ECE PARIS · LYON
ÉCOLE D'INGÉNIEURS

ING4 SI01

Network Security

WI-FI Security

Lab 1

Author(s):
Anastasia DUCHESNE
Idris FOUGHALI
Gabriel PADIS

Teacher(s):
Mr. Hatoum

Paris - Semester 7 - March 5, 2019

Contents

1 Airport / Stadium / Restaurant

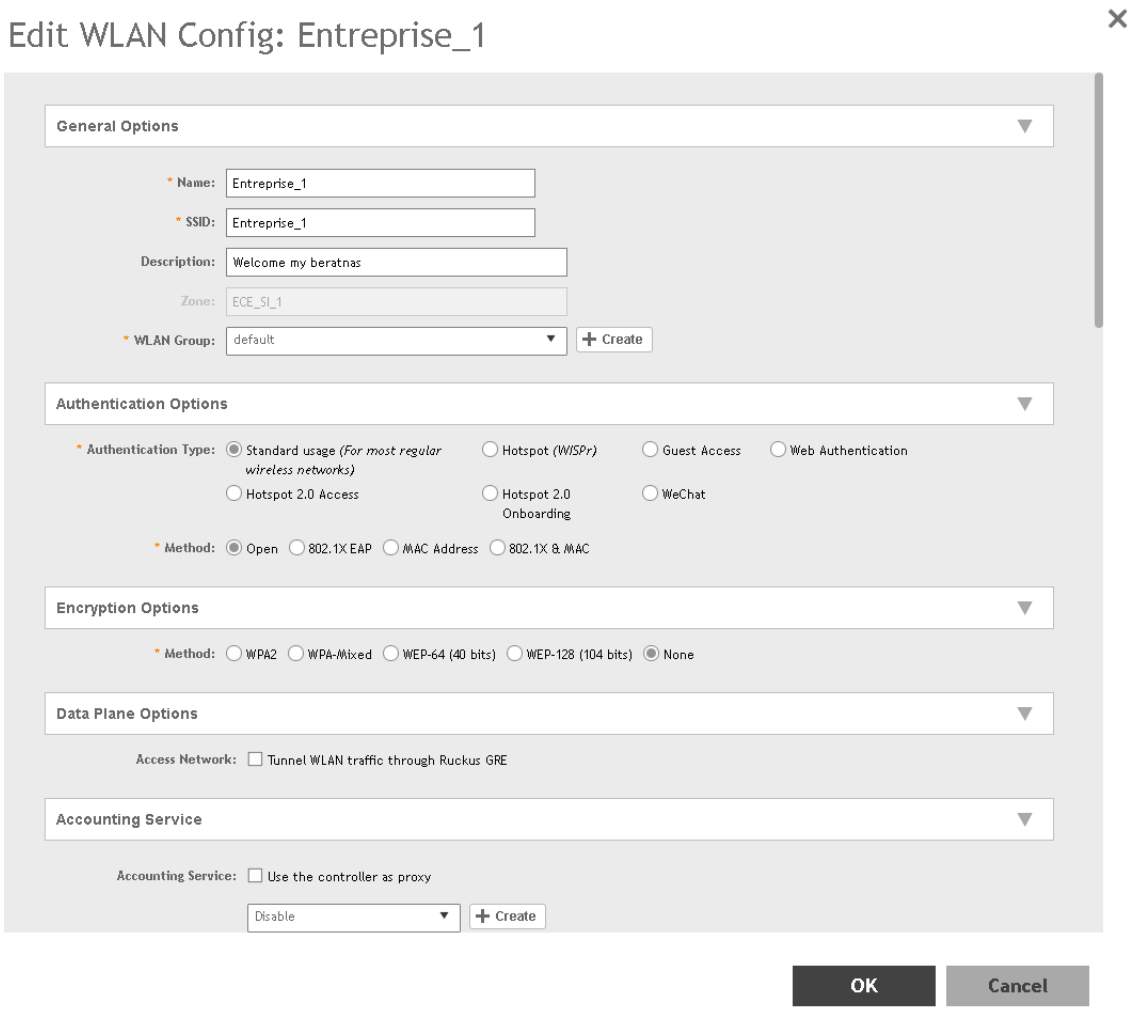

Figure 1: Configuration for Airport

1.1 Authentication method

For places with a huge number of visitors such as airports, stadiums and restaurants, we use open authentication. We have here a standard usage for our Wi-Fi in our network. Usually, the things the users will do on the Internet won't be too demanding in speed, and for a brief period. We want to set-up a simple access to the internet so standard usage is what we need as an authentication type.

We use the open method since we want anyone to be able to connect with it in the airport. It would be too complicated to give the password to everyone. So Open Authentication seems the best choice.

1.2 Encryption method

Although encrypting data through the network is a good thing to do, we have no way of distributing the keys to do so to everyone. So we choose to not have a encryption method.

Since there is no authentication nor encryption method, some parts of our data is plain text. The IP headers for example aren't encrypted and are easily accessible. It is the same for each http website you're visiting.

HTTPS packets are more secure though, because they have end-to-end encryption. So, the accessed website address is only partially shown : only everything before the / is plaintext.

1.3 Network components

We have 2 physical components in our network in this case:

- The Ruckus Access Point: It is a 802.11ac or 802.11ax equipment, the ax version is designed specifically for high-density public environments which is our case.
