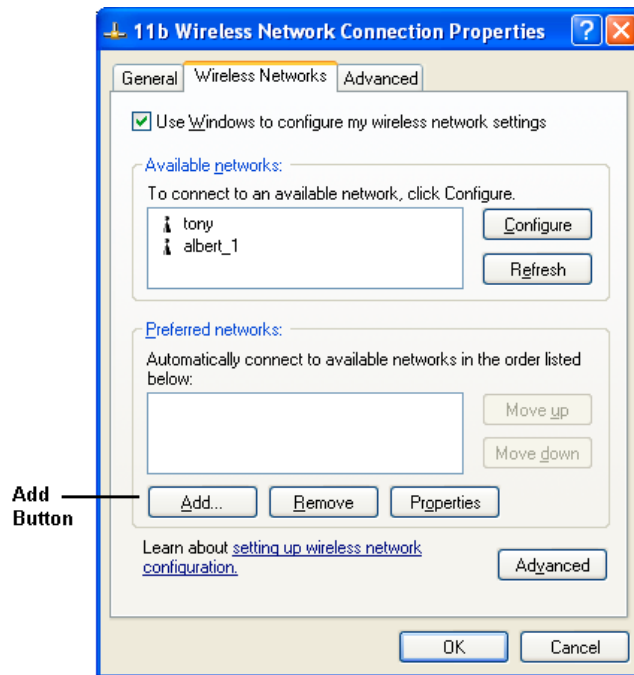


Abbildung 38: Nicht verzeichnetes WLAN

2. Klicken den Knopf *hinzufügen*. Sie sehen einen Bildschirm wie das Beispiel unten.

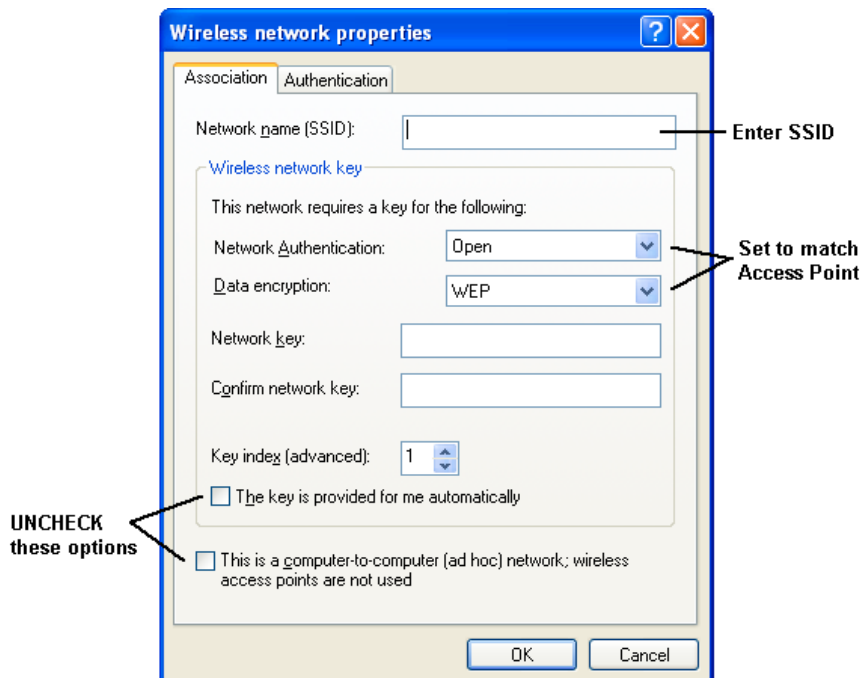


Abbildung 39: Fügen Sie ein WLAN hinzu

3. Konfigurieren Sie diesen Bildschirm wie folgt:
 - Geben Sie die richtige SSID, wie im WLAN ADSL Router verwendet, ein. Erinnern Sie sich daran, dass das SSID auf Groß- und Kleinbuchstaben reagiert.
 - Stellen Sie sicher, dass Netz-Authentifikation und Datenverschlüsselung zum WLAN ADSL Router passen.
 - Beim Verwenden der Datenverschlüsselung (WEP oder WPA-PSK) geben Sie exakt den auf dem WLAN ADSL Router benutzten Schlüssel ein. Siehe die vorangegangenen Abschnitte für Details von WEP und WPA-PSK.
 - Die Optionen der *Schlüssel wird automatisch bereitgestellt*, und *dies ist ein Computer-zu-Computer (ad hoc) Netzwerk* muß ausgeschaltet sein.
 - Klicken Sie auf OK, um zu sichern und die Prozedur abzuschließen.
4. Dieses Drahtlosnetzwerk wird dann in *bevorzugte Netze* auf dem Bildschirm unten aufgeführt.

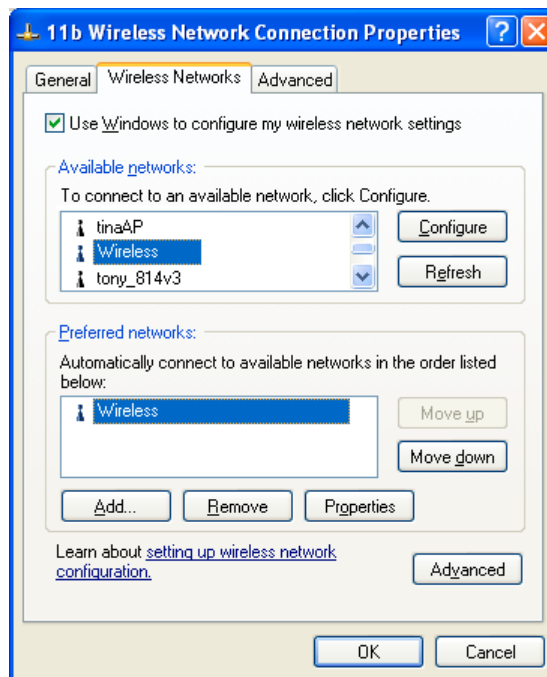


Abbildung 40: Bevorzugte Netze

5. Klicken Sie auf OK, um eine Verbindung zum WLAN ADSL Router herzustellen.

Kapitel 5

Betrieb und Status

Dieses Kapitel stellt die Handhabung des WLAN ADSL Routers und der Statusbildschirme ausführlich dar. Für Details des Betriebs im Bridge (Modem) Modus siehe Kapitel 8 - Modemmodus.

Operation - Routermodus

Sobald sowohl der WLAN ADSL Router als auch die PCs konfiguriert sind, ist Operation automatisch. Jedoch gibt es einige Situationen, wo es sein kann, dass zusätzliche Internetkonfiguration erforderlich ist. Siehe Kapitel 6 - erweiterte Merkmale für weitere Details.

Statusbildschirm

Verwenden Sie *Status* Link im Hauptmenü, um diesen Bildschirm zu betrachten.

The screenshot shows a 'Status' screen with a blue header. It is divided into several sections:

- ADSL**: Modem Status (Connecting), DownStream Connection Speed (0 kbps), UpStream Connection Speed (0 kbps), VC 1 Status (Enabled), VC 2 Status (Disabled), VC 3 Status (Disabled), VC 4 Status (Disabled). Includes an 'ADSL Details' button.
- Internet (VC 1)**: Connection Method: PPPoE, Connection Status: Idle, Internet IP Address: ---. Includes a 'Connection Details' button.
- LAN**: IP Address: 192.168.0.1, Network Mask: 255.255.255.0, DHCP Server: On, MAC Address: 00:C0:02:44:66:88.
- Wireless**: Name (SSID): allnet, Region: Europe, Channel: 3, Wireless AP: enable, Broadcast Name: enable.
- System**: Device Name: ALL0277DSL, Firmware Version: 2.10.00.

At the bottom, there are four buttons: 'Attached Devices', 'VPN Status', 'Refresh Screen', and 'Help'.

Abbildung 41: Statusbildschirm

Daten - Statusbildschirm

ADSL	
Modem Status	Dies zeigt den Status des ADSL Modems an.
DownStream Connection Speed	Zeigt die Geschwindigkeit der Down Stream Verbindung an.
UpStream Connection Speed	Zeigt die Geschwindigkeit der Up Stream (upload) ADSL Verbindung an.
VC1 Status VC2 Status VC 3 Status VC4 Status	Für jeden VC wird der aktuelle Status angezeigt. Dies kann entweder enabled oder disabled sein. Bemerkung: VC1 ist eine „normale“ Internetverbindung. VC2, VC3 und VC4 sind Bridge-Mode Verbindungen.
ADSL Details	Klicken Sie hier, um Details über jeden VC (Virtual Circuit) zu erfahren.
Internet (VC1)	
Connection Method	Zeigt die aktuelle Verbindungsmethode, wie im <i>Setup Wizard</i> eingestellt
Connection Status	Dies zeigt den aktuellen Status der Internet Verbindung <ul style="list-style-type: none"> • Active – Verbindung vorhanden • Idle – Keine Verbindung, aber auch kein Fehler. • Failed - Modem-Fehler oder Verlust der Verbindung zum ISP. <p>Im Fehlerfalle können Sie mit "Connection Details" Knopf mehr Information bekommen..</p>
Internet IP Address	Diese IP-Adresse wurde Ihnen vom ISP (Internet Service Provider) zugeteilt. Falls Sie eine dynamische IP Adresse verwenden, and gegenwärtig keine Verbindung aufgebaut ist, ist diese Information nicht verfügbar.
Connection Details	Hier bekommen Sie detaillierte Informationen über die aktuelle Verbindung.
LAN	
IP Address	Die IP Adresse des Wireless ADSL Routers.
Network Mask	Die Netzwerk Maske (Subnet Mask) zur IP Adresse.
DHCP Server	Dies zeigt den Status des DHCP Servers. Der Wert ist "Enabled" oder "Disabled".
MAC Address	Dies zeigt die MAC Adresse des Wireless ADSL Routers, wie sie vom LAN aus gesehen wird.
Wireless	
Name (SSID)	Wenn ESS (Extended Service Set, with multiple access points) verwendet wird, wird diese ID zur ESSID (Extended Service Set Identifier).

Region	Die gegenwärtige Region wie auf dem WLAN Bildschirm gesetzt.
Channel	Dies zeigt den Kanal, der gegenwärtig verwendet wird, wie auf dem WLAN Bildschirm gesetzt.
Wireless AP	Dies zeigt an, ob der Wireless Access Point eingeschaltet ist.
Broadcast Name	Dies zeigt an, ob Name des WLAN ADSL Routers gesendet wird.
Buttons	
Connection Details	Mit diesem Knopf erhalten Sie detaillierte Informationen über die aktuelle Verbindung.
Attached Devices	Dies zeigt eine Liste aller gegenwärtigen LAN und WLAN Stationen, die angeschlossen sind.
Refresh Screen	Update der Daten auf dem Bildschirm.
System	
Device Name	Der aktuelle Name des Routers. Dies ist auch der Hostname für Benutzer mit einer "@Home" Verbindung.
Firmware Version	Die aktuelle Firmware Version

Verbindungsstatus - PPPoE & PPPoA

Beim Verwenden von PPPoE (PPP über Ethernet) oder PPPoA (PPP über ATM) wird ein Bildschirm wie das folgende Beispiel angezeigt, wenn der "Verbindungsdetails" Knopf geklickt wird.

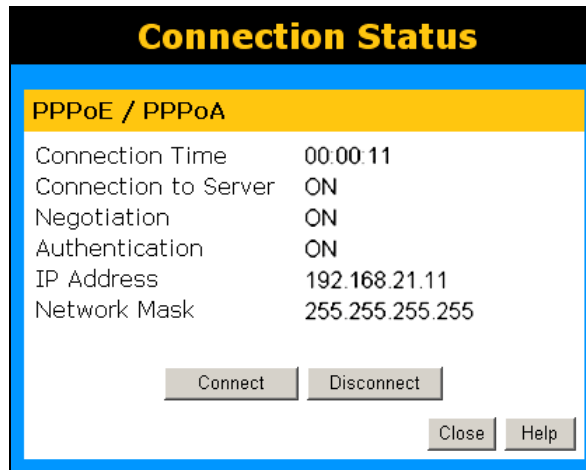


Abbildung 42: PPPoE Statusbildschirm

Daten - PPPoE/PPPoA Bildschirm

Connection Time	Dies zeigt an, wie lang die aktuelle Verbindung bereits besteht.
Connection to Server	Dies zeigt, ob die Verbindung gegenwärtig besteht. <ul style="list-style-type: none"> Falls nicht, kann mit dem <i>Connect</i> button eine Verbindung initiiert werden. Falls die Verbindung besteht, kann mit dem <i>Disconnect</i> Knopf die Verbindung abgebrochen werden. Normalerweise ist es nicht notwendig, <i>Connect</i> oder <i>Disconnect</i> zu verwenden, es sei denn "Connect automatically, as required" ist ausgeschaltet.
Negotiation	Dies zeigt den Status des PPPoE Server Login.
IP Address	Die IP Adresse des Gerätes, wie sie vom Internet aus gesehen wird. Diese Adresse wird vom ISP (Internet Service Provider) zugewiesen.
Network Mask	Die Netzwerk Maske passend zur IP Adresse oben..
Buttons	
Connect	Falls nicht verbunden, initiiert dies eine Verbindung zum ISP.
Disconnect	Falls verbunden, wird die Verbindung abgebrochen..
Close	Schließt das Fenster.

Verbindungsdetails - dynamische IP-Adresse

Wenn Ihre Zugangsmethode "Direkt" mit einer dynamischen IP-Adresse ist, sehen Sie einem Bildschirm wie das folgende Beispiel, wenn Sie den Knopf "Connection Details" angeklickt haben.

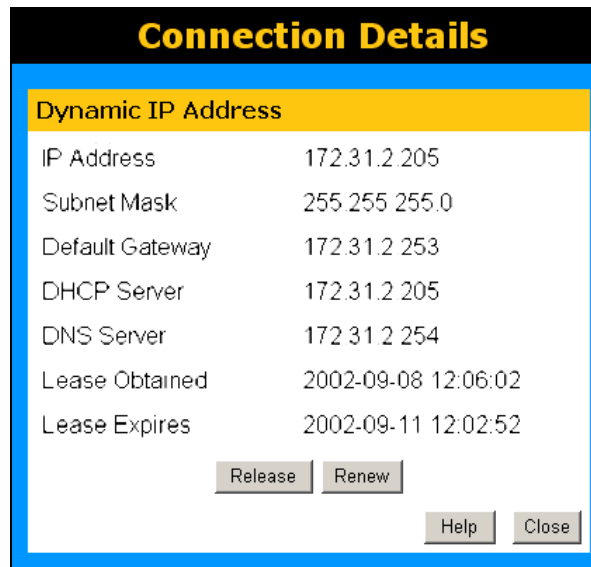


Abbildung 43: Verbindungsdetails - dynamische IP-Adresse

Daten - dynamische IP-Adresse

Internet	
IP Address	Die gegenwärtige IP-Adresse von diesem Gerät wie von Internetbenutzern gesehen. Diese Adresse wird von Ihrem ISP (Internet Service Provider) vergeben
Subnet Mask	Die Netzwerkmaske verbunden mit der IP-Adresse oben
Default Gateway	Die IP-Adresse vom entfernten Gateway oder Router verbunden mit der IP-Adresse oben.
DHCP Server	Die IP-Adresse vom DHCP Server Ihres ISP
DNS Server	Die IP-Adresse vom Domännennamensserver, der gegenwärtig benutzt wird.
Lease Obtained Lease Expires	Dies zeigt wann die gegenwärtige IP-Adresse erhalten wurde, und wie lange diese IP-Adresszuweisung (der DCHP Mietvertrag) noch gültig ist.
Buttons	
Release	Wenn eine IP-Adresse an den WLAN ADSL Router vergeben worden ist (durch den DHCP Server des ISP), wird durch klicken des "Freigabe" Knopf die Verbindung abgebrochen und die IP-Adresse freigegeben.
Renew	Wenn der DHCP Server des ISP keine IP-Adresse für den WLAN Router vergeben hat, wird durch den "erneuern" Knopf die Verbindung wieder hergestellt und eine neue IP-Adresse vom DHCP Server des ISP bezogen.

Verbindungsdetails - feste IP-Adresse

Wenn Ihre Zugangsmethode "Direkt" und mit einer festen IP-Adresse ist, erhalten Sie einem Bildschirm, wie den Folgenden, wenn Sie den Knopf "Connection Details" anklicken.

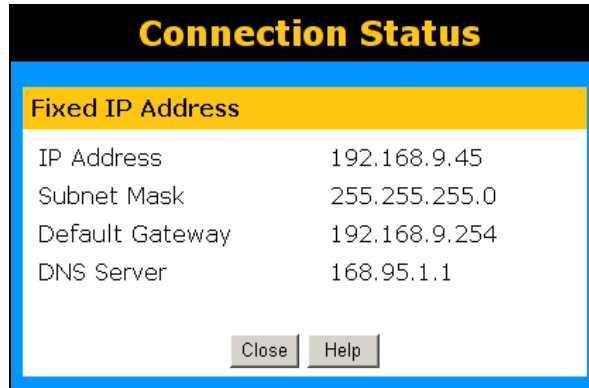


Abbildung 44: Verbindungsdetails - feste IP-Adresse

Daten - Feste IP-Adresse

Internet	
IP Address	Die IP-Adresse von diesem Gerät wie von Internetbenutzern gesehen. Diese Adresse wird von Ihrem ISP (Internet Service Provider) vergeben.
Subnet Mask	Die Netzwerkmaske verbunden mit der IP-Adresse oben
Default Gateway	Die IP-Adresse vom entfernten Gateway oder Router verbunden mit der IP-Adresse oben.
DNS Server	Die IP-Adresse vom Domännennamensserver, der gegenwärtig benutzt wird

Kapitel 6

Erweiterte Merkmale

Dieses Kapitel erklärt, wann und wie die "erweiterten" Merkmale des WLAN ADSL Routers zu verwenden sind.

Überblick

Die folgenden erweiterten Merkmale werden bereitgestellt:

- Internet:
 - DMZ
 - Spezielle Anwendungen
 - URL-Filter
- Dynamisch DNS
- Firewallregeln
- Firewall-Dienste
- Zeitplanung
- Virtuelle Server
- VPN

Internet

Dieser Bildschirm liefert Zugang zum DMZ, speziellen Anwendungen und URL-Filtermerkmalen.

