SUPPLEMENTARY MATERIALS 3

Title : « Securiting The Light Escaping In a Li-Fi Network Environment »
Author(s) : Dibson Diambeki, Reagan Mandiya, Kyandoghere Kyamakya, Selain Kasereka

SETTING UP A CAPTIVE PORTAL UNDER ZEROSHELL

A captive portal is a web page that appears to users newly connected to a wireless or wired network with a limited number of connections before they have full access to network resources.

They are mainly used in open wireless networks where users receive a welcome message informing them of the access conditions (authorized ports, responsibility, etc.). Administrators tend to do this to hold their own users accountable for their actions and to avoid legal liability. The Zeroshell captive portal o ers a number of con gurations and possibilities, not all of which will be detailed in this tutorial.

0.1 Architecture

For a captive portal to be set up, it must be the gateway to at least one network. Thus customers wishing to go out on the Internet will have to go through the Zeroshell and it will display the captive portal in order to request authentication from customers. Only customers with the correct identi ers will be able to go out on the Internet. Fig. 1 is an illustration of how the Zeroshell Captive Portal works:

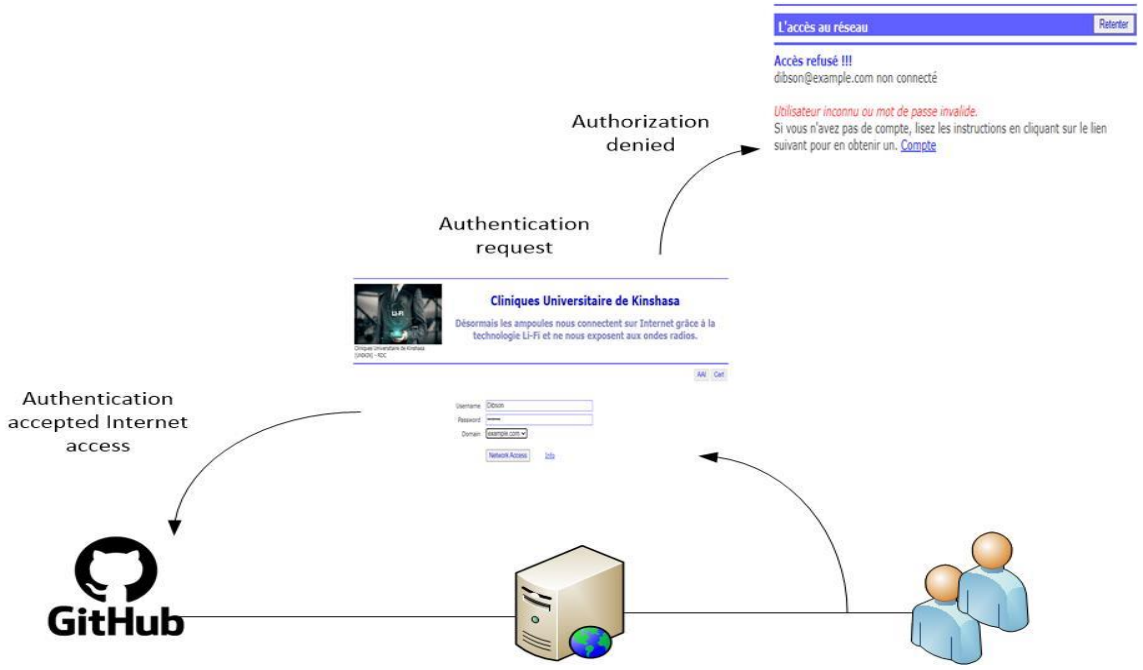

Figure 1: Architecture Zeroshell

0.2 Establishment

You must rst go to the graphical interface of our Zeroshell by browser. You must then log in and go to "Captive Portal". The rst thing to do is to determine on which interface our captive portal will operate. For example if our Zeroshell has its LAN side on the ETH00 interface, you must select ETH00 in the list at the top right then click on "Save". It is also possible to put the captive portal on several interfaces by clicking on "Multi" to have this window (Fig. 2):

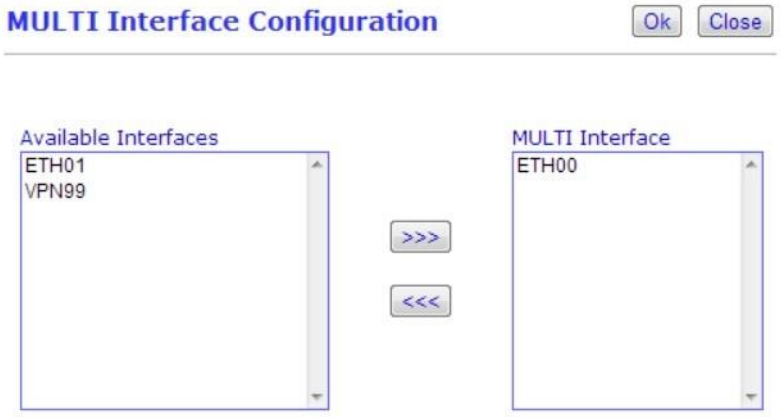

Figure 2: Con guration Interface

It is then necessary to pass the desired interfaces in "MULTI Interface" then click on "Ok" to validate. To nally make the captive portal e ective, you must check the box at the top left "GW" then click on "Save"

The captive portal is then active, it is now necessary to take care of the creation of the identi ers which will have the permission to be lodged on this one.