- The UCOPIA authenticator: It is a captive portal for our network to go trough after the access point. It handles the authentication and if it is successful it allows the connection to the internet.

1.4 Secure the network

In order to secure the network we are taking the following steps:

- Restricted internet until login
  The network request coming from the clients through the access point is blocked at the captive portal. Until the user is not logged in by the portal it will not have access to internet.
- Block all protocols and the corresponding ports not required for a simple usage in the airport
  HTTP, TCP, UDP, FTP, TLS and SSL are useful but SSH will be blocked for improved security. We could also block VPN but then users would not have the possibility to be hide their internet traffic for more security.
- Block some websites
  Not allowing access to some website will allow us to have control over our network. Download, streaming and torrent sites will be blocked to save bandwidth and preserve the network from downloading ill motivated materials. Sites with certain keywords and adult contents will be blocked too.

1.4.1 SSH block

Why should we block the SSH ?
We do not want anyone on the network to connect to badly protected IoT or to our network equipment. Indeed if you have the ip address of the components you can connect to it and take control over it.

It can be badly protected either with very weak combination of login and password or with the default credentials. In this case we were able to connect as admin to the Ucopia component and gain full access over it. We just had to search the internet for the set-up manual of Ucopia and then in it to find the default ssh credentials. We found it, it is :

