Contents

Hotspot Implementation

Scope

This document tries to introduce into perspective the whole workflow in DCR Hotspot implementation. It will explain step by step each component of the diagram such that the process is exhaustive, complementary and detailed.
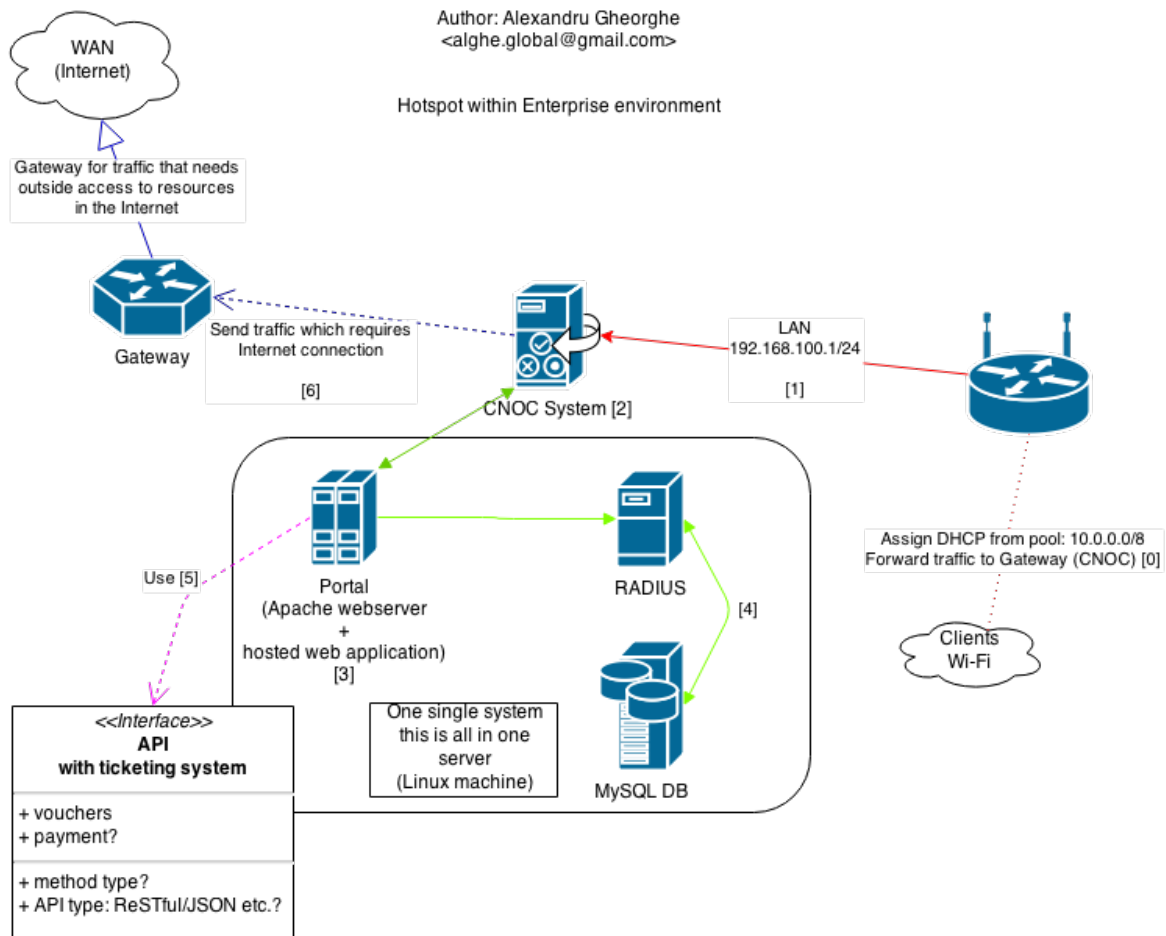
General flow

The general flow looks like the following:

> ### Note
>
> The network addressing schemes (in `CIDR` notation) are not fully explanatory. For more detail on this, please refer to the next sections.

