



Information

De Philippe Devaud
Date 5 Januar 2004
Sujet Wireless Sicherheit

distribué à

copie à

pour information

ID Class

Id. Doc

Version

3.0

Statut

Übersetzt

Remplace version

Date d'émission

Valable dès

5.01.2004

Valable jusqu'à

Nom du document

FT_WirelessSecurite_V3_d.doc

Classement

Archivage

Inhaltsverzeichnis

1	<u>Einleitung</u>	3
2	<u>Technologie Wireless Lan (Wlan)</u>	3
2.1	<u>Bemerkung</u>	3
3	<u>Wireless WLAN</u>	3
4	<u>Klare Zugriffsrechte aufs Netz mittels Wireless-Station</u>	4
4.1	<u>Beispiel für ungebetene Gäste</u>	4
4.2	<u>Sicherheitsmassnahmen</u>	4
4.3	<u>Verschlüsselung WEP aktivieren</u>	4
4.4	<u>Verwaltung der Basisstation : Zugang durch ein Passwort schützen</u>	4
4.5	<u>Zugangseinschränkung mit MAC-Adresse (Medium Access Control)</u>	4
5	<u>Konfigurationsbeispiel einer Basisstation mit Apple</u>	5
5.1	<u>Passwort für den Zugriff und WEP Aktivierung</u>	5
5.2	<u>Eingabe der MAC-Adresse</u>	6
5.3	<u>DHCP eines AirPort</u>	6
6	<u>Konfiguration unter Windows</u>	7
7	<u>Ziele und Abkürzungen</u>	7

1 Einleitung

Das Einrichten eines kabellosen Netzwerkes (Wireless) sollte gut durchdacht sein. Die Sicherheitsaspekte im Netz sollten durch die Zugriffsrechte garantiert werden.

Die technischen Begriffe sind am Ende des Dokuments in einem Glossar beschrieben.

2 Technologie Wireless Lan (Wlan)

Die Technologie basiert auf dem Standard IEEE 802.11. Die Frequenz des WLAN ist zwischen 2,4GHz und 5GHz. Die Bandbreite von 2.4000 bis 2.4835 GHz ist in 14 Kanäle unterteilt. Einige dieser Kanäle sind für das Militär reserviert.

Das WLAN hat eine Reichweite von 50m. Die Reichweite zwischen den Komponenten ist abhängig der ganzen WLAN-Ausrüstung. Wenn man sich 50m von der Basisstation entfernt, ist die Übertragungsrate 1Mb/s.

Im Moment gilt die Norm 802.11b als Standard. Basisstationen kosteten zwischen 250 und 1500 Fr.

Es sieht momentan aus, als ob sich die Vertreter an die Norm IEEE 802.11g anpassen.

Übertragungsrate	Distanz
802.11b -> 11Mb/s	50 m
802.11a -> 54Mb/s	50 m
802.11g -> 36/54 Mb/s	50 m

Die zusätzliche Verwendung von Bluetooth in einem lokalen WLAN vermindert die Leistung vom WLAN um 40%, weil die gleiche Frequenz genutzt wird.

Deshalb sollte man aufmerksam über die vorhandenen PDAs und Netels wachen.

2.1 Bemerkung

Das WLAN sollte als *Zusatz* zu einem bestehenden lokalen Netz genutzt werden. Die Übertragungsrate ist viel kleiner als die eines herkömmlichen Netzes (mit Kabel).

3 Wireless WLAN

Man spricht von WLAN, wenn alle mit dem kabellosen Netz verbunden sind. Das Platzieren des Wireless ist im Zusammenhang mit der Sicherheit und Reichweite ziemlich komplex. Präzise Bemessungen sind wichtig, um den Standort der Basisstation zu definieren und eine best mögliche Reichweite zu erhalten plus eine zentrale Verwaltung der Zugriffsrechte muss definiert werden. Die zugelassenen Benutzer müssen zentral kreiert werden, damit unzulässige Personen keinen Zugriff aufs Netz haben.

Das Einrichten eines WLAN ist momentan möglich. CISCO bietet eine Lösung zu den Bereichen Zugriffsbe-
rechtigung und Sicherheit.

Solche Lösungen werden bis jetzt in freiburger Schulen noch nicht verwendet.