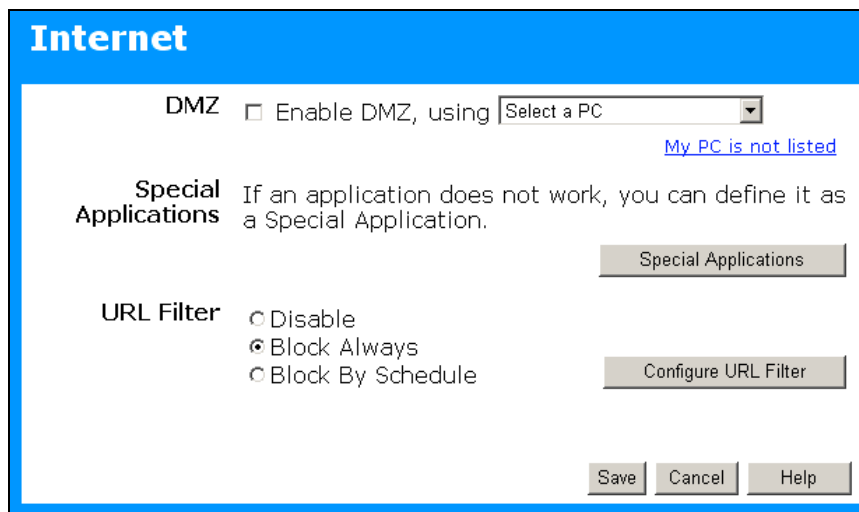


Abbildung 45: Internetbildschirm

DMZ ("De-Militarisierte Zone")

Dieses Merkmal ermöglicht, wenn aktiviert, dass der betreffende Computer in Ihrem LAN für alle Benutzer im Internet sichtbar und adressierbar ist.

- Dies ermöglicht, dass fast jede Anwendung auf dem "DMZ PC" verwendet werden kann.
- Der "DMZ PC" erhält alle "unbekannten" Verbindungen und Daten.
- Wenn das DMZ Merkmal aktiviert ist, müssen Sie den PC wählen, der als "DMZ PC" benutzt werden soll.

**Note!**

Der "DMZ PC" ist außerhalb der Firewall. Das macht ihn Angriffen gegenüber verwundbar. Deshalb sollten Sie DMZ für dann ermöglichen, wenn es unbedingt erforderlich ist.

Spezielle Anwendungen

Wenn Sie Internetanwendungen verwenden, die nicht Standard Verbindungen oder Portnummern verwenden, können Sie feststellen, dass sie ggf. nicht richtig funktionieren, weil sie von der Firewall des WLAN Routers blockiert werden. In diesem Fall können Sie die Anwendung als eine "spezielle Anwendung" definieren.

Der Bildschirm *Special Application* kann durch Klicken des entsprechenden Knopfes auf den Internetbildschirm erreicht werden.

Sie können dann Ihre speziellen Anwendungen definieren. Sie brauchen detaillierte Information über die Anwendung; diese sind normalerweise beim Lieferanten der Anwendung zu erfragen.

Bedenken Sie, dass sich die Bedingungen, "eingehend" und "ausgehend" auf diesem Bildschirm, sich auf dem Client (PC) beziehen.

Enable	Name	Outgoing Ports			Incoming Ports		
		Type	Start	Finish	Type	Start	Finish
1. <input type="checkbox"/>		TCP			TCP		
2. <input type="checkbox"/>		TCP			TCP		
3. <input type="checkbox"/>		TCP			TCP		
4. <input type="checkbox"/>		TCP			TCP		
5. <input type="checkbox"/>		TCP			TCP		
6. <input type="checkbox"/>		TCP			TCP		
7. <input type="checkbox"/>		TCP			TCP		
8. <input type="checkbox"/>		TCP			TCP		
9. <input type="checkbox"/>		TCP			TCP		
10. <input type="checkbox"/>		TCP			TCP		
11. <input type="checkbox"/>		TCP			TCP		
12. <input type="checkbox"/>		TCP			TCP		

Save Cancel Help Close

Abbildung 46: Special Applications Screen

Daten – Special Applications Screen

Checkbox	Verwenden Sie diese, um diese so erforderliche spezielle Anwendung ein- oder auszuschalten
Name	Geben Sie einen beschreibenden Namen ein, um diese spezielle Anwendung zu identifizieren.
Incoming Ports	<ul style="list-style-type: none">• Type - wählen Sie das Protokoll (TCP oder UDP), das verwendet wird, wenn Sie Daten von der speziellen Anwendung oder dem speziellen Dienst erhalten. (Hinweis: Einige Anwendungen verwenden verschiedene Protokolle für ausgehende und eingehende Daten).• Start – geben Sie den Anfang des Portnummer-Bereichs des Anwendungsservers ein. Wenn die Anwendung eine einzige Portnummer verwendet, geben Sie sie in den beiden "Start" und "Finish" Feldern ein.• Finish - geben Sie das Ende des Portnummer-Bereichs des Anwendungsservers ein
Outgoing Ports	<ul style="list-style-type: none">• Type - wählen Sie das Protokoll (TCP oder UDP), das verwendet wird, wenn Sie Daten zu dem entfernten System Dienst senden. (Hinweis: Einige Anwendungen verwenden verschiedene Protokolle für ausgehende und eingehende Daten).• Start – geben Sie den Anfang des Portnummer-Bereichs des Anwendungsservers ein. Wenn die Anwendung eine einzige Portnummer verwendet, geben Sie sie in den beiden "Start" und "Finish" Feldern ein.• Finish - geben Sie das Ende des Portnummer-Bereichs des Anwendungsservers ein

Die Verwendung einer speziellen Anwendung

- Konfigurieren Sie den so erforderlichen Bildschirm Special Applications.
- Verwenden Sie auf Ihrem PC die Anwendung ganz normal. Erinnern Sie sich daran, dass nur ein (1) PC zurzeit eine „spezielle Anwendung“ verwenden kann. Auch wenn 1 PC mit der speziellen Anwendung fertig ist, kann es einen Moment dauern, bevor ein anderer PC dieselbe spezielle Anwendung verwenden kann. Die "Auszeit" Periode kann bis zu 3 Minuten sein.

URL-Filter

Wenn Sie Zugang zu bestimmten Webseiten im Internet eingrenzen wollen, können Sie dieses Merkmal verwenden. Der URL-Filter überprüft jeden Websitezugriff. Wenn die Adresse oder ein Teil der Adresse in die Block-Liste steht, wird der Zugang verwehrt.

Auf dem Internetbildschirm wählen Sie die gewünschten Einstellungen:

- Disable - schaltet dieses Merkmal aus.
- Block By Schedule - blockiert entsprechend der Zeitplan Tabelle.
- Block Always – blockiert „rund um die Uhr“.

Klicken Sie auf Configure URL-Filter, um den URL-Filterbildschirm zu öffnen. Jetzt können Sie die zu filternden URLs eintragen oder modifizieren.

URL-Filterbildschirm

Auf diesem Bildschirm wird angezeigt, wenn der URL-Filter aufgerufen wird.

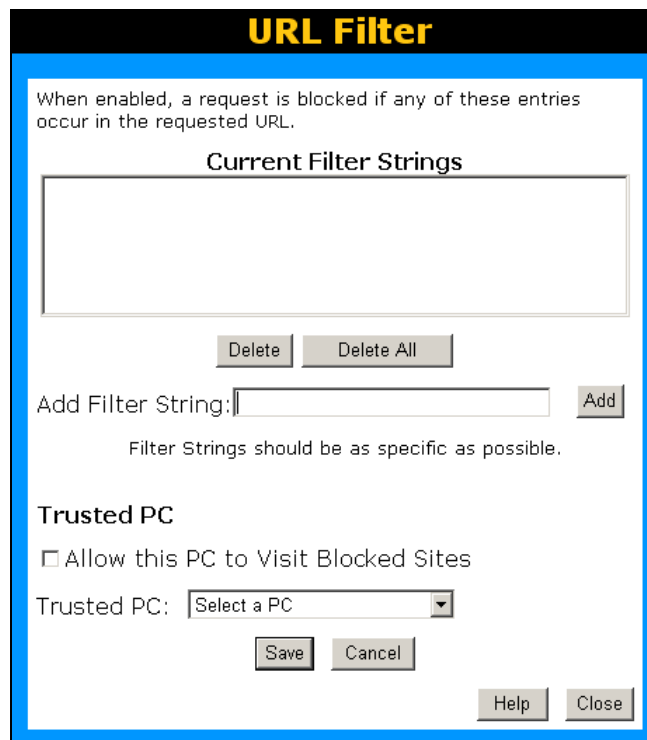


Abbildung 47: URL-Filterbildschirm

Daten - URL-Filterbildschirm

Current Filter Strings	
Current Filter Strings	<p>Diese Liste enthält die gegenwärtig zu blockierenden Einträge.</p> <ul style="list-style-type: none"> • Zum Einfügen, klicken Sie die Add Option.. • Zum Löschen klicken Sie den Delete Knopf. • Um alles zu löschen, klicken Sie den Delete All Knopf.
Add Filter String	<p>Um weitere Einträge hinzu zufügen schreiben Sie das WORT oder den Domännennamen und klicken Sie auf Add. Die „verbotenen Worte“ sollten so bestimmt wie möglich sein. Sonst können Sie Zugang zu viel mehr Websites blockieren, als beabsichtigt.</p>
Trusted PC	
Allow Trusted PC	<p>Ermöglicht, dass ein Computer unbeschränkten Zugang zum Internet hat. Für diesen PC wird der URL-Filter ignoriert. Wenn aktiviert, müssen Sie den vertrauenswürdigen PC auswählen.</p>
Trusted PC	<p>Wählen Sie den PC, der der vertrauenswürdige PC ist.</p>

Dynamische DNS (Domänen-Namensserver)

Dieser Gratisdienst ist in Verbindung mit dem Virtual Server Merkmal sehr nützlich. Er erlaubt Internetbenutzern, Ihre virtuellen Server mit Hilfe einer (fixen) URLs statt einer (dynamischen) IP-Adresse zu adressieren.

Dies löst auch das Problem, das eine dynamische IP-Adresse mit sich bringt. Mit einer dynamischen IP-Adresse ändert sich Ihre IP-Adresse jedes Mal wenn Sie sich mit dem Internet verbinden. Dies macht es schwierig, sich mit Ihrem virtuellen Server zu verbinden.

DDNS funktioniert wie folgt:

1. Sie müssen sich für den Dienst an einem der aufgelisteten DDNS Diensteanbieter anmelden.
2. Nach Registrierung verwenden Sie das normale Verfahren des Diensteanbieters, um Ihren gewünschten Domännennamen zu erhalten.
3. Geben Sie Ihren DDNS Daten in den DDNS Bildschirm des WLAN ADSL Routers ein und schalten Sie das DDNS Merkmal ein.
4. Der WLAN ADSL Router stellt dann automatisch sicher, dass Ihre gegenwärtige IP-Adresse am Domännennamensserver des DDNS Diensteanbieters bekannt ist.
5. Vom Internet werden Benutzer nun in der Lage sein, Ihren virtuellen Server (oder Ihren DMZ PC) mit Hilfe Ihres Domännennamens zu adressieren.

Dynamischer DNS Bildschirm

Wählen Sie, im Hauptmenü *Advanced*, dann *Dynamic DNS*, und Sie sehen einen Bildschirm wie folgt:

Abbildung 48: DDNS Bildschirm

Daten - dynamischer DNS Bildschirm

DDNS Service	
Use a Dynamic DNS Service	Hier schalten Sie DDNS aus bzw. ein.
Service Provider	Wählen Sie einen DDNS Service Provider aus.
Web Site	Klicken Sie diesen Knopf, um ein neues Fenster zu öffnen, und verbinden Sie sich mit der Website des gewählten DDNS Diensteanbieters.
DDNS Data	
Host Name	Geben Sie den an Sie vom DDNS Dienst vergebenen

	Domännennamen ein. Wenn Sie mehr als einen Namen haben, geben Sie den Namen ein, den Sie verwenden möchten.
User Name	Geben Sie Ihren Benutzernamen für den DDNS Dienst ein. (TZO.com verwendet Ihre E-Mail-Adresse.)
Password	Geben Sie das Passwort für den DDNS Service ein.
Domain Name	Geben Sie den an Sie vom DDNS Dienst vergebenen Domännennamen ein. Wenn Sie mehr als einen Namen haben, geben Sie den Namen ein, den Sie verwenden möchten.
DDNS Status	<ul style="list-style-type: none">• Diese Nachricht wird vom DDNS Server erzeugt.• Normalerweise sollte diese Nachricht sein "Update successful"• Wenn die Nachricht ein Problem anzeigt, müssen Sie dieses Problem mit dem DDNS Diensteanbieter korrigieren.

Firewallregeln

Der Firewallregel-Bildschirm erlaubt Ihnen, "Firewallregeln" zu definieren, die bestimmten Datenverkehr ermöglichen oder verhindern können.

Standard:

- Aller ausgehende Verkehr ist erlaubt.
- Aller eingehende Verkehr wird verhindert.

Wegen dieses Default-Verhaltens blockieren ausgehende Regeln im Allgemeinen Verkehr, und eingehende Regeln ermöglichen im Allgemeinen Verkehr.

Firewall-Regel-Bildschirm

Ein Beispielbildschirm wird unten gezeigt.

Firewall Rules

Incoming Rules

#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
Default	Yes	Any	BLOCK always	--	Any	Match

Add Edit Move Delete

Outgoing Rules

#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
Default	Yes	Any	ALLOW always	Any	Any	Never

Add Edit Move Delete

Save Cancel Help

Abbildung 49 Firewall-Bildschirm

Daten - Firewallregeln

Incoming Rules	
#	Für die Default Regel zeigt dies "Default" an. Für Regeln, die Sie selbst schaffen, zeigt dies einen Radioknopf an, der es Ihnen erlaubt, die Regel zu wählen
Enable	Zeigt an, ungeachtet dessen ob die Regel gegenwärtig aktiviert ist. Für Regeln, die Sie hinzugefügt haben, enthält diese Spalte eine Prüfbox, die Ihnen erlaubt, die Regel ein- oder auszuschalten. ("Save" nach dem Vornehmen von Änderungen klicken.)
Service Name	Der von dieser Regel betroffene Dienst.
Action	Die Aktion, die auf Grund dieser Regel erfolgt ist.
LAN Server	Der PC oder Server in Ihrem LAN zu welchem der von dieser Regel betroffene Datenverkehr gesandt wird.

WAN Users	Die WAN IP-Adresse oder die Adressen, die von dieser Regel betroffen sind.
Log	Zeigt an, ob Verbindungen, die von dieser Regel betroffen sind aufgezeichnet werden sollen.
Buttons	Nutzen Sie den <i>Add</i> Knopf um eine neue Regel zu schaffen. Die anderen Knöpfe - <i>Edit</i> , <i>Move</i> , oder <i>Delete</i> – erwarten, dass zuerst die Regel ausgewählt wird. Nutzen Sie den Radio Knopf in der linken Spalte, um den entsprechenden Knopf auszuwählen.
Outgoing Rules	
#	Für die Default Regel zeigt dies "Default" an. Für Regeln, die Sie selbst schaffen, zeigt dies einen Radioknopf an, der es Ihnen erlaubt, die Regel zu wählen
Enable	Zeigt an, ungeachtet dessen ob die Regel gegenwärtig aktiviert ist. Für Regeln, die Sie hinzugefügt haben, enthält diese Spalte eine Prüfbox, die Ihnen erlaubt, die Regel ein- oder auszuschalten. ("Save" nach dem Vornehmen von Änderungen klicken.)
Service Name	Der von dieser Regel betroffene Dienst.
Action	Die Aktion, die auf Grund dieser Regel erfolgt ist.
LAN Users	Der PC oder PCs im LAN, die von dieser regel betroffen sind.
WAN Servers	Die WAN IP-Adresse oder die Adressen, die von dieser Regel betroffen sind.
Log	Zeigt an, ob Verbindungen, die von dieser Regel betroffen sind aufgezeichnet werden sollen.
Buttons	Nutzen Sie den <i>Add</i> Knopf um eine neue Regel zu schaffen. Die anderen Knöpfe - <i>Edit</i> , <i>Move</i> , oder <i>Delete</i> – erwarten, dass zuerst die Regel ausgewählt wird. Nutzen Sie den Radio Knopf in der linken Spalte, um den entsprechenden Knopf auszuwählen.

Eingehende Regeln (einlaufende Dienste / Inbound Services)

Dieser Bildschirm wird angezeigt, wenn der "ADD "oder " Edit" Knopf für eingehende Regeln geklickt wird.

Abbildung 50 Inbound Services

Daten – Bildschirm eingehende Regeln

Inbound Services	
Service	Wählen Sie den gewünschten Dienst. Dies bestimmt, welche Pakete von dieser Regel abgedeckt werden. Wenn notwendig, können Sie einen neuen Dienst auf dem "Dienste" Bildschirm durch Definieren der Protokolle und Portnummern definieren, die vom Dienst verwendet werden.
Action	<p>Wählen Sie die gewünschte Aktion für von dieser Regel abgedeckte Pakete:</p> <ul style="list-style-type: none"> • ALLOW always • ALLOW by schedule, otherwise Block • BLOCK always • BLOCK by schedule, otherwise Allow <p>Hinweis:</p> <ul style="list-style-type: none"> • Jeder einlaufende Verkehr, der nicht von Regeln erlaubt wird, die Sie selbst schaffen, wird von der Default Regel blockiert. • Block, Regeln sind nur sinnvoll, wenn der Verkehr schon von einer ALLOW Regel abgedeckt wird. (Sie möchten z.B. eine Untermenge des Verkehrs blockieren, der gegenwärtig von einer anderen Regel erlaubt wird.) • Um den bei dieser Auswahl verwendeten Zeitplan zu definieren, benutzen Sie den "Schedule" Bildschirm.
Send to LAN Server	Wählen Sie den PC oder Server in Ihrem LAN, das den von dieser Regel abgedeckten einlaufenden Verkehr erhält.