Diagram

Author: Alexandru Gheorghe
<alghe.global@gmail.com>

Hotspot within Enterprise environment

WAN
(Internet)

Gateway for traffic that needs
outside access to resources
in the Internet

Gateway

Send traffic which requires
Internet connection

[6]

CNOC System [2]

LAN
192.168.100.1/24

[1]

Assign DHCP from pool: 10.0.0.0/8
Forward traffic to Gateway (CNOC) [0]

Clients
Wi-Fi

Use [5]

Portal
(Apache webserver
+
hosted web application)
[3]

RADIUS

[4]

One single system
this is all in one
server
(Linux machine)

MySQL DB

<<Interface>>
API
with ticketing system

+ vouchers
+ payment?

+ method type?
+ API type: ReSTful/JSON etc.?

How it works?

0. A client connects to the Wi-Fi network (the clients will come from the 16e network, will be served DHCP from 10.0.0.0/8 pool and be routed to CNOC for access, CNOC will see all requests from these IPs under the same MAC address)

1. CNOC listens for Internet requests on its LAN side which is the network will serve (it must be able to see users coming from 10.0.0.0/8)

2. CNOC will contact the Portal page: if the client requested a whitelisted Internet resource, allow him without filtering; if otherwise, redirect him to the Portal page until authenticated

3. The portal page will present the captiva portal (this is where the user has to sign in etc.). The user will send to the portal page his authentication credentials (which will be compared against the Voucher system for the created voucher)

4. CNOC at this stage, has to be aware if the user has authenticated successfully or not (either via API with the Voucher system or via MySQL db and RADIUS relationship, or a mixture between these), depending on the result, the appropriate action is taken: let the user browse (and count its activity: bandwidth, time etc.) or forcefully redirect again to the portal page (show invalid credentials or similar action)

5. If the client's credentials are valid and/or the API returns a successful login for the voucher then proceed further (the step 4 above)

6. Client is logged in (marked as allowed), track his time, session, bandwidth usage etc. Send traffic to the gateway for Internet access if his request doesn't fit into the already allowed websites policy (wikipedia etc.). CNOC at this stage should be aware of the limit that was imposed to the user using that voucher/username, if it exceeds it should cut his connection by presenting a page "Bandwidth limit reached. Contact your Agent in order to extend", or similar message. Besides this the rest of attributes should be tracked: IP, how much data sent/received, time spent on the session etc.

The process: in detail

Let's cover now each step of the process. The general flow can be seen at the outlined flow subsection. It presents each step that will be explained in the next subsections. The aim is to cover the full flow from the client all the way to the Internet.

Now, the flow will start with the one of the most important part of the implementation: **the client**. The whole service will revolve around this important part.

Outlined flow
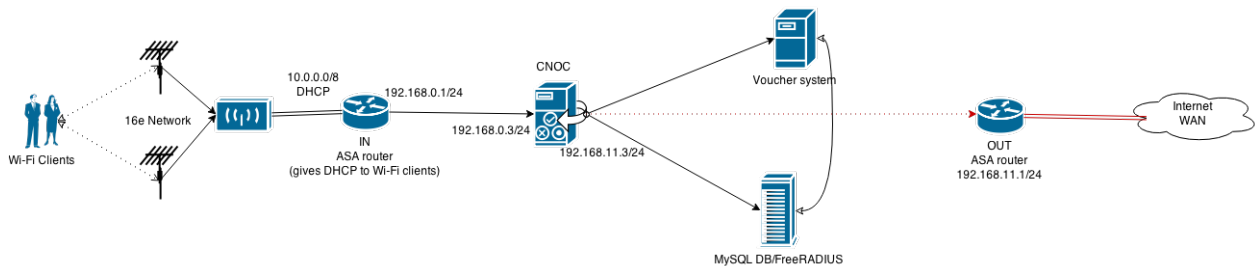
Summary

It is the user that will be served the service. Mainly, the service will consist of students so that the service will be generating content and will be developed towards student-focused content (free access to libraries, documentation etc.). But in parallel, as clients there will also be other customers that are not necessarily students. These will have other generated content.

When *generated content* is mentioned, it's actually refering to the Captive Portal page (see captive portal mockup as example). In order to get there (to the Captive Portal), the user will transparently go through a series of steps (next subsections) without knowing or caring about them.

The user will connect from various devices, such as the popular: Smartphones, Mobiles (that have a browser), Laptops, Tablets etc. It is thus important to preserve compatility throughout browsers in order to support these platforms and offer them the service in a readable, easy to use form.

