WAP-0010

MIMO Access Point

Benutzerhandbuch

Digital Data Communications GmbH
Zeche-Norm-Str. 25
44319 Dortmund

Technische Support Hotline: 01805-991002
E-Mail: support@level-one.de

Ver 1.00-0604

Inhaltsverzeichnis

Copyright

Der Inhalt dieser Publikation darf ohne schriftliche Zustimmung weder in Teilen noch vollständig in irgendeiner Form vervielfältigt, veröffentlicht oder in andere Sprachen übersetzt werden.

Marken und Warenzeichen

LevelOne und das LevelOne-Logo sind eingetragene Warenzeichen der Digital Data Communications GmbH. Andere Markennamen und Warenzeichen, die zum Zwecke der eindeutigen Identifikation in diesem Dokument genannt werden, sind in der Regel Warenzeichen der entsprechenden Firmen. Änderung der Angaben ohne vorherige Ankündigung sind vorbehalten.

FCC-Interferenzkonformität

Eine Prüfung der Geräte hat ergeben, dass die Grenzwerte für Digitalgeräte der Klasse B gemäß Teil 15 der FCC-Regeln eingehalten werden. Diese Grenzwerte wurden festgelegt, um ausreichenden Schutz vor Funkstörung in kommerzieller Umgebung zu gewährleisten. Diese Geräte können Hochfrequenzenergie erzeugen, nutzen und abstrahlen. Die Missachtung der Anweisungen für Installation und Betrieb in diesem Benutzerhandbuch kann Störungen der Fernmeldekommunikation zur Folge haben. Bei Betrieb dieser Geräte in häuslicher Umgebung kommt es mit großer Wahrscheinlichkeit zu Interferenzen. Der Benutzer muss die Kosten für erforderliche Maßnahmen zum Ausgleich dieser Interferenzen selbst tragen.

CE-Konformitätserklärung

Diese Geräte erfüllen alle Anforderungen im Hinblick auf elektromagnetische Verträglichkeit gemäß der Richtlinien 73/23/EWG, 89/336/EWG und 99/5/EG.
Dieses Gerät ist vorgesehen für die Verwendung in Wohnbereichen, Gewerbe- und Geschäftsbereichen sowie Kleinbetriebe. Es ist nicht vorgesehen für die Verwendung in Industriebereichen.
Änderung der Angaben ohne vorherige Ankündigung sind vorbehalten.
Hiermit erklärt Digital Data Communications, dass sich das Gerät WAP-0010 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Die EG-Konformitätserklärung ist einsehbar unter: http://www.level-one.de/support.php

Typenschild des WAP-0010

1. Einleitung

Gratulation zum Kauf dieses Wireless Access Points. Dieses Produkt wurde speziell für den Gebrauch in Klein- und Heimbüros entwickelt. Es stellt eine SOHO-Komplettlösung für Internetanwendungen dar, und kann selbst von Laien einfach konfiguriert und bedient werden. In diesem Handbuch wird die richtige Installation und Konfiguration des Access Points beschrieben. Damit Sie in den Genuss aller Funktionen des Geräts kommen, lesen Sie dieses Benutzerhandbuch bitte vor Installierung und Inbetriebnahme des Geräts sorgfältig durch.

1.1. Funktionen und Features

Grundfunktionen

- **Selbstschaltender Ethernet-Switch**
  mit 4 Ports
- **DHCP-Server-Unterstützung**
  Alle Computer im Netzwerk können die TCP/IP-Einstellungen automatisch über dieses Produkt abfragen.
- **Webbasierte Konfiguration**
  Konfiguration über den Webbrowser eines jeden Computers im Netzwerk mithilfe von Netscape oder Internet Explorer.

Wireless-Funktionen

- **Hochgeschwindigkeit für die Wireless LAN-Verbindung**
  Datenrate von bis zu 54 Mbps durch Verwendung von OFDM (Orthogonal Frequency Division Multiplexing).
- **Roaming**
  Ermöglicht nahtlosen Netzwechsel für WLANs nach IEEE 802.11b (11M) und IEEE 802.11g (54M).
- **IEEE 802.11b-kompatibel (11M)**
  Ermöglicht direkte Kommunikation zwischen Netzwerken verschiedener Anbieter.
- **IEEE 802.11g-kompatibel (54M)**
  Ermöglicht direkte Kommunikation zwischen Netzwerken verschiedener Anbieter.
- **Auto Fallback**
  54M, 48M, 36M, 24M, 18M, 12M, 6M Fallback-Datenraten im 802.11g-Modus.
  11M, 5.5M, 2M, 1M Fallback-Datenraten im 802.11b-Modus.

1.2. Packungsinhalt

- WAP-0010 MIMO Access Point
- Steckernetzteil
- Kat-5-Kabel
- CD-ROM mit Benutzerhandbuch

2. Informationen zu dieser Anleitung

2.1. Zweck und Ziel

Diese Anleitung informiert Sie über

- ✓ den bestimmungsgemäßen Verwendungsbereich
- ✓ die ordnungsgemäße Inbetriebnahme des Access Points

Sie erhalten außerdem wichtige Hinweise für den

- ✓ sicheren Gebrauch des Access Points und werden vor möglichen Risiken gewarnt, die durch Nichtbeachtung dieser Hinweise entstehen können.

2.2. Marken und Markenzeichen

LevelOne und das LevelOne Logo sind eingetragene Warenzeichen der Digital Data Communications GmbH. Andere Markennamen oder Warenzeichen, die zum Zwecke der eindeutigen Identifikation in diesem Dokument erwähnt werden, sind in der Regel Warenzeichen der entsprechenden Firmen.

2.3. Nachweis verwendeter Informationen

In der Erarbeitung der Sicherheitshinweise wurden unter anderem die Ausführungen des vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen IT-Grundschutzhandbuch (Stand Oktober 2003) berücksichtigt. Aufgrund des beschränkten Raumes, der im Rahmen einer Anleitung zur Verfügung steht, kann hier nur eine Auswahl der in der Praxis unter Umständen relevanten Aspekte dargestellt werden. Zusätzlich wird deswegen empfohlen, weitergehende Informationen aus den für den jeweiligen Anwendungsfall einschlägigen Abschnitten des IT-Grundschutzhandbuches, insbesondere des Gefährdungskataloges, zu beziehen:
http://www.bsi.bund.de/gshb/deutsch/menue.htm
Für die kriminologischen Erläuterungen zu Fachausdrücken wurden Fachliteratur sowie einschlägige Online-Quellen hinzugezogen, u. a. Themen aus dem Diskussionsforum de.com.security.

2.4. Haftung

- ✓ Der Inhalt dieser Installationsanleitung wurde auf der Grundlage von Fachinformationen, detaillierter Anwendungsanalyse des Installations-Vorganges und Erfahrungen von Anwendern mit größter Sorgfalt erarbeitet.
- ✓ Digital Data Communications GmbH behält sich das Recht vor, Änderungen dieses Access Points, die entweder Hardware oder Softwarekomponenten (Firmware) betreffen können, im Interesse der Weiterentwicklung und der Verbesserung von Funktionalität und Zuverlässigkeit des Produktes ohne vorherige Ankündigung durchzuführen.
  Die Beschreibungen und Abbildungen basieren auf dem Informationsstand zum Zeitpunkt der Erstellung dieses Dokumentes (März 2005).
- ✓ Ebenso behält sich der Herausgeber dieser Anleitung, die Digital Data Communications GmbH, das Recht vor, Korrekturen und Änderungen am Inhalt dieses Dokumentes ohne vorherige Ankündigung durchzuführen. Die jeweils aktuelle Dokumentation finden Sie unter: http://www.level-one.de/support.php

Aus den nachfolgend genannten Gründen kann **keine Gewähr** dafür übernommen werden, dass die angebotenen Informationen auch die in Ihrer Einsatzumgebung bestehenden Fragestellungen und Probleme in jedem Fall abdecken:

- ✓ Rasante technologische Entwicklung im Bereich der Informationstechnologie.
- ✓ PC-basierte Computernetzwerke bestehen aus einer Vielzahl von Einzelkomponenten. Die im Einzelfall gegebene Zusammensetzung und mögliche Kompatibilitätsprobleme können nicht vorab bekannt sein.
- ✓ Sicherheit- und Datenschutzrisiken in Verbindung mit der Internetnutzung.
- ✓ Anzeigen des Dokumentes

2.5. Abbildungen

Die in dieser Installationsanleitung abgebildeten Bildschirmfotos aus der Testinstallation wurden unter Microsoft Internet Explorer 6.0 mit Service Pack und aktiviertem Java Script erstellt. Wenn Sie einen anderen Webbrowser verwenden, wird das grafische Erscheinungsbild wahrscheinlich von den hier gezeigten Abbildungen abweichen.
Bitte beachten Sie, dass in vielen Fällen nicht das komplette Fenster des Internet Explorers abgebildet wird. Um überflüssige Bildinformationen zu vermeiden, wird in der Regel nur der Fensterbereich gezeigt, der die für die jeweilige Aktion relevanten visuellen Elemente enthält.
Auf Grund der Vereinheitlichung sind nur englische Screens in dieser Dokumentation abgebildet. Sie können sich selbstverständlich die Screens im Programm auf Deutsch anzeigen lassen. Nachdem Sie sich angemeldet haben, können Sie oberhalb der Menüleiste die Sprache wählen.

2.6. Druck dieser Anleitung

Diese Anleitung steht im Portable Document Format (PDF) zur Verfügung. Um das Dokument am Bildschirm darstellen oder ausdrucken zu können benötigen Sie die kostenfrei erhältliche Software Acrobat Reader von Adobe. Für das Anzeigen dieses Dokumentes wird die Verwendung des Acrobat Readers in der Version 7 empfohlen. Sie können Acrobat Reader 7 von der Adobe Downloadseite (www.adobe.de) herunterladen.
Abbildungen und Formate in dieser Anleitung sind für den Ausdruck optimiert. Um das Dokument auszudrucken, klicken Sie im Hauptmenü des Acrobat Reader auf den Menüpunkt „Datei“ und „Drucken“.

2.7. Verwendete graphische Symbole

In dieser Anleitung werden die folgenden graphischen Zeichen verwendet, um Warnungen vor möglichen Gefahren und Risiken optisch besonders zu kennzeichnen. Die Zeichen entsprechen den Vorgaben der Berufsgenossenschaftlichen Vorschrift für Sicherheit und Gesundheit bei der Arbeit (BGV A8) von 2002.

Symbol	Bedeutung
	Warnung vor möglichen Gefahren und Risiken, die zu **Sachschäden und / oder Personenschäden führen können.**
	Warnung vor möglichen Gefahren und Risiken aufgrund **elektrischer Spannung.**
	Warnung vor Stolpergefahr.
	**Verbot** Die mit diesem Zeichen gekennzeichnete Aktion ist zur Vermeidung von Gefahren unbedingt zu unterlassen.
	**Wichtiger Hinweis** Bei Nichtbeachtung sind Probleme möglich oder wahrscheinlich.

3. Sicherheitshinweise

Dieses Kapitel enthält:

- ✓ Sicherheitshinweise und Vorsichtsmaßnahmen beim Betrieb dieses Produkts
- ✓ Warnungen vor potentiellen Schäden durch möglichen Fehlgebrauch

Bitte lesen Sie vor der Inbetriebnahme dieses Produkts die in diesem Kapitel dargestellten Sicherheitshinweise aufmerksam durch und beachten Sie die Ihnen zur Verfügung gestellten Informationen und Hinweise.

3.1. Bestimmungsgemäße Verwendung

Dieser MIMO Access Point wurde konzipiert für den Einsatz in kleineren und mittleren Büros und an Heimarbeitsplätzen. Eine verbreitete Bezeichnung für diesen Anwendungsbereich lautet "Small Office - Home Office" (SO-HO). Der MIMO Access Point stellt Wireless Geräten einen gemeinsamen Verbindungspunkt zur Kommunikation untereinander zur Verfügung.

3.2. Bestimmungswidrige Verwendung

Folgende Verwendung des MIMO Access Points gilt als nicht bestimmungsgemäß:

- ✓ Einsatz im Außenbereich oder in feuchten Räumen.
- ✓ Einsatz in hochsensiblen Umgebungen, die ein absolut fehlerfreies Funktionieren des IT-Systems erfordern und in denen ein technisches Versagen oder eine unangemessene oder missbräuchliche Anwendung zum Tod, zu Verletzungen oder anderen Schädigungen von Personen oder zu beträchtlichen Sach- oder Umweltschäden oder zu wirtschaftlichen bzw. finanziellen Schäden führen kann.

Das Produkt darf aus diesem Grund nicht in derartigen Verwendungszusammenhängen zum Einsatz gebracht werden. Beispiele für nicht vorgesehene Verwendungszusammenhänge sind:

- ✓ Krankenhäuser
- ✓ Flug- und Verkehrssicherung
- ✓ sensible Überwachungsanlagen

Eigenmächtige bauliche Veränderungen, An- oder Umbauten oder Reparaturversuche sind verboten. Eigenmächtige Manipulationen am Produkt oder am mitgelieferten Steckernetzteil können Gefahren für Sicherheit und Gesundheit einschließlich der Gefährdung unbeteiligter Personen hervorrufen!

3.3. Elektrische Spannung

Achten sie darauf, dass keine Flüssigkeiten oder Gegenstände (z. B. Büroklammern) in das Gehäuse dieses Produkts gelangen! Sonst besteht Gefahr durch elektrischen Schlag und Kurzschluss.

3.3.1. Steckernetzteil

- ✓ Dieses Produkt darf nur mit dem mitgelieferten Steckernetzteil in trockenen Räumen betrieben werden.
- ✓ Der Spannungswert der Stromversorgung am Einsatzort muss innerhalb des zulässigen Bereichs (100-240 Volt, 50-60 Hz) liegen. Dieser ist oben auf dem Steckernetzteil angegeben.
- ✓ Um Gefährdungen durch elektrischen Strom zu vermeiden, darf das Steckernetzteil ausschließlich an eine ordnungsgemäß geerdete Steckdose (Schukosteckdose) angeschlossen werden. Verwenden sie keine Adapterstecker.

- ✓ Das Steckernetzteil darf durch den Benutzer auf keinen Fall geöffnet werden. Bitte versuchen Sie auf keinen Fall, das Steckernetzteil selbst zu reparieren. **Es besteht Gefahr durch Stromschlag!**

  Bei einem Defekt des Steckernetzteils oder der Kabelzuleitung kontaktieren Sie bitte zur Beschaffung eines Ersatznetzteils Ihren Händler oder nutzen Sie die Hotline des Herstellers.

- ✓ Spannungsführende Steckerkontakte oder Buchsen auf keinen Fall direkt oder mit spitzen, metallischen oder feuchten Gegenständen berühren! **Es besteht Gefahr durch Stromschlag!**

- ✓ Das Steckernetzteil darf nicht mehr verwendet werden, wenn Beschädigungen an der Kabeleinführung, dem Knickschutz oder der Isolierung der beweglichen Anschlussleitung vorliegen! **Es besteht Gefahr durch Stromschlag!**
- ✓ Nie am beweglichen Anschlusskabel des Steckernetzteils ziehen!

3.3.2. Blitzschlag und Überspannung

Ein Blitzschlag in der näheren Umgebung kann zu Schäden an den elektronischen Bauteilen und Überspannung führen. Schädigende Spannungsspitzen können sowohl im 230 Volt-Stromnetz als auch im Telefonleitungsnetz auftreten.

- ✓ Stellen Sie während eines Gewitters keine neuen Kabelverbindungen her und berühren Sie während des Gewitters keine Datenübertragungsleitungen.
- ✓ Trennen Sie vor Beginn eines Gewitters das Steckernetzteil des Produkts vom Stromnetz.

3.4. Aufstellort und Umgebungsbedingungen

Der Aufstellort des Produkts muss die folgenden Bedingungen erfüllen:

- ✓  mit dem Produkt verbundenen Kabel sind so zu verlegen, dass keine Stolpergefahr entsteht, und versehentliches Belasten der Kabel, Hängen bleiben etc. ausgeschlossen sind.
- ✓ Die Umgebung muss trocken sein.
- ✓ Stellen Sie das Produkt so auf, dass nicht versehentlich Flüssigkeiten mit dem Produkt in Kontakt kommen können, z.B. durch Umkippen von Getränken, Blumenvasen etc.
- ✓ Positionieren Sie das Produkt außerhalb der Reichweite von Kindern oder Haustieren.

3.4.1. Temperatur

- ✓ Stellen Sie das Produkt so auf, dass gute Belüftung von allen Seiten gewährleistet ist. Insbesondere ist darauf zu achten, dass die für die Gehäusebelüftung vorhandenen Lüftungsschlitze oder Gehäuseaussparungen nicht blockiert werden. Vermeiden Sie die Platzierung zwischen anderen Objekten.
- ✓ Schützen Sie das Produkt vor direkter Sonneneinstrahlung. Vermeiden Sie die Aufstellung in unmittelbarer Nähe eines Fensters.
- ✓ Stellen Sie das Produkt nicht auf elektronische Produkte oder andere Objekte, die sich erwärmen.
- ✓ Eine überhöhte Betriebstemperatur führt mit hoher Wahrscheinlichkeit zu vorübergehenden oder sogar anhaltenden Funktionsstörungen. Nach einer erwärmungsbedingten Funktionsstörung sollten Sie das Produkt für einige Minuten vom Stromnetz trennen.