WAN Users	Bestimmt, welche Pakete von der Regel auf Grundlage von ihrer Quellen(WAN) IP-Adresse abgedeckt werden. Wählen Sie die gewünschte Option: <ul style="list-style-type: none"> • ANY - alle IP-Adressen werden von dieser Regel bedeckt. • ADDRESS RANGE - wenn diese Option gewählt ist, müssen Sie die gewünschten Werte in die Felder "Single/Start" und "Finish" Felder eintragen, um den Adressbereich zu bestimmen. • SINGLE ADDRESS – tragen Sie die erforderlichen Adressen in die "Single / Start-" Felder ein.
Log	Dies bestimmt, ob von dieser Regel abgedeckte Pakete protokolliert werden. Wählen Sie die gewünschte Aktion. <ul style="list-style-type: none"> • ALWAYS - Protokollverkehr nach dieser Regel, ob er passt oder nicht, aufzeichnen. (Z.B., wenn sie Ihre Regeln debuggen.) • NEVER - Niemals Protokollverkehr, nach dieser Regel, ob er passt oder nicht, aufzeichnen • MATCH - Verkehr nur dann aufzeichnen, wenn er zu dieser Regel passt. (Die Aktion wird von dieser Regel bestimmt.) • NOT MATCH - Protokolliert den Verkehr, der von dieser Regel berücksichtigt wird, aber nicht passt, (die Aktion wird nicht von dieser Regel bestimmt.)

Ausgehende Regeln (Outbound Services, ausgehende Dienste)

Dieser Bildschirm wird angezeigt wenn der "ADD", oder "Edit" Knopf für ausgehende Regeln angeklickt wird.

The screenshot shows the 'Outbound Services' configuration window. It features a title bar with the text 'Outbound Services' in yellow on a black background. The main content area has a blue border and contains the following elements:

- Service:** A dropdown menu currently showing 'Any(ALL)(TCP/UDP:1,65535)'.
- Action:** A dropdown menu currently showing 'BLOCK always'.
- LAN Users:** A dropdown menu currently showing 'Any'.
- PC:** A dropdown menu currently showing 'Select a PC'.
- WAN Users:** A dropdown menu currently showing 'Any'.
- Single/Start:** Four empty input boxes separated by dots (.) for IP address entry.
- Finish:** Four empty input boxes separated by dots (.) for IP address entry.
- Log:** A dropdown menu currently showing 'Always'.
- Buttons:** 'Save', 'Cancel', 'Back', and 'Help' buttons are located at the bottom of the window.

Abbildung 51: Outbound Services Screen

Daten - auslaufender Regelbildschirm

Outbound Services	
Service	Wählen Sie den gewünschten Dienst. Dies bestimmt, welche Pakete von dieser Regel abgedeckt werden. Wenn notwendig, können Sie einen neuen Dienst auf dem "Dienste" Bildschirm durch Definieren der Protokolle und Portnummern definieren, die vom Dienst verwendet werden.
Action	<p>Wählen Sie die gewünschte Aktion für von dieser Regel abgedeckte Pakete:</p> <ul style="list-style-type: none"> • ALLOW always • ALLOW by schedule, otherwise Block • BLOCK always • BLOCK by schedule, otherwise Allow <p>Hinweis:</p> <ul style="list-style-type: none"> • Jeder einlaufende Verkehr, der nicht von Regeln erlaubt wird, die Sie selbst schaffen, wird von der Default Regel blockiert. • Block, Regeln sind nur sinnvoll, wenn der Verkehr schon von einer ALLOW Regel abgedeckt wird. (Sie möchten z.B. eine Untermenge des Verkehrs blockieren, der gegenwärtig von einer anderen Regel erlaubt wird.) • Um den bei dieser Auswahl verwendeten Zeitplan zu definieren, benutzen Sie den "Schedule" Bildschirm.
LAN Users	<p>Wählen Sie die entsprechende Option um zu entscheiden, welche PCs von den Regeln betroffen sind</p> <ul style="list-style-type: none"> • Any - All PCs sind betroffen. • Single PC – Nur der gewählte PC ist betroffen, Sie müssen einen PC wählen.
WAN Users	<p>Bestimmt, welche Pakete von der Regel auf Grundlage von ihrer Quellen(WAN) IP-Adresse abgedeckt werden. Wählen Sie die gewünschte Option:</p> <ul style="list-style-type: none"> • ANY - alle IP-Adressen werden von dieser Regel bedeckt. • ADDRESS RANGE - wenn diese Option gewählt ist, müssen Sie die gewünschten Werte in die Felder "Single/Start" und "Finish" Felder eintragen, um den Adressbereich zu bestimmen. • SINGLE ADDRESS – tragen Sie die erforderlichen Adressen in die "Single / Start-" Felder ein.
Log	<p>Dies bestimmt, ob von dieser Regel abgedeckte Pakete protokolliert werden. Wählen Sie die gewünschte Aktion.</p> <ul style="list-style-type: none"> • ALWAYS - Protokollverkehr nach dieser Regel, ob er passt oder nicht aufzeichnen. (Z.B., wenn sie Ihre Regeln debuggen.) • NEVER - Niemals Protokollverkehr, nach dieser Regel, ob er passt oder nicht, aufzeichnen • MATCH - Verkehr nur dann aufzeichnen, wenn er zu dieser Regel passt. (Die Aktion wird von dieser Regel bestimmt.) • NOT MATCH - Protokolliert den Verkehr, der von dieser Regel berücksichtigt wird, aber nicht passt, (die Aktion wird nicht von dieser Regel bestimmt.)

Benutzerdefinierte Dienste

Diese Dienste werden gebraucht, wenn sie Firewallregeln erstellen wollen.

Wenn Sie eine Firewallregel schaffen möchten, aber der erforderliche Dienst nicht in der "Service" Liste aufgeführt wird, können Sie dieses Merkmal verwenden, um den erforderlichen Dienst oder die Dienste zu definieren. Einmal definiert, werden diese Dienste in der "Service" Liste aufgeführt und können immer wieder verwendet werden.



Abbildung 52: Add Services Screen

Daten - benutzerdefinierte Dienste

Services	
Existing Services	Dies listet alle Dienste auf Sie definiert haben. Wenn Sie keine Dienste definiert haben, wird diese Liste leer sein. Sobald Sie einige Dienste definieren, werden sie hier aufgelistet und auch in der Dienstliste gezeigt, die verwendet wird, um Firewallregeln zu schaffen. (Benutzerdefinierte Dienste sind am Ende der Liste nach den vordefinierten Diensten.)
Add	Verwenden Sie dieses, um einen Unterbildschirm zu öffnen, wo Sie einen neuen Dienst hinzufügen können.
Edit	Um einen Dienst zu modifizieren, wählen Sie ihn aus und klicken Sie dann diesen Knopf.
Delete	Vordefinierte Dienste können nicht gelöscht werden, aber Sie können mit diesem Knopf Dienste löschen, die Sie definiert haben.

Add/Edit Service

Dieser Bildschirm wird angezeigt wenn Knopf ADD oder EDIT auf dem Dienstbildschirm angeklickt wird.

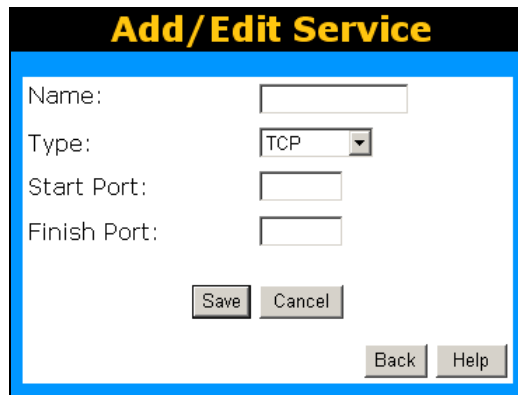


Abbildung 53: Fügen Sie einen Dienst hinzu/redigieren Sie ihn

Daten – Dienst hinzuzufügen/ redigieren

Services	
Name	Beim Redigieren zeigt dieses Feld den gegenwärtigen Namen des Diensts an. Beim Hinzufügen eines neuen Diensts wird dies leer sein, und Sie sollten einen geeigneten Namen eingeben.
Type	Wählen Sie das vom Dienst verwendete Protokoll.
Start Port	Geben Sie den Anfang des vom Dienst verwendeten Portbereichs ein.
Finish Port	Geben Sie das Ende des vom Dienst verwendeten Portbereichs ein.

Optionen

Dieser Bildschirm erlaubt fortgeschrittenen Benutzern, eine Anzahl von Einstellungen vorzunehmen oder zu ändern. Für den normalen Betrieb gibt es keinen Grund, diesen Bildschirm zu benutzen oder Einstellungen zu ändern.

Ein Beispieloptionsbildschirm wird unten gezeigt.

Abbildung 54: Optionsbildschirm

Daten - Optionsbildschirm

Internet	
Respond to Ping	<ul style="list-style-type: none"> • Wenn aktiviert, wird der Wireless Router will auf Ping (ICMP) Pakete aus dem Internet reagieren. • Wenn deaktiviert, warden Ping (ICMP) Pakete aus dem Internet ignoriert. Deaktivierung erhöht die Sicherheit ein bisschen.
MTU Size	Geben Sie einen Wert zwischen 1 and 1500 ein. Note: die MTU (Maximalübertragungseinheit) sollte nur geändert werden, wenn Ihnen vom technischen Support dazu geraten wird.
UPnP	
UPnP	<ul style="list-style-type: none"> • UPnP (Universal Plug and Play) gestattet automatische Konfiguration von Geräten, in Ihrem LAN. UPnP wird von Windows ME, XP unterstützt. • Wenn Enabled, ist der Router über UPnP sichtbar. • Wenn Disabled, ist der Router für UPnP nicht sichtbar.
Advertisement Period	Wert in Minuten. zwischen 1 und 1440.
Advertisement Time to Live	Wert in hops zwischen 1 und 255.

Schedule

Schedule

Schedule Use 24 hour clock. On all day: 00:00 to 24:00
Off all day: All fields blank

Day	Session 1		Session 2	
	Start	Finish	Start	Finish
Monday	00:00	12:00	12:00	24:00
Tuesday	00:00	12:00	12:00	24:00
Wednesday	00:00	12:00	12:00	24:00
Thursday	00:00	12:00	12:00	24:00
Friday	00:00	12:00	12:00	24:00
Saturday	00:00	12:00	12:00	24:00
Sunday	00:00	12:00	12:00	24:00

Local Time Time Zone: (GMT+01:00) Amsterdam, Berlin, Rome, Vienna ▼

Adjust for Daylight Savings Time

Use this NTP Server . . .

Current Time: 2002-09-08 16:01:58

Abbildung 55: Schedule Bildschirm

Data - Schedule Screen

Schedule	
Day	Jeder Wochentag kann separat behandelt werden
Session 1	Zwei (2) separate Sessions oder Periods können definiert werden. Session 2 kann frei bleiben, wenn nicht benötigt.
Session 2	
Start Time	Startzeit im 24 hr Schema.
Finish Time	Endezeit im 24 hr Schema.
Local Time	
Time Zone	Wählen Sie Ihre Zeitzone.
Adjust for Daylight Savings Time	Wählen Sie die Sommerzeit/Winterzeit Einstellung.
Use this NTP Server	Sie können einen NTP Server als Zeitbasis einstellen. Geben Sie die IP Adresse in das Adressfeld ein .
Current Time	Zeigt die aktuelle Zeit

Virtuelle Server

Dieses Merkmal, manchmal auch Portweiterleitung genannt, erlaubt Ihnen, Server in Ihrem LAN Internetbenutzern zugänglich zu machen. Normalerweise wären Internetbenutzer nicht in der Lage, auf einen Server in Ihrem LAN zuzugreifen, weil:

- Ihr Server keine gültige externe IP-Adresse hat
- Versuche, mit Geräten in Ihrem LAN zu kommunizieren, von der Firewall in diesem Gerät blockiert werden.

Das "virtuellen Server" Merkmal löst diese Probleme und erlaubt Internetbenutzern, Ihre Server zu direkt zu adressieren.

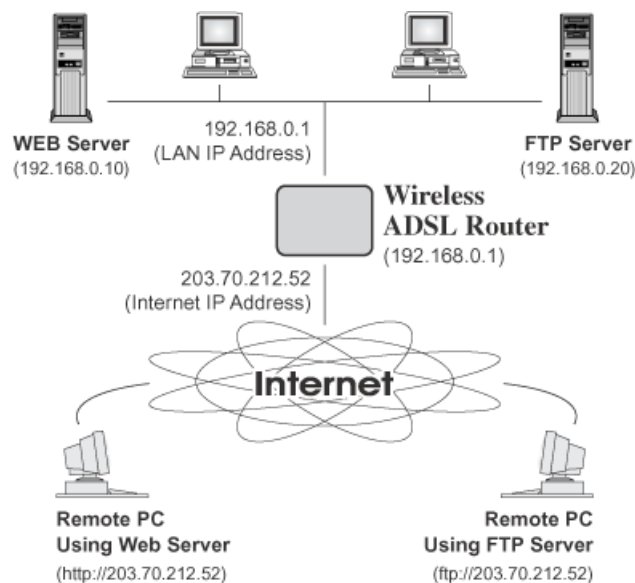


Abbildung 56: Virtuelle Server

Von Internetbenutzern gesehene IP-Adresse

Beachten Sie, dass in dieser Abbildung beide Internetbenutzer sich mit derselben IP-Adresse verbinden, aber verschiedene Protokolle verwenden.

Für Internetbenutzer haben alle virtuellen Server auf Ihrem LAN dieselbe IP-Adresse. Diese IP-Adresse wird von Ihrem ISP vergeben.

Diese Adresse sollte statisch statt dynamisch sein, um es für Internetbenutzer leichter zu machen, sich mit Ihren Servern zu verbinden. Jedoch können Sie das DDNS (dynamische DNS) Merkmal verwenden, um Benutzern zu erlauben, mit Ihren virtuellen Servern mit Hilfe einer URLs statt einer IP-Adresse zu kommunizieren.

Virtual Servers screen

- Das "virtuelle Server" Merkmal erlaubt Internetbenutzern, auf PCs auf Ihrem LAN zuzugreifen.
- Die PCs müssen die entsprechende Serversoftware ausführen.
- Für Internetbenutzer haben alle Ihre Server dieselbe IP-Adresse. Diese IP-Adresse wird von Ihrem ISP vergeben.

- Um es für Internetbenutzer leichter zu machen, an Ihre Server anzuschließen, können Sie das "DDNS" Merkmal verwenden. Dies erlaubt Internetbenutzern, an Ihre Server mit einem URL statt einer IP-Adresse anzuschließen. Diese Technik funktioniert, selbst wenn Ihr ISP dynamische IP-Adressen vergibt (Die IP-Adresse wird bei Verbindung neu vergeben, so dass sie sich jedes Mal ändern kann, wenn Sie sich verbinden).

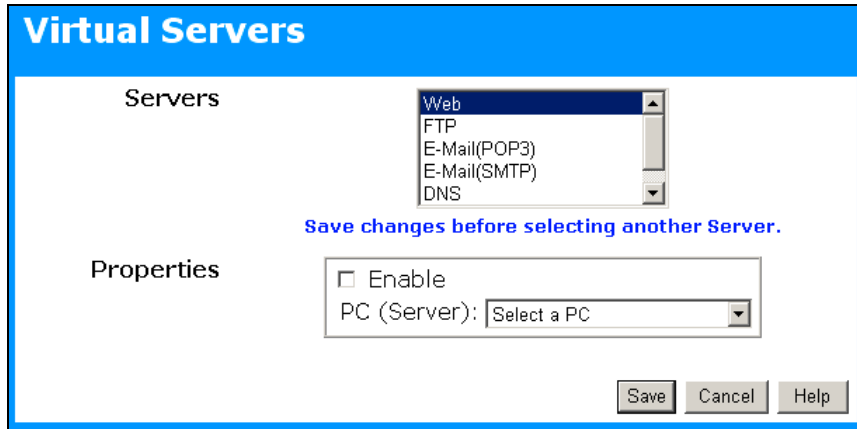


Abbildung 57: Virtueller Server Bildschirm

Daten - Virtuelle Server Bildschirm

Servers	
Servers	Dies listet eine Anzahl von gemeinsamen Serverarten auf. Wenn die gewünschte Serverart nicht aufgelistet wird, können Sie eine Firewallregel schaffen, um dieselbe Wirkung wie die virtueller Serverfunktion zu erreichen.
Properties	
Enable	Verwenden Sie dieses, um Unterstützung für diesen Server zu ermöglichen. Wenn aktiviert, müssen Sie den PC wählen, zu dem der Datenverkehr geschickt wird.
PC (Server)	Wählen Sie den PC für diesen Server. Der PC muss die entsprechende Serversoftware ausführen.



Note! Für jeden Eintrag muss der PC die entsprechende Serversoftware ausführen. Wenn die gewünschte Serverart nicht aufgelistet wird, können Sie Ihre eigenen Server mit Hilfe der Firewallregeln definieren.

Das Anschließen an virtuelle Server

Einmal konfiguriert, kann jeder im Internet sich an Ihre virtuellen Server anmelden. Sie müssen die Internet-IP-Adresse (die an Sie von Ihrem ISP vergebene IP-Adresse) verwenden.
z.B. <http://203.70.212.52> oder <ftp://203.70.212.52>

Es ist angenehmer, wenn Sie eine feste IP-Adresse von Ihrem ISP statt einer dynamischen verwenden. Jedoch können Sie das dynamische DNS Merkmal verwenden, um Benutzern zu erlauben, Ihre virtuellen Server mit Hilfe einer URLs anstatt einer IP-Adresse zu adressieren.

VPN Konfiguration

Das Feature VPN (Virtuelles privates Netzwerk), ermöglicht eine VPN Verbindung zu einem entfernten PC über zwei WLAN ADSL Router hinweg. Um vom entfernten PC eine VPN-Verbindung zum WLAN ADSL Router aufzubauen, benötigen Sie passende (IPSec) Software für den PC.