These users Wi-Fi signals will be captured by the 16e network. The antennas are throughout the city and will communicate the user sent data (DHCP request, HTTP requests after getting an IP etc.) via the CPE's.

Step by step

In order to get the full clear picture how all the puzzles fit in, let's go step by step into the process shown above in Outlined flow section. Let's start with what, in the real situation, a superadmin will start with.

> ### *Note*
>
> The below presented pictures (apart from the network diagrams) are **wireframes**, that is, representations that are not yet showing the final product, but have only an illustrative scope.

1: Voucher System
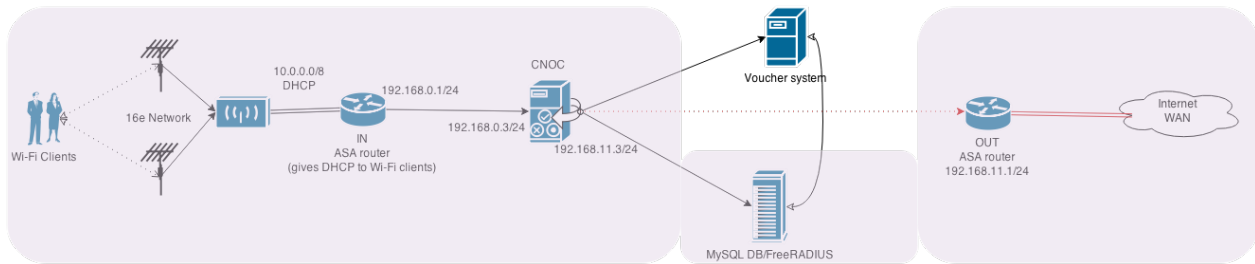
All begins from the `Superadmin`. The superadmin has the following attributes:

- Can manage the whole system, it is the highest user in hierarchy

- Edit the whitelist of websites (which do not require any authentication whatsoever and are free to be browsed by anyone connected)

- Has the access to manage `Agents` and `Resellers`

- All the vouchers will be assigned by the superadmin

- He/she can read the information regarding used and unused vouchers and their related agents and resellers

- Discounts can be given to selected agents and resellers based on their performance (data volume, sold vouchers to users, subscribed users etc.)

- Vouchers price will be decided by the superadmin, this price will be available for credit card purchase (E-com)

- He/she is able to fetch all the data regarding any voucher: how it was used, where it was used and by whom it was used. These statistics are important to generate graphs, (easy to be) visualized data and so on, in order to take further decisions and analysis based on performance of the service. It's also important to know how the vouchers distribute and how the roaming users are impacted by various strategies in the market.

- Statistics available to this user will also tell the usage per area

- Can determine the bandwidth available and speed limit of a voucher. For example, a group is created "Users" and to this group a batch of vouchers are generated, the general speed limit is automatically set on the group (which sets on the vouchers that are created/generated), an example: 100 symmetric Kbps for Quality of Service assurance and bandwidth assignment. Bandwidth limiting can mean: 1GB per day of traffic is the limit, once a user reaches this amount he/she will be disconnected with a message "You've reached your bandwidth limit. Come back in [int] time." where `[int] time` means, when the bandwidth counter will reset to 0.

- This user will also be in charge with commission management

- The superadmin page will also include a section: NOC Reporting, this is a section where the previous points are included (statistics) and also functions to export to several formats: CSV (Comma separated values) for Excel documents, PDF's etc. It's also where the superadmin can track the performance of agents and resellers.

- Other sections will include management of agents and resellers in the hierarchy

- Agents will be the ones that are assigned directly by Superadmin in hierarchy to sell the assigned vouchers in the market place

- The resellers are then assigned by the agents with the permission from Superadmin

- End client will purchase the voucher(s) from the resellers

- If reseller(s) is(are) out of stock (vouchers) then he'll/they'll request vouchers from agents

- If agent(s) is(are) out of stock (vouchers) then he'll/they'll request vouchers from superadmin

It is important to note that the information will be handled with the database in order to sync. this information. It is also important to observe how the CNOC will be reading information from here in order to perform actions on the users. For example: the bandwidth limit and/or speed limit is important to control the user's usage. The CNOC server will have to read from here in order to know this detail, which is set by superadmin.

