



# NetEasy by D-Link®

**NetAccess**  
**Benutzerhandbuch**

Rev. A2 (11/2001)

# Inhaltsverzeichnis

EINFÜHRUNG.....	3
INSTALLATION.....	4
APMANAGER – LEISTUNGSMERKMALE .....	5
APMANAGER – HAUPTFENSTER .....	6
KURZEINFÜHRUNG IN DRAHTLOSE NETZWERKE .....	9
WLANS VERWALTEN .....	11
ACCESS POINTS VERWALTEN .....	13
DIALOGFELD „NETWORK SETTINGS“ .....	16
ACCESS POINTS SUCHEN.....	17
IP-ADRESSEN MANUELL PROGRAMMIEREN .....	19
SICHERHEITSVERWALTUNG.....	20
ZUGRIFFSKONTROLLE .....	24
AKTUALISIEREN DER ACCESS POINT-EINSTELLUNGEN.....	25
IEEE 802.11 WEP-SICHERHEIT .....	27
WEITERE INFORMATIONEN ZU ZELLEN .....	28
KOMPATIBILITÄT .....	28
GLOSSAR .....	29

# Einführung

Vielen Dank, dass Sie sich für den Kauf des DRC-1000 Wireless LAN Access Point entschieden haben. Dieses Handbuch beschreibt Installation und Konfiguration dieses Modells. NetEasy unterstützt zur Zeit leider noch **nicht** die Betriebssysteme: Windows CE, Linux und Unix.

Vergewissern Sie sich, dass folgende Dinge in der Lieferung vorhanden sind:

- Benutzerhandbuch
- DRC-1000AP Access Point
- Netzteil
- Eine Diskette mit der AP Manager Software.

Sollten Teile fehlen, wenden Sie sich bitte an den Händler, von dem Sie dieses Produkt erworben haben. Ein drahtloses LAN wird gewöhnlich in einem begrenzten Gebiet eingesetzt. Ein solches Netzwerk ist an bestimmten Punkten mit Access Points ausgerüstet, jeder ein Gebiet abdeckend, in dem drahtlose Kommunikation erfolgen kann. Diese Access Points sind mit einem verdrahteten Netzwerk verbunden, und kommunizieren auf diese Weise sowohl untereinander als auch mit den Servern und Clients dieses Netzwerkes. Der DRC-1000AP Access Point kann an ein 10 Mbit/s-Netzwerk (Ethernet) mittels eines RJ45-Steckverbinders (UTP) angeschlossen werden.

# Installation

Führen Sie folgende Schritte durch, um den DRC-1000AP zu installieren:

1. Montieren Sie den DRC-1000AP fest an der Position der Mauer, die während der Standortbesichtigung festgelegt wurde. Eine Bohrschablone wird als separates Blatt mit diesem Handbuch mitgeliefert.
2. Stellen Sie sicher, dass die Antennen vertikal ausgerichtet sind. Drehen Sie sie bei Bedarf um 90 Grad.
3. Schließen Sie die Stromzufuhr an.
4. Verbinden Sie das UTP-Ethernetkabel mit dem Access Point.
5. Schalten Sie den Access Point ein.

An der Vorderseite des Access Point befinden sich drei LED-Anzeigen.

Bei ordnungsgemäßem Betrieb leuchtet die mittlere LED (Power) grün. Sowohl die linke (WLAN) als auch die rechte LED (verdrahtetes LAN) blinken, sobald Datenverkehr in den jeweiligen Netzwerken stattfindet. Beim drahtlosen LAN findet dieser in Form eines Funkfeuers mindestens 10 Mal pro Sekunde statt. Der Access Point erkennt das Netzwerk automatisch. Wenn das Kabelnetzwerk erkannt wurde, leuchtet die Netzwerk-LED gelb.

Die Einstellungen des Access Points können auf die vordefinierten Werkseinstellungen zurückgesetzt werden. Führen Sie dazu eine Büroklammer in die kleine Öffnung neben dem Netzschalter ein. Die ACT-Sequenz ist aktiviert und dauert bis zum Erlöschen der LED an.

Wenn Sie den Access Point während des Betriebs zurücksetzen, wird nur die vom APManger™ (Par 4.5) gesetzte Sperre deaktiviert.

