BLACK BOX
NETWORK SERVICES

Black Box explains:

Data Security in Hotspots

Table of Contents

We care! If you have any questions about the applications, our products, or this white paper, please call the Black Box Free Tech Support or visit to black-box.eu and click on "Talk to a Tech." We will call you back for free - in seconds.

1. Introduction

Today, Internet is so important that we don't want to miss it while we are travelling around. A common way is using a Internet Hot Spot, available in hotels, restaurants, train stations etc.

Mostly, the Internet is now accessed by a wireless LAN, ie by radio. Laptops, iPhones and iPads provide integrated wireless LAN network cards. Wireless standards like IEEE 802.11b/g/n ensure interoperability on an international level. The user just needs simple basic know how to access the Internet via the hot spots. Many users established wireless networks at home too, because there are simply much more practical than using cabled networks.

In the home environment, the security of a wireless LAN primarily concentrates on the encryption of data, to ensure that no neighbors read along private bank account or credit card information. All authorized users of this wireless LAN know the encryption.

2. Hot Spot Access

In an Hot Spot, encryption would be inappropriate. Such networks are usually freely available. Security therefore gets a new meaning. To keep your data private, you have to act differently.

The keyword is the technical isolation of communications channels. Indeed, all participants of the Hot Spots , while working in the same cell, are isolated in a way that they can only communicate with or over the Internet, never directly with each other.

This client isolation is provided by wireless LAN Access Points, the radio stations in the network . The operation is relatively simple but very effective. Every network card - wired or wireless - has a unique identity called MAC address. Often you can find this ID even printed on your notebook in a format like "00-1B-9E-78-6E-D3". The MAC address of your Windows Laptop, you can found within the DOS prompt using the command "ipconfig / all". In Windows systems, the MAC address is written as „-„, Linux and other systems use „:“. Any network or data communication includes the MAC address and is therefore identifiable. A mapping between IP address and MAC address is done separately.

3. Client Isolation

The "client isolation" of an access point works doesn't allow per Software a data communication between two at the same Access Point registered devices. Once one of the isolated clients (device or user) is connected to a different Access Points, or uses a different connection technology (cable, radio), client isolation won't work any longer. An insulation in Hot Spots between users of different Access Points or different routes needs IP isolation. The IP address is considered to be more accurate. An IP address in a Internet-enabled network basically consists of four columns of numbers. Each column in turn consists of four numbers from 0 to 255. (Not mentioning deviations, distracting from our topic).

The first column represents the actual IP address, for example, 192.168.1.1. This part also includes a subnet mask like 255.255.255.0 The subnet determines the size of your IP address range, in other words, the higher the number, the smaller is the range of addresses. Using the subnet mask 255.255.255.0 allows the communication with 253 units. This special subnet mask is commonly referred to as a Class C network. Hot Spots reduce the subnet size to a smaller number of communication units. A typical subnet mask found in a Hot Spot will be something like 255.255.255.255. With this subnet mask, the communication is limited to your single device via L3 or IP isolation. The next two columns of the IP address give information about where the router is found and which gateway is used. The fourth column is the DNS server, converting Internet Addresses into IP addresses for the computer.

4. Go online with Apple devices

Apple devices have a special technique to execute the Internet access. Featuring the Apple Filing Protocol (AFP), apple devices use a fake MAC address within a wireless LAN, that varies from the actual ID. This procedure however prevents client isolation.

To improve the communication between two Maccbooks, Apple has implemented additional features like Multicast and Broadcast by passing also L3/IP-Isolation. Sometimes Apple even uses a data communication over an Internet server.

5. AFP Firmware Update for the WINDRy Access Point (LIGW54B) from Black Box

Hot Spots being technically built and installed by Black Box feature all state-of-the-art security mechanisms such as L3 and client isolation. A Windows user registering at the Hot Spot can find no other computers within his network environment. An Apple user would see also other connected devices. To avoid this unwanted visibility of connected devices, a software upgrade for the Black Box Access Point WINDRy has been developed that completely suppresses AFP.

Michael Wüst

Black Box Deutschland GmbH, Tel. +49 811 5541 411, michael.wuest@black-box.de