Let's see how the superadmin will now configure a voucher after logging in and going to the voucher page (image serves as illustration purpose).
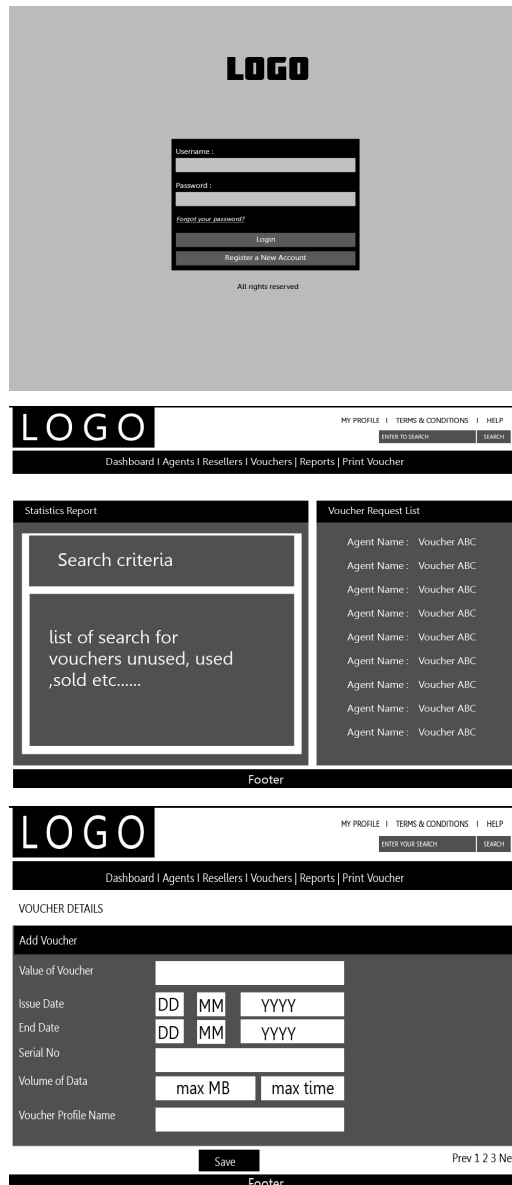
The physical voucher which is to be allowed to be used by any user on any hotspot will have the following attributes:

- Normal value of the voucher (price/cost amount)

- Issue date of voucher

- End date of voucher (expiration)

- Serial number of voucher (unique)

- Volume of data (data limitation: 1GB per day/10GBs per week/100GBs per month etc.)

- Max bandwidth usage (how much bandwidth can a user actually occupy, this is for QoS)

- User profile or voucher profile name

- Name of the company

- Logo

- Reseller ID and name

- Agent ID and name which allocated to the reseller

The hierarchy workflow looks like the following:
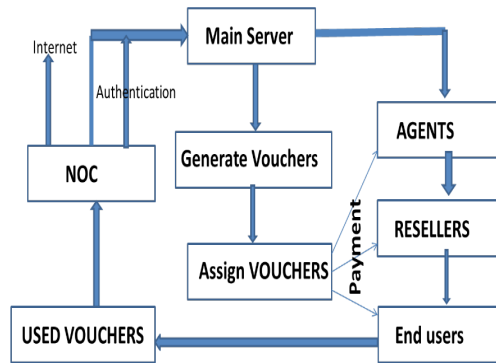
It's important that these details will be written to the database. CNOC will then integrate with this database and share the data, update some and having the technology interconnected will ensure the functionality of the service.

It is also important that the system is scalabe so in the future if newer modules are needed they can be easily added in and integrated with the database, in the voucher system or in CNOC.