3.4.2. Feuchtigkeit

- ✓ Berühren Sie das Steckernetzteil oder das Produkt niemals mit nassen oder feuchten Händen.
- ✓ Das Gerät und das Steckernetzteil dürfen niemals mit Wasser oder anderen Flüssigkeiten in Kontakt kommen, nass oder feucht werden.
- ✓ Das Produkt darf nicht betrieben werden, wenn die Luftfeuchtigkeit den im Datenblatt angegebenen zulässigen Höchstwert übersteigt.
- ✓ Das Produkt darf nicht eingesetzt werden in feuchten Bereichen im Innenraum wie z.B. Badezimmern oder Küchen, in feuchten Kellerräumen oder in Kellerräumen ohne eigene Entwässerung.
- ✓ Stellen Sie das Produkt nicht in unmittelbarer Nähe eines Fensters auf. Ferner kann das Produkt bei geöffnetem oder gekipptem Fenster (bzw. Oberlicht) im Falle von plötzlich einsetzendem starken Regen im ungünstigen Fall nass werden, was unbedingt zu vermeiden ist.

3.5. Vorsichtsmaßnahmen zum Schutz von Kindern

Stellen Sie das Produkt so auf, dass es für Kinder nicht erreichbar ist.

3.6. Zielgruppe und Anforderungen an den Benutzer

Dieses Produkt ist ausgelegt für den Einsatz durch Computernutzer, die über hinreichende Fachkenntnis im Umgang mit dem PC verfügen und die Beachtung der Sicherheitshinweise gewährleisten können.
Für die Inbetriebnahme und Konfiguration / Wartung dieses Produkts sind die folgenden Voraussetzungen und Kenntnisse erforderlich:

- ✓ Sichere und verantwortliche Handhabung von elektrischen Produkten und Telekommunikationseinrichtungen.
- ✓ Kenntnisse über Ihr Betriebssystem und TCP-IP-Netzwerke.

Wenn diese Voraussetzungen nicht erfüllt sind, sollte die Inbetriebnahme und Konfiguration/ Wartung durch Fachpersonal ausgeführt werden, um Risiken und mögliche Schäden infolge Fehlbedienung oder Fehlkonfiguration zu vermeiden.
Dieses Produkt ist nicht speziell ausgelegt und vorbereitet für Einsatz und Verwendung durch

- ✓ Menschen mit Behinderungen
- ✓ Senioren
- ✓ Kinder

Die Nutzung dieses Produkts, z. B. für die Anbindung an das Internet, ist für die o. g. Verwendergruppen deswegen nur unter der Voraussetzung möglich, dass Unterstützung und falls notwendig Beaufsichtigung durch eine sachkundige Person erfolgt.

3.6.1. Ausfall des IT-Systems

Bereits in kleinen Netzwerken kann der Ausfall einer einzigen Komponente, insbesondere an zentralen Knotenpunkten des Systems, zu einem Ausfall des gesamten Systems führen.
Neben technischem Versagen und höherer Gewalt (z.B. Überspannung nach einem Blitzeinschlag) sind es häufig Bedienungsfehler bzw. menschliches Fehlverhalten, die für den Ausfall einer IT-Komponente verantwortlich sind.

3.6.2. Notwendige Maßnahmen zum Schutz Ihres Netzwerkes

Im Rahmen von Inbetriebnahme des MIMO Access Points sind die folgenden Maßnahmen zum Schutz Ihres Netzwerkes und Ihrer Daten vor unbefugtem Eindringen von außen unbedingt durchzuführen:

- ✓ Sicheres Administrator-Passwort setzen
- ✓ Verschlüsselung des Datenverkehrs

4. Hardwareinstallation

4.1. Bedienelemente und Anschlüsse

4.1.1. Vorderseite des Geräts

LED	Anzeige von	Farbe	Status	Beschreibung
Power	Status der Spannungs-versorgung	Grün	Ein	Gerät ist mit dem Stromnetz verbunden.
Status	System-status	Grün	blinkt	System befindet sich im Normalbetrieb.
WLAN	Status der Wireless-Verbindung	Grün	blinkt	Der WAN-Port sendet oder empfängt Daten.
			blinkt	Daten werden über die Wireless-Verbindung gesendet oder empfangen.
Link 1~4	Verbindungs-status	Grün	Ein	Eine aktive Station ist an den entsprechenden LAN-Port angeschlossen.
10 / 100M	Datenrate	Grün	blinkt	Der entsprechende LAN-Port sendet oder empfängt Daten.
			Ein	Daten werden in 100 Mbps auf dem entpsrechenden LAN-Port übertragen.
Reset				Zurücksetzen des Geräts auf die werksseitigen Voreinstellungen

Änderung der Angaben ohne vorherige Ankündigung sind vorbehalten.

4.1.2. Rückseite des Geräts

Port	Beschreibung
PWR	Eingang Spannungsversorgung, 12 V 1A
LAN Ports 1-4:	Die Ports, mit denen Computer im Netzwerk und andere Geräte verbunden werden
3 Schraubanschlüsse:	Anbringung der Antennen

4.2. Installation der Hardware

1. Aufstellen des Wireless-Geräts

Sie können das Wireless-Gerät sowohl auf einem Tisch oder einer anderen waagerechten Oberfläche platzieren als auch an der Wand montieren. Platzieren Sie das Wireless-Gerät möglichst zentral in Ihrer Räumlichkeit an einem störungsfreien Ort. Eine mögliche Störungsquelle ist z. B. eine Metallwand oder eine Mikrowelle. Am Aufstellort müssen eine Netzsteckdose sowie ein Netzwerkanschluss vorhanden sein.

2. Einrichten der LAN-Verbindung

a. Wired LAN-Verbindung: Verbinden Sie das Kabel des Ethernet-Ports Ihres Computers mit einem LAN-Port dieses Produkts.

b. Wireless LAN-Verbindung: Platzieren Sie das Gerät an geeigneter Stelle, um eine optimale Übertragungsleistung zu erreichen.

3. Einschalten

Beim Einschalten nach Anschluss des Stromkabels führt dieses Produkt automatisch einen Selbsttest durch. In dieser Testphase leuchtet die Status-LED etwa 10 Sekunden lang konstant und blinkt dreimal, wenn der Vorgang abgeschlossen ist. Wenn die Status-LED einmal pro Sekunde blinkt, befindet sich das Produkt im Normalbetrieb.

5. Netzwerkeinstellungen und Softwareinstallation

5.1. Netzwerkeinstellungen auf Ihrem Computer

Die Standard-IP-Adresse dieses Produkts ist 192.168.123.254 und die der Subnetzmaske 255.255.255.0. In diesem Benutzerhandbuch werden die Standardwerte genannt. Sie können die Adressen jedoch nach Ihren Wünschen ändern. Wenn die TCP/IP-Umgebung Ihres PC noch nicht konfiguriert wurde, ist dies zunächst erforderlich. Eine Beschreibung des Vorgangs finden Sie in Anhang A. Nehmen Sie z. B. folgende Einstellungen vor:

1. IP-Adresse 192.168.123.1, Subnetzmaske 255.255.255.0 und Gateway 192.168.123.254, oder (noch einfacher):
2. Konfigurieren Sie Ihren PC so, dass dieser die TCP/IP-Einstellung automatisch über den DHCP-Server dieses Produkts vornimmt.

Nach Installation des TCP/IP-Protokolls können Sie die Verbindung des PCs mit diesem Produkt mithilfe des "Ping"-Befehls testen. Das folgende Beispiel zeigt diesen Vorgang für das Windows-Betriebssystem. Geben Sie den Befehl

```
ping 192.168.123.254
```

ein. Wenn Sie die Nachricht

```
Pinging 192.168.123.254 with 32 bytes of data:
Reply from 192.168.123.254: bytes=32 time=2ms TTL=64
```

erhalten, war der Verbindungsaufbau zwischen Ihrem PC und dem Gerät erfolgreich. Lautet die Nachricht jedoch

```
Pinging 192.168.123.254 with 32 bytes of data:
Request timed out.,
```

war der Installationsvorgang fehlerhaft. Überprüfen Sie in diesem Fall bitte der Reihe nach die folgenden Punkte:

1. Ist das Ethernet-Kabel zwischen dem PC und dem Gerät korrekt angeschlossen?

   Tipp: Die LAN-LED dieses Produkts und die Link-LED der Netzwerkkarte Ihres PC müssen leuchten.

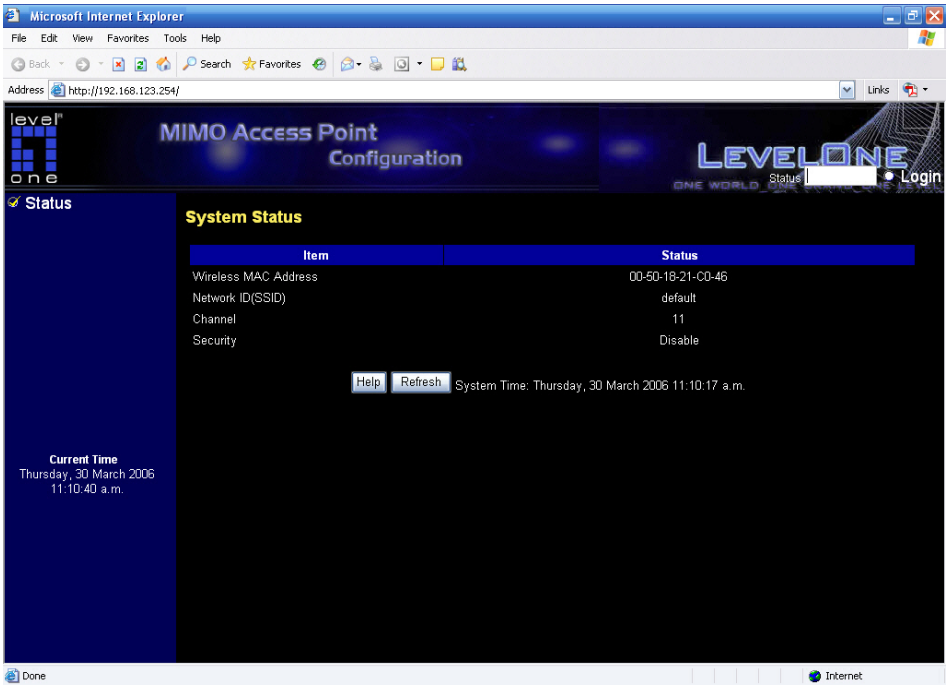
2. Ist die TCP/IP-Umgebung Ihres PCs richtig konfiguriert?

   Tipp: Wenn die IP-Adresse des Geräts 192.168.123.254 ist, muss für Ihren Computer die IP-Adresse 192.168.123.X eingestellt sein, und für den Standard-Gateway 192.168.123.254.

6. Konfiguration des Wireless-Geräts

Dieses Produkt ermöglicht eine webbasierte Konfiguration über Ihren Web-Browser, wie z. B. Netscape Communicator oder Internet Explorer. Dies gilt für alle MS Windows-, Macintosh- und UNIX-Betriebssysteme.

Systemstart und Log-in



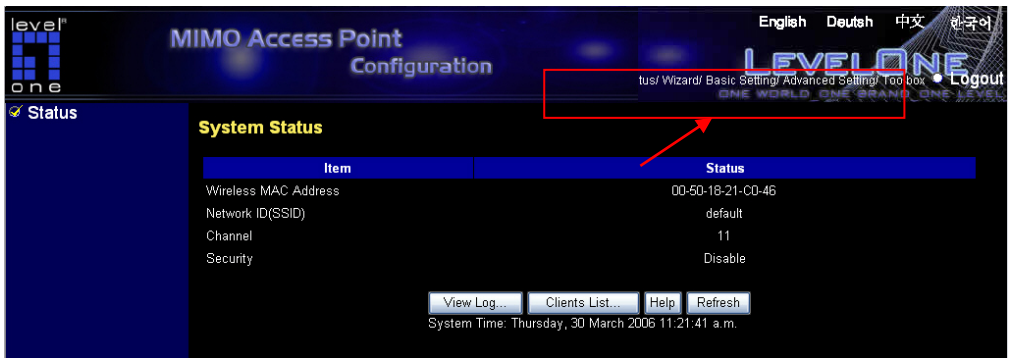
Öffnen Sie Ihren Browser und deaktivieren Sie den Proxyserver bzw. tragen Sie die IP-Adresse des Produkts als Ausnahme ein. Geben Sie anschließend die IP-Adresse des Geräts im Feld „Location“ (Netscape) bzw. „Adresse“ (IE) ein und klicken Sie auf „OK“. Beispiel: http://192.168.123.254.

Nachdem die Verbindung hergestellt wurde erscheint die webbasierte User-Schnittstelle dieses Produkts. Es gibt zwei verschiedene Bildschirme für die User-Schnittstelle: einen für normale Benutzer und einen für Systemadministratoren.

Um sich als Administrator anzumelden, geben Sie das System-Passwort (werksseitig voreingestellt ist „admin“) in das gleichnamige Feld ein und klicken Sie auf die „Login“-Schaltfläche. Wenn das korrekte Passwort eingegeben wurde, erscheint der Bildschirm des Administrator-Konfigurationsmodus. Die verschiedenen Optionen für die Systemverwaltung sind im Hauptmenü aufgelistet.

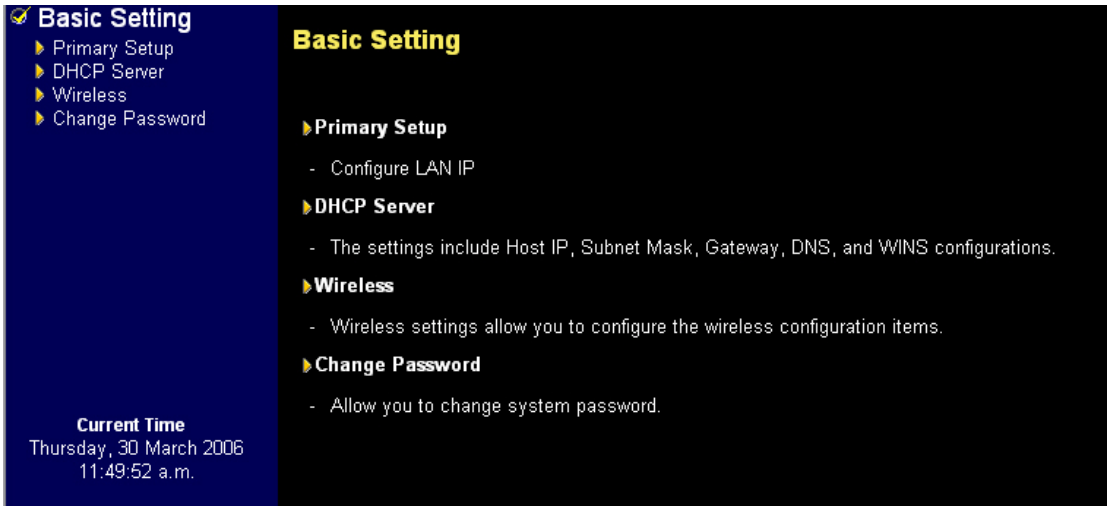
Systemmenü

Wenn Sie sich für den WAP-0010 anmelden, erscheint das Systemmenü oben rechts.

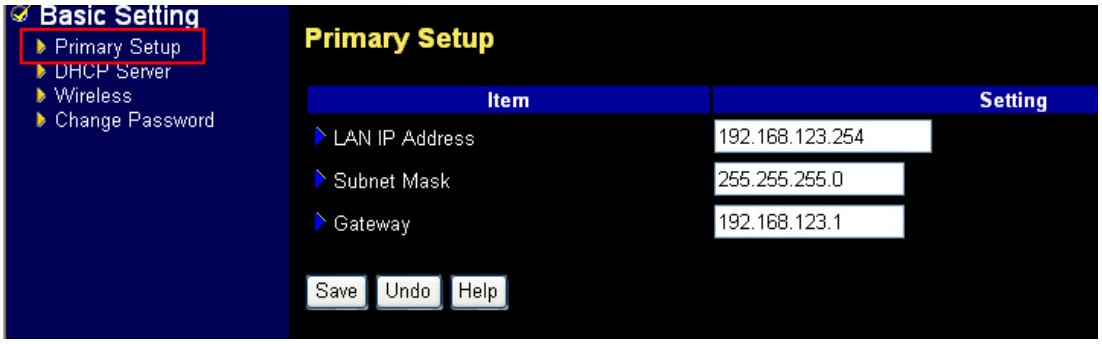


6.1. Grundeinstellungen

In diesem Menü können Sie IP-Adresse, DHCP, Wireless und Passwort einstellen.