Weitere Informationen dazu finden Sie im Appendix C

VPN "Policies" / Regeln

Eine VPN „Policy“ bzw. Regel beinhaltet alle Konfigurationsdaten für eine bestimmte VPN Verbindung. Grundsätzlich müssen Sie für jeden Teilnehmer, mit dem Sie eine VPN-Verbindung nutzen wollen, eine VPN-Policy erstellen. Die Gegenseite muß eine dazu passende Konfiguration verwenden.

- Datenverkehr, der über eine aktivierte Policy gesendet oder empfangen wird, erfolgt durch einen so genannten VPN Tunnel. Falls der Tunnel noch nicht existiert, wird er automatisch aufgebaut.
- Der VPN Tunnel wird so aufgebaut, wie durch die Parameter in der SA (Security Association) beschrieben.
- Der entfernte PC/Server muß über eine SA mit passenden Eintragungen verfügen, oder der VPN-Verbindungsversuch wird abgebrochen.

Es gibt zwei Arten von VPN Policies.

- **Manual (von Hand)** – Alle Eintragungen einschließlich der Schlüssel für den VPN Tunnel müssen bei beiden VPN-Teilnehmern von Hand eingegeben werden.
- **Auto (automatisch)** – Einige Parameter für den VPN-Tunnel werden automatisch erzeugt. Dies erfordert die Verwendung des IKE Protokolls (Internet Key Exchange) zwischen den beiden VPN-Endpunkten.

VPN Policies Screen

Diesen Bildschirm sehen Sie, wenn Sie **VPN** im Menü **Advanced** anklicken. Hier können Sie VPN Policies erstellen, verändern und verwalten.

Wenn Sie noch keine Policies angelegt haben, ist diese Tabelle leer.

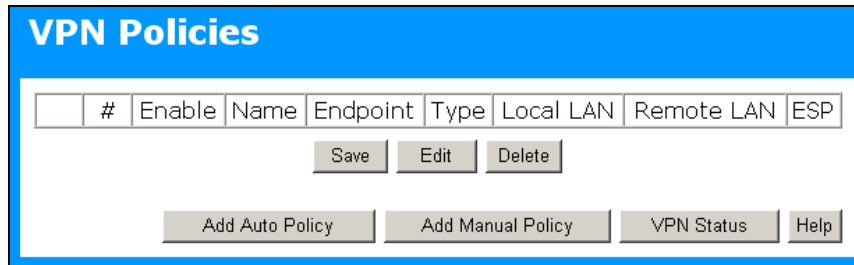


Abbildung 58: VPN Policies Bildschirm-Maske

Daten – VPN Policies Bildschirm

Policy Table	<p>Die Policy Table enthält die folgenden Daten:</p> <ul style="list-style-type: none"> • Enable – Hiermit entscheiden Sie, ob eine Policy benötigt wird oder nicht. Mit "Save" sichern Sie Ihre Änderungen. • Name - Jede Policy hat einen eindeutigen Namen. Dieser Name ist der VPN Gegenstelle nicht bekannt. Er wird nur für Verwaltungszwecke verwendet. • Endpoint – Die Adresse der entfernten VPN Station. • Type – Dies ist entweder "Auto" oder "Manual" wie zuvor erklärt. • Local LAN - IP Adresse oder Subnet Ihres lokalen LANs. Datenverkehr muss zu oder von dieser Adresse kommen, um von der Policy betroffen zu sein. • Remote LAN - IP Adresse oder Subnet des entfernten LAN. Datenverkehr muss zu oder von dieser Adresse kommen, um von der Policy betroffen zu sein. • ESP - ESP (Encapsulating Security Payload) Ver- bzw. Entschlüsselungsprotokoll, das für die VPN Daten verwendet wird.
Buttons /Einstell-Knöpfe	
Save	Sichert für jede Policy die Änderungen.
Edit	Modifiziert die ausgewählte Policy.
Delete	Löscht die ausgewählte Policy.
Add Auto Policy	Fügt eine "Auto" Policy hinzu. Im Folgenden finden Sie weitere Details.
Add Manual Policy	Fügt eine "Manual" Policy hinzu. Im Folgenden finden Sie weitere Details.
VPN Status	Zeigt Details jedes laufenden VPN Tunnels (Verbindung) in einem Sub-Fenster an. Sie können auch das VPN Log-Buch ansehen.

VPN Auto Policy Bildschirm

Diese Bildschirmmaske wird angezeigt, wenn Sie den Knopf **Add Auto Policy** auf dem Bildschirm **VPN Policies** anklicken, oder wenn Sie eine Vorhandene Auto Policy ändern (Edit). Hier können Sie eine Auto Policy erstellen bzw. ändern.

Eine Auto VPN Policy nutzt das IKE Protokoll (Internet Key Protocol) zum Austausch und Einstellung der IPSec-SA Parameter. Deshalb ist es nicht notwendig, dass alle Einstellungen der beiden VPN Endpunkte 100%ig übereinstimmen. Einstellungen, die passend sein müssen, werden angezeigt.

VPN - Auto Policy

General Policy Name:
Remote VPN Endpoint
Address Type:
Address Data:
 NetBIOS Enable

Local LAN IP Address
IP address: . . .
Subnet Mask: . . .

Remote LAN IP Address
IP address: . . .
Subnet Mask: . . .

IKE Direction:
Exchange Mode:
Diffie-Hellman (DH) Group:
Local Identity Type:
Data:
Remote Identity Type:
Data:

SA Parameters Encryption:
Authentication:
Pre-shared Key:
SA Life Time: (Seconds)
 Enable PFS (Perfect Forward Security)

Abbildung 59: VPN Auto-Policy Bildschirmmaske

Daten – VPN Policy – Automatische Konfiguration

General / Allgemein	
Policy Name	Jede Policy hat einen eindeutigen Namen. Dieser Name ist der VPN Gegenstelle nicht bekannt. Er wird nur für Verwaltungszwecke verwendet
Remote VPN Endpoint	Falls der entfernte Endpunkt über eine dynamische IP-Adresse verfügt, wählen Sie "Dynamic IP address". Es ist keine Eingabe bei "Address Data" notwendig. Sonst wählen Sie die entsprechende Option (IP address oder Domain Name) und geben die Adresse des entfernten VPN Endpunktes ein. Bemerkung: Der entfernte VPN Endpunkt muss die VPN Gateway Adresse als "Remote VPN Endpoint" eintragen.
NetBIOS Enable	Wenn Sie es wünschen, dass auch NETBIOS Datenverkehr durch den VPN Tunnel geleitet wird, markieren Sie dieses Feld.
Iht lokales Netzwerk LAN	
Local LAN	Hier wird entschieden, welche PCs Ihres LAN von der Policy abgedeckt werden sollen. Für jede Auswahl müssen folgende Daten eingegeben werden: <ul style="list-style-type: none"> • Single address Geben Sie die IP Adresse in das Feld "IP address" ein. Typisch, falls Sie einen Server für Remote-Nutzer verfügbar machen wollen. • Subnet address Geben Sie die gewählte Network Mask in das Feld "Subnet Mask" ein. Der Entfernte VPN Endpunkt muss diese IP Adressen als "Remote" Adresse eingeben.
Entferntes LAN	
Remote LAN	Hier wird entschieden, welche PCs des entfernten LAN von der Policy abgedeckt werden sollen. Für jede Auswahl müssen folgende Daten eingegeben werden: <ul style="list-style-type: none"> • Single PC - no subnet Wählen Sie diese Option, falls auf der gegenstelle kein LAN, sondern nur ein einzelner PC angeschlossen ist. Es werden keine weiteren Daten benötigt. • Single address Geben Sie die IP Adresse in das Feld "IP address" ein. Dies muss eine Adresse des entfernten LANs sein. Dies ist die typische Einstellung, wenn Die einen entfernten Server in einem LAN erreichen wollen. • Subnet address geben Sie die IP-Adresse in das Feld "IP address" ein und die Netzwerk Maske in das Feld "Subnet Mask". Der Entfernte VPN Endpunkt muss diese IP Adressen als "Remote" Adresse eingeben.

IKE	
Direction	<p>Wählen Sie die Option</p> <ul style="list-style-type: none"> • Responder only – Nur eingehende Verbindungen sind zugelassen. Ausgehende werden verhindert. • Initiator and Responder – Eingehende und Ausgehende Verbindungen sind zulässig.
Exchange Mode	<p>IPSec verfügt über zwei Betriebsarten - "Main Mode" und "Aggressive Mode". Es wird derzeit der "Main Mode" unterstützt. Stellen Sie sicher, dass die gegenseitig ebenfalls auf "Main Mode" eingestellt ist.</p>
Diffie-Hellman (DH) Group	<p>Der Diffie-Hellman Algorithmus wird verwendet, wenn Schlüssel ausgetauscht werden. Hier wird die bit size number festgelegt. Dieser Wert muss mit der Gegenstelle übereinstimmen.</p>
Local Identity Type	<p>Wählen Sie die Option "Remote Identity Type" an der Gegenstelle.</p> <ul style="list-style-type: none"> • WAN IP Address – Ihre Internet IP Adresse. • Fully Qualified Domain Name - Ihr Domain name. • Fully Qualified User Name – Ihr Name, E-mail Adresse, oder andere ID.
Remote Identity Type	<p>Wählen Sie die Option "Local Identity Type" an der Gegenstelle.</p> <ul style="list-style-type: none"> • IP Address – Die Internet IP Adresse des entfernten VPN Endpunktes. • Fully Qualified Domain Name - Der Domain Name des entfernten VPN Endpunktes. • Fully Qualified User Name - Der Name, E-mail Adresse, oder eine andere ID des entfernten VPN Endpunktes.
Remote Identity Data	<p>Gene Sie die Daten für die Auswahl (oben) ein. (Falls Sie "IP Adresse" gewählt haben, sind keine weiteren Eingaben notwendig)</p>
SA Parameters	
Encryption	<p>Der verwendete Algorithmus für IKE und IPSec. Diese Einstellung muss mit der des entfernten VPN Endpunktes übereinstimmen.</p>
Authentication	<p>Authentication Algorithmus für IKE und IPSec. Diese Einstellung muss mit der des entfernten VPN Endpunktes übereinstimmen..</p>
Pre-shared Key	<p>Der Key muss bei beiden Stationen identisch eingegeben werden. Eine CA (Certificate Authority) wird nicht benötigt.</p>
SA Life Time	<p>Hier wird die Zeitspanne entschieden, für die der SA (Security Association) gültig ist. (Wenn notwendig, wird sie automatisch erneuert.) Mit einer kurzen Zeitspanne wird die Sicherheit erhöht, aber die Performance schlechter. Eine Stunde (3600 Sekunden) ist ein vernünftiger Wert.</p>

IPSec PFS (Perfect Forward Secrecy)	Falls eingestellt, wird der Key nach bestimmten Intervallen automatisch geändert. Falls ein Schlüssel gebrochen sein sollte, behalten die Anderen Ihren Wert. Sie sind nicht voneinander abgeleitet. Die Einstellung gilt für IKE und IPSec SA. Bei der Konfiguration des entfernten VPN Punktes, müssen Sie ggf. Die so genannte "Key Group" definieren. Die "Key Group" entspricht der "DH Group" in der IKE Sektion.
--	--

VPN – Manual Policy Screen

Diese Bildschirmmaske wird angezeigt, wenn Sie in **VPN Policies** das **Add Manual Policy** Feld anklicken, oder wenn Sie eine vorhandene Policy verändern. Eine „Manual“ VPN Policy erwartet, dass an beiden VPN Endpunkten alle Daten eingegeben werden. Die beiden Endpunkte ermitteln keine Werte automatisch.

Abbildung 60: VPN Policy Bildschirm – Manuelle Eingaben

Daten – VPN Policy Bildschirmmaske – Manuelle Eingaben

General / Allgemein	
Policy Name	Jede Policy hat einen eindeutigen Namen. Dieser Name ist der VPN Gegenstelle nicht bekannt. Er wird nur für Verwaltungszwecke verwendet.
Remote VPN Endpoint	Bestimmen Sie die richtige Option (IP Adresse oder Domain Name) und geben Sie die Adresse des entfernten VPN Endpunktes ein. Bemerkung: Der entfernte VPN Endpunkt muß diese VPN Gateway Adresse als seine "Remote VPN Endpoint" gespeichert haben.
NETBIOS Enable	Wenn Sie es wünschen, dass auch NETBIOS Datenverkehr durch den VPN Tunnel geleitet wird, markieren Sie dieses Feld.

Local LAN / Ihr lokales Netzwerk	
Local LAN	<p>Hier wird entschieden, welche PCs Ihres LAN von der Policy abgedeckt werden sollen. Für jede Auswahl müssen folgende Daten eingegeben werden:</p> <ul style="list-style-type: none"> • Single address Geben Sie die IP Adresse in das Feld "IP address" ein. Typisch, falls Sie einen Server für Remote-Nutzer verfügbar machen wollen. • Subnet address Geben Sie die gewählte Network Mask in das Feld "Subnet Mask" ein. <p>Der Entfernte VPN Endpunkt muss diese IP Adressen als "Remote" Adresse eingeben.</p>
Remote LAN / Das Entfernte LAN	
Remote LAN	<p>Hier wird entschieden, welche PCs des entfernten LAN von der Policy abgedeckt werden sollen. Für jede Auswahl müssen folgende Daten eingegeben werden:</p> <ul style="list-style-type: none"> • Single PC - no subnet Wählen Sie diese Option, falls auf der gegenstelle kein LAN, sondern nur ein einzelner PC angeschlossen ist. Es werden keine weiteren Daten benötigt. • Single address Geben Sie die IP Adresse in das Feld "IP address" ein. Dies muss eine Adresse des entfernten LANs sein. Dies ist die typische Einstellung, wenn Sie einen entfernten Server in einem LAN erreichen wollen. • Subnet address geben Sie die IP-Adresse in das Feld "IP address" ein und die Netzwerk Maske in das Feld "Subnet Mask". <p>Der Entfernte VPN Endpunkt muss diese IP Adressen als "Remote" Adresse eingeben.</p>
ESP Konfiguration	
SPI	<p>Geben Sie die erforderlichen SPIs ein. Jede Policy benötigt eindeutige SPIs. Diese Einstellungen müssen mit denen des entfernten VPN Endpunktes 100% übereinstimmen. Bedenken Sie dass die "in" Werte hier den "out" Werten des entfernten VPN Endpunktes entsprechen müssen und umgekehrt.</p>
Encryption	<p>Wählen Sie den entsprechenden Verschlüsselungs-Algorithmus und geben Sie die Schlüssel ein.</p> <ul style="list-style-type: none"> • DES: Der Schlüssel muß 8 (acht) ASCII Zeichen (16 Hex Zeichen) lang sein. • 3DES: Der Schlüssel muß 24 (vierundzwanzig) ASCII Zeichen (48 Hex Zeichen) lang sein.
Authentication	<p>Wählen Sie den Authentication Algorithmus und geben Sie dazu den Schlüssel ein.</p> <ul style="list-style-type: none"> • MD5: Der Schlüssel muß 16 (sechzehn) ASCII Zeichen (32 Hex Zeichen) lang sein. • SHA-1: Der Schlüssel muß 20 (zwanzig) ASCII Zeichen (40 Hex Zeichen) lang sein.

VPN Status Bildschirm

Dieser Bildschirm wird angezeigt, wenn Sie im **VPN Policies Bildschirm** oder dem **Status Bildschirm** den Button **VPN Log** anklicken.

Hiermit können Sie Detailinformationen zu jedem einzelnen laufenden VPN Tunnel erfahren. Besteht keine Verbindung, bleiben die Felder Leer.

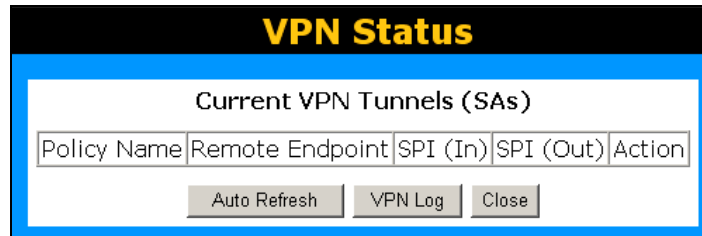


Abbildung 61: VPN Status Bildschirm

Daten – VPN Status Bildschirm

<p>Tunnel Table</p>	<p>Diese Tabelle enthält die folgenden Informationen über jede laufende Verbindung.</p> <ul style="list-style-type: none"> • Policy Name – Der Name der Policy. Wenn eine Policy erstellt wird, muß sie zur Identifikation einen eindeutigen Namen erhalten. • Remote Endpoint – Die Adresse des entfernten VPN Endpunktes. • SPI (In) – Indexnummer zur Identifikation der eingehenden Verbindung. "Auto" policies erstellt diesen Index automatisch. Bei "Manual" policies muß der SPI während der Konfiguration eingegeben werden. • SPI (Out) - Indexnummer zur Identifikation der ausgehenden Verbindung. "Auto" policies erstellt diesen Index automatisch. Bei "Manual" policies muß der SPI während der Konfiguration eingegeben werden. • Action – Hiermit können Sie die laufende VPN-Verbindung abbrechen (terminate).
<p>Buttons / Schaltknöpfe</p>	
<p>Auto Refresh</p>	<p>Mit "auto-refresh" entscheiden Sie, dass dieser Bildschirm automatisch aktualisiert wird. Dies wird mit Hilfe des "status bar" am unteren Rand des Schirms angezeigt.</p>
<p>VPN Log</p>	<p>Hiermit schalten Sie um zum "VPN log" Bildschirm. Dieser zeigt die Details einer jeden VPN Verbindung an.</p>

Kapitel 7

Weiterführende Verwaltungsfunktionen

Dieses Kapitel erklärt die verfügbaren Einstellungen im Abschnitt "Verwaltung" des Menüs.

Überblick

Normalerweise ist es nicht notwendig, diese Bildschirme zu benutzen oder Einstellungen zu ändern. Diese Bildschirme und Einstellungen werden nur bereitgestellt, um nicht übliche Situationen zu behandeln oder zusätzliche Optionen für fortgeschrittene Benutzer zu liefern.