## **APManager – Leistungsmerkmale**

APManager bietet eine konsistente Übersicht des drahtlosen Netzwerks. Der Systemadministrator kann APManger zur Kontrolle einer großen Zahl von DRC-1000AP-Access Points von einem einzigen Ort aus verwenden. Die Access Points werden über SNMP (Simple Network Management Protocol) fernaktualisiert.

### **Leistungsmerkmale:**

- Access Points hinzufügen und entfernen
- Zugriff auf das drahtlose Netzwerk beschränken
- Datenschutzoptionen wie z.B. IEEE 802.11 WEP verwalten
- Funkkanäle für optimale Zellenverwaltung zuweisen
- Das drahtlose Netzwerk in mehreren WLANs mit individueller Zugriffskontrolle und Sicherheitsoptionen gruppieren
- Einen Access Point mit einer bestimmten IP-Adresse programmieren
- Die Zeichenkette für die SNMP-Write Community einstellen
- Access Point-Konfigurationen auf der Festplatte speichern
- Den Status aller Access Points im Netzwerk überprüfen

## **APManager – Hauptfenster**

Das Hauptfenster des APManagers sieht ähnlich wie in der Abbildung aus. Bevor auf weitere Einzelheiten eingegangen wird, sollte deutlich sein, welche Art von Informationen erwartet werden können. Gegebenenfalls können Sie zum Abschnitt „Kurzeinführung in drahtlose Netzwerke“ springen.

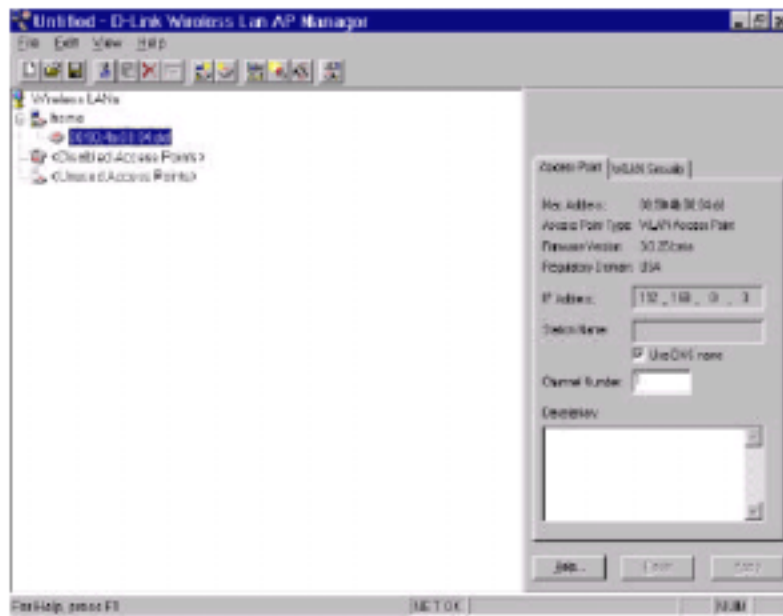


Abbildung 1: AP Manager

Die Baumstruktur links im Fenster zeigt eine Liste von WLANs (Wireless LANs) und die Access Points, die Teil jedes WLANs sind. Das Musterbild oben zeigt einen einzelnen Access Point mit der Hardware-Adresse 00:90:4b:08:04:dd, der dem mit „home“ bezeichneten WLAN zugeordnet ist. Die Symbole zeigen den Status der WLANs und ihre zugehörigen Access Points an.

Sie können durch Klicken, Doppelklicken, Ziehen usw. die Eigenschaften der Access Points anzeigen lassen oder einen Access Point in ein anderes WLAN verschieben usw. Siehe „WLANs verwalten“. Der Name (oder ESSID) des WLANs wird zur Identifizierung des WLANs verwendet. Client-Geräte haben freien Zugang über Access Points mit der gleichen ESSID. Deshalb sind die Sicherheitsoptionen für alle Access Points mit der gleichen ESSID identisch. Die Sicherheitsoptionen können über die Seite „WLAN-Sicherheitseigenschaften“ verwaltet werden. Siehe „Sicherheitsverwaltung“.