In order to depict how the Agents look, let's see the next mockups:
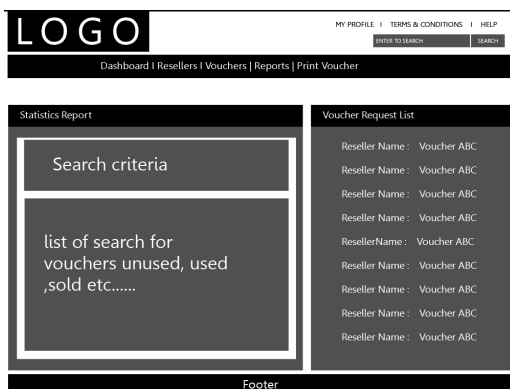
How the superadmin sees them:
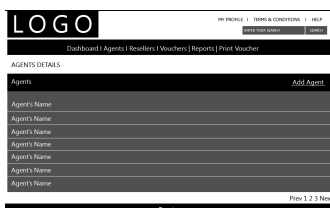
And now let's see the reseller and the vouchers:
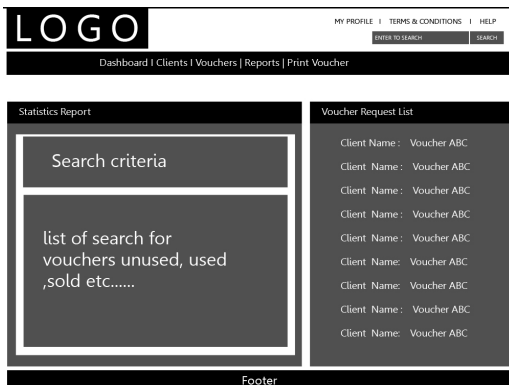
How the superadmin sees them:
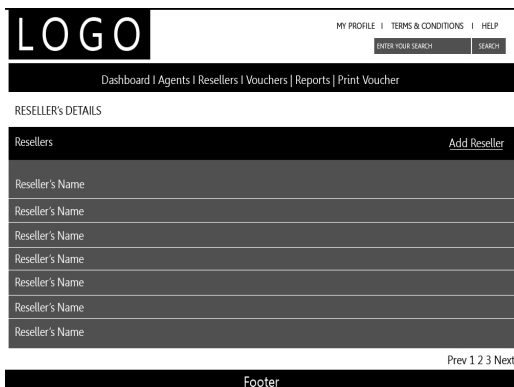
API

The Voucher system will have an API reachable in order to standardize voucher checking (if allocated/valid etc.) and to interconnect with the rest of the system: billing and CNOC. The Captive Portal page will also make use of this in order to validate the user's introduced credentials and further more, extend scalability.

The Voucher System should allow the CNOC server to query it's database in order to:

- know if a voucher is valid (and, optionally, was allocated to a certain username)
- retrieve details for a given voucher: max bandwidth usage (download/upload), max data usage (KB/MB/GB)
- update the session time for a user in order to get statistics (from CNOC to Voucher System)

Also the Voucher system should connect with the Billing system through API's in order to:

- validate a payment and set for usage a voucher
- allocate certain vouchers to a payment or reserve them for future usage
- query if a voucher was purchased
- details about payment: who bought it, what time and date etc.
- allow details to be exported for future analysis and documentation to also generate statistics

2: The Client
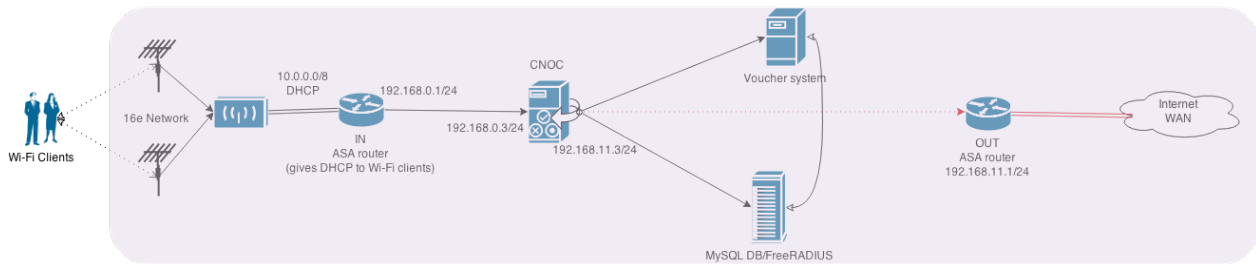
Once the voucher was managed through the whole hierarchy from Superadmin all the way to Agent and Reseller, the client has now purchased a voucher from a given Reseller. This information is stored in the database and the API of the Voucher system makes this data available for CNOC (for limitations and such) and also to export statistics, generate documented analysis, make future checks of performance of Agents/Resellers etc.