0.3 Creating captive portal users

The identi ers used for the captive portal are the identi ers registered in the Zeroshell users, so you have to go to "User" in the menu column on the left then in "Add" at the top to add some. You must then enter the identi ers of this user, the important elements are the "Username" which will be the login to use and the password which will also be entered. To nish creating the user, click on "Submit".

It’s time to test our captive portal, from a user workstation located on the LAN side of your Zeroshell, open a browser and try to access a web page (Fig. 3):

Figure 3: captive portal users

The redirection will be made either to a speci ed URL or to the URL that the client wanted to access the database. This parameter is managed in a menu that we will detail later. A pop-up window will also appear, this one is present to keep the connection open for the authenticated client, it is preferable not to close it or the client will be automatically disconnected. It is nevertheless possible to con gure the disconnection delay after closing this window (Fig. 4) :

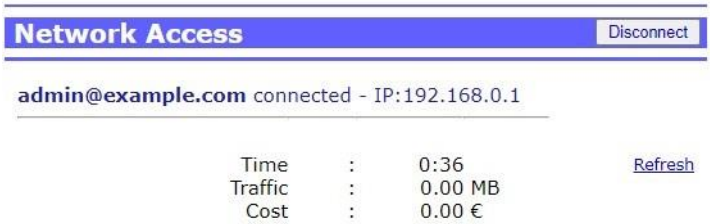

Figure 4: Network Access

We also see that it is possible to set up a system of monetization of Internet access.

0.4 Connection management

In the "Gateway" menu of the captive portal, we can manage the basic parameters of client authentication. The left panel allows you to see the users connected to our captive portal (Fig. 5) :

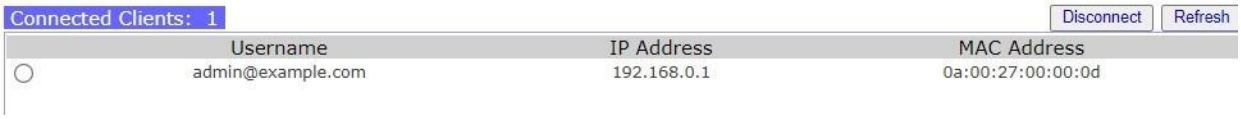

Figure 5: Management

It is possible to see the IP and address of the user and the credentials he used. From this panel we can disconnect the user by clicking on "Disconnect". The panel at the top right of the captive portal window allows you to view and modify the main parameters.

For example, we can con gure whether we want to identify clients by their IP and their MAC or just by their IP. We can also determine whether you want to allow the simultaneous use of a login ID or not. Authorizing this multiple connection is useful, for example, in a Hotel or a public space where it would be complex to create a user for each connection request (Gig. 6).

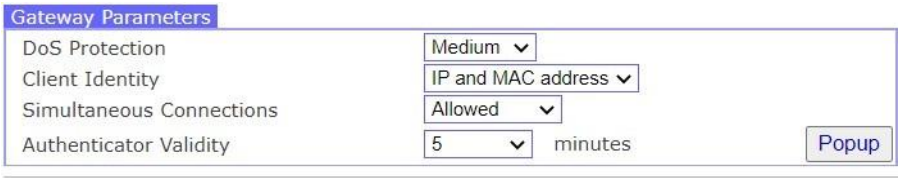

Figure 6: Gateway Parameters

The Authenticator Validity is the parameter that will determine how long the connection will remain active after the connection window is closed on the client side. It is determined in minutes and can be set to "in nite" if the client authentication must always remain active. Once the parameters have been modi ed, you must click on "Save" to validate them.

The third panel is for determining exceptions for using the Captive Portal. For example, we can put an IP which will be that of a station with xed IP, this IP will then not need to be authenticated to access the Internet. To do this, select "Clients" to the right of "Free Authorized" then click on the "+" and nally enter the IP and the mask of this client (Fig. 7).

Figure 7: Authorized Client

Finally, you must click on "Save" to validate the addition of the exception. We can also put a service there by selecting "Services" then by clicking on the "+", it is then necessary to enter the name of the service, the source IP of this service and the port it uses then click on "Save".