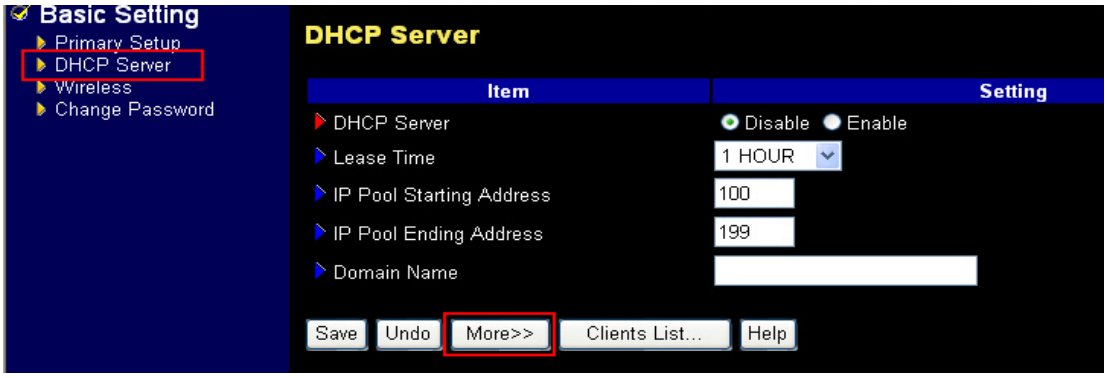
6.1.1. Anfangssetup



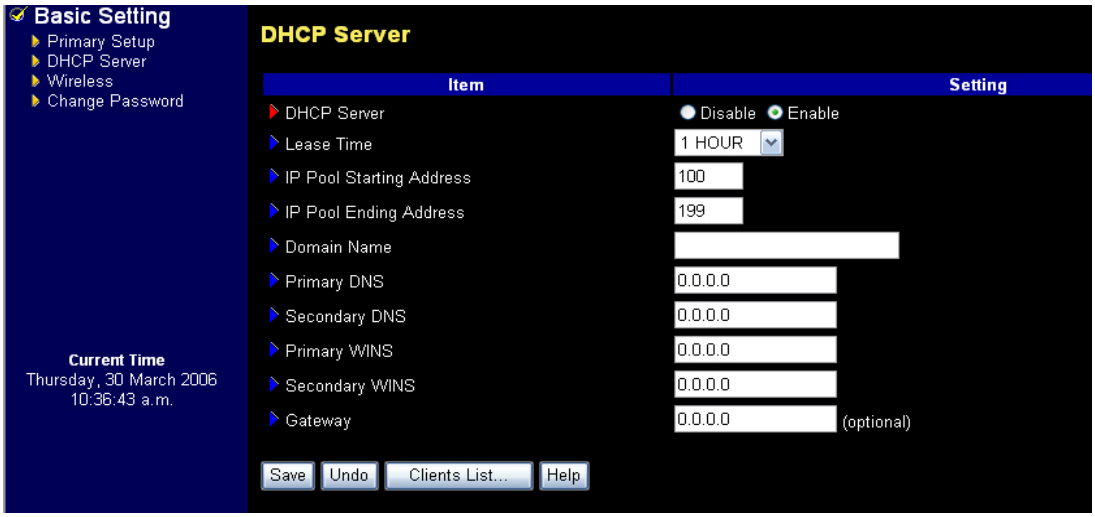
Dies ist eine Primär-Option für die einwandfreie Funktion dieses Produkts. Geben Sie hier die IP-Adresse des WAP-0010 ein. Die standardmäßig vorgegebene IP-Adresse lautet **192.168.123.254.**

LAN IP Address: Dies ist die lokale IP-Adresse des Geräts. Bei allen Computern Ihres Netzwerks muss die LAN IP-Adresse dieses Produkts eingestellt sein. Wenn erforderlich, können Sie diese IP-Adresse ändern.

6.1.2. DHCP-Server



Klicken Sie auf „More>>".

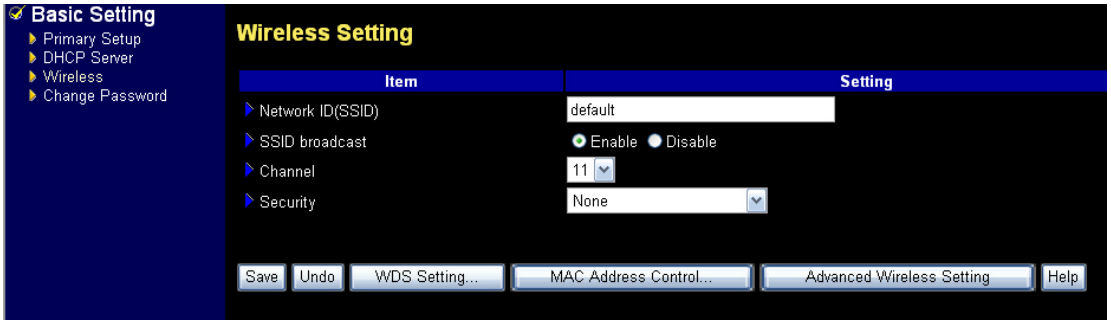


Die Einstellungen der TCP/IP-Umgebung umfassen die Konfiguration der Host-IP, der Subnetzmaske, des Gateways sowie des DNS. Die manuelle Konfiguration aller Computer und Geräte Ihres Netzwerks ist nicht einfach. Der DHCP-Server bietet eine vereinfachte Möglichkeit, diese Einstellungen vorzunehmen. Das Gerät unterstützt diese Funktion des DHCP-Servers. Wenn Sie den DHCP-Server dieses Produkts aktivieren und die automatische IP-Zuweisung wählen, dann lädt das Gerät die richtigen TCP/IP-Einstellungen automatisch nach Einschalten des Computers. Die DHCP-Server-Einstellungen umfassen die folgenden Punkte:

1. **DHCP Server**: Wählen Sie „Diable" oder „Enable". Die Standardeinstellung ist „Disable" (deaktiviert).
2. **IP Pool Starting Address / IP Pool Ending Address**: Wenn ein Computer dies anfordert, weist der DHCP-Server

   diesem automatisch eine neue IP-Adresse aus dem IP-Adress-Pool zu. Hierzu müssen Sie den Umfang des IP-Adress-Pools durch die Angabe einer Anfangs- und Endadresse spezifizieren.
3. **Domain Name**: Optional. Diese Information wird an den Client weitergegeben.
4. **Primary DNS / Secondary DNS**: Über dieses Feature können Sie DNS-Server zuweisen.
5. **Primary WINS / Secondary WINS**: Über dieses Feature können Sie WINS-Server zuweisen.
6. Gateway: Bei der Gateway-Adresse handelt es sich um eine alternative Gateway-IP-Adresse.
7. Hier können Sie Ihrem Computer einen weiteren Gateway zuweisen, wenn der DHCP-Server dem Computer eine IP anbietet.

6.1.3. Wireless-Setup



Über den Bildschirm „Wireless Setting“ können verschiedene Einstellungen für Wireless vorgenommen werden.

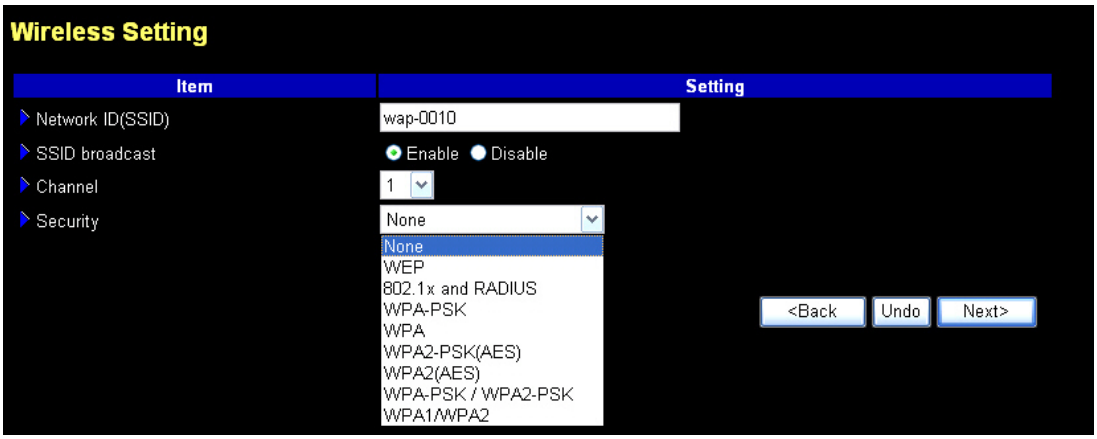
Network ID (SSID): Service Set Identifier (SSID). Die Netzwerk-ID dient der Identifizierung des Wireless LAN (WLAN). Im Empfangsbereich dieses Geräts sowie über Geräte, die die gleiche Netzwerk-ID (die Werkseinstellung ist „default“) haben, können Client-Stationen frei roamen (wandern). Die maximale Länge beträgt 32 Zeichen.

SSID Broadcast: Das Gerät überträgt Signale, die Informationen enthalten.
So weiß der Wireless-Client, wie viele ap-Geräte zur Verfügung stehen, indem er das Netzwerk durchsucht. Wenn diese Funktion deaktiviert ist, kann der Wireless-Client die Geräte nicht über die Signale finden.

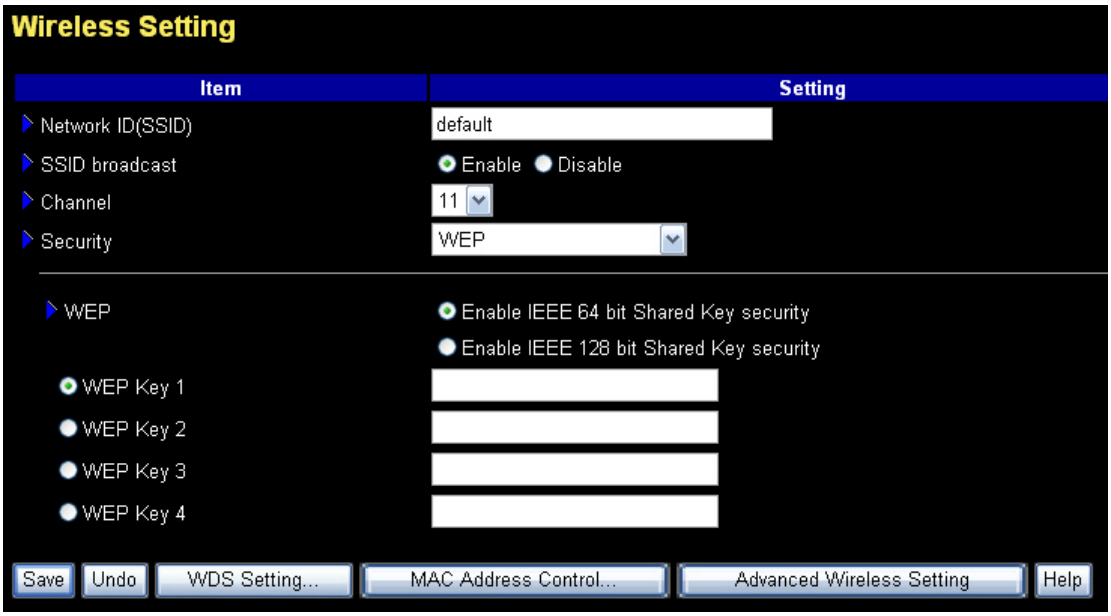
Channel: Der 802.11-Standard definiert insgesamt 14 Frequenzkanäle. Der FCC stellt in den USA die Kanäle 1 bis 11 zur Verfügung; in Europa können meist die Kanäle 1 bis 13 verwendet werden, in Japan hingegen die Kanäle 1 bis 14.

Security: Wählen Sie den gewünschten Datenverschlüsselungs-Algorithmus. Durch Aktivierung der „Security“-Funktion können Sie Ihre Daten während des Transports von einer Station zur anderen schützen.

6.1.4. Wireless-Sicherheitsarten



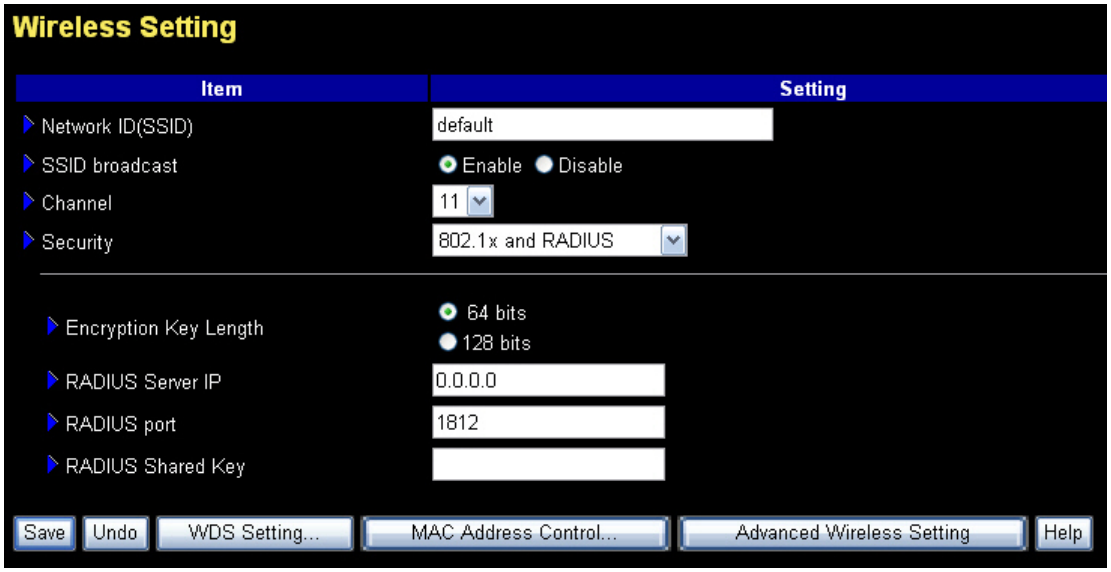
WEP (Wired Equivalent Privacy)



Dieser Dienst verwendet ein auf RC4 (Ron's Code 4) basierendes Verschlüsselungsschema, um die Ladung der 802.11-Datenrahmen einzukapseln. Dieses Schema wird auch WEP (Wired Equivalent Privacy) genannt. WEP kann nur mit einem gemeinsamen Schlüssel verwendet werden. Es verwendet den symmetrischen RC4-Algorithmus und einen Zufallszahlengenerator. Die vorgegebenen Standardwerte umfassen Schlüssellängen von 40 (a.k.a. 64) und 128 Bits und einen Initialisierungsvektor (IV) von 24 Bits.

Wenn Sie die 128 oder 64 Bit WEP Key-Verschlüsselung aktivieren, wählen Sie bitte einen zu verwendenden WEP-Schlüssel aus und geben Sie 26 bzw. zehn Hexadezimalzeichen (0, 1, 2…8, 9,A, B…F) ein.

802.1X



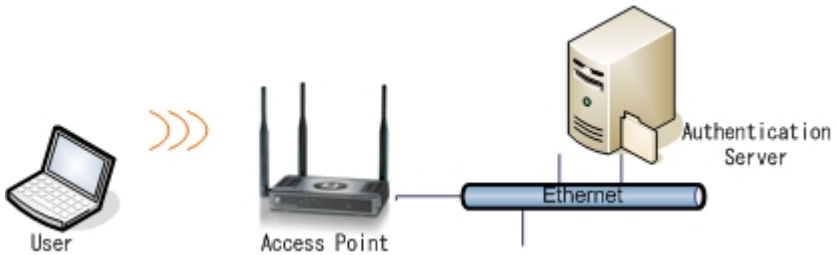
IEEE 802.1X bietet einen effizienten Rahmen für die Authentifizierung und Steuerung des Benutzerverkehrs zu einem geschützten Netzwerk sowie die dynamische Variierung der Kodierungsschlüssel. 802.1X verbindet ein Protokoll namens EAP (Extensible Authentication Protocol) mit verkabelten und Wireless-Medien und unterstützt unterschiedliche Authentifizierungsmethoden, wie zum Beispiel „Token Cards“, Kerberos, Einmalpasswörter, Zertifikate und „Public Key Authentication“. Weitere Details hierzu finden Sie in Anhang B.

Das Ankreuzfeld wird zum Aktivieren bzw. Deaktivieren der 802.1X-Funktion verwendet. Durch Aktivieren der 802.1X-Funktion wird erreicht, dass sich jeder Wireless-Netzwerk-User vor dem Verbindungsaufbau zunächst für dieses Gerät authentifizieren muss.

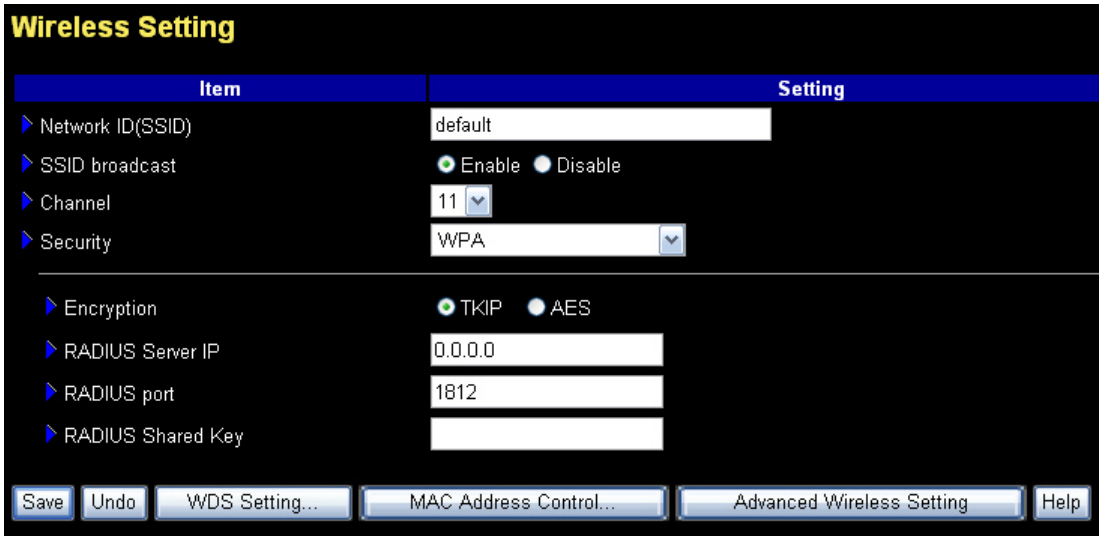
RADIUS-Server

RADIUS Server IP oder Domainname des 802.1X-Servers
RADIUS port : Die standardmäßig vorgegebene Einstellung ist 1812.
RADIUS Shared Key : Geben Sie hier den gemeinsamen Schlüsselwert des RADIUS-Servers und dieses Geräts ein. Beide Werte stimmen überein.