- login: admin
- password: bhu85tgb

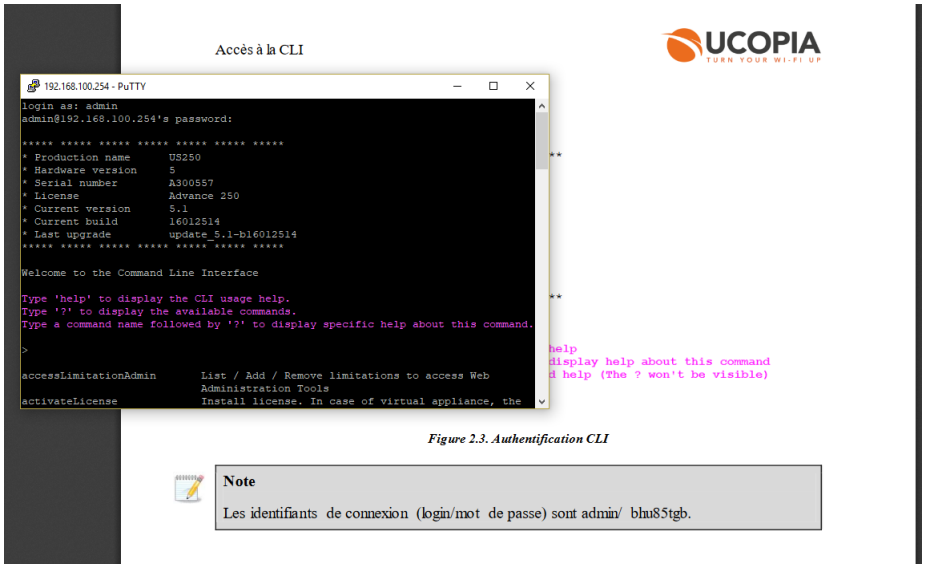

Figure 2.3. Authentification CLI

Figure 2: Connect as admin via ssh and default credentials

1.5 Control the access to the resources

Through the open authentication (OpenID or OAuth) provided by a captive portal, we're going to collect data on people who connect to our Wi-Fi. For example, we're going to request them through a portal to enter some information such as a name, an email address or even to connect with a social network, before accessing to the Internet connection.

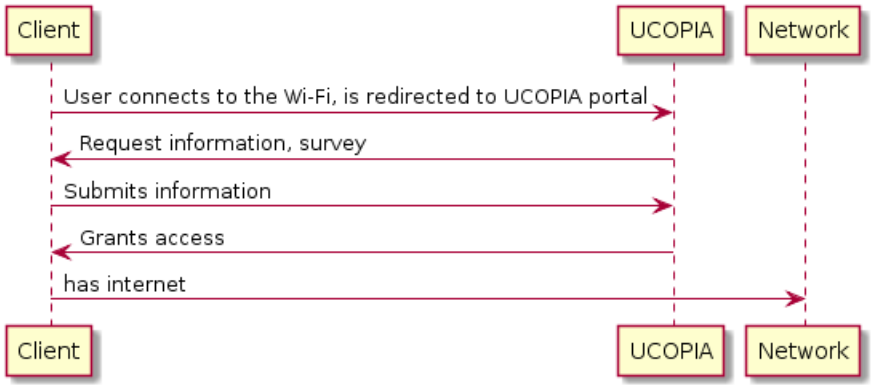

Figure 3: Sequence diagram of connection via login

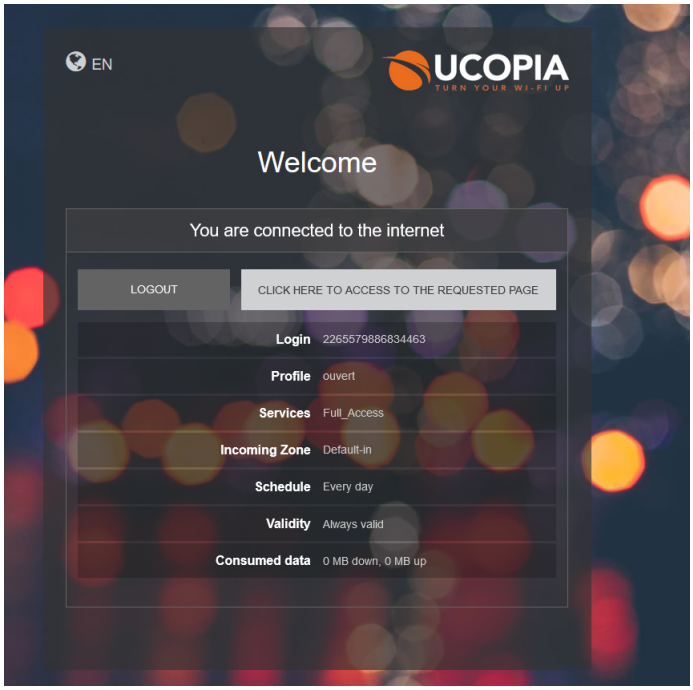

Figure 4: Connect via login

1.6 Benefits of the implementation of the this WI-FI connection method

We decided to implement our WIFI this way because we know that there would be heavy traffic on our network, so making a passphrase with the WPA-2 Personnel or entreprise is out of the question, because this would mean sending passwords physically to our clients (via mail, or on posters around the place, etc.). Instead, we've implemented a Standard usage authentication type with an open method, in order to let everyone connect to the hotpost. This portal then redirects our hotspot clients to the Portal server in order for them to authenticate and be able to access the internet.