Die Seite „Access Point-Eigenschaften“ wird hauptsächlich zum Auswählen eines Funkkanals für jeden Access Point verwendet. Siehe „Access Points verwalten“ weiter unten.



# Kurzeinführung in drahtlose Netzwerke

Um das drahtlose Netzwerk erstmals in Betrieb zu nehmen, sind sieben Schritte erforderlich:

1. Verbinden Sie die Access Points mit dem Ethernet-LAN. Vergewissern Sie sich, dass diese angeschaltet sind. Das drahtlose Netzwerk von D-Link ist sofort in Betrieb. Wenn Sie mit den Voreinstellungen zufrieden sind, sind keine weiteren Konfigurationen nötig. Wahrscheinlich jedoch sollen noch jedem Access Point unterschiedliche Funkfrequenzen zugewiesen oder Nutzungseinschränkungen definiert werden.
2. Um die Access Points via SNMP verwalten zu können, braucht jeder Access Point eine eigene IP-Adresse. Wenn Sie in Ihrem Netzwerk DHCP oder BOOTP zur Verfügung stellen (und freie IP-Adressen haben), läuft dieser Vorgang automatisch ab. Ist dies nicht der Fall, konsultieren Sie den Abschnitt „Manuelles Zuweisen von IP-Adressen“.
3. Starten Sie den APManager, und konfigurieren Sie die ihrem Netzwerk entsprechenden Einstellungen im Menü „Edit/Network Settings“. Nähere Informationen entnehmen Sie bitte dem Abschnitt „Netzwerkeinstellungen“.
4. Erstellen Sie mindestens ein WLAN „Edit/Insert Wireless LAN“, und wählen Sie die gewünschten Sicherheitseinstellungen.

5. Benutzen Sie die eingebaute Scan-Funktion „Edit/Search Access Points“, um Informationen über die Access Points zu erhalten. Nähere Informationen entnehmen Sie bitte dem Abschnitt „Suchen der Access Points“. Ziehen Sie den neuen Access Point in ein beliebiges WLAN.
6. Wählen Sie den Funkkanal der Access Points nach Ihrem Zellenplan. Näheres dazu finden Sie im Abschnitt „Weitere Informationen zu Zellen (More about Cells)“. Kommentieren Sie jeden Access Point, um ihn später leichter identifizieren zu können.
7. Speichern Sie die Konfigurationen (beispielsweise auf eine Diskette) ab und übernehmen Sie die neuen Einstellungen durch klicken auf die Schaltfläche



Abbildung 2: Schaltfläche

Beachten Sie, dass die Einstellungen der Access Points nicht verändert werden, bis die Funktion „Commit to Network“ ausgeführt wird. Wenn Sie den APManger™ beenden, gibt es eine dahingehende Rückfrage.

Nähere Informationen finden Sie im Abschnitt „Aktualisieren der Access Point Einstellungen“.

Sie können die Konfigurationsdatei jederzeit öffnen, um Änderungen am Netzwerk vorzunehmen.

## WLANs verwalten

Ein WLAN (Wireless Local Area Network) besteht aus einer Reihe Access Points, welche zusammen einen nahtlosen Zugriff auf jeden in Reichweite befindlichen, drahtlos vernetzten Computer zur Verfügung stellen.



WLAN erstellen:

Wählen Sie „Edit/Insert Wireless LAN“, um ein neues WLAN in die Liste aufzunehmen. Geben Sie den Namen (ESSID) des neuen WLANs ein.



WLAN entfernen:

Entfernen Sie ein leeres WLAN, indem Sie die Taste „Entf“ drücken oder in der Menüleiste „Edit/Clear“ wählen.



WLAN umbenennen:

Klicken Sie auf die Beschriftung des WLAN, um den Namen (ESSID) zu ändern. Beachten Sie, dass WLAN-Clients den Namen benutzen, um das WLAN zu erkennen.

Ein Access Point kann entweder durch einfaches Ziehen mit der Maus oder durch „Edit/Cut“ und

anschließendes „Edit/Paste“ einem anderen WLAN zugeordnet werden.

Es gibt zwei WLANs mit Sonderbedeutung für den APManger™. Unbenutzte Access Points und deaktivierte Access Points werden in zwei speziellen WLANs zusammengefasst.