4 Klare Zugriffsrechte aufs Netz mittels Wireless-Station

Das Einbinden der Basisstation in ein lokales Kabelnetzwerk ist eine einfache Sache. Die Station kommt dazu und öffnet den mobilen Zugriff auf verschiedene Zonen.

Ausrüstungen, welche nicht in den zentralen und globalen Sicherheitsrahmen passen, bieten ein hohes Eindringrisiko. Deshalb ist es unbedingt nötig den Netzzugriff via Basisstation zu sichern.

4.1 Beispiel für ungebetene Gäste

- Die kabellosen nicht geschützten Netzwerke können von fremden Personen für den Zugang ins Internet ohne ihr Wissen genutzt werden. Somit kann die Personen mit der Schulidentifikation gratis alle Websites besuchen -> auch Website über Gewalt, Rassismus,
- Hat eine fremde Person Zugang zum Netz, kann sie alle öffentlichen Dokumente des internen Netzwerkes einsehen. Sie kann auch das System auskundschaften oder verstellen, weil das System den Eindringling als Mitglied betrachtet.
- Der Eindringling kann unerkannt alle Übermittlungen „abhören“ und hat auch zu vertraulichen Dokumenten Zugriff.

4.1.1 Sicherheitsmassnahmen

Die folgenden Punkte erklären, wie man ein Wireless-Netzwerk sichern kann. Wir empfehlen die simultane Aktivierung der 3 Punkte.

4.1.2 Verschlüsselung WEP aktivieren

Das Protokoll *WEP* (Wired Equivalent Privacy) ist ein Verschlüsselungsprotokoll mit einem geheimen Schlüssel für Kodierung und Dekodierung, erhältlich mit der Verschlüsselung von 40, 64 und 128 Bits. Diese Verschlüsselung vermeidet, dass ungebetene Gäste Einblick in die übermittelten Daten haben. Normalerweise verlangsamt der Einsatz des WEP-Protokolls die Übertragung nur leicht.

Damit die Verschlüsselung sicher ist, braucht es ein komplexes Passwort, bestehend aus 8 verschiedenen Zeichen (Zahlen, Buchstaben, Zeichen) und einen Schlüssel mit der grösstmöglichen Länge von 128 Bits.

4.1.3 Verwaltung der Basisstation : Zugang durch ein Passwort schützen

Die Zugriffsrechte können normalerweise übers Netz konfiguriert werden. Diese Einstellungsoptionen sollten mit einem Passwort geschützt werden, damit nicht irgendeine Person Zugriff hat. Man muss deshalb den Passwortschutz aktivieren.

4.1.4 Zugangseinschränkung mit MAC-Adresse (Medium Access Control)

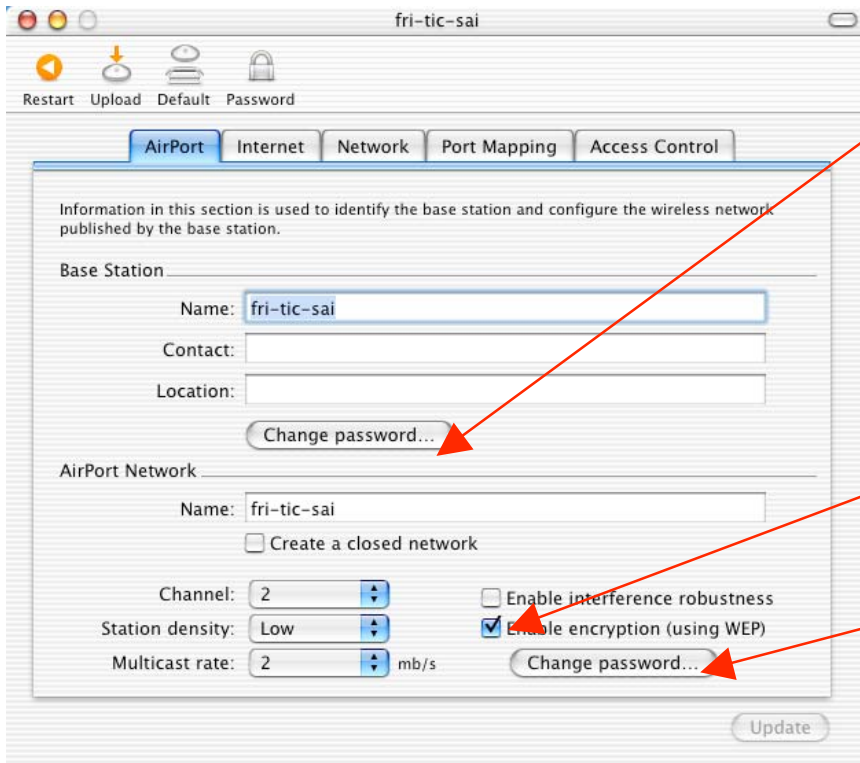
Es ist möglich den Zugriff über die MAC-Adresse der Netzwerkkarte der Benutzer zu definieren. Die Computer am Netz sind über ihre Netzwerkkartennummer einmalig und weltweit identifiziert; Die MAC-Adresse, die 48Bits beansprucht, schreibt sich im Hexadezimalsystem (0-9; A-F): XX:XX:XX:XX:XX:XX