Die verfügbaren Einstellungen und Merkmale sind:

PC Database	Dies ist die Liste von PCs, wenn Sie den "DMZ PC" oder einen "virtuellen Server" wählen. Diese Datenbank wird automatisch erstellt, aber Sie können Einträge für PCs hinzufügen und löschen, die eine feste (statische) IP-Adresse verwenden.
Config File	Sichern Sie die Konfigurationsdatei für den WLAN ADSL Router oder stellen Sie sie wieder her. Diese Datei enthält alle Konfigurationsdaten.
Logging & Email	Ansehen und löscher aller Protokolle. Konfiguriert E-Mailing von Log-Files und Alarmen.
Diagnostics	Führen Sie ein Ping oder DNS Lookup durch.
Remote Admin	Erlauben Sie die Fernadministration.
Routing	Wird nur benötigt, wenn Ihr LAN auch andere Router oder Gateway verwendet.
Upgrade Firmware	Upgrade der Firmware (Software) innerhalb Ihres Wireless ADSL Router.

PC-Datenbank

Die PC-Datenbank wird jedes Mal gebraucht, wenn Sie einen PC (z.B. für den "DMZ" PC) auswählen müssen.

- Es vermeidet die Notwendigkeit, mit IP-Adressen zu arbeiten.
- Auch müssen Sie keine festen IP-Adressen auf Ihrem LAN verwenden.

Jedoch, wenn Sie eine feste IP-Adresse auf einigen Geräten in Ihrem LAN verwenden, sollten Sie Details von diesen Geräten in die PC-Datenbank mit Hilfe des PC-Datenbankbildschirms eingeben.

PC-Datenbankbildschirm

Ein Beispiel-PC-Datenbankbildschirm wird unten gezeigt.

PC Database

DHCP Clients are automatically added and updated.
If not listed, try restarting the PC.

PCs using a Fixed IP address can be added and deleted below.

Known PCs
IngridLin 192.168.0.2 (LAN) 00:20:ED:29:08:E4 (DHCP)

< Add

Name:

IP Address: . . .

Delete

Refresh Generate Report

Advanced Administration Help

Abbildung 62: PC-Datenbank

- PCs, die "DHCP Klienten" sind, werden automatisch der Datenbank hinzugefügt und falls erforderlich aktualisiert.
- Standardmäßig wirken Nicht-Serverversionen von Windows als "DHCP Klienten";
- Der WLAN ADSL Router verwendet die "Hardwareadresse", um jeden PC, nicht den Namen oder die IP-Adresse zu identifizieren. Die "Hardwareadresse" kann man nur ändern, wenn Sie die Netzwerkkarte des PCs ändern.
- Dieses System bedeutet, dass Sie keine festen (statischen) IP-Adressen auf Ihrem LAN verwenden müssen. Jedoch können Sie PCs mit Hilfe von festen (statischen) IP-Adressen zur PC-Datenbank hinzufügen, wenn erforderlich.

Daten - PC-Datenbankbildschirm

Known PCs	Dies listet alle gegenwärtigen Eingänge auf. Angezeigte Daten sind Name (IP-Adresse) Art. „TYPE“ zeigt an, ob der PC an das LAN angeschlossen ist.
Name	Wenn Sie der Liste einen neuen PC hinzuzufügen, geben Sie seinen Namen hier ein. Er ist am besten, wenn dies zum "Hostnamen des PCs" passt.
IP Address	Die IP-Adresse des PC. An den PC wird ein "PING" gesandt, um seine Hardwareadresse zu bestimmen. Wenn der PC nicht verfügbar (nicht verbunden oder nicht eingeschaltet) ist, wird er nicht hinzugefügt.
Buttons	
Add	Dies fügt der Liste den neuen PC hinzu. An den PC wird ein "PING" gesandt, um seine Hardwareadresse zu bestimmen. Wenn der PC nicht verfügbar (nicht verbunden oder nicht eingeschaltet) ist, wird er nicht hinzugefügt.
Delete	Löschen Sie den gewählten PC von der Liste. Dies sollte in 2 Situationen getan werden: <ul style="list-style-type: none">• Der PC ist aus Ihrem LAN entfernt worden.• Der Eintrag ist falsch.
Refresh	Aktualisieren Sie den Bildschirm.
Generate Report	Zeigt eine schreibgeschützte Liste an, die volle Details von allen Einträgen in der PC-Datenbank zeigt.
Advanced Administration	Betrachten Sie die erweiterte Version des PC-Datenbankbildschirms - PC-Datenbank (Verwaltung).

Erweiterte PC-Datenbank

Dieser Bildschirm wird angezeigt, wenn der Knopf „Advanced Administration“ auf der PC-Datenbank angeklickt wird. Er liefert mehr Einstellungsmöglichkeiten als der Standard-PC-Datenbankbildschirm.

Abbildung 63: PC-Datenbank (Verwaltung)

Daten – Erweiterte PC-Datenbank

Known PCs	Dies listet alle gegenwärtigen Eingänge auf. Angezeigte Daten sind Name (IP-Adresse) Art. „TYPE“ zeigt an, ob der PC an das LAN angeschlossen ist.
PC Properties	
Name	Wenn Sie der Liste einen neuen PC hinzuzufügen, geben Sie seinen Namen hier ein. Er ist am besten, wenn dies zum "Hostnamen des PCs" passt.
IP Address	Die IP-Adresse des PC. An den PC wird ein "PING" gesandt, um seine Hardwareadresse zu bestimmen. Wenn der PC nicht verfügbar (nicht verbunden oder nicht eingeschaltet) ist, wird er nicht hinzugefügt.

MAC Address	<p>Wählen Sie die entsprechende Option</p> <ul style="list-style-type: none"> • Automatic discovery - wählen dieses, um den WLAN ADSL Router sich an den PC wenden zu lassen um seine MAC-Adresse zu finden. Dies ist nur möglich, wenn der PC mit dem LAN verbunden und eingeschaltet ist. • MAC address is – geben Sie die Pakete ein. Die Pakete wird auch die "Hardware-Adresse", "physische Adresse" oder "Netzadapteradresse" genannt. Der WLAN ADSL Router verwendet diese, um eine eindeutige Kennzeichnung für jeden PC zu liefern. Wegen diesem kann die Pakete nicht leer sein.
Buttons	
Add as New Entry	Fügen Sie der Liste einen neuen PC hinzu. Wenn "automatische Entdeckung" (für MAC-Adresse) gewählt wird, wird an den PC ein "PING" gesandt, um seine Hardwareadresse zu bestimmen. Dazu muß der PC mit dem LAN verbunden und eingeschaltet sein.
Update Selected PC	Aktualisieren Sie (modifizieren) den gewählten PC mit Hilfe der Daten im Kasten "Properties".
Clear Form	Löscht die "Properties" box.
Refresh	Aktualisieren Sie den Bildschirm.
Generate Report	Zeigt eine schreibgeschützte Liste an, die volle Details von allen Einträgen in der PC-Datenbank zeigt.
Standard Screen	Kicken Sie, um zum Standard Schirm PC Database zurückzukehren.

Config Datei

Dieses Merkmal erlaubt Ihnen, die gegenwärtigen Einstellungen vom WLAN ADSL Router herunterzuladen und sie in eine Datei auf Ihren PC zu sichern.

Sie können eine zuvor heruntergeladene Konfigurationsdatei im WLAN ADSL Router dadurch wiederherstellen, dass Sie sie auf den WLAN ADSL Router hochladen.

Dieser Bildschirm erlaubt Ihnen auch, den WLAN ADSL Router in den Auslieferungszustand zurück zu versetzen. Vorgenommene Änderungen werden dabei gelöscht.

Ein Beispielbildschirm wird hier gezeigt.

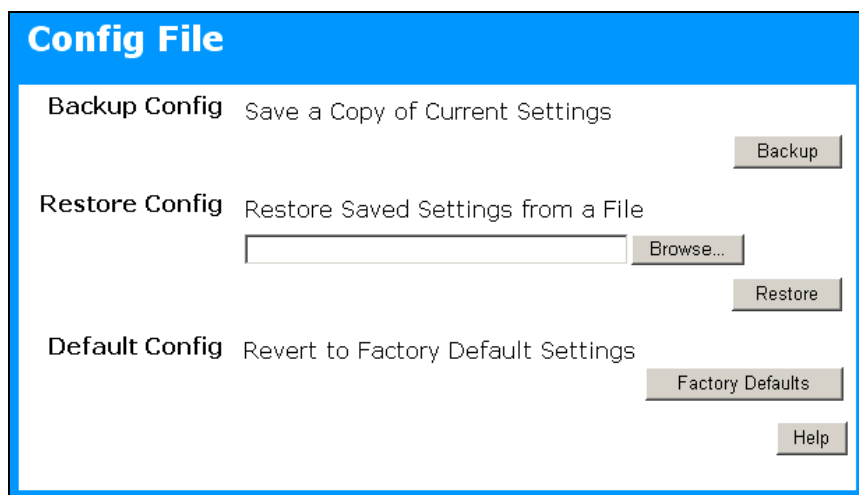


Abbildung 64: Konfigurationsbildschirm

Daten - Config Bildschirm

Backup Config	Hiermit können Sie eine Kopie der gegenwärtigen Konfiguration auf Ihren PC zu ablegen.
Restore Config	Dies erlaubt Ihnen, eine zuvor gesicherte Konfigurationsdatei im WLAN ADSL Router wiederherzustellen. Klicken Sie auf Browse um die Datei zu finden. Und dann auf Restore um die Konfigurationsdatei hochzuladen. WARNUNG ! Dies zerstört (überschreibt) alle vorhandenen Einstellungen.
Default Config	Den Knopf Factory Defaults anklicken, um den Auslieferungszustand wieder herzustellen.. WARNUNG ! Dies löscht alle vorhandenen Einstellungen.

Logs / Logbücher / Protokolle

Die Protokolle zeichnen verschiedene Arten der Aktivität auf dem WLAN ADSL Router auf. Diese Daten sind für Fehlerbehebung nützlich, aber, alle Protokolle zu generiert erzeugt eine große Datenmenge und beeinflusst die Leistung negativ.

Da nur ein beschränktes Maß an Protokolldaten im WLAN ADSL Router gespeichert werden kann, können Protokolldaten Ihrem PC auch per Email geschickt werden. Benutzen Sie den E-Mail-Bildschirm, um dieses Merkmal zu konfigurieren.

Logs

Logs Current time: 2002-09-08 16:22:34

```

Sun, 2002-09-08 13:05:46 - Administrator logi
Sun, 2002-09-08 13:00:00 - Router start up
Sun, 2002-09-08 13:17:59 - Administrator logi
Sun, 2002-09-08 13:22:53 - Administrator logi
Sun, 2002-09-08 13:35:42 - Administrator logi
Sun, 2002-09-08 13:44:30 - Administrator logi
Sun, 2002-09-08 13:51:08 - Administrator logi
Sun, 2002-09-08 14:08:36 - Administrator logi
Sun, 2002-09-08 14:12:06 - Administrator logi
Sun, 2002-09-08 14:22:03 - Administrator logi
Sun, 2002-09-08 14:36:42 - Administrator logi
Sun, 2002-09-08 15:15:24 - Administrator logi
Sun, 2002-09-08 15:21:30 - Administrator logi
Sun, 2002-09-08 16:14:22 - Administrator logi
    
```

Refresh Clear Log Send Log

Include in Log

- Attempted access to blocked sites
- Connections to the Web-based interface of this Router
- Router operation (start up, get time etc)
- Known DoS attacks and Port Scans

Syslog

- Disable
- Broadcast on LAN
- Send to this Syslog Server: [] . [] . [] . []

Save Cancel Help

Abbildung 65: Protokoll-Bildschirm

Logs	
Current Time	Die gegenwärtige Zeit des WLAN ADSL Router
Log Data	Gegenwärtige Protokolldaten sind in dieser Tabelle
Buttons	Es gibt drei (3) Knöpfe <ul style="list-style-type: none"> • Refresh - aktualisiert die Protokolldaten. • Clear Log - Löscht das Protokoll und start es neu. Dies hilft beim lesen neuer Nachrichten. • Send Log - schickt das Protokoll sofort per Email. Dies funktioniert nur, wenn der E-Mail-Bildschirm konfiguriert worden ist.

Logs	
Include in Log (Checkboxes)	<p>Entscheiden Sie hiermit, welche Ereignisse aufgezeichnet werden sollen. Wenn Sie alles aufzeichnen, wird die Log-Datei sehr groß. Schließen Sie deshalb aus, was nicht wirklich wichtig ist.</p> <ul style="list-style-type: none"> • Attempted access to blocked sites – Zeichne blockierte Internetzugriffe auf. • Connections to the Web-based interface of this Router – Zeichnet Zugriff zu diesen Router auf, statt durch diesen Router. • Router operation – Weiter Routeraktionen werden aufgezeichnet • Known DoS attacks and Port Scans - Denial of Service attacks, und port scans werden aufgezeichnet.
Syslog	
Disable	Daten werden nicht an einen Syslog Server gesandt.
Broadcast on LAN	Die Syslog Daten werden als Broadcast, anstatt an einen bestimmten Syslog Server gesandt. Verwenden Sie diese Einstellung, wenn Ihr Syslog Server keine feste IP-Adresse hat.
Syslog	Wenn Ihr Syslog Server eine feste IP-Adresse hat, wählen Sie diese Option und geben Sie die IP-Adresse von Ihrem Syslog Server.hier ein.

E-Mail

Dieser Bildschirm erlaubt Ihnen, Protokolle und Alarme per Email zu schicken. Ein Beispielbildschirm wird hier gezeigt.

Abbildung 66: E-Mail-Bildschirm

Daten - E-Mail-Bildschirm

E-Mail Notification	
Turn E-mail Notification on	Wenn aktiviert, muss die E-Mail-Adressinformation (unten) geliefert werden.
Send to this E-mail address	Geben Sie die E-mail Adresse an, an die das Protokoll gesendet werden soll. Dies ist auch die E-Mail Absender Adresse.
Outgoing (SMTP) Mail Server	Geben Sie die Adresse oder IP Adress des SMTP (Simple Mail Transport Protocol) Servers an, den Sie für ausgehende Mail verwenden.
My SMTP Mail Server requires authentication	Um Spammer zu blockieren, verlangen viele SMTP Postserver, dass Sie sich anmelden, um Post zu senden. In diesem Fall geben Sie die Anmeldungsinformation (Benutzernamen und Kennwort) in die Felder unten ein.
User Name	Wenn auf Sie zutrifft: "mein SMTP Postserver erfordert Bestätigung", (siehe oben), geben Sie den zu Ihrem SMTP Server erforderlichen Benutzernamen ein.

Password	Wenn auf Sie zutrifft: "mein SMTP Postserver erfordert Bestätigung", (siehe oben), geben Sie das zu Ihrem SMTP Server erforderlichen Passwort ein.
E-mail Alerts	
Send E-mail alerts immediately	<p>Der Broadband ADSL Router kann Sie sofort alarmieren, wenn er ein wichtige Sicherheitsbedrohung entdeckt:</p> <ul style="list-style-type: none"> • Ein Hacker Angriff auf Ihre IP Adresse • A Computer aus dem Internet scannt Ihre IP Adresse nach offenen Ports • Jemand in Ihrem LAN versucht, eine Blockierte Website zu besuchen.
E-mail Logs	
Send Logs	<p>Wählen Sie die Option, um Logdateien per E-mail zu versenden.</p> <ul style="list-style-type: none"> • Never (default) – Logs werden nicht geschickt. • When log is full – Logs werden geschickt, wenn der Log-Speicher voll ist.. • Hourly, Daily, Weekly... – Die Logdatei wird in Anhängigkeit des zeitintervalls geschickt. <ul style="list-style-type: none"> • Bei Daily wird der Log zu der angegebenen Zeit verschickt. • Bei Weekly wird die Log-Datei einmal in der Woche an dem spezifizierten Tag und Uhrzeit verschickt.. <p>Achtung: Falls die Log-Datei schon vor dem Termin voll ist, wird sie automatisch verschickt..</p>

Netzwerkdiagnose / Fehlersuche

Dieser Bildschirm erlaubt Ihnen, ein "PING" oder eine "DNS Suche" durchzuführen. Diese Aktivitäten können beim Lösen von Netzproblemen nützlich sein. Ein Beispiel-Netzdiagnosebildschirm wird hier gezeigt.

Abbildung 67: Netzdiagnosebildschirm

Daten - Netzwerkd Diagnosebildschirm

Ping	
Ping this IP Address	Geben Sie diejenige IP-Adresse ein, die Sie "Anpingen" wollen. Die IP-Adresse kann im LAN, oder im Internet sein. Wenn die Adresse sich im Internet befindet und gegenwärtig keine Verbindung existiert, bekommen Sie einen "Time-Out" Fehler. In diesem Fall warten Sie einige Sekunden und versuchen Sie es nochmals.
Ping Button	Nachdem Sie die IP Adresse eingegben haben, klicken Sie diesen Knopf, um die "Ping" Prozedur zu starten. Das Ergebnis finden Sie unter Ping Results .
DNS Lookup	
Internet name	Geben Sie den Domänennamen oder URL ein, für den Sie eine DNS (Domänennamensserver) Suche wollen. Wenn gegenwärtig keine Verbindung zum Internet existiert, bekommen Sie einen "Time-Out" Fehler. In diesem Fall warten Sie einige Sekunden und versuchen Sie es erneut.
Lookup Button	Nach dem Eingeben der Domänennamens/URLs klicken Sie diesen Knopf, um mit dem "DNS Suche" Verfahren zu beginnen.
Routing	
Display	Klicken Sie diesen Knopf, um die interne Routingtabelle anzuzeigen. Diese Information kann vom Support verwendet werden.

Remote / Fern-Administration

Wenn aktiviert, erlaubt Ihnen dieses Feature, den WLAN ADSL Router über das Internet zu verwalten.