#### Unbenutzte Access Points

Der APManger™ verwaltet unbenutzte Access Points nicht innerhalb des aktuellen Menüs; diese Access Points werden ignoriert. Einige Informationen sind zugänglich (beispielsweise der Funkkanal), können aber nicht geändert werden.

Die Eigenschaften dieser Access Points werden nicht geändert, wenn „File/Commit to Network“ gewählt wird. Dies ist sinnvoll, wenn verschiedene Personen unterschiedliche Access Point-Sets verwalten.



#### Deaktivierte Access Points

Access Points in diesem Ordner sind für Clients nicht mehr erreichbar, sobald sie aktualisiert wurden.

## Access Points verwalten

Einzelne Access Points werden über deren Hardware-Adresse erkannt (bzw. über die MAC-Adresse). Um einen neuen Access Point in das APManger™-Dokument von Hand einzufügen, muss die Hardware-Adresse bekannt sein. Sie können in Ihrem Netzwerk automatisch nach Access Points suchen; weitere Informationen finden Sie unter „Access Points suchen“.



Insert an Access Point:

Wählen Sie „Edit/Insert Access Point“, um einen neuen Access Point in das gewählte WLAN einzufügen. APManger™ fragt nach der Hardware-Adresse des Access Point.



Disable an Access Point:

Verschieben Sie einen Access Point in das spezielle WLAN „Disabled“, indem Sie „Entf“ drücken oder „Edit/Clear“ auswählen. Access Points in diesem speziellen WLAN sind für Client-Geräte nicht verfügbar. Siehe „WLANs verwalten“.

Die Access Points werden zusammen mit einem der folgenden Symbole angezeigt.



On-line:  
Access Point ist online verfügbar.



Off-line:  
Der Access Point ist im Moment nicht verfügbar, oder die IP-Adresse ist unbekannt oder falsch.



Locked:  
Der Access Point ist dauerhaft gesperrt. Seine Eigenschaften können nicht geändert werden.

Wählen Sie Access Point-Eigenschaftenseite, um die Einstellungen des gewählten Access Points anzuzeigen oder zu ändern. Diese Seite dient hauptsächlich zum Programmieren des Funkkanals für den Access Point entsprechend dem Zellenplan. Weitere Informationen finden Sie unter „Weitere Informationen zu Zellen (More about Cells)“.

Zu den angezeigten schreibgeschützten Eigenschaften gehören Hardware-Adresse, Marke und Version sowie die Steuerdomäne.

Access Point: WLAN Security

Mac Address: 00:13:91:03:07:23

Access Point Type: WLAN Parrot 1100 Access

Firmware: 2.2.0 #150 (Nov 18 1999)

Regulatory Domain: JSA

IP Address: 192.160.1.226


Station Name: apl.dlink.cin

Use DNS name

Channel Number: 1

Description:

- Hardware-Adresse (MAC address)
- Marke, Typ und Versionsdaten.
- Die Steuerdomäne, für der Access Point konfiguriert wurde (Werkseinstellung).

 Hinweis: Die Verwendung des Access Points außerhalb der festgelegten Domäne ist unzulässig. Weitere Informationen finden Sie unter „Steuerdomänen“.

- Die „IP-Adresse“ und der Hostname für diesen Access Point.
- Die Funkkanalnummer. Die zulässigen Kanäle hängen von der Steuerdomäne ab.

- Ein optionales Feld für Beschreibungen als Schnellreferenz.

## Dialogfeld „Network Settings“



Abbildung 3: Dialogfeld „Network Settings“

Wählen Sie den Menüpunkt „Edit/Network Settings“ (oder klicken Sie auf die entsprechende Schaltfläche in der Werkzeuggestreife wie in Abbildung 3). Das Dialogfeld „Network Settings“ wird angezeigt. Verwenden Sie dieses Dialogfeld, um die Netzwerkkonfiguration für APManger™ einzustellen. APManger™ benötigt diese Informationen, um nach Access Points zu suchen.

