WLAN absichern; wie wird das eingestellt?

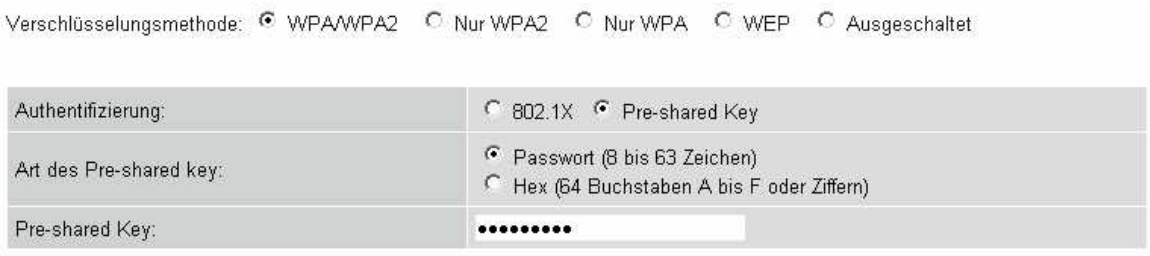
Im Folgenden werden die verschiedenen Schritte am Beispiel eines Routers vorgestellt. Bei anderen Geräten sieht es vielleicht ein wenig anders aus, das Prinzip ist jedoch das gleiche und die verschiedenen Seiten tragen in der Regel die gleichen Bezeichnungen.

Zum Einstellen des Routers starten Sie Ihren Internet-„Browser“, also den Internetexplorer, Firefox, Opera oder was Sie sonst verwenden. Geben Sie in dem Adressfeld die IP-Adresse Ihres Routers ein. Die finden Sie auf der Unterseite des Gerätes oder im Handbuch. In der Regel beginnt sie mit 192.168… Es öffnet sich dann das Anmeldefenster des Routers. Hier müssen Sie den Benutzernamen und das Passwort eingeben (manchmal auch nur das Passwort). Die Daten finden Sie auf der Unterseite des Gerätes oder im Handbuch.

Einstellen der SSID

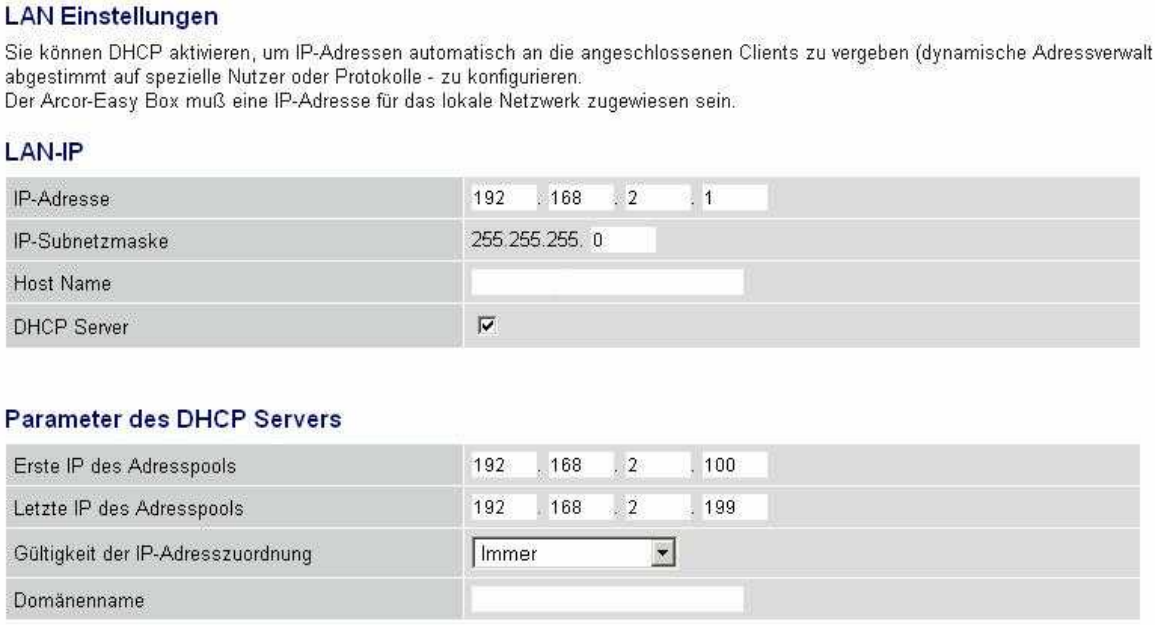
Tragen Sie unter **SSID** einen Namen ein, der nichts über Ihre Person, den Standort und das Gerät verrät! Die Kennung sollte **ausgestrahlt** werden, da manche „Clients“ Probleme haben, wenn sie nicht gesendet wird. Wählen Sie den **Übertragungsmodus**, den Ihre Rechner **und** der Router können. Verwenden Sie stets das neueste und beste Verfahren. Informationen dazu finden Sie im Handbuch, in der Hilfe oder im Internet. Da die Entwicklung bei der Absicherung und den Angriffen auf Netzwerke im ständigen Wandel begriffen ist, können wir an dieser Stelle keine anderen Hinweise geben. Den Funkkanal sollten Sie auf „Automatik“ stellen, wenn dies möglich ist. Wenn nicht, wählen Sie einen Kanal, der in der Nachbarschaft nicht verwendet wird. Wenn der Empfang schlecht ist, sollten Sie 2 Kanäle rauf oder runter wechseln. Mitunter können DECT-Telefone in der Nähe zu Störungen führen.