Beispiel



WPA (Wi-Fi Protected Access)



Ein Versuch der Wi-Fi Alliance, Sicherheitslücken von WEP auszubessern. WPA ist eine Untergruppe der Wireless-Sicherheitsspezifikationen von IEEE 802.11i. Der Schlüssel bei WPA ist der Gebrauch von TKIP (Temporal Key Integrity Protocol), um die Verschlüsselung von Wireless-Paketen zu unterstützen. Außerdem verwendet WPA 802.1x- und EAP-Authentifizierung und wird basierend auf einem zentralen Authentifizierungsserver, wie zum Beispiel RADIUS, verwendet.

Über das Ankreuzfeld wird die WPA-Funktion aktiviert bzw. deaktiviert. Durch Aktivieren der WPA-Funktion wird erreicht, dass sich jeder Wireless-Netzwerk-User vor dem Verbindungsaufbau zunächst für dieses Gerät authentifizieren muss.

RADIUS-Server

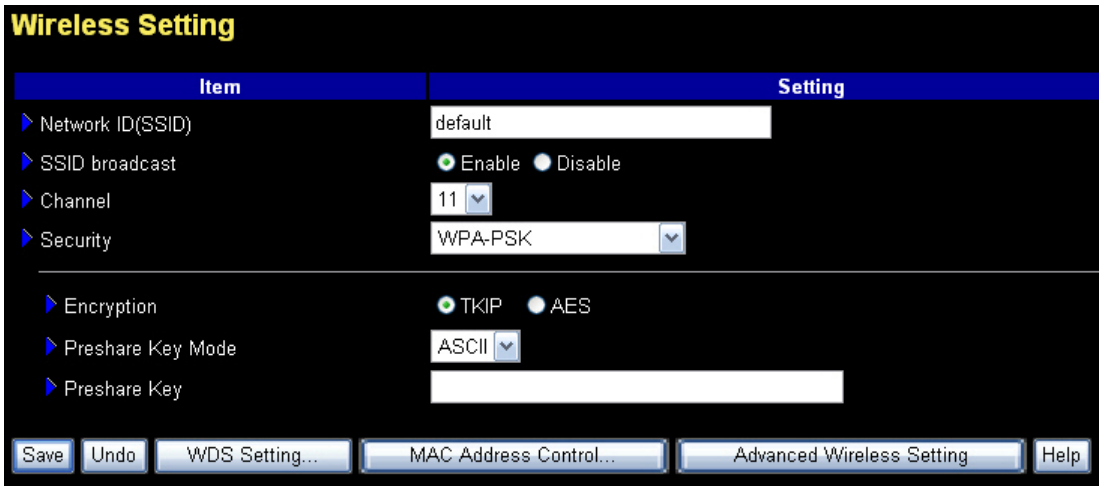
Encryption

TKIP: Temporal Key Integrity Protocol; ist ein Teil des IEEE 802.11i-Verschlüsselungsstandards für Wireless LANs. TKIP ist die nächste Generation von WEP, dem Wired Equivalency Protocol, das zur Sicherheit von 802.11 Wireless LANs verwendet wird. TKIP bietet eine paketweise Verschlüsselung, eine Nachrichtenintegritätsprüfung und einen Re-Keying-Mechanismus. Dadurch werden die Schwächen von WEP ausgebessert.

AES: Advanced Encryption Standard, auch bekannt als Rijndael; hierbei handelt es sich um einen Blockchiffre, der als Verschlüsselungsstandard von der US-Regierung übernommen wurde. Er wird wie sein Vorgänger (DES = Data Encryption Standard) weltweit verwendet und analysiert.

RADIUS IP address oder Domainname des 802.1X-Servers
RADIUS port: Die standardmäßig vorgegebene Einstellung ist 1812.
RADIUS Shared Key: Geben Sie hier den gemeinsamen Schlüsselwert des RADIUS-Servers und dieses Geräts ein. Beide Werte stimmen überein.

WPA-PSK (WPA Pre Shared Key)



WPA Pre-Shared Key (oder kurz: WPA-PSK) ist eine WPA-Variation. Bei WPA-PSK handelt es sich um eine vereinfachte, jedoch immer noch leistungsstarke Form von WPA, die besonders für Wi-Fi-Netzwerke im Heimgebrauch zu empfehlen ist. Für die Verwendung von WPA-PSK muss eine Person, genau wie bei WEP, einen statischen Schlüssel oder eine Passphrase bestimmen. Beim Gebrauch von WPA-PSK mit TKIP ändert sich der Schlüssel jeweils nach einem bestimmten Zeitintervall. Dadurch wird es Hackern erschwert, diesen Schlüssel zu finden und auszuwerten.

TKIP: Temporal Key Integrity Protocol; ist ein Teil des IEEE 802.11i-Verschlüsselungsstandards für Wireless LANs. TKIP ist die nächste Generation von WEP, dem Wired Equivalency Protocol, das zur Sicherheit von 802.11 Wireless LANs verwendet wird. TKIP bietet eine paketweise Verschlüsselung, eine Nachrichtenintegritätsprüfung und einen Re-Keying-Mechanismus. Dadurch werden die Schwächen von WEP ausgebessert.

AES: Advanced Encryption Standard, auch bekannt als Rijndael; hierbei handelt es sich um einen Blockchiffre, der als Verschlüsselungsstandard von der US-Regierung übernommen wurde. Er wird wie sein Vorgänger (DES = Data Encryption Standard) weltweit verwendet und analysiert.

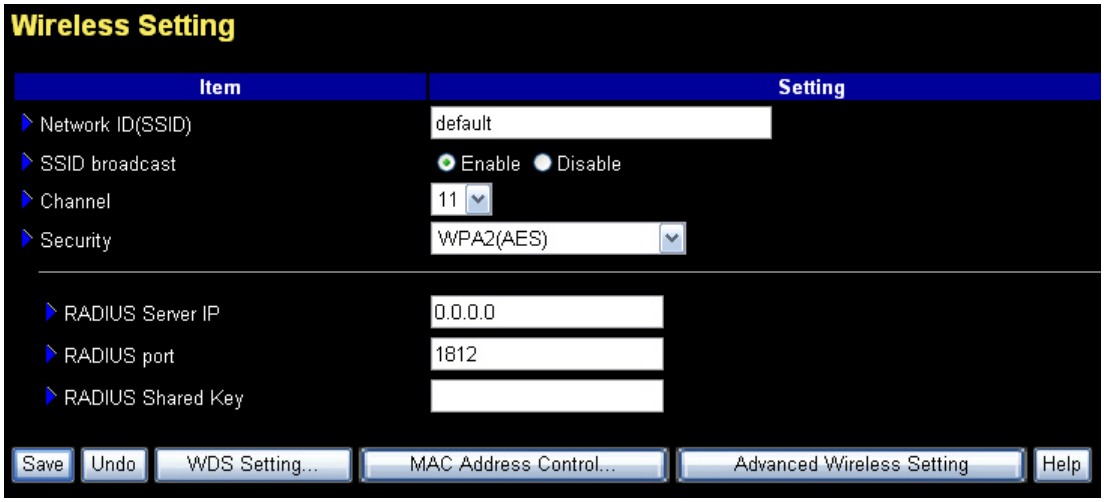
1. Treffen Sie eine Auswahl für „Encryption“ und „Preshare Key Mode“.

   Wenn Sie „HEX” auswählen, müssen Sie 64 hexadezimale Zeichen (0, 1, 2…8, 9, A, B…F) eingeben.

   Wenn Sie „ASCII” auswählen, liegt die Länge des Schlüssel zwischen acht und 63 Zeichen.

2. Geben Sie z. B. 12345678 als „Preshare Key“ ein

WPA2(AES) Advanced Encryption Standard



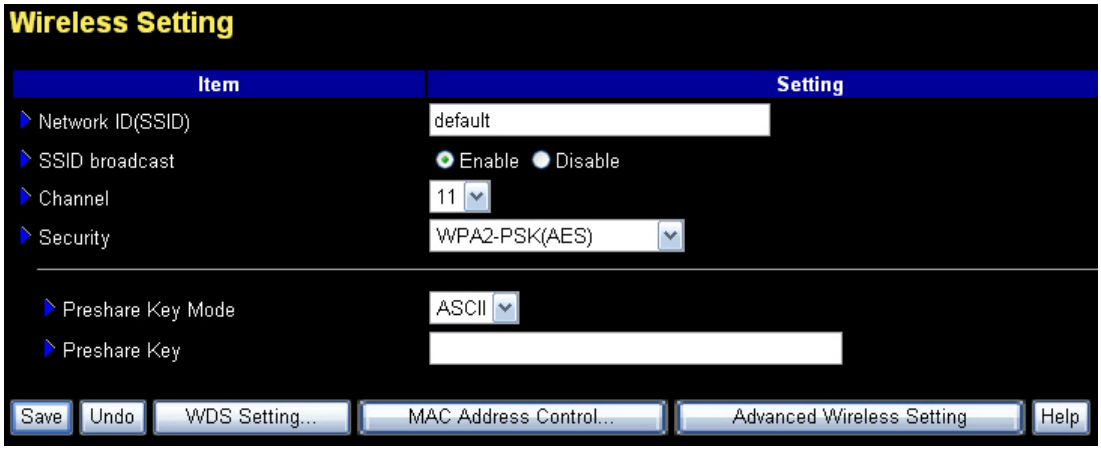
IEEE 802.11i, auch bekannt unter dem Namen WPA2, ist eine Neufassung des 802.11-Standards, der die Sicherheitsmechanismen für Wireless-Netzwerke bestimmt. Der WPA2-Standard ersetzt die vorherige Sicherheitsspezifikation WEP (Wired Equivalent Privacy), da sich bei dieser folgeschwere Schwächen offenbart haben. WPA2. 802.11i verwendet AES-Blockchiffren; WEP und WPA verwenden RC4-Stromchiffren.

Über das Ankreuzfeld wird die WPA-Funktion aktiviert bzw. deaktiviert. Durch Aktivieren der WPA2-Funktion wird erreicht, dass sich jeder Wireless-Netzwerk-User vor dem Verbindungsaufbau zunächst für dieses Gerät authentifizieren muss.

RADIUS-Server

RADIUS IP address oder Domainname des 802.1X-Servers
RADIUS port : Die standardmäßig vorgegebene Einstellung ist 1812.
RADIUS Shared Key : Geben Sie hier den gemeinsamen Schlüsselwert des RADIUS-Servers und dieses Geräts ein. Beide Werte stimmen überein.

WPA2-PSK(AES)



Ähnlich wie der WPA Pre-Shared Key; hier werden jedoch AES-Blockchiffren verwendet.

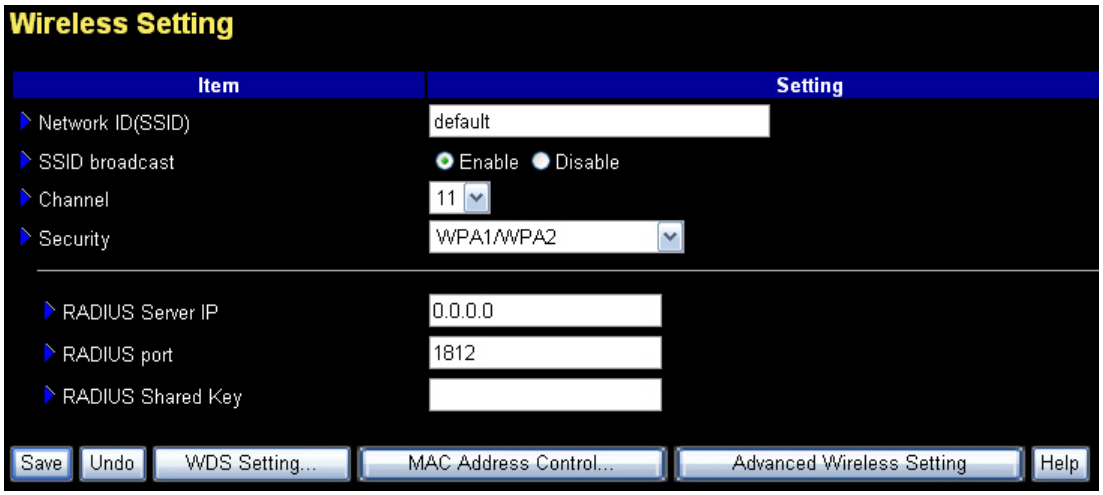
1. Treffen Sie eine Auswahl für den „Preshare Key Mode“.

   Wenn Sie „HEX” auswählen, müssen Sie 64 hexadezimale Zeichen (0, 1, 2…8, 9, A, B…F) eingeben.

   Wenn Sie „ASCII” auswählen, liegt die Länge des Schlüssels zwischen acht und 63 Zeichen.

2. Geben Sie z. B. 12345678 als „Preshare Key“ ein

WPA1 / WPA2

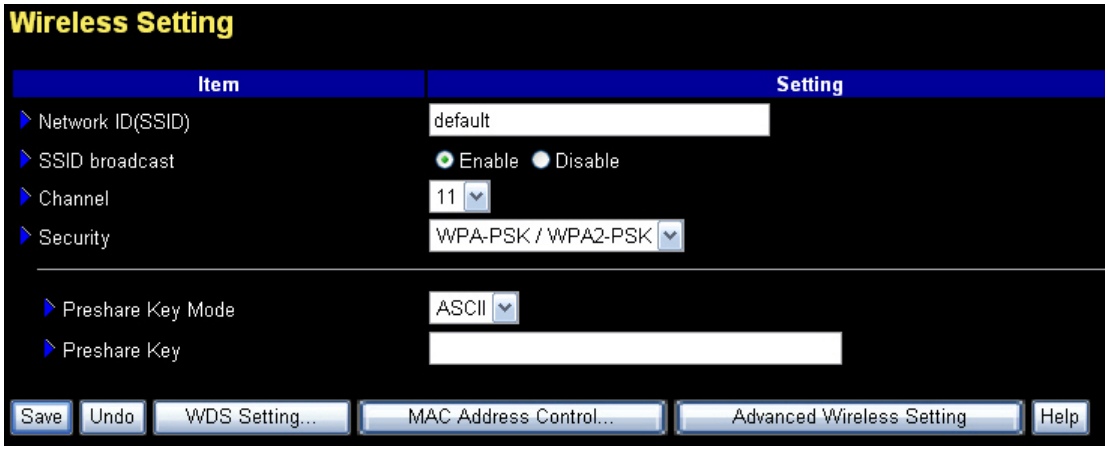


Das Gerät erkennt automatisch, welchen Sicherheitstypen (WPA1 oder WPA2) der Client zur Verschlüsselung verwendet.

Über das Ankreuzfeld wird die WPA1 / WPA2-Funktion aktiviert oder deaktiviert. Wenn diese Funktion aktiviert ist, muss sich jeder Wireless-Netzwerkbenutzer vor dem Verbindungsaufbau zunächst für das Gerät authentifizieren.RADIUS-Server

RADIUS IP address oder Domainname des 802.1X-Servers
RADIUS port : Die standardmäßig vorgegebene Einstellung ist 1812.
RADIUS Shared Key : Geben Sie hier den gemeinsamen Schlüsselwert des RADIUS-Servers und dieses Geräts ein. Beide Werte stimmen überein.

WPA-PSK / WPA2-PSK



Das Gerät erkennt automatisch, welchen Sicherheitstypen (WPA-PSK oder WPA2-PSK) der Client zur Verschlüsselung verwendet.

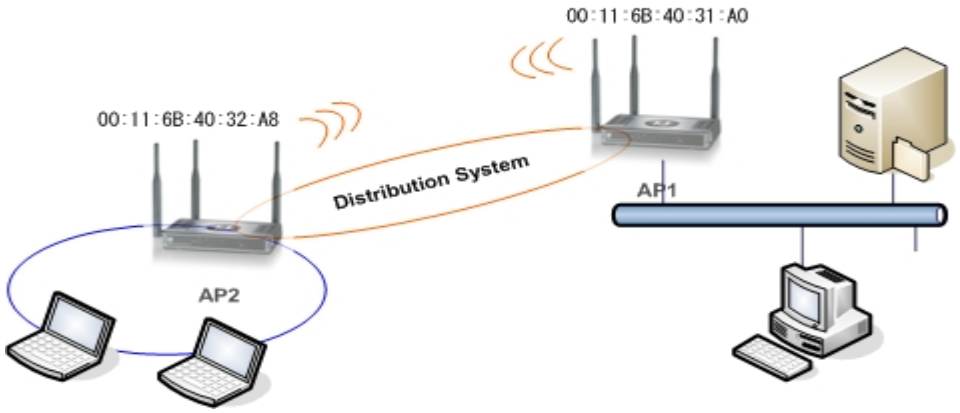
1. Treffen Sie eine Auswahl für den „Preshare Key Mode“.