Thus now we're to the client phase where it will connect with his or hers purchased voucher. Since it connected to one of the Access Points/CPE's it will be redirected to the ASA router which will give to the client an IP. This IP will show up to the CNOC trying to access the Internet.

CNOC at this moment will first check the user IP to see if it's authenticated (based on voucher and/or username), but before this, will check if the HTTP request resource web link is whitelisted (configured by superadmin) and if it is, will let the user browse the website with no redirection. If however, the requested resource is not in the whitelist and the user is not authenticated, the Captive Portal Page will be shown via a forced redirection, until the user is authenticated and marked as such, at which moment, he/she can browse freely with the assigned attributes (bandwidth usage, maximum data usage etc.), and tracked accordingly.
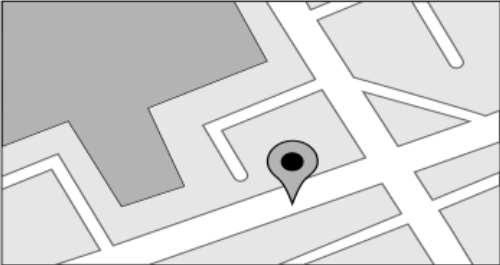
Captive Portal

This Captive Portal Page has several functions:

1. it immediately tells to the user via GPS location what are the nearby hotspots should him or her have to move through the city (students will often move to cafeteria and such and is beneficial to have them informed of nearby hotspots they can use), but it also tells to the other customers either travelling on business, or simply being busy

2. informs the user about the library of the free resources, for students will of course be libraries and such information, while for other users can be business oriented information; both will have sections for commercial and advertisments to generate income

3. tells the user how to stay in touch via the social media networks (YouTube, Facebook etc.)

4. allows the user to authenticate via a voucher (and possibly via a username and/or password)

Once the user signs in he/she will be allowed to browse upon his or hers established voucher data. It's also important to note that a next page will be shown during successful authentication which will present to the user his or hers session time, the amount of bandwidth used (optional), and the amount of data generated (so she/he will know when the session will end up, this will allow the user to maximize the service usage).

Now let's understand more in depth what really happens when this occurs by visiting the next sections regarding the 16e network.
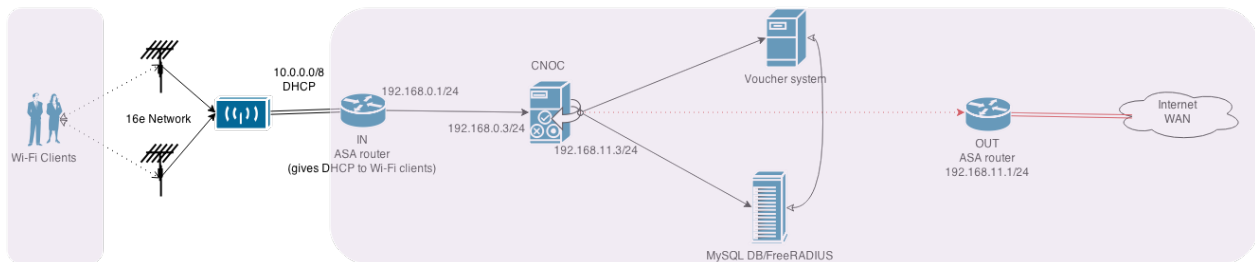
API

A last detail to note is that this authentication mechanism is communicating with CNOC, Voucher system and the database. The RADIUS keeps informed the systems about the user.

> **Warning**
>
> Decide how RADIUS integrates into the picture.

3: 16e Network

Reaching the 16e network, this is how the users are captured and how it is made possible to redirect them to the Captive Portal in order to benefit from the service. When the users device connects to this network it will try to get an IP via DHCP, the 16e network has the responsibility to catch this traffic and transmit it to the router (see next section: `FIX ME`_), at which point the router will assign the IP.

This network is very important from a coverage standpoint. Since it will be backed by *AUF (Agence Universitaire de la Francophonie)* backhaul it will link several hotspots across *DRC (Democratic Republic of the Congo)*'s Kinshasa:

Warning

to continue