Abbildung 68: Remote Administration Bildschirm

Daten - Remote Administration Bildschirm

Remote Administration	
Enable Remote Management	Hier entscheiden Sie, ob Fern-Administration über das Internet möglich sein soll.
Current IP Address	Dies ist die IP-Adresse, die Sie verwenden wollen, wenn Sie auf dieses Gerät über das Internet zugreifen. Sehen Sie Details und ein Beispiel unten.
Port Number	Geben Sie eine Portnummer zwischen 1 und 65535 ein. Default für HTTP (Web) ist Port 80. Allerdings können Sie dann nicht mehr einen Web "Virtual Server" in Ihrem LAN verwenden. Es wird empfohlen, stattdessen lieber den Port 8080 zu verwenden. Die Portnummer muß in Ihrem Browser spezifiziert werden, wenn Sie sich verbinden wollen. Weitere Details siehe unten.
Access Permission	
Allow Remote Access	Wählen Sie die gewünschte Option. <ul style="list-style-type: none"> • Everyone – ermöglicht den Zugang durch jeden im Internet. • Only This Computer - ermöglichen Zugang durch nur eine bestimmte IP-Adresse. Geben Sie die IP-Adresse ein. • IP Address Range - ermöglicht Zugang von einem Bereich von IP-Adressen im Internet. Geben Sie einen Anfang und End-IP-Adresse ein, um den erlaubten Bereich zu definieren. • Für Sicherheit sollten nur wenige externen IP-Adressen Zugang haben.

Sich von einem entfernten PC durch das Internet einwählen

1. Stellen Sie sicher, dass Ihre Internetverbindung hergestellt ist, und starten Sie Ihren Web-Browser.
2. Im Adressfeld geben Sie ein: "HTTP: //" folgte von der Internet-IP-Adresse vom WLAN ADSL Router. Wenn die Portnummer nicht 80 ist, ist auch die Portnummer erforderlich. (Nach der IP-Adresse, Eingabe, folgte ": " von der Portnummer.)

z.B.

HTTP: // 123.123.123.123:8080

Dieses Beispiel nimmt an, dass die WAN IP-Adresse 123.123.123.123 ist, und die Portnummer 8080. Sie werden nun aufgefordert Anmeldenamen und Kennwort für dieses Gerät einzugeben.

Routing

Überblick

- Wenn Sie keine anderen Router oder Gateways auf Ihrem LAN haben, können Sie die "Routing" Seite völlig ignorieren.
- Wenn der WLAN ADSL Router nur als Gateway für das lokale LAN-Segment wirkt, ignorieren Sie die "Routing" Seite, selbst wenn Ihr LAN andere Router hat.
- Wenn Ihr LAN einen Standard Router (z.B. Cisco) in Ihrem LAN hat und der WLAN ADSL Router als Gateway für alle LAN-Segmente wirken soll, ermöglichen Sie RIP (Routingsinformationsprotokoll) und ignorieren Sie die statische Routingstabelle.
- Wenn Ihr LAN andere Gateways und Router hat und Sie kontrollieren möchten, welche LAN-Segmente jedes Gateway verwenden, schalten Sie RIP aus. Konfigurieren Sie die statische Routingstabelle stattdessen. (Sie müssen auch die anderen Router konfigurieren.)
- Beim Benutzen des Windows 2000 Datenzentrumservers als einen SoftwareRouter ermöglichen Sie RIP auf dem WLAN ADSL Router und stellen Sie sicher, dass die folgenden Windows 2000 Einstellungen getan wurden.
- Open Routing and Remote Access
- Im Konsolen- Tree, wählen Sie „Routing“ und d“Remote Access“, [Servernamen], IP Routing, RIP.
- In "Details" klicken Sie auf die Schnittstelle, die Sie für RIP Version 2 konfigurieren wollen, und klicken Sie dann "Eigenschaften".
- IM TAB "allgemein" setzen Sie *Outgoing packet protocol* auf "RIP version 2 broadcast" und *Incoming packet protocol* auf "RIP version 1 and 2"

Routingbildschirm

Auf die Routingtabelle wird vom Routing Link aus dem Administration zugegriffen.

Benutzen dieses Bildschirms

Im Allgemeinen verwenden Sie entweder RIP oder die Static Routing Table, wie oben erklärt. Es ist jedoch möglich, beide Methoden simultan zu verwenden.

Statische Routingtabelle

- Wenn RIP nicht verwendet wird, wird ein Eintrag in der Routingtabelle für jedes LAN-Segment auf Ihrem Netz außer dem Segment benötigt, woran dieses Gerät angeschlossen ist.
- Die anderen Router müssen auch konfiguriert werden. Sehen Sie auch unter *Fehler! Verweisquelle konnte nicht gefunden werden.* diesem Kapitel für weitere Details.

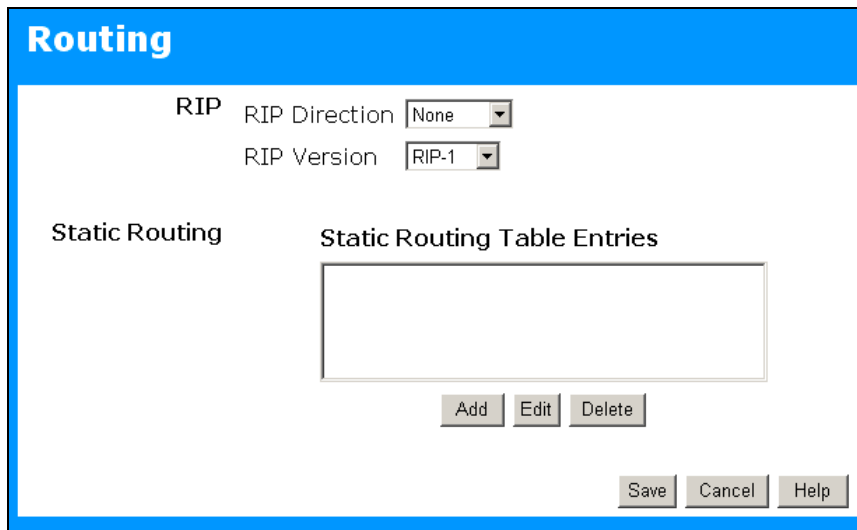


Abbildung 69: Routingbildschirm

Daten – Routing Screen

RIP	
RIP Direction	Wählen Sie die gewünschte RIP-Richtung.
RIP Version	Wählen Sie die RIP-Version für den Server.
Static Routing	
Static Routing Table Entries	<ul style="list-style-type: none"> • Diese Liste zeigt alle Einträge in der Routingtabelle. • Dieser Bereich zeigt Details in der Liste. • Ändern Sie erforderlichen Einträge und klicken Sie dann den "Editieren" Knopf, um die Änderungen zu sichern.
Buttons	
Add	Fügen Sie der statische Routingtabelle einen neuen Eingang mit Hilfe der im "Properties" Bereich gezeigten Daten hinzu. Der in der Liste gewählte Eintrag wird ignoriert und hat keine Wirkung.
Edit	Aktualisieren Sie den gegenwärtigen statische Routingtabelleneintrag mit Hilfe der in der Tabelle gezeigten Daten.
Delete	Löschen Sie den gegenwärtigen statische Routingtabelleneintrag
Save	Sichern Sie die RIP Settings. Dies hat keine Wirkung auf die statische Routingtabelle.

Das Konfigurieren von anderen Routern in Ihrem LAN

Es ist wesentlich, dass alle IP Pakete für Geräte, die nicht im LAN sind, an den WLAN ADSL Router weitergereicht werden, so dass sie an das externe LAN, WAN oder das Internet weitergeleitet werden können. Um dieses zu erreichen, muss das LAN konfiguriert werden, um den WLAN ADSL Router als die Default Route oder das Default Gateway zu verwenden.

Lokaler Router

Der lokale Router ist der auf demselben LAN-Segment wie der WLAN ADSL Router angebrachte Router. Dieser Router erfordert, dass die default Route der WLAN ADSL Router selbst ist. Normalerweise haben Router einen speziellen Eintrag für die default Route. Er sollte wie folgt konfiguriert werden.

Destination IP Address	Normalerweise 0.0.0.0, prüfen Sie Ihre Router Dokumentation.
Network Mask	Normalerweise 0.0.0.0, prüfen Sie Ihre Router Dokumentation.
Gateway IP Address	Die IP-Adresse vom WLAN ADSL Router.
Metric	1

Andere Router auf dem lokalen LAN

Andere Router im lokalen LAN müssen den lokalen Router des WLAN ADSL Routers als die default Route verwenden. Die Einträge werden wie die des lokalen Routers und des WLAN ADSL Routers sein mit Ausnahme der Gateway-IP-Adresse.

- Für einen Router mit einer direkten Verbindung zum lokalen Router des WLAN ADSL Routers ist die Gateway-IP-Adresse die Adresse vom lokalen Router des WLAN ADSL Routers.
- Für Router, die vor dem Erreichen vom lokalen Router des WLAN ADSL Routers Pakete an einen anderen Router weiterleiten müssen, ist die Gateway-IP-Adresse die Adresse des MittelRouters.

Statische Routing - Beispiel

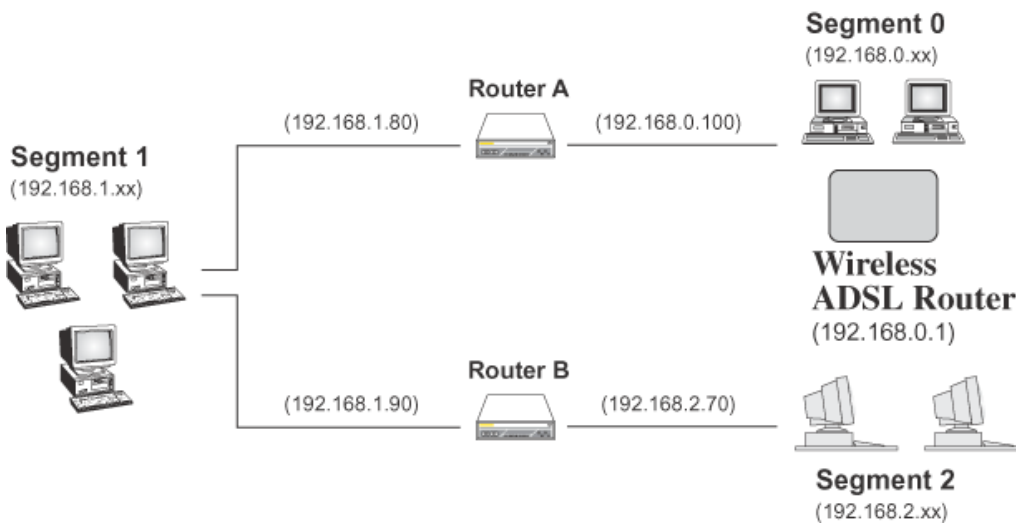


Abbildung 70: Routingbeispiel

Für die Routingtabelle des WLAN ADSL Routers

Für das oben gezeigte LAN mit 2 Routern und 3 LAN-Segmenten, erfordert der WLAN ADSL Router 2 Einträge wie folgt.

Entry 1 (Segment 1)	
Destination IP Address	192.168.1.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100 (lokale Router des WLAN ADSL Routers)
Metric	2
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0 (Standard Class C)

Gateway IP Address	192.168.0.100
Metric	3

Default Route für Router A

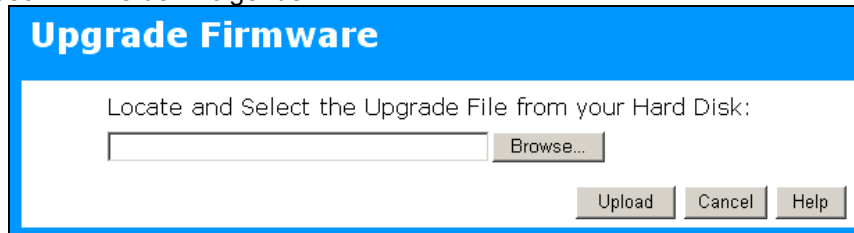
Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.0.1 (IP-Adresse des WLAN ADSL Routers)

Default Route für Router B

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 der lokale Router des WLAN ADSL Routers)

Firmware Update

Die Firmware (Software) im WLAN ADSL Router kann mit Hilfe Ihres Web-Browsers aktualisiert werden. Sie müssen die Update-Datei zuerst herunterladen, dann Firmware Update im Admin-Menü wählen. Sie sehen einen Bildschirm wie den Folgenden.



Upgrade Firmware

Locate and Select the Upgrade File from your Hard Disk:

Browse...

Upload Cancel Help

Abbildung 71: Firmware Update / Upgrade

Update durchführen:

1. Klicken auf BROWSE und navigieren Sie dann zur Upgrade Datei.
2. Wählen Sie die die UPGRADE Datei. Ihr Name erscheint im Feld UPGRADE.
3. Klicken Sie den Knopf UPLOAD, um den Vorgang zu beginnen.



Note! Der WLAN ADSL Router ist während des Upgradeprozesses nicht verfügbar und muss neu starten, wenn der Vorgang beendet ist. Verbindungen zu oder durch den WLAN ADSL Router gehen verloren.

Kapitel 8

Modemmodus

Dieses Kapitel erklärt Konfiguration und Betrieb, wenn sich das Gerät im Modus "Modem" oder "Brücke" befindet.

Überblick

Es gibt zwei Modi, die auf dem Modusbildschirm verfügbar sind.

- Router - sowohl der ADSL Modem als auch die Routermerkmale sind betriebsbereit. In diesem Modus kann dieses Gerät gemeinsamer Internetzugang für alle Ihre LAN Benutzer sein. Es stellt standardmäßig einen DHCP Server dar, und liefert allen WLAN und LAN-Benutzern eine IP-Adresse und verwandte Information..
- Modem - nur der ADSL Modembestandteil ist betriebsbereit. Alle Routermerkmale sind ausgeschaltet. Dieses Gerät ist "transparent" - es führt keine Operationen aus und macht keine Änderungen am Netzverkehr. Sie müssen einen DHCP Server auf Ihrem LAN haben, um den WLAN Clients IP-Adressen mit Hilfe dieses Accesspoints zu liefern.

Dieses Kapitel beschreibt Operation, im Modemmodus, auch Brückenmodus genannt

Leitungsverbindungen

Wenn dieses Gerät in Modemmodus neu startet, ändert sich die IP-Adresse nicht. Der DHCP Server ist ausgeschaltet. Jedoch bewahrt Ihr PC die vom DHCP Server gelieferte IP-Adresse, so dass die Verbindung automatisch wieder hergestellt wird. Sie müssen dann sicherstellen, dass die IP-Adresse von diesem Modem für Ihr LAN geeignet ist.

- Sie müssen einen DHCP Server auf Ihrem LAN haben, um den WLAN Clients IP-Adressen mit Hilfe dieses Accesspoints zu liefern.
- Dieses Modem/AP muss in Ihrem LAN ein gültiges Gerät sein, um Leitungsverbindungen zu ermöglichen. Sie müssen eine (feste) IP-Adresse zuteilen, die innerhalb des auf Ihrem LAN verwendeten Adressbereichs, aber nicht innerhalb des von Ihrem DHCP Server verwendeten Adressbereichs ist.

Wenn Sie sich in Zukunft mit dem Internet verbinden, tun es wie immer, jedoch mit der IP-Adresse, die Sie zuteilt haben.

1. Starten Sie Ihren Web-Browser.
2. Im Adresskasten tippen Sie ein "HTTP: //" und die gegenwärtige IP-Adresse, vom WLAN ADSL Modem, wie in diesem Beispiel, welches die default IP-Adresse des WLAN ADSL Modems verwendet:
HTTP: // 192.168.0.1
3. Wenn Sie zur Eingabe von Benutzernamen und Kennwort aufgefordert werden, geben Sie ein: adm i n für den Benutzernamen und das gegenwärtige Kennwort, wie auf dem Kennwortbildschirm gesetzt. (Das Kennwort ist das Gleiche ohne Rücksicht auf den Modus.)

Home Screen

Im Modemmodus, sieht der „Home“-Bildschirm wie das Beispiel unten aus.

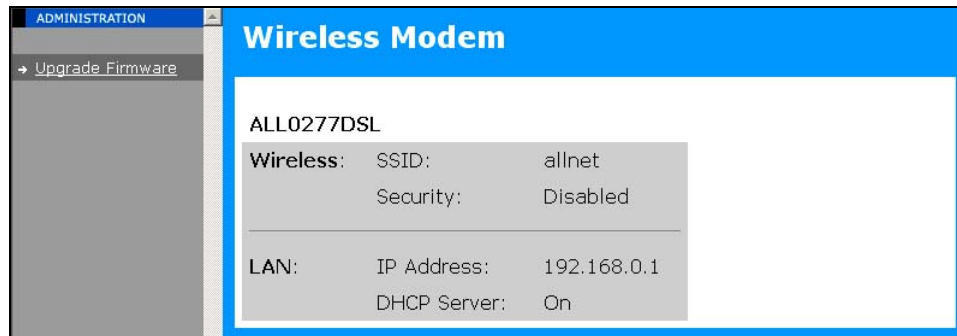


Abbildung 72: Home Screen – Modemmodus

Bedenken Sie, dass das Menü sich geändert hat, viele der Optionen in Routermodus sind nicht verfügbar. Die verfügbaren Bildschirme sind:

- Modus - Änderung zurück zu Routermodus, wenn gewünscht.
- LAN - setze IP-Adresse, Maske und Gateway. Dies ist das Gleiche wie in Routermodus, außer das der DHCP Server nicht verfügbar ist..
- Drahtlos - dieser Bildschirm, und die Unterbildschirme sind die Gleichen wie in Routermodus.
- Kennwort - dieser Bildschirm ist der Gleiche wie in Routermodus.
- Upgrade der Firmware - dieser Bildschirm ist der Gleiche wie in Routermodus.
- Status - zeigt gegenwärtige Eingaben und den Status an. Siehe den folgenden Abschnitt für Details.

Modusbildschirm

Mit diesem Bildschirm kommen Sie zurück zum Routermodus, wenn gewünscht.