Fügen Sie Ihre Netzwerkadressen (und Subnets) hinzu, indem Sie die korrekten Informationen in die Felder „Network address“, „mask“ und „default gateway“ eingeben. Klicken Sie für jedes Netzwerk/Subnet auf die Schaltfläche „Set“. Um die Details für ein bestimmtes Netzwerk anzuzeigen, klicken Sie in der Liste auf das Feld „Address“. Klicken Sie auf die Schaltfläche „Remove“, um ein Netzwerk aus der Liste zu löschen. Wenn der Computer, auf dem APManger ausgeführt wird, direkt mit all Ihren Netzwerken verbunden ist, können Sie die Option „Auto Add Local Networks“ verwenden, um die Netzwerke zur Liste hinzuzufügen. Wenn auf dem Netzwerk Subnetting



verwendet wird, sind die von dieser Funktion generierten Netzwerkadressen möglicherweise nicht korrekt und müssen manuell angepasst werden.

## Access Points suchen

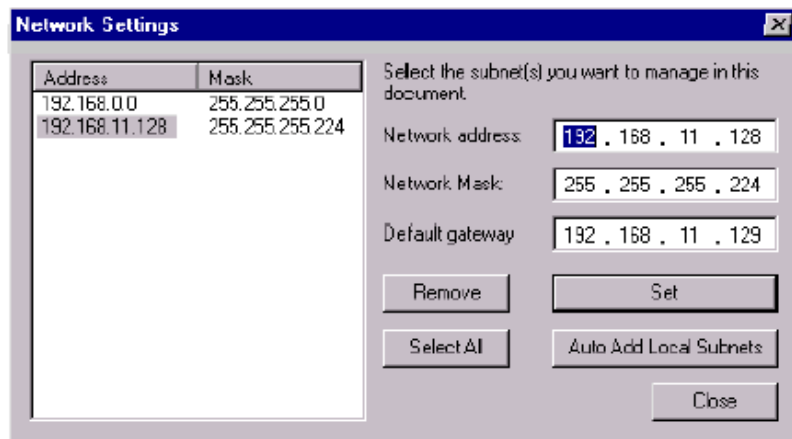


Abbildung 4: Konsole und Symbole „Network Settings“

APManager™ besitzt eine leicht zu bedienende Access Point-Erkennungsfunktion, die die Verwaltung von Access Points in Ihrem Netzwerk vereinfacht. Normalerweise verwenden Sie die Suchfunktion in einer der folgenden Situationen:

- Neue Access Points wurden zum Netzwerk hinzugefügt
- Die IP-Adresse eines oder mehrerer Access Points ist nicht mehr gültig oder bekannt, weil der DHCP- oder BOOTP-Server möglicherweise eine andere IP-Adresse zugewiesen hat. Sie sind möglicherweise darüber informiert, weil die Access Points von APManger™ in einem solchen Fall offline gemeldet werden.

Starten Sie die Suchfunktion, indem Sie „command Edit/Search Access Points“ wählen oder auf die entsprechende Schaltfläche in der Werkzeugleiste klicken. Sie können weiterarbeiten, während APManger™ das Netzwerk durchsucht. Wenn nötig, können Sie einen Suchvorgang mit der Schaltfläche „Abort Search“ abbrechen.



Abbildung 5: Fortschrittsanzeige

In der Statuszeile wird eine Fortschrittsanzeige gemäß Abbildung 5 angezeigt.

## IP-Adressen manuell programmieren

Die bevorzugte Methode zur Bereitstellung von IP-Adressen für Ihre Access Points besteht in der Verwendung eines DHCP- oder BOOTP-Servers in Ihrem Netzwerk. Ist dies der Fall, erhalten die Access Points automatisch eine IP-Adresse von diesem Server. Wenn Sie keinen DHCP-Server besitzen, können Sie die IP-Adresse für Ihre Access Points über APManger™ manuell eingeben.

1. Verbinden Sie die Access Points und den Computer, auf dem APManger™ ausgeführt wird, physisch mit dem selben Ethernet-Segment.
2. Stellen Sie sicher, dass dort kein DHCP- oder BOOTP-Server aktiv ist.
3. Schalten Sie den Access Point ein. Die Netzwerk-LED sollte rot aufleuchten.
4. Konfigurieren Sie die Access Points als Teil des gewünschten Netzwerks. Weitere Informationen finden Sie im Abschnitt „Dialogfeld 'Network Settings“.
5. Geben Sie die Hardware-Adressen der Access Points über den Menüpunkt „Edit/Insert Access Point“ ein, oder klicken Sie auf die entsprechende Schaltfläche in der Werkzeugleiste.