Diese Zugangseinschränkung ist sehr sicher.

5 Konfigurationsbeispiel einer Basisstation mit Apple

Die folgenden Screenshots beschreiben, wie die Sicherheitsmassnahmen eines AirPorts aktiviert werden. Um sich bei einer Basisstation anzumelden braucht es „Airport Admin Utility“, welches unter /Applications/Utilities/ zu finden sind.

5.1 Passwort für den Zugriff und WEP Aktivierung

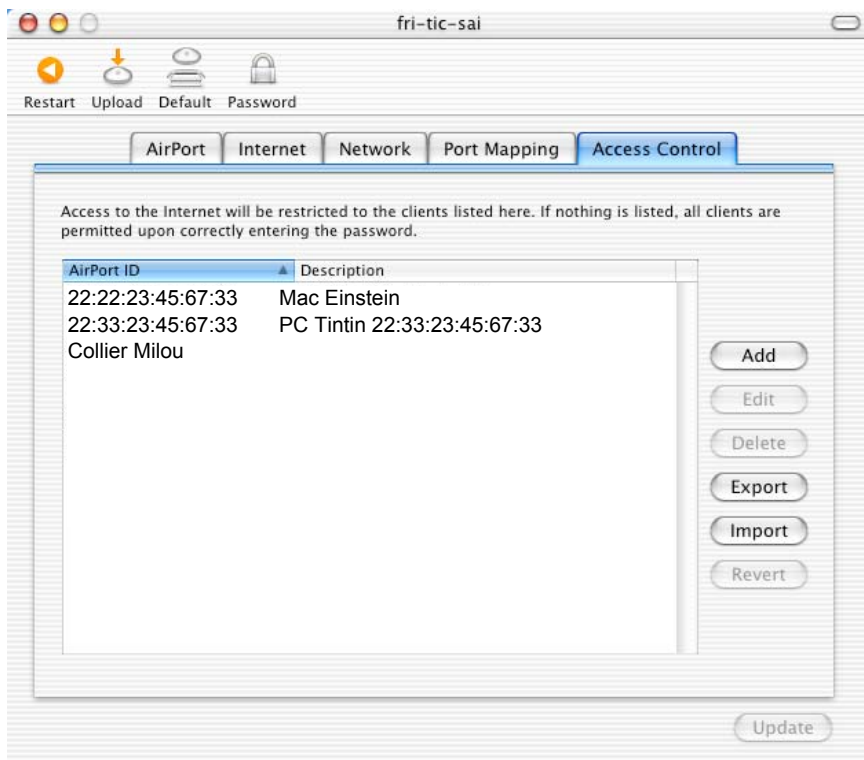


Das Passwort für die Zugriffsrechte kann hier erfasst werden.

WEP wird hier aktiviert.

Das Passwort für die Verschlüsselung kann hier erstellt /geändert werden.