Einstellen der Verschlüsselung



Auch bei der Verschlüsselung wählen Sie das Verfahren, das alle Geräte können, und das Neueste und Sicherste! Auch darüber finden Sie Hinweise im Handbuch und im Internet. Bei dem Passwort oder Schlüssel (Key) sollten Sie nur die Ziffern 0 bis 9 und die Buchstaben A bis F verwenden. MS-Windows - Systeme können sonst mit der Verbindung Schwierigkeiten haben.

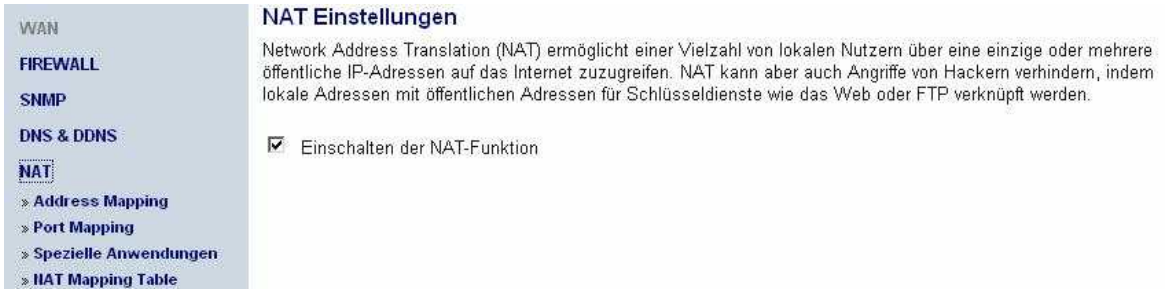
LAN-Einstellungen



Die **LAN-IP** sollten Sie nur ändern, wenn Sie Geräte mit fester IP in Ihrem Netz haben. Die **Subnetzmaske** oder Subnetmask beschreibt den Teil der Adresse, der als Netzwerkadresse verwendet wird Der Rest ist die Adresse des Gerätes.. Bei 255.255.255.0 sind die ersten drei Zahlen die Netzwerkadresse. Ist die Maske anders, sollten Sie einen Fachmann zu Rate ziehen. In dem Beispiel ist die Netzwerkadresse 192.168.2. Häufig wird die Adresse 192.168.0 verwendet. Wenn es Geräte wie Drucker, Server oder Datenspeicher (NAS Network Atached Storage) in Ihrem Netz gibt, müssen Sie die Adresse ändern. **Ändern Sie aber nur die 3. Zahl** (Im Beispiel 2) weil sonst Adresskonflikte auftreten können!
DHCP (Dynamic Host Configuration Protokoll) sollte eingeschaltet sein. (Andernfalls sollten Sie sich mit den IP-Adressen auskennen) Die DHCP-Parameter erlauben es, den Bereich, der automatisch vergeben wird, einzuschränken. Im Beispiel von 100 bis 199. Also können 100 verschiedene Rechner im Netz eine Adresse zugewiesen bekommen. Normaler Weise werden die Adressen nur für eine bestimmte Zeit vergeben (Leasing). Wenn die Geräte häufig wechseln, wie in einem Hotel oder Café ist das sinnvoll. Sind aber immer dieselben Rechner im Netz, ist es besser, wenn sie immer die gleiche Adresse erhalten. Dazu stellt man die größte mögliche „Leasingdauer“ oder „immer“, wie im Beispiel, ein.