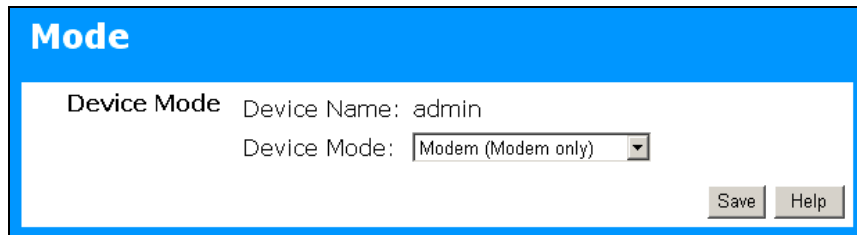


Abbildung 73: Modusbildschirm

Daten – Modusbildschirm

Device Name	Dieses Feld zeigt den gegenwärtigen Namen dieses Geräts an.
Device Mode	<p>Wählen Sie den gewünschten Gerätemodus für den Router:</p> <ul style="list-style-type: none">• Router - sowohl der ADSL Modem als auch die Routermerkmale sind betriebsbereit. In diesem Modus kann dieses Gerät gemeinsamer Internetzugang für alle Ihre LAN Benutzer sein. Standardmäßig stellt es einen DHCP Server dar, weil es allen WLAN und LAN-Benutzern eine IP-Adresse und verwandte Information liefert.• Modem - nur der ADSL Modembestandteil ist betriebsbereit. Alle Routermerkmale sind ausgeschaltet. Dieses Gerät ist "transparent" - es führt keine Operationen aus und macht keine Änderungen am Netzverkehr.. Sie müssen einen DHCP Server in Ihrem LAN haben, um den WLAN Clients IP-Adressen mit Hilfe dieses Accesspoints zu liefern. <p>Dieser Modus wird auch Bridge-Modus genannt. Nach dem Ändern des Modus startet dieses Gerät neu. Das dauert einige Sekunden. Das Menü ändert sich je nach dem Modus, in dem Sie sind.</p>

Operation / Betrieb

Der Betrieb ist automatisch und transparent.

- WLAN Clients können sich mit dem Accesspoint verbinden, falls sie das richtige SSID und die richtige Sicherheit haben, aber sie müssen in ihrem LAN eine IP-Adresse vom DHCP Server beziehen.
- Der Modem benimmt sich wie jeder andere ADSL Modem. Es wird kein Routing durchgeführt. Es wird keine Client-Anmeldung gemacht. Wenn eine Client-Anmeldung erforderlich ist, muss sie von Ihrem Router/Gateway oder von Software auf Ihrem PC ausgeführt werden.

Statusbildschirm

In Modemmodus sieht der Statusbildschirm wie das Beispiel unten aus.

Status - Bridge Mode

ADSL	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Modem Status</td> <td style="text-align: right;">Connecting</td> </tr> <tr> <td>DownStream Connection Speed</td> <td style="text-align: right;">0 kbps</td> </tr> <tr> <td>UpStream Connection Speed</td> <td style="text-align: right;">0 kbps</td> </tr> <tr> <td>VC 1 Status</td> <td style="text-align: right;">Enabled</td> </tr> <tr> <td>VC 2 Status</td> <td style="text-align: right;">Disabled</td> </tr> <tr> <td>VC 3 Status</td> <td style="text-align: right;">Disabled</td> </tr> <tr> <td>VC 4 Status</td> <td style="text-align: right;">Disabled</td> </tr> </table>	Modem Status	Connecting	DownStream Connection Speed	0 kbps	UpStream Connection Speed	0 kbps	VC 1 Status	Enabled	VC 2 Status	Disabled	VC 3 Status	Disabled	VC 4 Status	Disabled
Modem Status	Connecting														
DownStream Connection Speed	0 kbps														
UpStream Connection Speed	0 kbps														
VC 1 Status	Enabled														
VC 2 Status	Disabled														
VC 3 Status	Disabled														
VC 4 Status	Disabled														
<input type="button" value="ADSL Details"/>															
LAN	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">IP Address:</td> <td style="text-align: right;">192.168.0.1</td> </tr> <tr> <td>Network Mask:</td> <td style="text-align: right;">255.255.255.0</td> </tr> <tr> <td>MAC Address</td> <td style="text-align: right;">00:C0:02:44:66:88</td> </tr> </table>	IP Address:	192.168.0.1	Network Mask:	255.255.255.0	MAC Address	00:C0:02:44:66:88								
IP Address:	192.168.0.1														
Network Mask:	255.255.255.0														
MAC Address	00:C0:02:44:66:88														
Wireless	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Name (SSID)</td> <td style="text-align: right;">allnet</td> </tr> <tr> <td>Region</td> <td style="text-align: right;">Europe</td> </tr> <tr> <td>Channel</td> <td style="text-align: right;">3</td> </tr> <tr> <td>Wireless AP</td> <td style="text-align: right;">enable</td> </tr> <tr> <td>Broadcast Name</td> <td style="text-align: right;">enable</td> </tr> </table>	Name (SSID)	allnet	Region	Europe	Channel	3	Wireless AP	enable	Broadcast Name	enable				
Name (SSID)	allnet														
Region	Europe														
Channel	3														
Wireless AP	enable														
Broadcast Name	enable														
System	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Device Name:</td> <td style="text-align: right;">ALL0277DSL</td> </tr> <tr> <td>Firmware Version:</td> <td style="text-align: right;">2.10.00</td> </tr> </table>	Device Name:	ALL0277DSL	Firmware Version:	2.10.00										
Device Name:	ALL0277DSL														
Firmware Version:	2.10.00														

Abbildung 74: Statusbildschirm –Modem / Brückenmodus

Daten - Statusbildschirm (Modem / Brückenmodus)

ADSL	
Modem Status	Dies zeigt den Staus des ADSL Modem an.
DownStream Connection Speed	Zeigt die Geschwindigkeit der DownStream Verbindung an.
UpStream Connection Speed	Zeigt – wenn verbunden – die Geschwindigkeit der Up Stream (upload) ADSL Verbindung an.
ADSL Details	Click this button to open a sub-window and view the details of each VC (Virtual Circuit).
LAN	
IP Address	Die IP-Adresse vom WLAN ADSL Router.
Network Mask	Netzmaske (Unternetzmaske) für die IP-Adresse oben
MAC Address	Dies zeigt die MAC-Adresse für den WLAN ADSL Router, wie auf der LAN-Schnittstelle gesehen.
Wireless	
Name (SSID)	Beim Verwenden eines ESSs (erweitert mit mehrfachen Accesspoints) wird diese Kennung ESSID (erweiterte Dienstsatzkennzeichnung) genannt.

Region	Die gegenwärtige Region wie auf dem WLAN Bildschirm gesetzt.
Channel	Dies zeigt den Kanal an, der gegenwärtig verwendet wird, wie auf dem WLAN Bildschirm gesetzt.
Wireless AP	Dies zeigt an, ob der Wireless Access Point eingeschaltet ist.
Broadcast Name	Dies zeigt an, ob SSID auf "Broadcast" gesetzt ist.
Associated Devices	Dies erzeugt eine Liste der gegenwärtig angeschlossenen WLAN Geräte.
Buttons	
Refresh Screen	Aktualisiert die Daten im Bildschirm.
System	
Device Name	Der gegenwärtige Name des WLAN ADSL Routers. Dies ist auch der "Hostname", den der ISP vorgesehen hat..
Firmware Version	Zeigt die aktuelle Firmware-Version

Anhang A

Fehlerbehebung

Dieser Anhang deckt die wahrscheinlichsten Probleme und ihre Lösungen ab.

Überblick

Dieses Kapitel behandelt Probleme, auf die Sie stoßen können, während Sie den WLAN ADSL Router verwenden, und einige mögliche Lösungen. Wenn Sie die vorgeschlagenen Schritte ausführen und der WLAN ADSL Router immer noch nicht richtig funktioniert, wenden Sie sich an Ihren Fachhändler.

Allgemeine Probleme

- Problem 1:** Ich kann den WLAN ADSL Router nicht erreichen, um ihn zu konfigurieren
- Solution 1:** Überprüfen Sie Folgendes:
- Wurde der WLAN ADSL Router richtig installiert, sind die LAN-Verbindungen in Ordnung, und ist er eingeschaltet?
 - Stellen Sie sicher, dass Ihr PC und der WLAN ADSL Router auf demselben Netzsegment sind. (Wenn Sie keinen Router haben, muss dies der Fall sein.)
 - Wenn Ihr PC DHCP Client ist, starten ihn neu.
 - Wenn Ihr PC eine feste (statische) IP-Adresse verwendet, stellen Sie sicher, dass er eine IP-Adresse innerhalb des Bereichs 192.168.0.2 bis 192.168.0.254 verwendend und mit der Default IP-Adresse des WLAN ADSL Routers von 192.168.0.1 auf diese Art kompatibel ist.
 - Auch sollte die Netzmaske auf 255.255.255.0 gesetzt werden, um zum WLAN ADSL Router zu passen.
 - In Windows können Sie diese Einstellungen durch Verwenden des Controlpanels überprüfen.

Internetzugang

- Problem 1:** Wenn ich eine URL oder eine IP-Adresse eingebe, bekomme ich einen „Time-Out“
- Solution 1:** Eine Anzahl von Dingen kann dies verursachen. Versuchen Sie die folgenden Fehlerbehebungsschritte.
- Überprüfen Sie, ob dies mit anderen PCs funktioniert. Wenn ja, überprüfen Sie die IP Einstellungen. Beim Verwenden einer festen (statischen) IP-Adresse überprüfen Sie die Netzmaske, Default Gateway und sowohl DNS als auch die IP-Adresse.
 - Wenn die PCs konfiguriert richtig konfiguriert sind, aber immer noch nicht funktionieren, überprüfen Sie den WLAN ADSL Router. Stellen Sie sicher, dass er angeschlossen ist, und eingeschaltet.
 - Überprüfen Sie den Statusbildschirm des WLAN ADSL Routers, ob er richtig funktioniert.

Problem 1:

Einige Anwendungen laufen nicht richtig, wenn ich den WLAN ADSL Router verwende.

Solution 1:

Der WLAN ADSL Router verarbeitet die Daten, die durch ihn gehen, so dass er nicht transparent ist.

Für eingehende Verbindungen müssen Sie die virtuellen Server- oder Firewallregeln verwenden, um den PC anzugeben, der den eingehenden Datenverkehr erhält.

Sie können auch die Funktion DMZ verwenden. Dies sollte mit fast jeder Anwendung arbeiten, außer:

- Es ist ein Sicherheitsrisiko, da die Firewall ausgeschaltet ist.
- Nur ein (1) PC kann dieses Merkmal verwenden.

WLAN Zugang

Problem 1:

Mein PC findet den Wireless Access Point nicht.

Solution 1:

Überprüfen Sie wie folgt:

- Ist Ihr PC im *Infrastructure Mode*. (Access Points müssen immer im *Infrastructure Mode* sein)
- Die SSID im PC und dem WLAN Accesspoint sind identisch.
- Erinnern Sie sich daran, dass das SSID fallempfindlich ist. So passt zum Beispiel "arbeitsgruppe" nicht zu "Arbeitsgruppe".
- Sowohl Ihr PC als auch der WLAN ADSL Router müssen die gleichen Daten für WEP haben. Die Standardeinstellung für den WLAN ADSL Router ist ausgeschaltet, so dass Ihre WLAN Station auch WEP ausgeschaltet haben sollte.
- Wenn WEP auf dem WLAN ADSL Router aktiviert ist, muss Ihr PC WEP aktiviert haben, und der Schlüssel muss passen.
- Wenn der WLAN Bildschirm des WLAN ADSL Routers so eingestellt ist, dass nur vertrauenswürdige PCs Zugang haben, dann muss jede Ihrer WLAN Stationen als "vertrauenswürdig" bestimmt worden sein, oder der WLAN Port wird blockiert.
- Um zu sehen, ob Funkstörungen ein Problem verursachen, prüfen Sie, ob eine Verbindung möglich ist, wenn nahe bei dem WLAN ADSL Router. sind

Problem 2:

WLAN Verbindungsgeschwindigkeit ist sehr langsam

Solution 2:

Das WLAN System verbindet sich mit der am höchsten möglichen Geschwindigkeit je nach dem Abstand und der Umgebung. Um die am höchsten mögliche Verbindungsgeschwindigkeit zu erhalten, können Sie mit dem Folgenden experimentieren:

- WLAN ADSL Routerstandort.

Versuchen Sie, die Lage und den Antennenrichtung des WLAN ADSL Routers einzustellen.

- WLAN Kanal

Wenn Funkstörung das Problem ist, kann es eine merkliche Verbesserung bringen, zu einem anderen Kanal zu wechseln.

- Funkstörung

Es kann sein, dass andere Geräte Überlagerungen verursachen. Sie können durch Ausschalten von anderen Geräten experimentieren und sehen, ob dies hilft. "Störende" Geräte sollten abgeschirmt werden.

Anhang B

Über Wireless LANs

Dieser Anhang liefert eine Hintergrundinformation über das Verwenden von Wireless LANs (WLANs).

Modi

Wireless LANs können in einem von zwei (2) Modi funktionieren:

- Ad hoc
- Infrastruktur

Ad hoc Modus

Ad hoc Modus erfordert keinen Accesspoint oder ein verdrahtetes (Ethernet--) LAN. WLAN Ports (z.B. Notebook-PCs mit WLAN Karten) kommunizieren direkt mit einander.

Infrastrukturmodus

In Infrastrukturmodus werden ein oder mehrere Accesspoints verwendet, um WLAN Ports (z.B. Notebook-PCs mit WLAN Karten) mit einem verdrahteten (Ethernet--) LAN zu verbinden. Die WLAN Ports können dann auf alle LAN-Ressourcen zugreifen.



Notel

Accesspoints können nur in "Infrastruktur" Modus funktionieren und können nur mit WLAN Ports kommunizieren, die auf "Infrastruktur" Modus gestellt sind.

BSS/ESS

BSS

Eine Gruppe von WLAN Ports und ein einzelner Accesspoint, die alle dieselbe Kennung (SSID) verwenden, formen einen Basic Service Set (BSS).

Dasselbe SSID zu verwenden, ist wesentlich. Geräte mit anderem SSIDs sind außerstande, mit einander zu kommunizieren.

ESS

Eine Gruppe von WLAN Ports und mehrere Accesspoints, die alle dieselbe Kennung (ESSID) verwenden, formen einen erweiterten, extended (ESS).

Verschiedene Accesspoints innerhalb eines ESS können verschiedene Kanäle verwenden. Deshalb wird es, um Überlagerung zu reduzieren, empfohlen, dass benachbarte Accesspoints verschiedene Kanäle verwenden sollten.

Da WLAN Ports physisch durch den von einem ESS abgedeckten Bereich bewegt werden, wechseln sie automatisch zum Accesspoint, welcher die wenigste Störungen oder beste Leistung hat. Diese Fähigkeit wird Roaming genannt. (Accesspoints haben oder erfordern keine Roaming Fähigkeiten.)

Kanäle

Der WLAN Kanal setzt die für Kommunikation verwendete Funkfrequenz

- Accesspoints verwenden einen festen Kanal. Sie können den verwendeten Kanal wählen. Dies erlaubt Ihnen, einen Kanal zu wählen, der die wenigsten Störungen und die beste Leistung liefert. In den USA und Kanada sind 11 Kanäle verfügbar. Beim Verwenden von mehreren Accesspoints ist es besser, wenn benachbarte Accesspoints verschiedene Kanäle verwenden, um Störungen zu reduzieren.
- Im "Infrastruktur" Modus durchsuchen WLAN Ports normalerweise alle Kanäle, wenn sie einen Accesspoint suchen. Wenn mehr als ein Accesspoint verwendet werden kann, wird der mit dem stärksten Signal gebraucht. (Dies kann nur innerhalb eines ESSs geschehen.)
- Beim Verwenden des "ad hoc" Modus (keine Accesspoints) sollten alle WLAN Ports vorbereitet werden, denselben Kanal zu verwenden. Jedoch durchsuchen die meisten WLAN Ports immer noch alle Kanäle, um zu sehen, ob es eine vorhandene "ad hoc" Gruppe gibt, in die sie eintreten können.

WEP

WEP (Wired Equivalent Privacy) ist eine Norm für Daten-Verschlüsselung, vor dem Senden. Dies ist wünschenswert, weil es unmöglich ist, „Schnüffler“ daran zu hindern, alle Daten zu erhalten, die von Ihren WLAN Stationen gesendet werden. Aber, wenn die Daten verschlüsselt werden, dann sind sie bedeutungslos, es sei denn, der Empfänger kann sie entschlüsseln.

Wenn WEP verwendet wird, müssen die WLAN Ports und der Accesspoint dieselben Einstellungen haben:

WEP	Off, 64 Bit, 128 Bit
Key	Bei 64 Bit und 128 Bit Verschlüsselung muß der Schlüssel passen.
WEP Authentication	Open System oder Shared Key.

WPA-PSK

WPA-PSK ist eine andere Norm für Datenverschlüsselung vor dem Senden. Dies ist ein neuerer Standard als WEP und ist sicherer. Daten werden mit Hilfe eines 256 Bit Schlüssels verschlüsselt, der automatisch generiert und oft ausgewechselt wird.

Wenn alle Ihre WLAN Stationen WPA-PSK unterstützen, sollten Sie dieses statt WEP verwenden. Wenn WPA-PSK verwendet wird, müssen die WLAN Ports und der Accesspoint dieselben Einstellungen haben:

WPA PSK (Pre-shared Key)	Tragen Sie denselben Wert bei jeder Station und AP ein. Das PSK muss zwischen 8 und 63 Zeichen lang sein. Der für die tatsächliche Verschlüsselung benutzte 256 Bit Schlüssel ist von diesem Schlüssel abgeleitet.
Encryption	Dieselbe Verschlüsselungsmethode muss verwendet werden. Die übliche Verschlüsselungsmethode ist TKIP. Eine andere häufig unterstützte Methode ist AES.

