

# White Paper Multi SSID

Author: Dr. Andreas Anton Bloom

Copyright © 2005 Funkwerk Enterprise Communications GmbH, all rights reserved

Version 1.0

Date: 13/7/2005

## Table of Contents

<i>White Paper Multi SSID</i> .....	1
<i>Table of Contents</i> .....	2
<i>Why Does the Application of Multi SSIDs Make Sense?</i> .....	2
<i>SSID</i> .....	2
<i>Multi SSID</i> .....	3
<i>Multi SSID with VLAN</i> .....	3
<i>Multi SSID and Routing with Bintec Devices</i> .....	4
<i>Stateful Inspection Prevents Burglary</i> .....	4
<i>Content Filtering Ensures Legal Security</i> .....	4
<i>Summary</i> .....	5

## Why Does the Application of Multi SSIDs Make Sense?

Ever since Wireless LANs have been available in the market, the issue of security has continuously been dealt with by vendors and users. Since everybody is able to tap transmissions over the air interface, security is of much greater significance here than in wired networks. Standard 802.11 passed in 1997 defined WEP as encryption standard, which by now is considered insecure. The standard was enhanced by the WiFi Alliance by WPA in 2003 and enhanced again this year by WPA2. In contrast to WEP, WPA offers actual user authentication. WPA2 supports the improved encryption standard AES. Moreover, additional security mechanisms are available, such as access control lists or the so-called Service Set Identity (SSID).

### SSID

SSID is a name given to the access point. It serves to identify the access point and is sent out by the access point in regular intervals. If required, this mechanism can be used to filter out the appropriate access point out of a multitude of other access points. Anybody who has ever tried to access a hotspot at an airport will be acquainted with this problem. When scanning the air interface, several access points with different names are usually found, and the user has to select the hotspot out of them. Transmitting the Multi SSID, however, may also constitute a security gap. It permits hackers to detect the existence of an access point. If, moreover, the company name was selected as SSID, the hacker will know at once that the access point indicated stands for attorney-at-law Jones or medical practitioner Smith and can, thus, continue hacking in a more targeted manner. To prevent this, the transmission of the SSID can by now be deactivated for almost all access

points. This means that the user has to know the SSID of the access point in order to see it and to set up a connection to it.

This mechanism serves to fight off casual hackers who only want to see what's going on in the air. If someone really wants to find out which access points are set up in his surroundings, he can do this easily with freely or commercially available tools, such as "Airsnot" or "Networkstumbler". The reason for this is that the access point continues to transmit data, since authorized users must be able to find it.

Deactivating the SSID, therefore, does not provide for sufficient protection against being detected. Protection against intruders is offered by other mechanisms.

## **Multi SSID**

By now, some access points are able to support the Multi SSID function. Here, the access point cannot be assigned only one SSID, which has to be used by everybody; instead, it can be assigned several SSIDs. The advantage of this measure consists in the fact that each SSID can be assigned a different security level. With the conventional procedure, it was only possible to give all users the same rights, since they all had to log on at the same SSID. In this context, WEP or WPA can, for instance, be applied as encryption methods over the air. If a further user group with differing user rights was to be admitted to the data traffic, it was so far necessary to install a second access point or to select an access point with two radio modules. Multi SSID, however, makes it possible, for instance, to admit a user group with WPA-encrypted data traffic and to assign all rights to it, while a second group is permitted to log on at the access point in unencrypted mode. As a rule, only the open SSID will be sent in this case. Obviously, this does only make sense if the user groups logged on in different modes can be treated in different ways.

## **Multi SSID with VLAN**

To be able to treat users in different manners, VLANs (Virtual LANs) are used in the case of most access points. In the VLAN, an identifier is transmitted prior to each IP packet which defines to which group (to which VLAN) the IP packet belongs. The packets are processed according to this identifier. It is, thus, possible to separate the above-mentioned user groups into internal users with full user rights and into external users with limited rights only. External users, for instance, are not authorized to access internal servers. They can merely access the Internet via the existing infrastructure. Whatever they do there and which kind of data traffic they generate, however, cannot be controlled by the access point, as the latter only sets up the connection to the network behind it. To treat the users in different ways, it is not only necessary that the access point supports VLAN; the complete network must be VLAN-capable. This option, however, is still unavailable to the major part of networks configured today. Due to a lack of know-how, many small-scale companies decide to do without this function.

## Multi SSID and Routing with bintec Devices

Some vendors endeavor to assist administrators confronted with this dilemma offering combinations of access points and routers. The manner of implementation is decisive for the success of this approach. The bintec X2250 device implements the concept of the virtual interface. A virtual interface does not exist as a physical, but as a logical interface. In spite of that, all that can be done with a real interface is also possible with a virtual interface. In practical application, this means that a virtual interface is connected with an SSID and constitutes an interface for the user. The user can, thus, be assigned different rights. Firewall rules or temporary authorizations can be assigned for this interface. According to the setting made, the admitted packets will be routed differently. In this way, it is possible to implement a guest access in addition to the access to the enterprise network without resorting to a VLAN infrastructure. And all that can be done at economically-priced costs and in an absolutely secure manner.

## Stateful Inspection Prevents Burglary

As soon as you set up a connection to the Internet, you run the risk of intrusion from outside. Many attempts can already be prevented by a very simple NAT implementation. But this alone does not suffice as a security measure. Services should be limited as far as possible. It is not advisable, for instance, to permit services like FTP if you do not really need them. In this context, it does not suffice to check the SPI (Stateful Packet Inspection) checkbox. This is a nice try, but no sufficient protection. You should use devices which work with a real Stateful Inspection Firewall that can be adapted to your specific requirements. For a WLAN guest access via Multi SSID, for instance, it makes sense only to admit http and no other services at the open SSID. Well-configured implementations will block all other services once that one service has been set up. This corresponds to the philosophy that you will always be reminded that you have forgotten to activate a service when the users start complaining. If you admit all services which have not explicitly been forbidden you run the risk of forgetting something. And this will very probably be detected and exploited by hackers.

## Content Filtering Ensures Legal Security

The solution presented above serves to provide for a comfortable service for visitors, while the employees of the company can access their data via the air interface at the same time. When providing Internet access via a Multi SSID for your guests, you want to prevent unauthorized persons from using this access to open websites with racist or pornographic contents. Other examples of misuse are sending spam mails or hacking attacks against other users in the Internet. It is of vital interest to providers of Internet access to exclude all these kinds of misuse. In the worst case, they will be held responsible for these acts. If the police, for instance, find out with the help of an IP address that an Internet access is used to propagate child pornography, this may lead to the confiscation of all computers of the person in question.

To prevent these actions right from scratch, content filtering offers the option to establish sets of rules for the users regularizing the contents they view and work with. This function is already integrated into the new

devices of the bintec brand of the company Funkwerk. If you obtain the corresponding license, a service can be activated which causes the device to send an inquiry to a central server asking to which category a website belongs before it is opened. Specific categories can be blocked via the configuration of the devices. Subsequently, they will not be displayed. This makes sure that a user cannot misuse the Internet access you have provided to him. In particular with regard to legal aspects, this procedure has to be recommended.

## **Summary**

With the Multi SSID function, you can conveniently implement new solutions. You should make sure, however, that now follow-up costs will arise due to the necessity of reconfiguring the complete LAN for the use of VLAN-capable devices and that an appropriate security level is attained, both on the network level and with regard to the contents.