   Wenn Sie „HEX” auswählen, müssen Sie 64 hexadezimale Zeichen (0, 1, 2…8, 9, A, B…F) eingeben.

   Wenn Sie „ASCII” auswählen, liegt die Länge des Schlüssels zwischen acht und 63 Zeichen.
2. Geben Sie z. B. 1ghteza&jggi als „Preshare Key“ ein

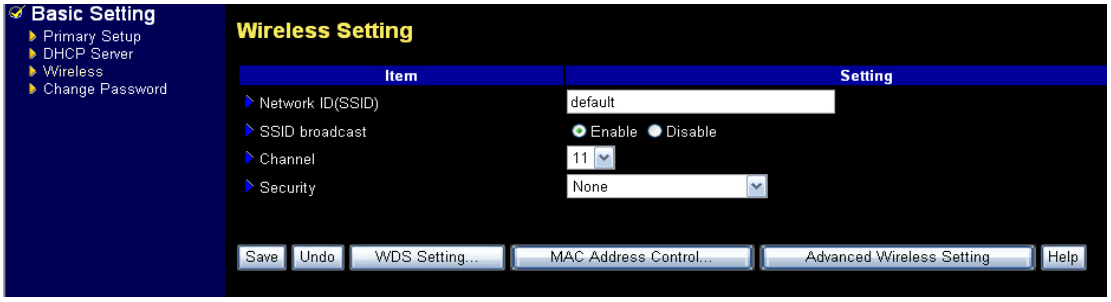
WDS (Wireless Distribution System)

WDS-Betrieb nach IEEE802.11-Standard ist möglich. Wenn WDS verwendet wird, können Geräte kabellos miteinander verbunden werden. So kann eine bereits verkabelte Infrastruktur auf Orte ausgedehnt werden, an denen eine Verkabelung nicht möglich oder unpraktisch ist. Weitere Details hierzu finden Sie in Anhang C.



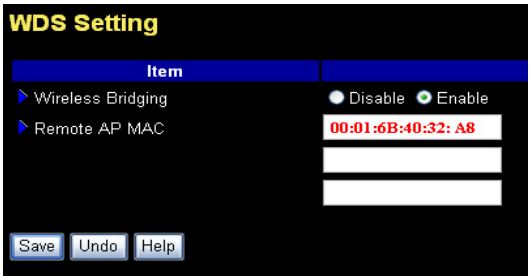
Um eine WDS-Verbindung herzustellen, müssen die Access Points an einem Ende der WDS-Verbindung mit der MAC-Adresse der PC-Karte im Access Point am anderen Ende der Verbindung konfiguriert werden. Der folgende Bildschirm zeigt die GUIs, die bearbeitet werden müssen.

1. Klicken Sie auf „WDS Setting…“

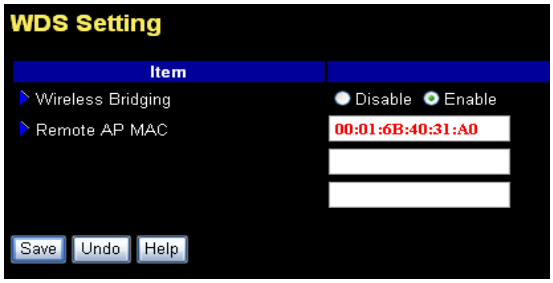


2. Wählen Sie „Enable” und geben Sie die AP-MAC-Adresse der Remoteseite ein, für die eine WDS-Verbindung benötigt wird. Beispiel: Für AP1 geben Sie 00:01:6B:40:32:A8 ein. Konfigurieren Sie außerdem die MAC-Adresse für den AP2-WDS als 00:01:6B:40:31:A0.

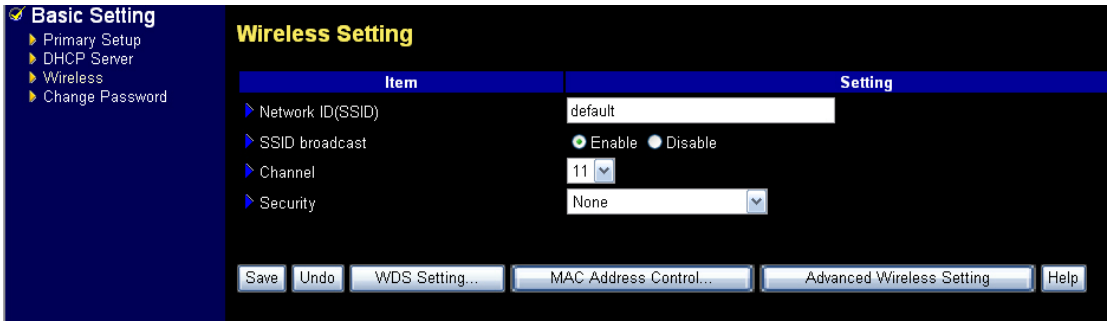
AP1

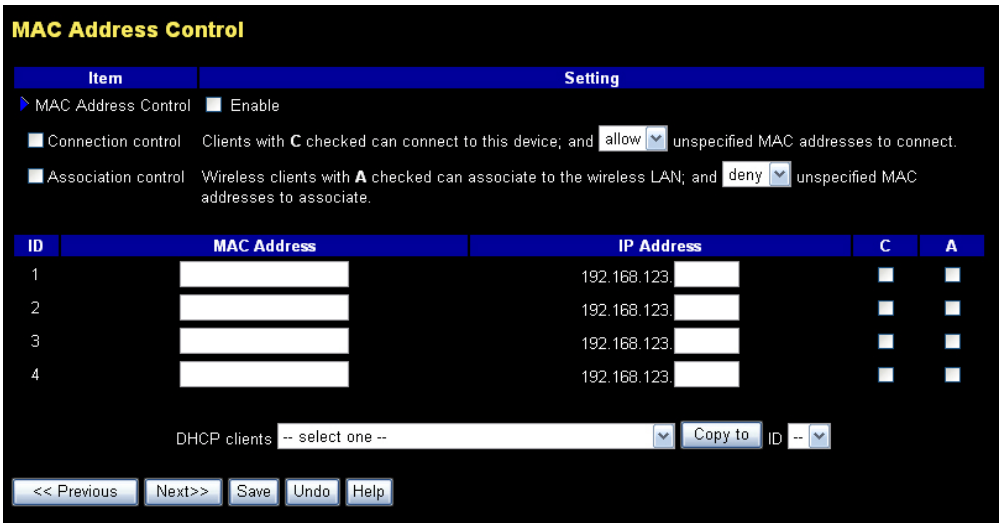


AP2



Steuerung der MAC-Adressen





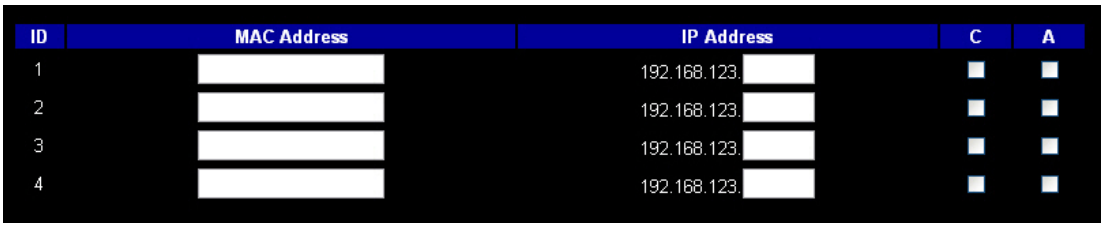
Die MAC-Adressensteuerung ermöglicht es, verschiedenen Nutzern unterschiedliche Nutzungsrechte sowie bestimmten MAC-Adressen bestimmte IP-Adressen zuzuweisen.

MAC Address Control: Markieren Sie „Enable", um die MAC-Adressensteuerung zu aktivieren. Sämtliche Einstellungen auf dieser Seite werden erst wirksam, wenn Sie „Enable" aktivieren.

Connection control: Aktivieren Sie das Kästchen „Connection control", wenn Sie festlegen möchten, welcher Client dieses Gerät nutzen darf. Wenn einem Client die Anwahl des Geräts gesperrt wird, bedeutet dies gleichzeitig, dass dieser Client keinen Zugriff auf das Internet hat. Wählen Sie „allow", wenn Sie den Clients, deren MAC-Adressen nicht in der Tabelle „Zugriffskontrolle" aufgeführt sind, die Anwahl des Geräts gestatten möchten und „deny", wenn Sie diesen Clients die Nutzung des Geräts verweigern möchten.

Association control:Markieren Sie „Association control", um zu steuern, welcher Wireless-Client mit welchem Wireless LAN verbunden werden kann. Wenn ein Client keinen Zugriff auf ein Wireless LAN erhält, bedeutet dies auch, dass der Client keine Daten über dieses Gerät senden oder empfangen kann. Wählen Sie „allow", wenn Sie den Clients, deren MAC-Adressen nicht in der Tabelle „Zugriffskontrolle" aufgeführt sind, die Verbindung mit dem Wireless LAN gestatten wollen, und „deny", wenn Sie diesen Clients die Nutzung des Wireless LAN verweigern wollen.

Tabelle „Zugriffskontrolle“



Die Tabelle „Zugriffskontrolle” befindet sich unten auf der Seite „MAC Address Control“. Jede Tabellenzeile enthält die MAC-Adresse sowie die erwartete IP-Adresse eines Clients. Die Tabelle hat drei Zeilen:

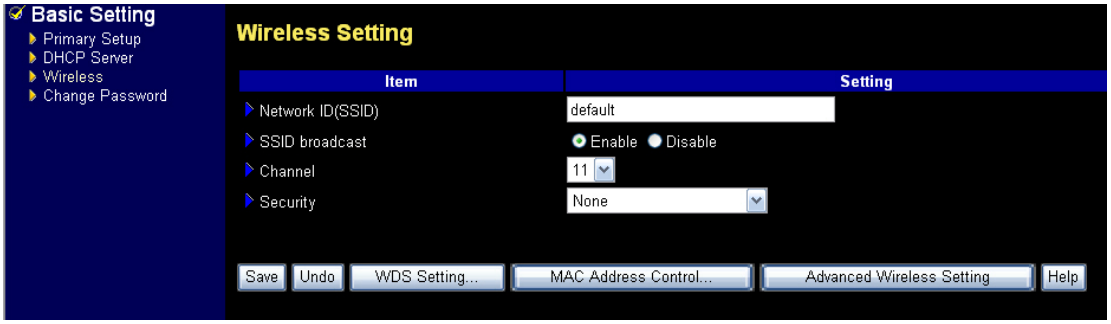
MAC Address	Die MAC-Adresse repräsentiert einen bestimmten Client.
IP Adress	Anzunehmende IP-Adresse des entsprechenden Clients. Lassen Sie das Feld leer, wenn Ihnen die Adresse nicht bekannt ist.
C	Wenn das Kästchen „Connection control” aktiviert ist, kann einem Client durch Aktivieren des Kästchens „C“ der Zugriff auf dieses Gerät gestattet werden.
A	Wenn das Kästchen „Association control” aktiviert ist, kann einem Client durch Aktivieren des Kästchens „A“ der Zugriff auf das Wireless LAN gestattet werden.

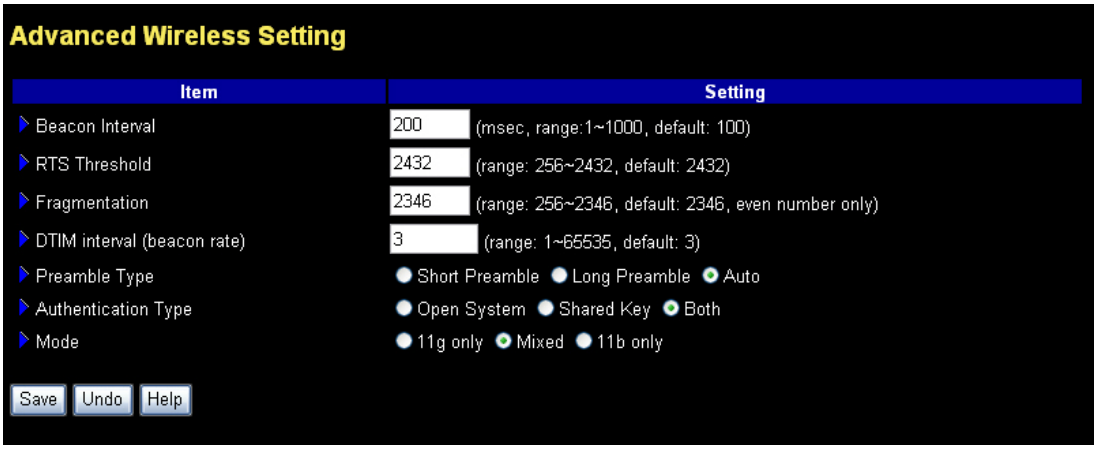
Folgendes Auswahlmenü mit „Copy to“-Schaltfläche erleichtert Ihnen die Eingabe der MAC-Adressen:

Wählen Sie im Menü „DHCP clients” den gewünschten Client aus und kopieren Sie durch Klicken auf die Schaltfläche „Copy to” die entsprechende MAC-Adresse hinüber in das Auswahlmenü „ID“.

Previous page / Next page: Zwecks einfacher und übersichtlicher Gestaltung der Konfigurationsseite erstreckt sich die Tabelle „Zugriffskontrolle“ über zwei Seiten. Verwenden Sie zum navigieren die Schaltflächen „<<Previous“ und „Next>>“.

Erweiterte Wireless-Einstellungen





Beacon Interval: Wenn ein Wireless-Netzwerkgerät ein Signal sendet, wird automatisch ein Leitstrahlintervall mitgesendet, das den Zeitpunkt bestimmt, an dem das Signal erneut gesendet wird. Das Intervall informiert die empfangenden Geräte im Netzwerk darüber, wie lange sie im Low-Power-Modus bleiben können, bis sie das Signal bearbeiten müssen. Der Verwalter des Netzwerks kann das Leitstrahlintervall einstellen. Es wird für gewöhnlich in Millisekunden (ms) gemessen.

RTS threshold (Request-to-Send Threshold): Die RTS-Schwelle bestimmt die Paketgröße einer RTS-Übertragung. Dadurch kann der Verkehrsfluss an einem Access Point kontrolliert werden, besonders dann, wenn viele Clients vorhanden sind.

Fragment: Beim Netzwerkbetrieb werden Pakete, deren Größe die Bandbreite des Netzwerks überschreitet, in kleinere Teile geteilt, sogenannte Fragmente.

DTIM interval: Ein DTIM-Intervall, auch „Data Beacon Rate" genannt, ist die Frequenz, bei der das Signal eines Access Points eine DTIM einschließt. Die Frequenz wird für gewöhnlich in Millisekunden (ms) gemessen.

Preamble Type: Bei einer Präambel handelt es sich um ein Signal, das in einer Wireless-Umgebung verwendet wird, um die Übertragungszeit einschließlich der Synchronisation und dem Start Frame Delimiter zu synchronisieren.

Authentication Type: Der Authentifizierungstyp bestimmt Konfigurationsoptionen für die gemeinsame Nutzung eines Wireless-Netzwerks, um die Identität und die Zugangsberechtigung von „roamenden" Wireless-Netzwerkkarten zu verifizieren. Sie können zwischen „Open System", „Shared Key" und „Both" wählen.

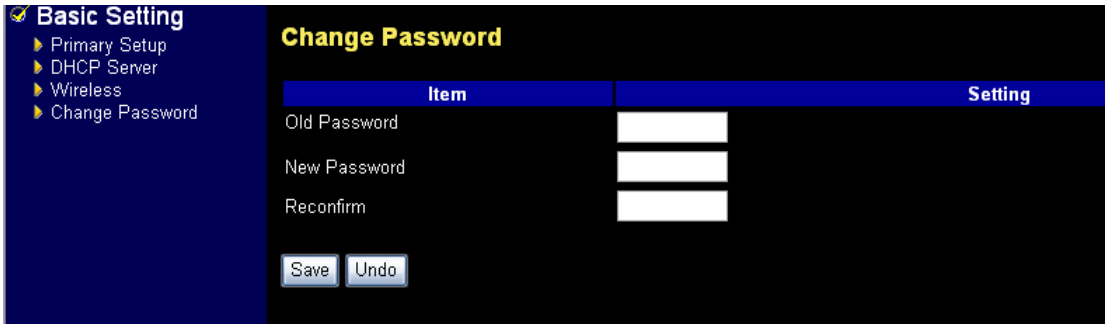
- **Open System:** Wenn ein Access Point „Open System" verwendet, muss sich der Wireless-Adapter im selben Authentifizierungsmodus befinden.

- **Shared Key:** „Shared Key" bedeutet, dass sowohl der Sender als auch der Empfänger einen gemeinsamen Schlüssel verwenden.

- **Both:** Wählen Sie „Both", damit der Netzwerkadapter, je nach Authentifizierungsmodus des Access Points, den Authentifizierungsmodus automatisch auswählt.