WLAN LAN-Konfiguration

Damit WLAN Ports den Accesspoint verwenden können, müssen die WLAN Ports und der Accesspoint dieselben Einstellungen wie folgt verwenden:

Mode	Alle Clients und WLAN Ports müssen auf den Modus "Infrastruktur" gesetzt werden. (Der Accesspoint ist immer im "Infrastruktur" Modus.)
SSID (ESSID)	WLAN Ports sollten dasselbe SSID (ESSID) wie der Accesspoint verwenden, mit dem sie sich verbinden möchten. Alternativ kann das SSID auf "any" oder null (leer) gestellt werden, um Verbindung zu jedem Accesspoint zu ermöglichen.
Wireless Security	Die WLAN Ports und der Accesspoint müssen dieselben Einstellungen für WLAN Sicherheit verwenden. (Keines, WEP, WPA-PSK). WEP: Wenn WEP verwendet wird, müssen die Schlüsselgröße (64 Bit, 128 Bit), der Schlüsselwert und die Authentifikationseinstellungen die Gleichen in den WLAN Ports und dem Accesspoint sein. WPA-PSK: Wenn WPA-PSK verwendet wird, müssen alle WLAN Ports vorbereitet werden, WPA-PSK zu verwenden, und dasselbe gemeinsame Schlüssel- und Verschlüsselungssystem nutzen. Für ad hoc Netze (keinen Accesspoint) müssen alle WLAN Ports dieselben Sicherheitseinrichten verwenden.

Anhang C

Über VPNs

Überblick

Ein VPN (Virtual Private Network) stellt eine sichere Datenverbindung zwischen zwei Punkten in einem unsicheren Netzwerk, z.B. dem Internet bereit. Diese Datenverbindung nennt man **VPN Tunnel**. Für VPNs existieren verschiedene Standards und Protokolle. Dieser Wireless ADSL Router verwendet das Verfahren **IPSec**.

IPSec

Der Standard IPSec ist quasi überall in Zusammenhang mit TCP/IP Netzwerken vorhanden. Er arbeitet paket-bezogen, verschlüsselt und authentiziert alle Pakete, die durch den VPN Tunnel übertragen werden. So ist es gleichgültig, welche Anwendungen auf Ihrem PC verwendet werden. Jede mögliche Anwendung kann das VPN wie irgendeine andere Netzwerkverbindung auch verwenden. IPSec VPNs tauschen Informationen durch logische Anschlüsse, genannt SAs aus (Security Associations). Ein SA ist einfach eine Definition der Protokolle, der Algorithmen und der Schlüssel, die zwischen den zwei VPN Geräten (Endpunkte) verwendet werden.

Ein jedes IPSec VPN hat zwei SAs – eins für jede Richtung. Falls **IKE** (Internet Key Exchange) verwendet wird, um so genannte "exchange keys" zu generieren, gibt es zusätzlich SA's für die IKE Verbindung. Es gibt bei IPSec zwei Betriebsarten:

- **Transport Mode** – Der "Nutzlast-Anteil" des Paketes ist eingekapselt durch die Verschlüsselung, aber die IP Header bleiben unverschlüsselt.

Dieser Wireless ADSL Router unterstützt diese Betriebsart NICHT.

- **Tunnel Mode** – alles ist verschlüsselt, einschließlich der original IP Header-Informationen. Ein neuer IP Header wird erzeugt. Nur dieser neue Header ist unverschlüsselt. Diese Betriebsart ist die sicherere von beiden.

Dieser Wireless ADSL Router unterstützt IMMER die Betriebsart Tunnel Mode.

IKE

IKE (Internet-Schlüssel-Austausch) ist ein optionales, aber allgemein verwendetes Bestandteil von IPSec. IKE liefert eine Methode des Verhandels und des Erzeugens der Schlüssel und der Identifikationen, die von IPSec benötigt werden. Wenn man IKE verwendet, wird nur ein einzelner Schlüssel während der Konfiguration benötigt. Auch IKE unterstützt **Certificates** (bereitgestellt von CAs - Certification Authorities) zur sicheren Identifikation des Remotebenutzers. Wenn IKE NICHT verwendet wird, dann müssen alle Schlüssel und Identifikationen (SPIs) manuell eingetragen werden. CAs können NICHT verwendet werden. Dieses wird "manueller Schlüsselaustausch" genannt. Wenn man IKE verwendet, gibt

es 2 Phasen zum Herstellen des VPN Tunnels:

- Phase I ist die Vermittlung und die Einrichtung des IKE Anschlusses
- Phase II ist die Vermittlung und die Einrichtung oben des IPSec Anschlusses.

Weil IKE und IPSec Anschlüsse unterschiedlich sind, haben sie auch unterschiedliche SAs.

Policies

VPN Konfigurations-Einstellungen werden in den **Policies** gespeichert.

Beachten Sie, dass unterschiedliche Anbieter auch unterschiedliche Begriffe verwenden. Grundsätzlich haben die Begriffe "VPN Policy", "IPSec Policy" und "IPSec Proposal" die gleiche Bedeutung. Einige Anbieter trennen IKE Policies (Phase 1 Parameters) von IPSec Policies (Phase 2 Parameters).

Für diesen Wireless ADSL Router gilt; jede VPN Policy enthält sowohl die Parameter der Phase 1 als auch der Phase 2 (falls IKE genutzt wird). Jede Policy definiert:

- Die Adresse des entfernten VPN Endpunktes
- Die Daten, die den VPN Tunnel nutzen dürfen
- Die Parameter für die IPsec SA (Security Association)
- Falls IKE genutzt wird, die Parameter für IKE SA (Security Association)

Grundsätzlich benötigen Sie mindestens eine (1) VPN Policy für jede entfernte Station, mit der Sie einen VPN Tunnel aufbauen wollen. Es ist möglich und manchmal sinnvoll, für die gleiche entfernte Station mehrere Policies zu haben. Es darf aber zu einem Zeitpunkt immer nur eine aktiv sein.

VPN Konfiguration

Grundsätzlich gilt, dass jeder VPN Endpunkt zueinander passende Policies verwenden muss:

VPN Endpoint address	Jeder VPN Endpunkt muss so konfiguriert sein, dass er eine ausgehende VPN Verbindung initiieren oder eine ankommende akzeptieren kann. Normalerweise bedeutet dies, dass eine feste Internet IP Adresse vorhanden sein muß. Es ist für einen VPN Remote Client jedoch möglich, eingehende Verbindungen zu akzeptieren, auch wenn die IP Adresse nicht bekannt ist.
Local & Remote LAN definition	Dieses legt fest, bei welchem abgehenden Verkehr ein VPN Tunnel aufgebaut werden darf und welcher kommende Verkehr angenommen wird. Jeder Endpunkt muß so konfiguriert werden, dass der gewünschte Daten-Verkehr vom Remote-Endpunkt geführt oder angenommen werden kann. Wenn man Zwei (2) LANs anschließt, erfordert dieses das: <ul style="list-style-type: none">• Jeder Endpunkt muß die IP Adressen berücksichtigen, die auf dem anderen Endpunkt verwendet werden• Die 2 LANs MÜSSEN unterschiedliche IP Adressbereiche benutzen.
IKE parameters	Wenn Sie IKE verwenden (empfohlen), müssen die IKE Parameters exakt zusammen passen (außer für SA lifetime)
IPsec parameters	Die IPsec Parameters müssen bei beiden Endpoints exakt zueinander passen.

Typische VPN Situationen und Konstellationen

VPN Pass-through

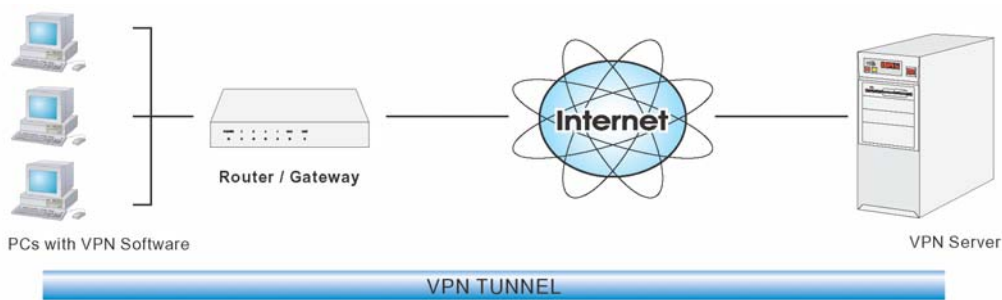


Abbildung1: VPN Pass-through

Hier verwenden PCs im LAN hinter dem Router/Gateway VPN Software, aber der Router/Gateway ist nicht als VPN Endpunkt aktiv. Er lässt nur die VPN Verbindung zu.

- Die PC Software nutzt irged ein VPN Protokoll, das auch der VPN-Server unterstützt.
- Der VPN Server muss die PCs hinter dem NAT-Router unterstützen. Diese haben eine IP Adresse, die im Internet ungültig ist.
- Der Router/Gateway erwartet keine VPN Konfiguration, da er nicht als VPN Tunnel Endpunkt arbeitet.

Client PC mit VPN Gateway

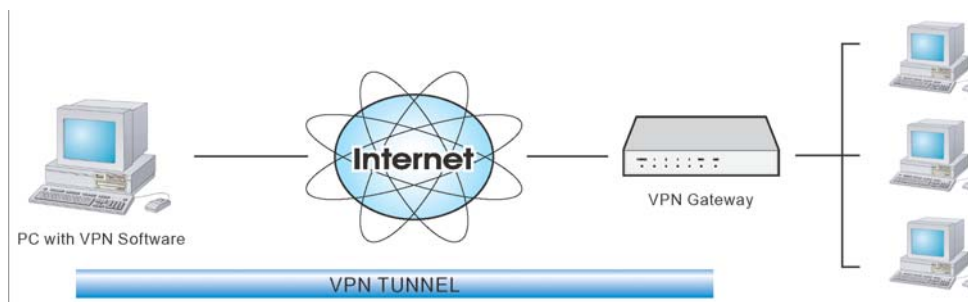


Abbildung2: Client PC to VPN Server

In dieser Situation, läuft auf dem PC passende VPN Software, um über das Internet mit dem Wireless ADSL Router oder einem anderen VPN Gateway einen VPN Tunnel aufzubauen. Einmal verbunden, hat der PC den gleichen Zugang zum LAN und den daran angeschlossenen Ressourcen wie PCs im lokalen LAN (es sei denn, der Network Administrator hat den Zugriff beschränkt).

- IPsec ist nicht das einzige mögliche Protokoll, aber der Wireless ADSL Router unterstütz ausschließlich Ipsec.
- Windows 2000 und Windows XP beinhalten ein IPsec VPN Client Programm. Jedoch ist die Konfiguration dieser Client Programme für den betrieb mit dem Wireless ADSL Router sehr komplex und wird durch in diesem Dokument nicht behandelt.

Verbindung zweier LANs mit VPN Tunnel

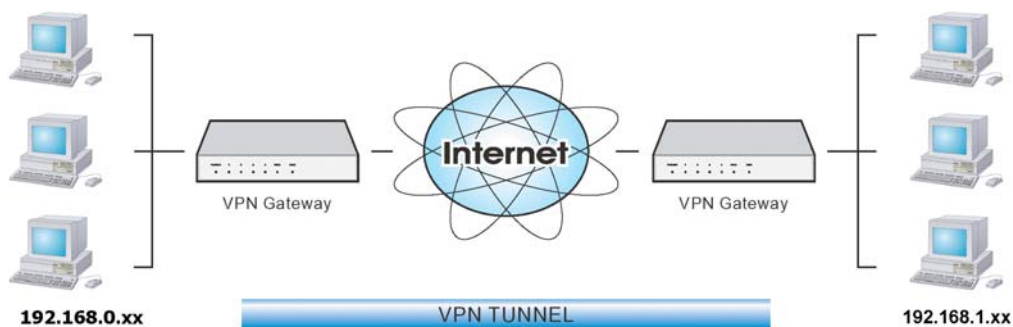


Abbildung3: Verbindung zweier VPN Gateways

Es können zwei (2) LANs mit einem VPN-Tunnel verbunden werden. PCs auf beiden Seiten haben sicheren Zugriff zu den Ressourcen der jeweils anderen Seite.

- Die zwei LANs MÜSSEN unterschiedliche IP Adressbereiche verwenden.
- Die VPN Policies an jedem Ende entscheiden, ob und wenn ein VPN Tunnel aufgebaut wird und auf welches System oder entfernte LAN durch den VPN Tunnel zugegriffen werden kann.
- Es ist möglich simultan VPN Verbindungen zu mehreren entfernten Punkten zu betreiben.

VPN Beispiel

In diesem Beispiel sind 2 LANs durch VPN verbunden. Beide verfügen über einen Wireless ADSL Router.

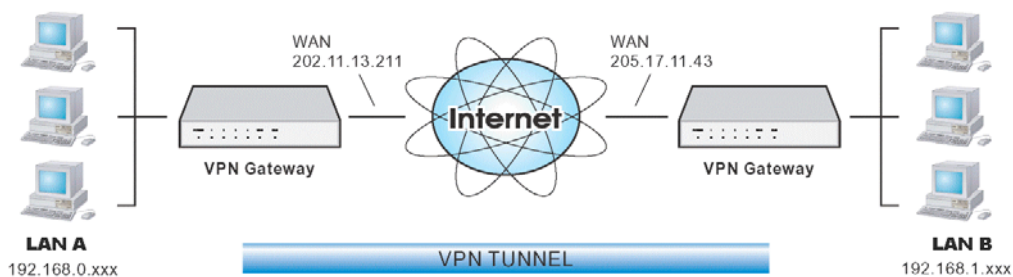


Abbildung4: Verbindung von 2 Wireless ADSL Routers

Beachten Sie

- beide LANs MÜSSEN unterschiedliche IP Adressbereiche verwenden.
- Beide Endpunkte haben feste WAN (Internet) IP Adressen.
- In diesem Beispiel wird die "Auto" Policy und IKE verwendet.

Konfiguration - Gateway A

Gateway A sollte wie hier gezeigt konfiguriert werden.

VPN - Auto Policy

General Policy Name:
Remote VPN Endpoint
Address Type:
Address Data:
 NetBIOS Enable

Local LAN IP Address
IP address:
Subnet Mask:

Remote LAN IP Address
IP address:
Subnet Mask:

IKE Direction:
Exchange Mode:
Diffie-Hellman (DH) Group:
Local Identity Type:
Data:
Remote Identity Type:
Data:

SA Parameters Encryption:
Authentication:
Pre-shared Key:
SA Life Time: (Seconds)
 Enable PFS (Perfect Forward Security)

Abbildung 5: Gateway A Konfiguration

Konfiguration - Gateway B

Gateway B sollte wie hier gezeigt konfiguriert werden.

VPN - Auto Policy

General Policy Name:

Remote VPN Endpoint
 Address Type:
 Address Data:

NetBIOS Enable

Local LAN IP Address

IP address:

Subnet Mask:

Remote LAN IP Address

IP address:

Subnet Mask:

IKE Direction:

Exchange Mode:

Diffie-Hellman (DH) Group:

Local Identity Type:

Data:

Remote Identity Type:

Data:

SA Parameters Encryption:

Authentication:

Pre-shared Key:

SA Life Time: (Seconds)

Enable PFS (Perfect Forward Security)

Abbildung 6: Gateway B

Einstellungen

Setting	LAN A Gateway	LAN B Gateway	Notes
Policy Name	Example	Example	Eigentlich ohne Belang, aussagekräftigen Namen verwendet.
Remote VPN Endpoint	Fixed IP Address 205.17.11.43	Fixed IP Address 202.11.13.211	WAN (Internet) IP Adresse des anderen Endpunktes.
NetBIOS	Enable	Enable	Disable, wenn nicht

			benötigt.
Local LAN IP address Mask	192.168.0.0 255.255.255.0	192.168.1.0 255.255.255.0	Lokale Subnet- Maske. Enger fassen, wenn möglich.
Remote LAN IP address Mask	192.168.1.0 255.255.255.0	192.168.0.0 255.255.255.0	Entfernte Subnet- Maske. Enger fassen, wenn möglich.

IKE

Direction	Initiator & responder	Initiator & responder	Müssen nicht unbedingt zusammen passen. Jeder Endpunkt kann eine Richtung blockieren.
Exchange mode	Main Mode	Main Mode	Muss exakt passen.
DH Group	Group 2 (1024 bit)	Group 2 (1024 bit)	Muss exakt passen.
Local Identity	IP address	IP address	IP Adresse ist die gebräuchlichste ID Methode
Remote Identity	WAN IP address	WAN IP address	IP Adresse ist die gebräuchlichste ID Methode

SA Parameters

Encryption	3DES	3DES	Muss exakt passen.
Authentication	MD5	MD5	Muss exakt passen.
Pre-shared Key	xxxxxxxxxx	xxxxxxxxxx	Muss exakt passen. Sie können beliebige Zeichen verwenden.
SA Life time	28800	28800	Muss nicht exakt passen. Kürzere Zeit erhöht Sicherheit.
PFS	Disabled	Disabled	Muss exakt passen.

Anmerkung:

Einige VPN Gateways und Programme erlauben, dass Sie die folgenden Einstellungen separat für IKE und IPSec vornehmen können. Bei diesem Gerät werden für IKE und IPSec die gleichen Einstellungen verwendet.

- Authentication
- Encryption
- SA Lifetime

IPSec gestattet auch "AH Authentication" unter Verwendung von MD5 oder SHA-1. Bei diesen Gerät ist "AH Authentication" grundsätzlich ausgeschaltet (DISABLED).

Anhang D

Spezifikationen

Multi-Function Wireless ADSL Router

Model	Wireless ADSL Router
ADSL Interface	T1.413, G.DMT, G.lite, multi-mode
Dimensions	153mm(W) * 102mm(D) * 35.5mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	4 * 10/100BaseT (RJ45) LAN connection 1 * RJ11 for ADSL line
LEDs	13
Power Adapter	12 V DC External

Wireless Interface

Standards	IEEE802.11b, IEEE802.11g WLAN, 802.11G-plus (Texas Instruments proprietary enhanced mode)
Frequency	2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Channels	Maximum 14 Channels, depending on regulatory authorities
Modulation	CCK, DQPSK, DBPSK, OFDM/CCK
Data Rate	Up to 54 Mbps (802.11g), 64 Mps (TI 802.11G-plus)
Security	WEP 64Bit, WPA 128Bit, WPA-PSK, MAC address checking
Output Power	13dBm (typical)
Receiver Sensitivity	-80dBm Min.

Regulatory Approvals

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Approval

CE Standards

This product complies with the 99/5/EEC directives, including the following safety and EMC standards:

- EN300328-2
- EN301489-1/-17
- EN60950

CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.