6. Wählen Sie für jeden Access Point den Menübefehl „Edit/Set IP Address“, und geben Sie die erforderliche IP-Adresse manuell ein. Sobald Sie auf „Apply“ klicken, erhält der Access Point die angegebene IP-Adresse. Innerhalb weniger Sekunden sollte die Netzwerk-LED an diesem Access Point grün aufleuchten.

Sofern die IP-Adresse im aktuellen Ethernet-Segment gültig ist, können Sie jetzt mit dem Access Point kommunizieren.

## **Sicherheitsverwaltung**

Die Sicherheitsverwaltung in einer drahtlosen LAN-Umgebung unterscheidet sich in gewisser Hinsicht von einem verkabelten Netzwerk, da die Funkwellen sich nicht auf ein Gebäude beschränken. Abhörversuche oder nicht autorisierte Zugriffe von außerhalb des Gebäudes können eine ernste Bedrohung darstellen.

Es gibt drei Arten von Sicherheitsmaßnahmen:

- Schutz der Daten bei der Übertragung von einer Station zur anderen. Dazu sind in den meisten Umgebungen Verschlüsselungstechniken notwendig (Datenschutz).
- Kontrolle der Benutzer des drahtlosen Netzwerks (Zugriffskontrolle).

- Schutz der Netzwerkkonfiguration gegen unberechtigte Zugriffe sowohl von innerhalb als auch von außerhalb der Organisation (Sicherheitsverwaltung).

Datenschutz:

Ein DRC-1000AP unterstützt drei verschiedene Datenschutzalgorithmen:

unverschlüsselte Daten; standardisiertes IEEE 802.11 WEP (basierend auf einem 40-Bit-Schlüssel) und No Wires Needed AirLock™ (basierend auf automatisch generierten 128-Bit-Session-Schlüsseln).

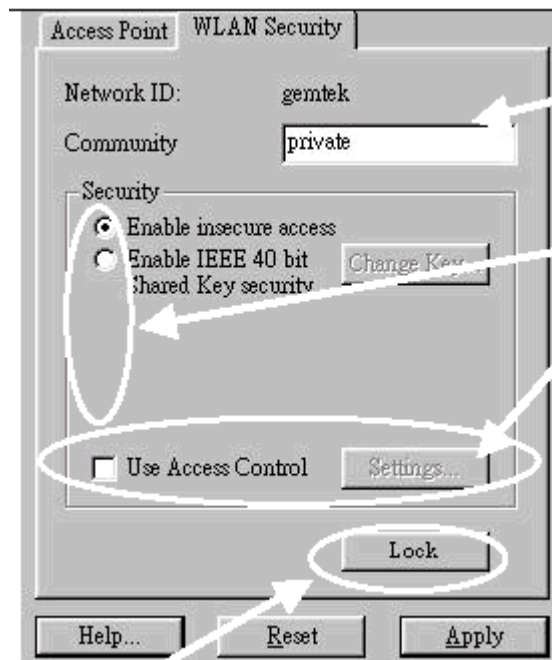
Zugriffskontrolle:

Der IEEE 802.11-Standard ermöglicht eine Zugriffskontrolle, die auf der Hardware-Adresse des Client-Geräts basiert und vollständig durch den DRC-1000AP implementiert ist. Wenn AirLock™ aktiviert ist, wird die Hardware-Adresse auch anhand kryptografischer Techniken verifiziert. Weitere Informationen finden Sie im Abschnitt „AirLock™-Sicherheitsarchitektur“.

Sicherheitsverwaltung:

Der primäre Schutz für jeden SNMP-Agenten gegen unberechtigte Zugriffe ist der Write Community String (WCS), der wie ein Kennwort für Netzwerk-Verwaltungsbefehle funktioniert. Der WCS wird in Ihrem Netzwerk als einfacher Text übertragen. Dieses ist daher innerhalb Ihrer Organisation anfällig gegen Abhörangriffe. Der WCS wird jedoch nicht drahtlos übertragen. Wenn Sie wollen, können Sie Ihre Access Points sperren. Nach dem Sperren können die Access Points nicht mehr über SNMP verwaltet werden. Drücken Sie den versenkten Rücksetztaster auf der Rückseite des Access Points, um den Access Point zu entsperren.