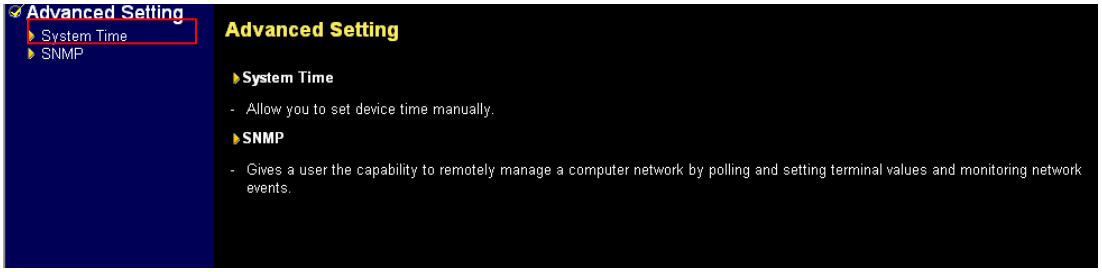
Mode: Wenn alle Geräte den 802.11g-Modus verwenden, belassen Sie die Einstellung bei 802.11g. Wenn einige Geräte jedoch auf 802.11b eingestellt sind, können Sie den Modus „Mixed" auswählen.

6.1.5. Passwort ändern

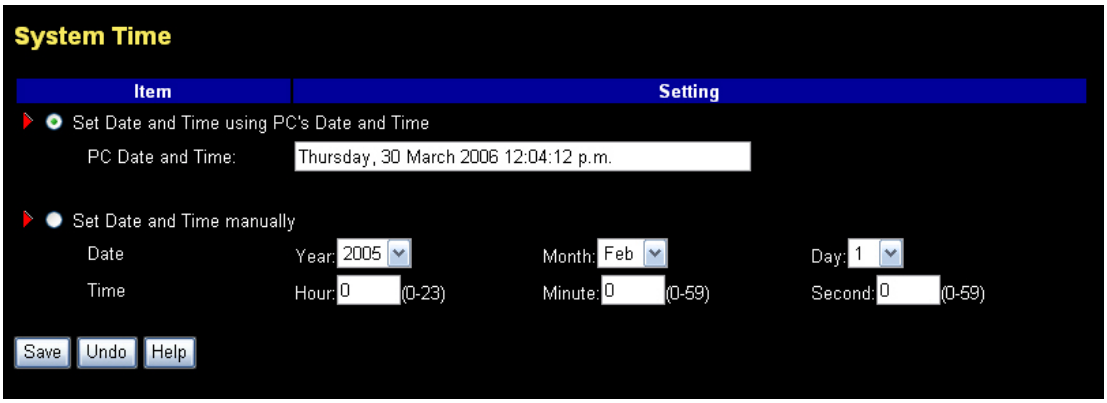


Hier können Sie das Passwort ändern. Aus Sicherheitsgründen empfehlen wir dringend, das Systempasswort zu ändern.

6.2. Erweiterte Einstellungen



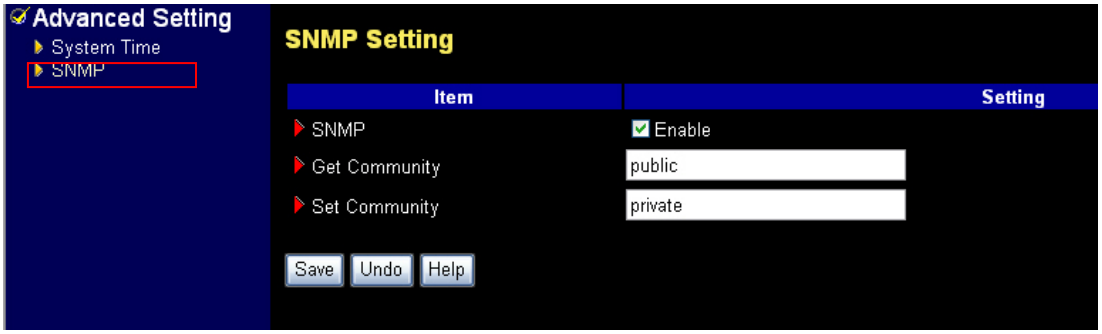
6.2.1. Systemzeit



Set Date and Time using PC's Date and Time: Aktivieren Sie diesen Punkt, um die Uhrzeit des Geräts mit der Uhrzeit des verbundenen PCs zu synchronisieren.

Set Date and Time manually: Aktivieren Sie diesen Punkt, wenn Sie eine manuelle Datums- und Zeiteinstellung vornehmen möchten.

6.2.2. SNMP-Einstellungen



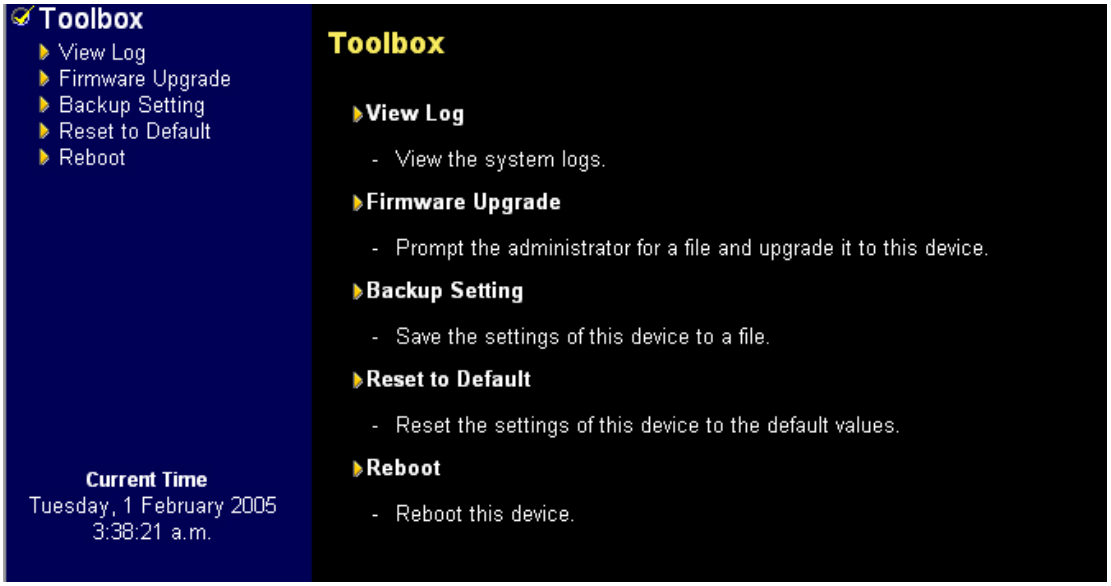
Das „einfache Protokoll für die Netzwerkverwaltung” (SNMP), ist, kurz gesagt, ein Protokoll, mit dem ein User ein Computernetzwerk extern verwalten kann. Dies geschieht durch zyklisches Abfragen, Setzen von Terminalwerten und Überwachung von Netzwerkereignissen.

Enable SNMP: Markieren Sie das Feld, um die SNMP-Funktion zu aktivieren.

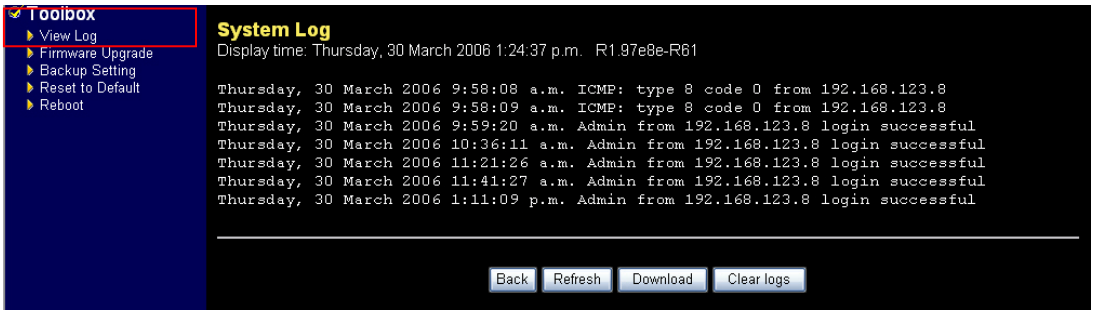
Get Community: Geben Sie hier die Gruppe ein, deren Anfragen (GetRequest) das Gerät beantworten soll.

Set Community: Geben Sie hier die Gruppe an, deren Eingaben (SetRequest) das Gerät entgegennehmen soll.

6.3. Toolbox



6.3.1. Loganzeige



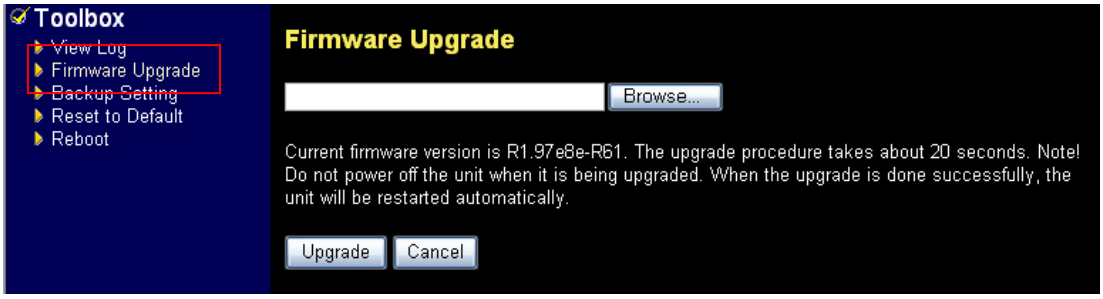
Klicken Sie im seitlichen Menü auf „View Log“, um die Systemlogdatei anzusehen.

Refresh: Klicken Sie auf „Refresh”, um die Systemlogseite zu aktualisieren.

Download: Klicken Sie auf „Download”, um die Logdatei im Textformat zu speichern.

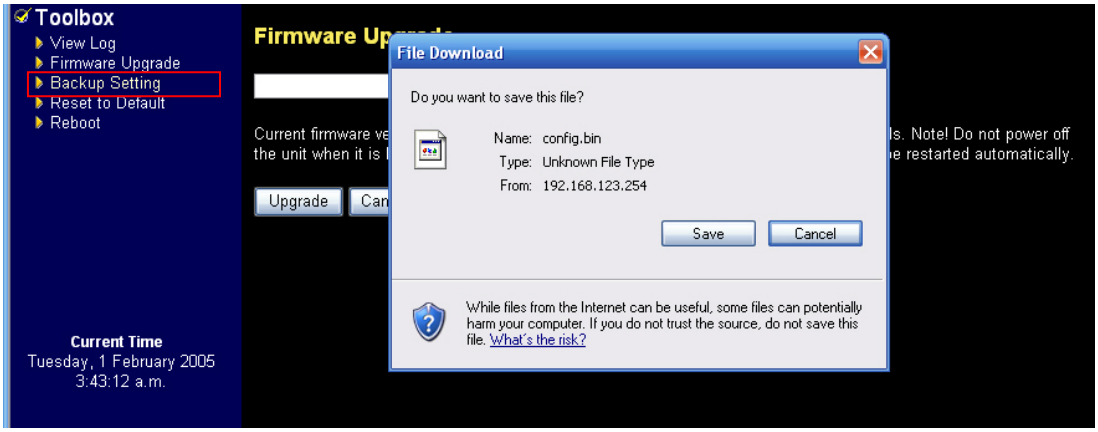
Clear logs: Löscht Loginhalte.

6.3.2. Firmware-Upgrade

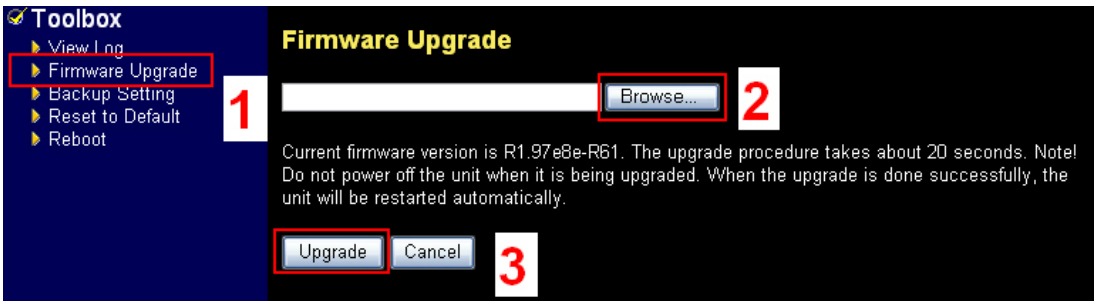


Klicken Sie auf „Firmware Upgrade“, um ein Upgrade der Firmware durchzuführen.

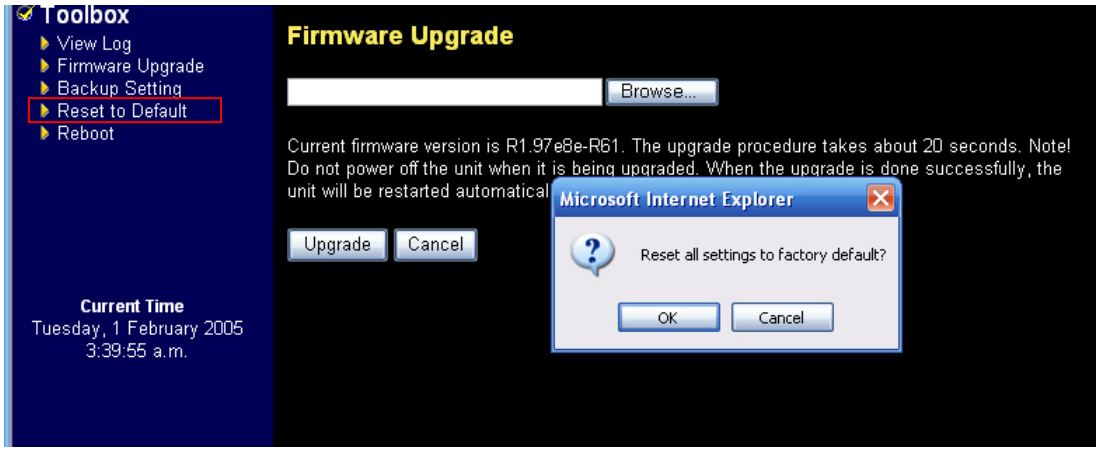
6.3.3. Sicherung der Einstellungen



Klicken Sie auf „Backup Setting", um für sämtliche Einstellungen ein Backup (Sicherungskopie) zu erstellen und dieses als *.bin-Datei abzuspeichern. Wenn Sie die Einstellungen wiederherstellen möchten, klicken Sie zunächst auf „Firmware Upgrade“, dann auf „Browser“ und wählen Sie die von Ihnen gesicherte Datei. Klicken Sie abschließend auf „Upgrade“.

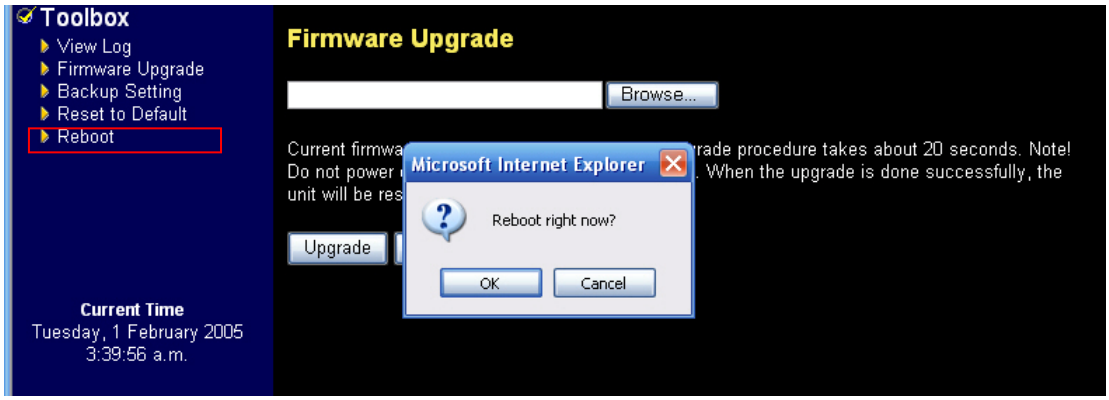


6.3.4. Zurücksetzen auf die werksseitigen Voreinstellungen



Durch Klicken auf „Reset to Default" im seitlichen Menü habe Sie die Möglichkeit, die Einstellungen auf die werksseitigen Voreinstellungen zurückzusetzen.

6.3.5. Neustart



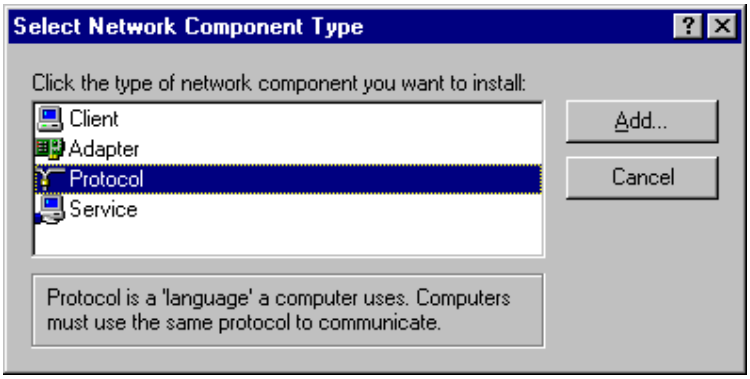
Klicken Sie auf „Reboot" im seitlichen Menü, um einen Neustart durchzuführen.