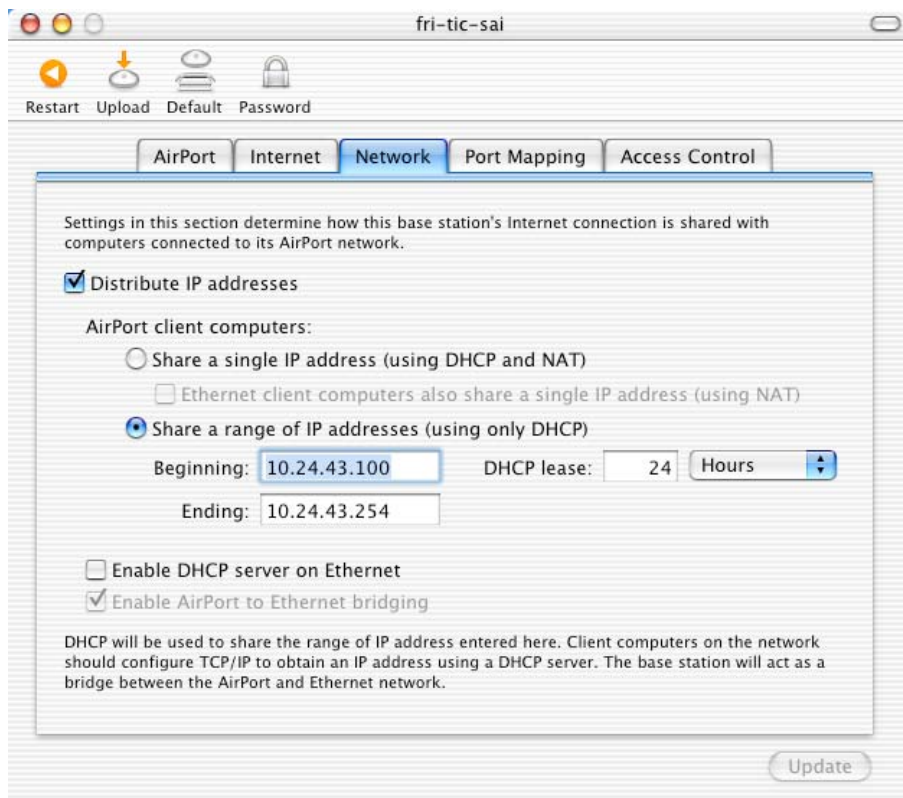
5.2 Eingabe der MAC-Adresse



Die MAC-Adresse kann im Register « Access Control » eingegeben werden.

Es können nur die eingegebenen MAC-Adressen Zugriff auf das Netzwerk haben.

5.3 DHCP eines AirPort



Eine praktische Funktion eines AirPort ist das Verteilen der IP-Adressen mit DHCP.

6 Konfiguration mit Windows

Das Konfigurieren von Basisstationen mit Windows ist herstellerabhängig. Die Einstellungen sind im Prinzip die gleichen wie im oben gezeigten Beispiel.

7 Ziele und Abkürzungen

Bluetooth	Übertragung mittels Mikrowelle zwischen Laptop, Computer, Telefon. Funktioniert in der Bandbreite von 2.4GHz. Diese Norm erlaubt den Austausch bis zu einem 1Mbps.
IP	Internet Protocol: Übermittlungsprotokoll im Internet. Es beschreibt auch die Netzwerkadresse.
bootP	Bootstrap Protocol: Es erlaubt dem Benutzer, den Server anzufragen, welches seine IP im Netz ist. Sie wird oft benutzt, um Workstations herunterzufahren oder sie automatisch zu konfigurieren.
DHCP	Dynamic Host Configuration Protocol: dynamische Adresszuweisung in einem IP-Netzwerk, basierend auf bootP. Das DHCP weist den angeschlossenen PCs (Clients) aus einem festgelegten Bereich von IP-Adressen automatisch eine IP-Adresse zu und spart so viel Konfigurationsarbeit bei größeren Netzen.
MAC	Medium Access Control Das verbreitetste physische Übertragungsprotokoll ist Ethernet Die Computer im lokalen Netzwerk sind mit einer Nummer identifiziert (einmalige Nummer auf der ganzen Welt), die sich auf der Netzwerkkarte befindet: MAC-Adresse. Sie besteht aus 48 Bits und ist folgendermassen notiert (Hexadezimal: 0...9 ; A...F): XX:XX:XX:XX:XX:XX
WEP	Wired Equivalent Privacy: Verschlüsselungsprotokoll mit Kodier- und Dekodierschlüssel
WLAN	Wireless Local Area Network: lokales Netzwerk ohne Kabel
Wireless	Installation ohne Kabel
PDA	Personal digital Assistant: Persönlicher Digitaler Assistent; kleiner Computer ohne Tastatur, welches z.B. einen Kalender/Agenda zur Verfügung stellt
Basisstation	Sender und Empfänger in einem: erlaubt den Zugriff auf ein Netzwerk ohne Kabel
Roaming	Roaming (zu deutsch: herumwandern) beschreibt das Wechseln mobiler Stationen von einer Basisstation zur nächsten.