Wählen Sie die erforderlichen Sicherheitsoptionen auf der Seite „WLAN Security property“.



1. Bearbeiten Sie das Feld „Community String“, um den SNMP Write Community String für alle Access Points im gewählten WLAN zu ändern.
2. Wählen Sie die Datenschutzalgorithmen, die Sie in den Access Points unterstützen wollen.
3. Weitere Informationen finden Sie im Abschnitt „Zugriffskontrolle“.
4. Verwenden Sie diese Schaltfläche, um die Einstellungen der Access Points (nahezu) dauerhaft zu sperren

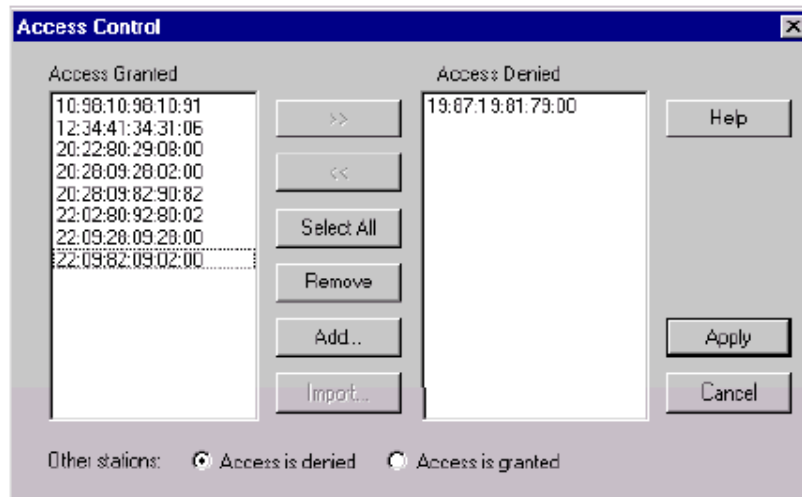
## Zugriffskontrolle

Innerhalb des IEEE 802.11-Framework basiert die Zugriffskontrolle auf der Hardware-Adresse der Client-Geräte. Sie können für jeden Client festlegen, ob dieser auf die drahtlose Netzwerkinfrastruktur zugreifen kann oder nicht. Aktivieren Sie auf der Registerkarte „WLAN Security“ das Kontrollkästchen „Use Access Control“, um die Zugriffskontrolle zu aktivieren. Ist dieses Kontrollkästchen deaktiviert, kann sich jeder Client mit Ihrem Netzwerk verbinden.

Klicken Sie in der Registerkarte „WLAN Security“ auf die Schaltfläche „Access Control Settings“, um das Dialogfeld „Access Control“ zu öffnen. Klicken Sie auf „Add“, um die Clients hinzuzufügen, denen Zugriff gewährt werden soll. Die Zugriffskontrolle für Clients kann standardmäßig aktiviert bzw. deaktiviert sein. Damit wird gleichzeitig festgelegt, ob sich nicht registrierte Clients mit dem Netzwerk verbinden können. Sie können Clients zwischen den Listen „Access Granted“ und „Access Denied“ verschieben, indem Sie auf die Schaltflächen „>>“ und „<<“ klicken oder die Pfeiltasten (nach links bzw. rechts) drücken.

Klicken Sie auf „Apply“, um die Änderungen zu bestätigen und das Dialogfeld zu schließen.