NAT Einstellung

Wechseln sie nun von der Startseite zur Seite „Erweitert“. Hier sind weitere Einstellungen möglich. Die meisten verlangen besondere Netzwerkkenntnisse. Wenn Sie dort aber wie unten NAT-Einstellungen finden, sollten diese eingeschaltet sein.



NIC oder MAC – Adressen filtern

Zugangskontrolle der Funkteilnehmer über die MAC-Adresse

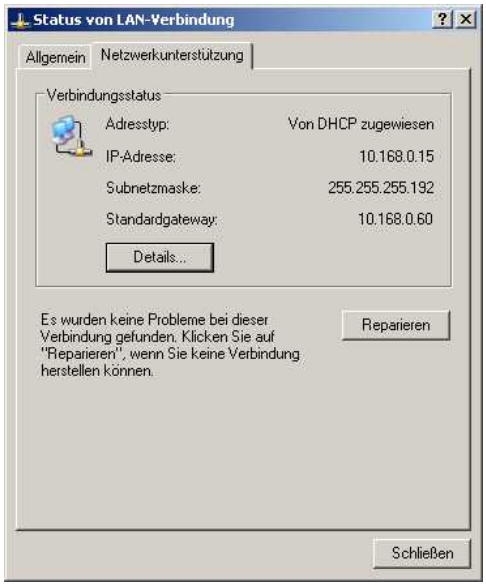
Zur Erhöhung der Sicherheit in einem Funknetzwerk können Sie festlegen, dass nur bestimmte Funkteilnehmer Zugang zur Basisstation (Access Point) erhalten. Bis zu 32 MAC-Adressen können in einer Filtertabelle eingetragen werden. Wenn aktiviert, werden alle registrierten MAC-Adressen über die Zugangsregel verwaltet.

☑ Einschalten der MAC-Filterfunktion

Zugangsregel für registrierte MAC-Adresse: ◉ Zulassen ○ Zurückweisen

MAC-Filtertabelle (bis zu 32 Stationen):

ID	MAC-Adresse
1	00 : 60 : B3 : B2 : 15 : B2
2	00 : 60 : B3 : B2 : 15 : 7D
3	00 : 13 : CE : E1 : FE : A2
4	C4 : 17 : FE : 3B : 62 : 2F
5	00 : 12 : CA : E1 : FF : A3
6	00 : 00 : 00 : 00 : 00 : 00



Um Unbefugten den Zugang in Ihr Netz weiter zu erschweren, schalten Sie auf der Seite „Erweitert“ unter „Wireless/Access Control“ die Filterfunktion für die Netzwerkkarten ein. Dann müssen Sie die Adressen der berechtigten Geräte ermitteln und eintragen.

Um diese Adressen zu erhalten, gehen Sie bei MS-Windows (ab 2000) folgendermaßen vor: Zeigen Sie

mit der Maus auf „Netzwerkumgebung“ auf dem Desktop oder in der Systemsteuerung und drücken die rechte Taste. Wählen Sie dann „**Eigenschaften**“. Nun werden alle LAN-Verbindungen angezeigt. Markieren Sie nun die WLAN-Verbindung und drücken wieder die rechte Maustaste.

In dem erscheinenden Menü wählen Sie „**Status**“. Dann erscheint ein neues Fenster mit Informationen über den Zustand der Verbindung. Dort wählen Sie die Registerkarte „**Netzwerkunterstüzung**“. Mit der Taste „**Details**“ erhalten Sie eine Auflistung der zu dieser Verbindung gehörenden Daten. Der Wert hinter „Physikalische Adresse“ ist das, was Sie in die Filtertabelle eintragen müssen.

Verwaltername und Passwort

Um den Namen und das Passwort des Router - Verwalters zu ändern, wechseln Sie zu „Extras“.

Unter „Anmeldeeinstellungen“ können Sie Das Passwort und bei vielen Geräten auch den Namen des Verwalters ändern. Wenn Sie beides ändern, erschweren Sie einen Angriff auf Ihren Router erheblich. Der Name des Verwalters ist standardmäßig „root“ oder „admin“. Wer das Gerät kennt, weiß auch den Namen des Verwalters. Damit muss nur noch das Passwort „geknackt“ werden. Haben Sie auch den Namen geändert, wird es erheblich schwerer. Vermeiden Sie jedoch Namen, die sich leicht ableiten lassen.

Wenn möglich sollten sie auch eine zwangsweise Abmeldung einrichten, wie im Beispiel unten. Hier wird der Verwalter nach 10 Minuten abgemeldet, wenn er nicht aktiv ist.