7. Anhang A TCP/IP-Konfiguration

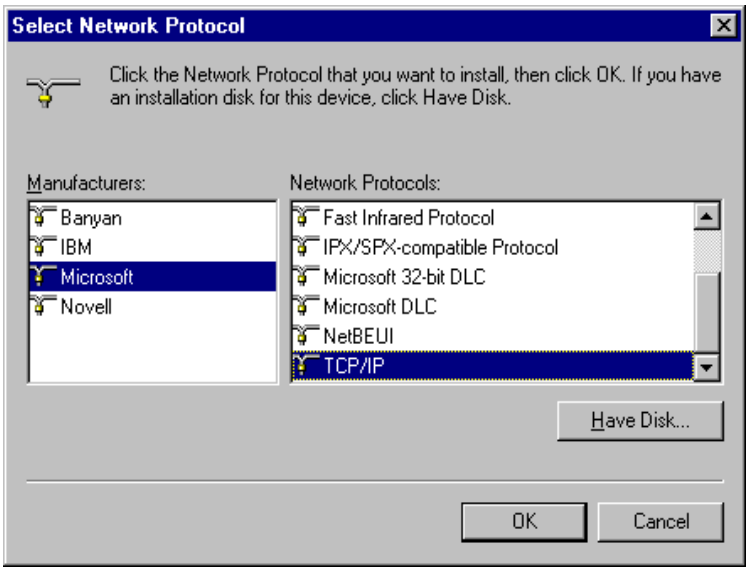
Dieser Abschnitt gibt Ihnen einen einführenden Überblick, wie Sie das TCP/IP-Protokoll für Ihre Netzwerkkarte einrichten. Voraussetzung für die Einrichtung des TCP/IP-Protokolls ist, dass auf Ihrem PC eine Netzwerkkarte korrekt installiert ist. Sollte dies nicht der Fall sein, lesen Sie die Bedienungsanleitung Ihrer Netzwerkkarte. In Abschnitt B.2 wird darüber hinaus die richtige Einstellung der TCP/IP-Werte erläutert, die für einen korrekten Betrieb in Kombination mit diesem Gerät erforderlich ist. (Beispiel für Windows 98SE)

A.1 Einrichtung des TCP/IP-Protokolls auf Ihrem PC

1. Klicken Sie auf „Start", „Einstellungen" und anschließend auf „Systemsteuerung".
2. Klicken Sie doppelt auf das Netzwerk-Symbol und wählen Sie im Netzwerk-Fenster die Registerkarte „Konfiguration" aus.
3. Klicken Sie auf die Schaltfläche „Hinzufügen", um eine Netzwerkkomponente auf Ihrem PC hinzuzufügen.
4. Klicken Sie doppelt auf „Internetprotokoll (TCP/IP)", um ein TCP/IP-Protokoll hinzuzufügen.



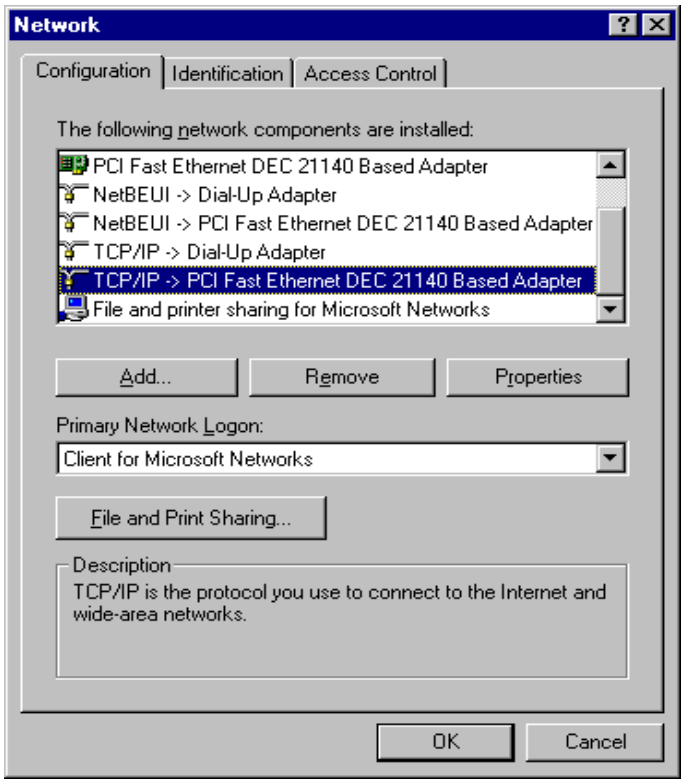
5. Wählen Sie in der Herstellerliste „Microsoft“ aus. Wählen Sie dann „TCP/IP” unter „Netzwerkprotokolle“. Klicken Sie auf „OK” um zurück zum Netzwerkfenster zu gelangen.



6. Das eingerichtete TCP/IP-Protokoll sollte nun im Netzwerkfenster angezeigt werden. Zum Abschluss des Einrichtvorgangs klicken Sie auf „OK“ und führen Sie anschließend einen Neustart des Computers durch, um das TCP/IP-Protokoll zu aktivieren.

A.2 Konfiguration des TCP/IP-Protokolls für den Betrieb des Geräts

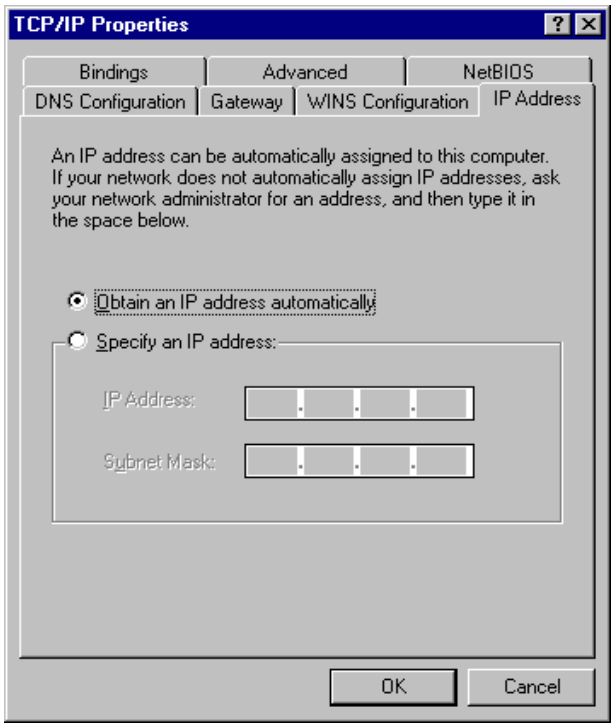
1. Klicken Sie auf „Start", „Einstellungen" und anschließend auf „Systemsteuerung".
2. Klicken Sie doppelt auf das Netzwerk-Symbol. Wählen Sie auf der Registerkarte „Konfiguration" im Netzwerk-Fenster das für Ihre Netzwerkkarte eingerichtete TCP/IP-Protokoll aus.



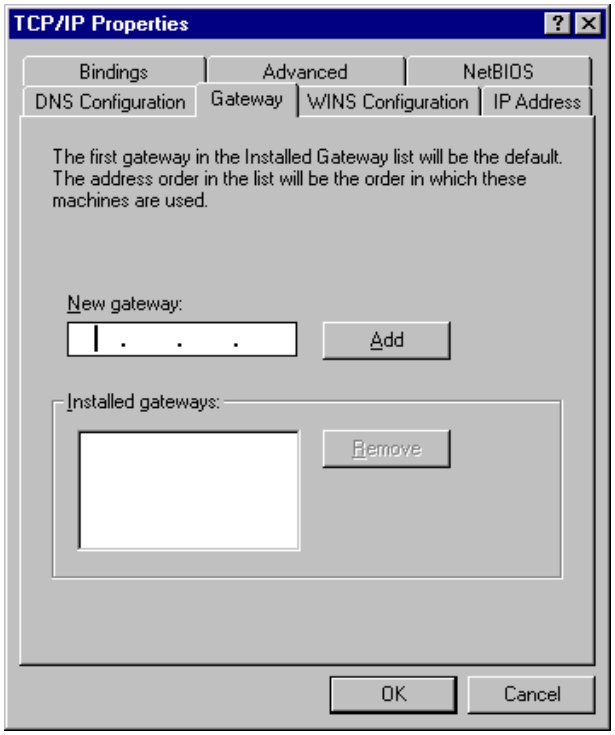
3. Klicken Sie auf die Schaltfläche „Eigenschaften", um das TCP/IP-Protokoll für den Betrieb des Geräts zu konfigurieren.
4. Es gibt zwei Möglichkeiten, die Einstellungen vorzunehmen:

A:

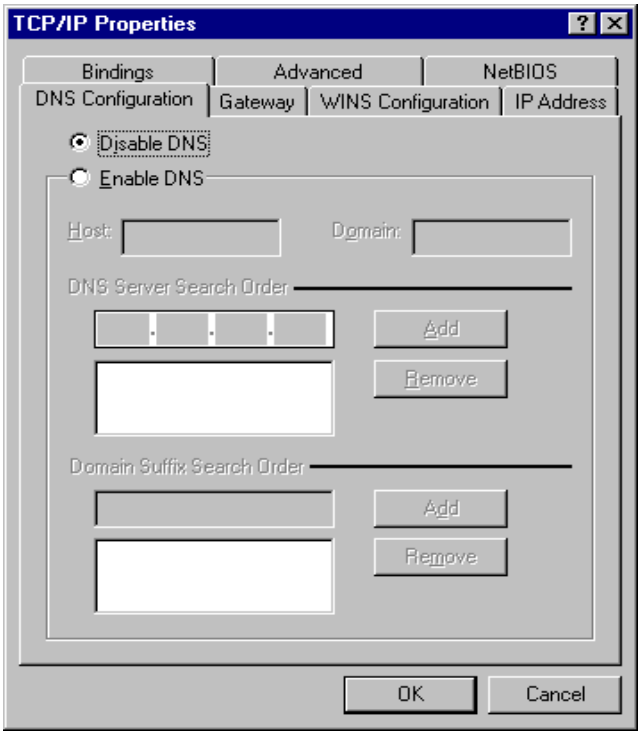
a. Durch Auswahl von „IP-Adresse automatisch beziehen” auf der Registerkarte „IP-Addressen“ wird die IP-Adresse automatisch vom System ermittelt.



b. Nicht-Eingabe eines Werts auf der Registerkarte „Gateway”.

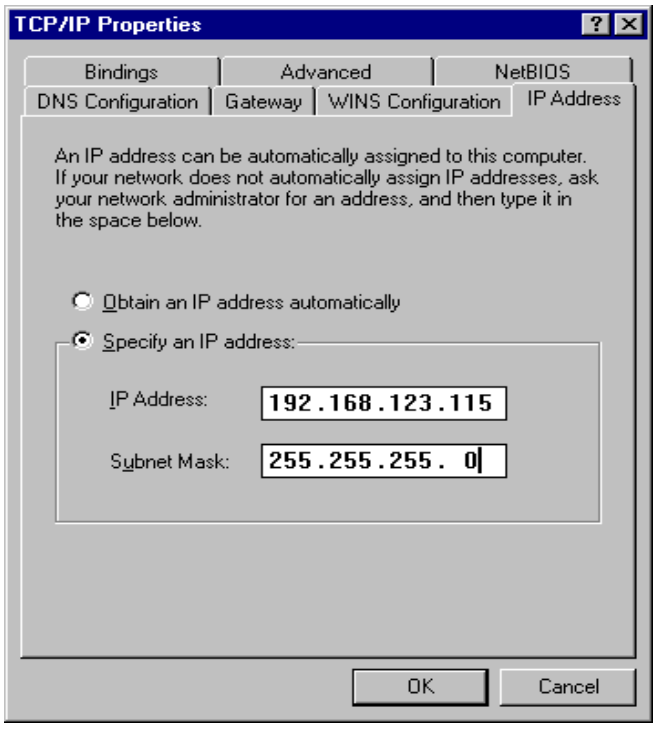


c. Auswahl von „DNS deaktivieren” auf der Registerkarte „DNS-Konfiguration“.

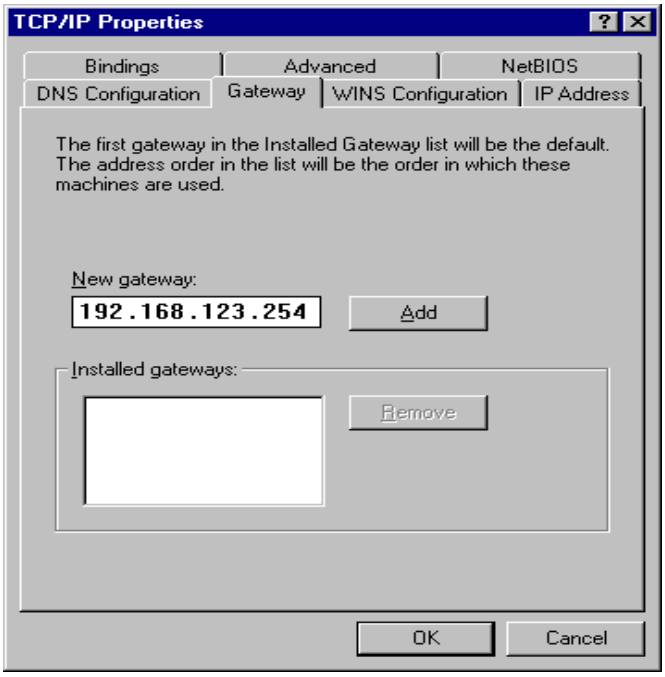


B. Manuelle Konfiguration der IP-Adresse

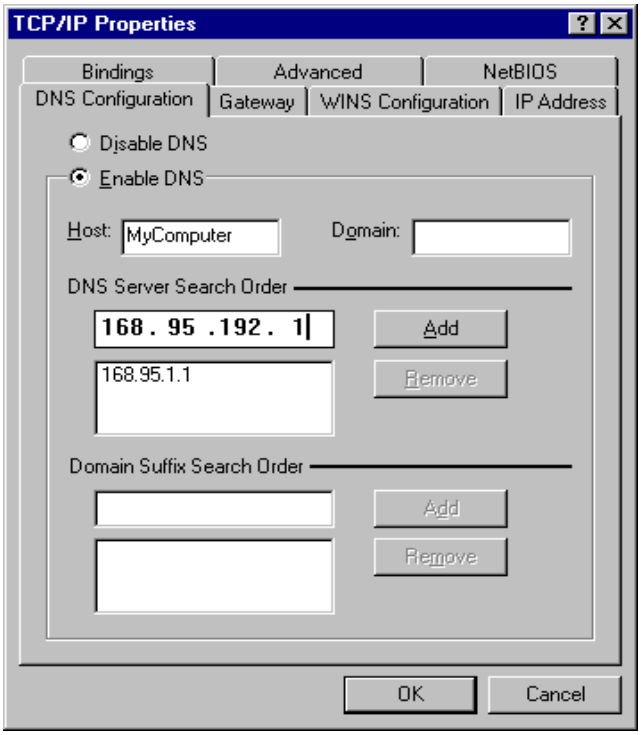
a. Wählen Sie zur manuellen Konfiguration „IP-Adresse festlegen“ auf der Registerkarte „IP-Adresse“ aus. Die Standard-IP-Adresse dieses Produkts ist 192.168.123.254. Geben Sie im Feld „IP-Adresse“ folglich 192.168.123.xxx (für xxx eine Zahl zwischen 1 und 253) ein, und in das Feld „Subnet Mask“ 255.255.255.0.



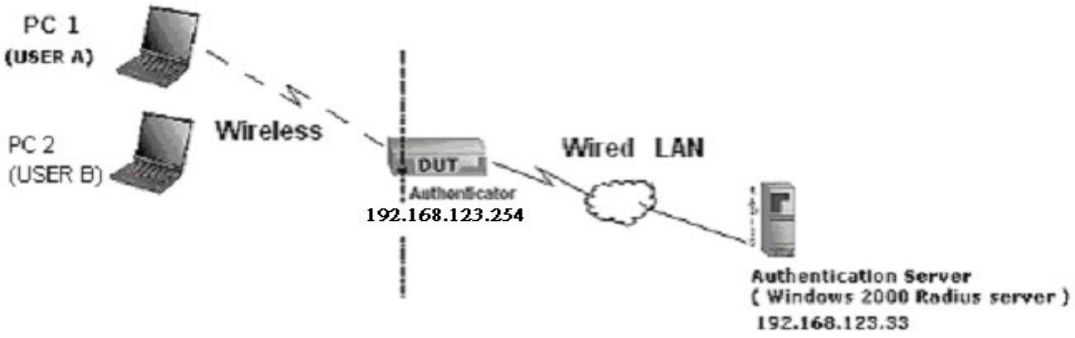
b. Geben Sie auf der Registerkarte „Gateway“ in das Feld „Neuer Gateway“ die IP-Adresse dieses Produkts ein (standardmäßig 192.168.123.254) und klicken Sie auf die Schaltfläche „Hinzufügen” (Add).



c. Geben Sie auf der Registerkarte „DNS-Konfiguration“ in das Feld „Suchreihenfolge für DNS-Server“ die DNS-Werte ein, die Sie von Ihrem ISP erhalten haben, und klicken Sie auf „Hinzufügen“ (Add).



8. Anhang B Einstellungen für 802.1x



8.1. Ausstattung

PC1:

Microsoft Windows XP Professional ohne Service Pack 1.

Wireless Cardbus

PC2:

Microsoft Windows XP Professional mit Service Pack 1a oder dem neuesten Stand.

Wireless Cardbus

Authentifizierungs-Server: Windows 2000 RADIUS-Server mit Service Pack 3 und HotFix Q313664.