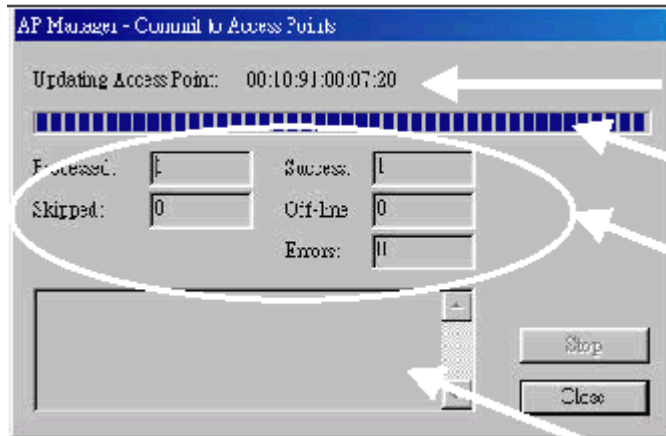


## Aktualisieren der Access Point-Einstellungen



Abbildung 6: Symbol „Update Access Point“

Nach dem Ändern des geöffneten APManger™-Dokuments sollten Sie die Access Points mit den neuen Einstellungen aktualisieren. Aktualisieren Sie alle Access Points mit „File > Commit to Network“ gleichzeitig. Sie können auch auf die Schaltfläche „Commit to Network“ in der Werkzeugleiste klicken. Das Ergebnis ist jeweils das gleiche. Während der Aktualisierung wird folgendes Dialogfeld angezeigt:



1. Access Point, der gerade verarbeitet wird.
2. Fortschrittsanzeige
3. Aktualisierungszähler. Der Zähler 'Skipped' bezieht sich auf Access Points im WLAN 'Unused'.
4. Spezielle Fehlermeldungen.

Der Access Point trennt alle Clients innerhalb von 10 Sekunden nach der erfolgreichen Aktualisierung und startet automatisch mit den neuen Einstellungen neu. Die LED leuchtet in dieser Phase rot.

## IEEE 802.11 WEP-Sicherheit

Der IEEE 802.11-Standard beinhaltet WEP („Wired Equivalent Privacy“), einen Datenschutzmechanismus mit gemeinsamen Schlüssel.

WEP besitzt folgende Leistungsmerkmale:

- Datenverschlüsselung mit einem gemeinsamen 40-Bit-Schlüssel
- Kein Schlüsselverteilungsmechanismus. Der gemeinsame Schlüssel (Kennwort) muss manuell an alle Benutzer verteilt und jeweils lokal auf der Festplatte gespeichert werden.
- Einfache Authentifizierung des Clients, basierend auf der Hardware-Adresse.

## **Weitere Informationen zu Zellen**

Jeder Access Point im Netzwerk bildet das Zentrum einer Zelle bzw. eines BSS (Basic Service Set). Die Zellen sollten sich leicht überlappen, um überall im Netzwerk nahtlose Konnektivitätsübergänge zu erhalten. Benachbarte Access Points sollten für maximalen Durchsatz vorzugsweise auf verschiedenen Kanälen senden und empfangen.

Die Erstellung eines Zellenplans für Ihre Site kann kompliziert sein und wird normalerweise von Experten vorgenommen, die dafür spezielle Messgeräte verwenden. Welche Funkkanäle verwendet werden können, hängt sowohl von den Eigenschaften der verwendeten PC-Karte als auch von den Bestimmungen in Ihrem Gebiet ab.

## **Kompatibilität**

Das APManager Utility Version 1.1.0 ist nur mit dem NetEasy by D-Link DRC-1000AP Access Points kompatibel.

# Glossar

## **BSS**

„Basic Service Set“. Synonym für Access Point.

## **Zelle**

Gebiet, in dem das Funksignal eines Access Points ausreichend stark ist, um eine Verbindung aufzubauen.

## **ESS**

„Extended Service Set“. Eine Gruppe von Access Points mit gleichen Einstellungen, zwischen denen ein Client wechseln kann. Ein ESS bildet den Kern eines WLAN.

## **Algorithmus mit gemeinsamem Schlüssel**

Verschlüsselungsschema, bei dem sowohl Sender als auch Empfänger den (gleichen) Schlüssel kennen müssen.

## **SNMP**

„Simple Network Management Protocol“

## **WLAN**

„Wireless LAN“. Gesamtheit aller Access Points und drahtlosen Clients, die zusammen ein LAN (Local Area Network) bilden.

## **Write Community String**

SNMP-Kennwort

## **WEP**

„Wired Equivalent Protection“

Datenschutzmechanismus, der auf einem gemeinsamen Algorithmus mit 40-Bit-Schlüssel basiert wie im IEEE 802.11-Standard beschrieben.