Der Windows 2000 RADIUS-Server unterstützt PEAP (Protected Extensible Authentication Protocol) erst nach dem Upgrade mit Service Pack 3 und HotFix Q313664

8.2. Testgerät

Konfiguration:

1.Aktivieren Sie den DHCP-Server.

2.WAN-Einstellung: Statische IP-Adresse

3.LAN IP-Adresse: 192.168.123.254/24

4. Geben Sie die RADIUS-Server IP ein.

5. Geben Sie den gemeinsamen Schlüssel des RADIUS-Servers ein.

6. Konfigurieren Sie die WEP Key- und die 802.1X-Einstellungen.

Der folgende Test verwendet die integrierte 802.1X-Authentifizierung wie z. B. EAP_TLS, PEAP_CHAPv2 (nur Windows XP mit SP1) und PEAP_TLS (nur Windows XP mit SP1), in Verbindung mit der Smart Card oder einem anderen Zertifikat unter Windows XP Professional.

8.3. Einstellung von Testgerät und Windows 2000 Radius-Server

8.3.1. Einrichten des RADIUS-Servers von Windows 2000

Die Authentifizierungsmethode muss auf „MD5_Challenge“ oder „Smart card or other certificate“ auf dem RADIUS-Server eingestellt werden und den Testbedingungen entsprechen.

8.3.2. Einrichten des Testgeräts

1. Aktivieren Sie 802.1X (durch Aktivieren des „Enable“-Kästchens).

2.Geben Sie die RADIUS-Server IP ein.

3.Geben Sie hier den gemeinsamen Schlüssel ein. (Dies ist der für RADIUS-Server und Testgerät gemeinsam genutzte Schlüssel).

4. Ändern Sie bei anderen Testbedingungen die Länge des 802.1X-Schlüssels entsprechend.

8.3.3. Einrichten des Netzwerkadapters auf dem PC

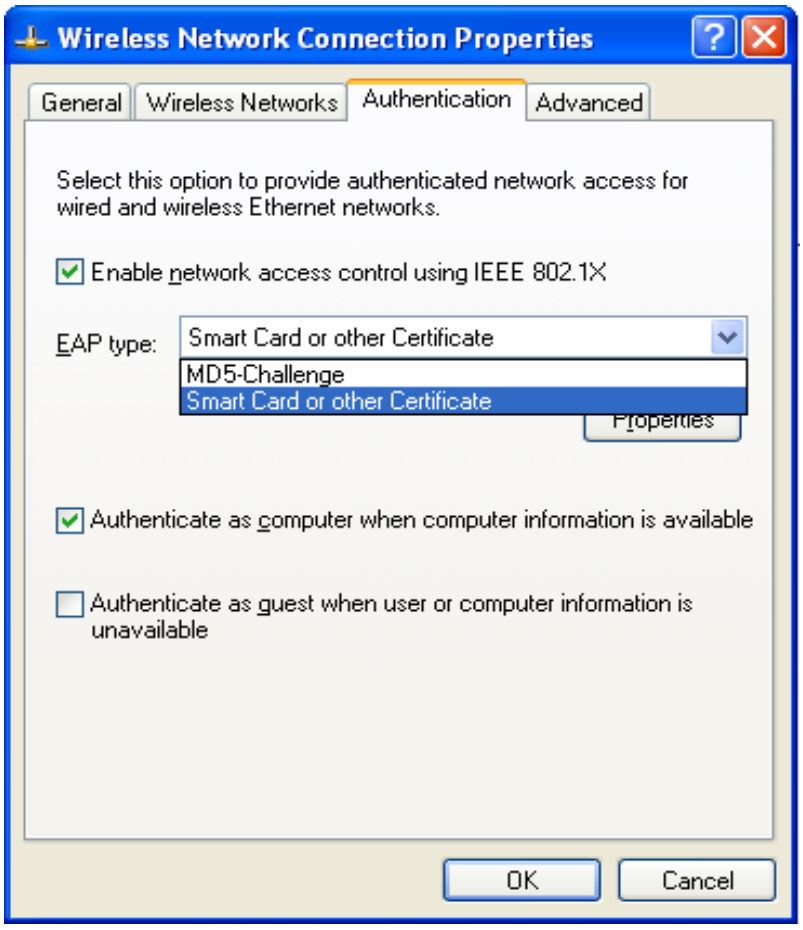
Wählen Sie IEEE802.1X als Authentifizierungsmethode aus.

Abbildung 2 zeigt ein Einstellungsfenster für Windows XP ohne Service Pack 1. Nach dem SP1-Upgrade gibt es die Option „MD5-Challenge“ in der Liste „EAP type“ nicht mehr. Stattdessen gibt es die neue Option „Protected EAP” (PEAP).

1. Wählen Sie als EAP-Typ “MD5-Challenge” oder “Smart Card or other Certificate”.

2.Wenn Sie „Smart Card or other Certificate“ als EAP-Typ auswählen, müssen Sie auch die Verwendung eines Zertifikats für diesen Computer aktivieren. Markieren Sie dazu die Schaltfläche „Enable network access control using IEEE 802.1X“.

3. Ändern Sie bei anderen Testbedingungen den EAP-Typ entsprechend.



8.4. Testen der Windows 2000 RADIUS-Server Authentifizierung:

8.4.1. Das Testgerät authentifiziert PC1 anhand des Zertifikats. (Für PC2 ist der Testablauf identisch.)

1. Laden Sie das Zertifikat herunter und installieren Sie es auf PC1.

2. PC1 wählt den SSID (Service Set Identifier) des Testgeräts als Gerät aus.

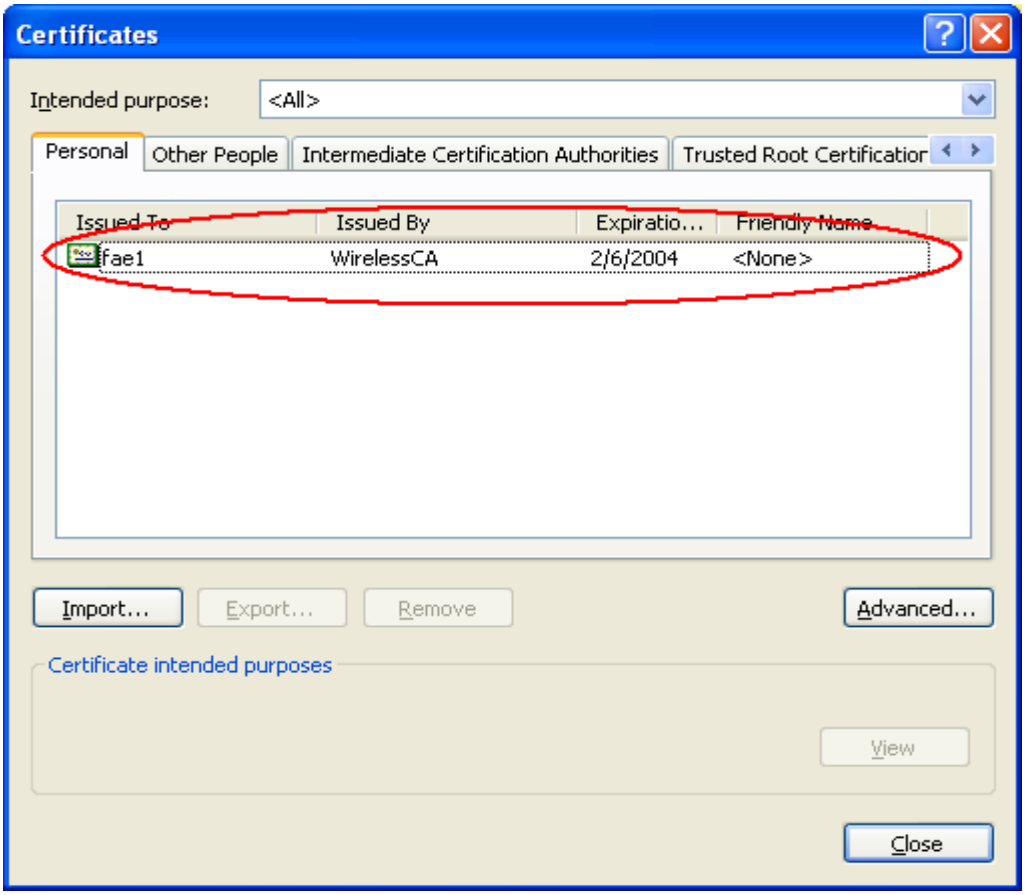
3. Stellen Sie für Wireless Client sowie RADIUS-Server EAP_TLS als Authentifizierungstyp ein.

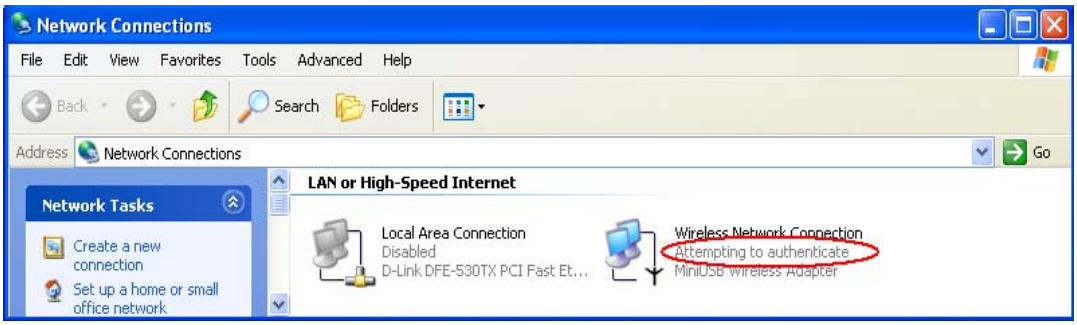
4. Deaktivieren Sie die Wireless-Verbindung und aktivieren Sie sie anschließend wieder.

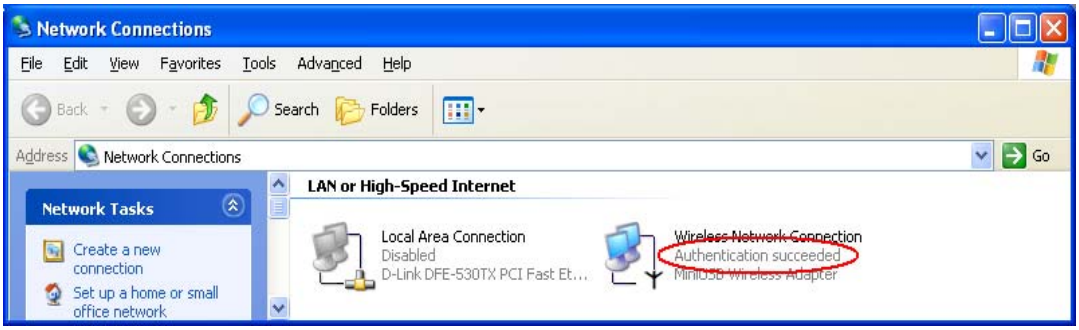
5. Das Testgerät sendet das Anwenderzertifikat an den RADIUS-Server und sendet die Ergebnisse der Authentifizierung an PC1.

6. Windows XP gibt an, ob der Authentifizierungsvorgang erfolgreich war und beendet den Vorgang dann.

7. Beenden Sie den Test, wenn PC1 eine dynamische IP erhalten und erfolgreich ein Ping an den Remote Host gesendet hat.







8.4.2. Testgerät authentifiziert PC2 mittels PEAP-TLS.

1. PC2 wählt den SSID (Service Set Identifier) des Testgeräts als Gerät aus.

2. Stellen Sie für Wireless Client sowie RADIUS-Server PEAP_TLS als Authentifizierungstyp ein.

3. Deaktivieren Sie die Wireless-Verbindung und aktivieren Sie sie anschließend wieder.

4.Das Testgerät sendet das Anwenderzertifikat an den RADIUS-Server und sendet die Ergebnisse der Authentifizierung an PC2.

5. Windows XP gibt an, ob der Authentifizierungsvorgang erfolgreich war und beendet den Vorgang dann.

6. Beenden Sie den Test, wenn PC2 eine dynamische IP erhalten und erfolgreich ein Ping an den Remote Host gesendet hat.

Unterstützte Authentifizierungstypen:

Das Gerät unterstützt die Typen der 802.1X-Authentifizierung: PEAP-CHAPv2 und PEAP-TLS.

1. PC1 läuft unter Windows XP ohne Service Pack 1.
2. PC2 läuft unter Windows XP mit Service Pack 1a.
3. PEAP wird nur von Windows XP mit Service Pack 1 unterstützt.
4. Windows XP mit Service Pack 1 ermöglicht 802.1X-Authentifizierung nur dann, wenn die Datenverschlüsselungsfunktion aktiviert ist.

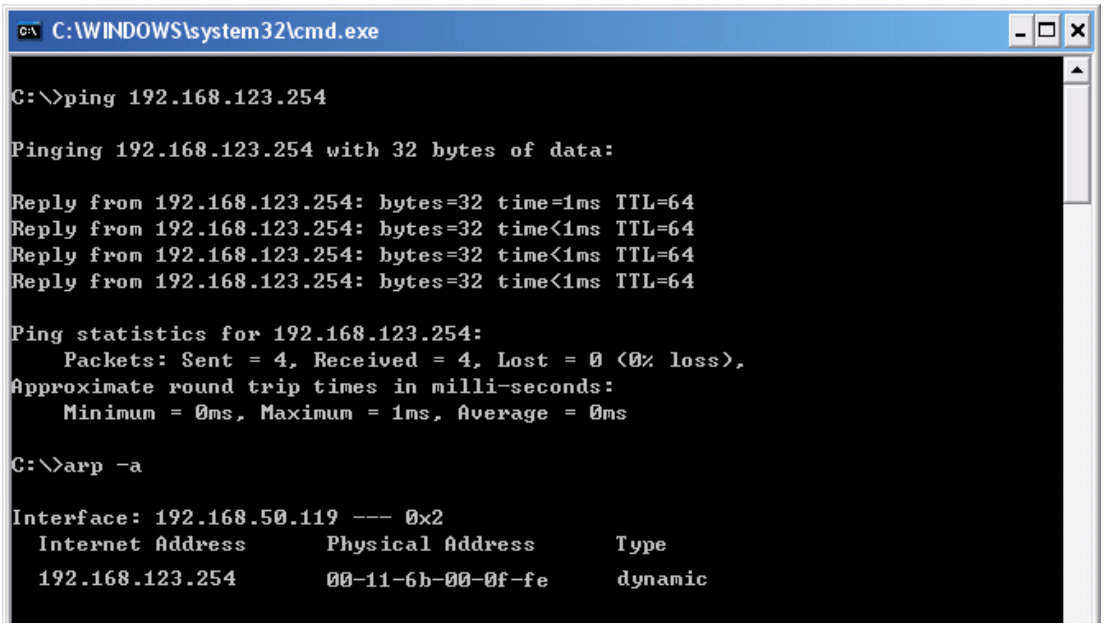
9. Anhang C WDS-Einstellungen

9.1. Einstellungen und Betrieb:

Überprüfen Sie die WLAN-MAC-Adressen von AP1, AP2 und AP3. Wechseln Sie dann in den Befehlsmodus und verwenden Sie

“Arp -a ”.

Wenn Sie die MAC-Informationen nicht finden können, stecken Sie das Kabel in den LAN-Port des Access Points und pingen Sie die IP-Adresse des LANs. Verwenden Sie dann den Befehl „arp -a“. Die Informationen werden auf dem Bildschirm angezeigt. Beispiel:



AP1	AP2	AP3
IP:192.168.123.254	IP:192.168.123.253	IP:192.168.123.252
Mac:00-11-6b-00-0f-fe	Mac:00-11-6b-00-0f-fd	Mac:00-11-6b-00-0f-fc
SSID: Default	SSID: Default	SSID: Default
Channel: 11	Channel: 11	Channel: 11
DHCP-Server: Enable		

Orange: Wireless

Schwarz: verkabelt

Wenn die Einstellungen ordnungsgemäß vorgenommen wurden, stellt Ihnen der DHCP-Server die IP vom AP1 zur Verfügung. Client 1 und

Client 2 können dann gegenseitige Informationen erhalten.

AP1-Einstellungen:

AP1←→ AP2(Remote Mac: 00-11-6b-00-0f-fd)

AP1←→ AP3(Remote Mac: 00-11-6b-00-0f-fc)

AP2-Einstellungen:

AP2←→ AP1(Remote Mac: 00-11-6b-00-0f-fe)

AP3-Einstellungen:

AP3←→ AP1(Remote Mac: 00-11-6b-00-0f-fe)

10. Entsorgung

Der Gesetzgeber verpflichtet uns, Sie darauf hinzuweisen, dass das Gerät hochwertige Materialien enthält, die der Wiederverwertung zugeführt werden sollen. Entsorgen Sie das Gerät daher nicht über den Hausmüll, sondern geben Sie es an einer Sammelstelle für Elektrogeräte zur Entsorgung ab.

Symbol „Elektromüll nicht über die Hausmülltonne entsorgen“

Wenn Sie diesbezügliche weitere Informationen wünschen, können Sie sich auch an unseren telefonischen Support wenden. Die Nummer finden Sie auf dem Titelblatt dieser Anleitung.

11. GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.
You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange;

or,

Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange;

or,

Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

The Code for this product can be downloaded at
http://www.level1.com/support.php