So in brief, this method enables us the ease of providing internet to a very large public without having to worry about the security part, since the the authentication will then be managed by the portal (depending on how the portal will be configured to authenticate the user/client) after the logging, we can just reroute the authenticated clients to the public interface of our public router, so that they can get internet access.

1.7 Schema of the connection

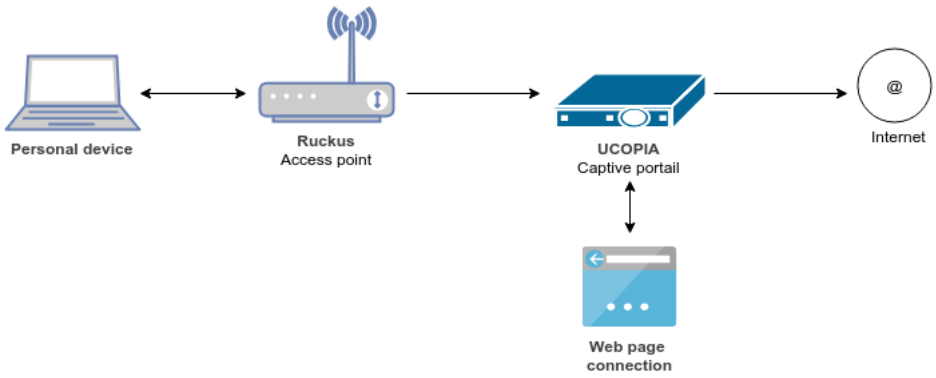

Figure 5: Diagram of an AirPort Wi-Fi

1.8 Social Media authentication integration

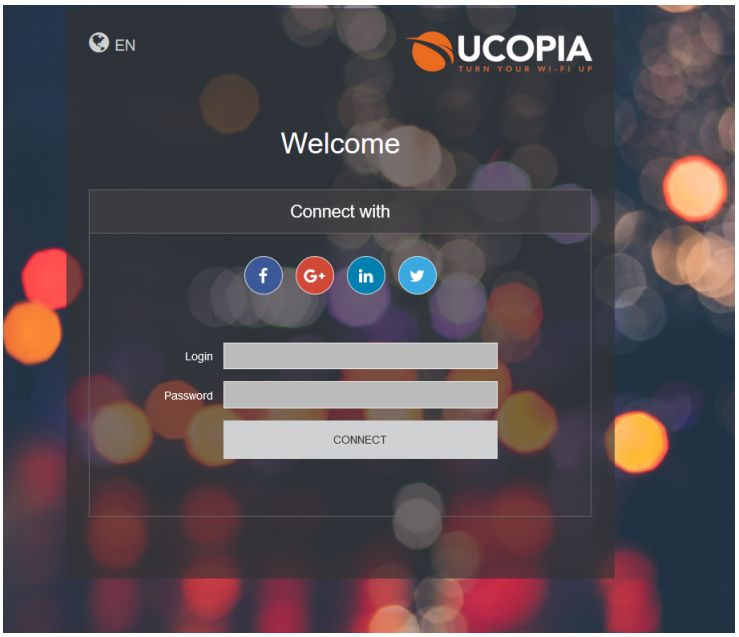

Figure 6: Social media integration

To configure the social media authentication integration, we have to do it through the captive portal, in our case UCOPIA. You have to disable the password/login connection, and to enable the connection through social network.
The user will choose his preferred social network on the portal. Then, UCOPIA will redirect him to the redirectURI, which works like the entry point of the app through which he's trying to connect. Once he is connected to the app, he has to allow to share some of his data such as his email address or his name. The app calls the redirectURI, with an authorization code. The user is able to pass the redirect URI now, and can access to internet.

Some of the collected data will be transmitted as plain text to UCOPIA.

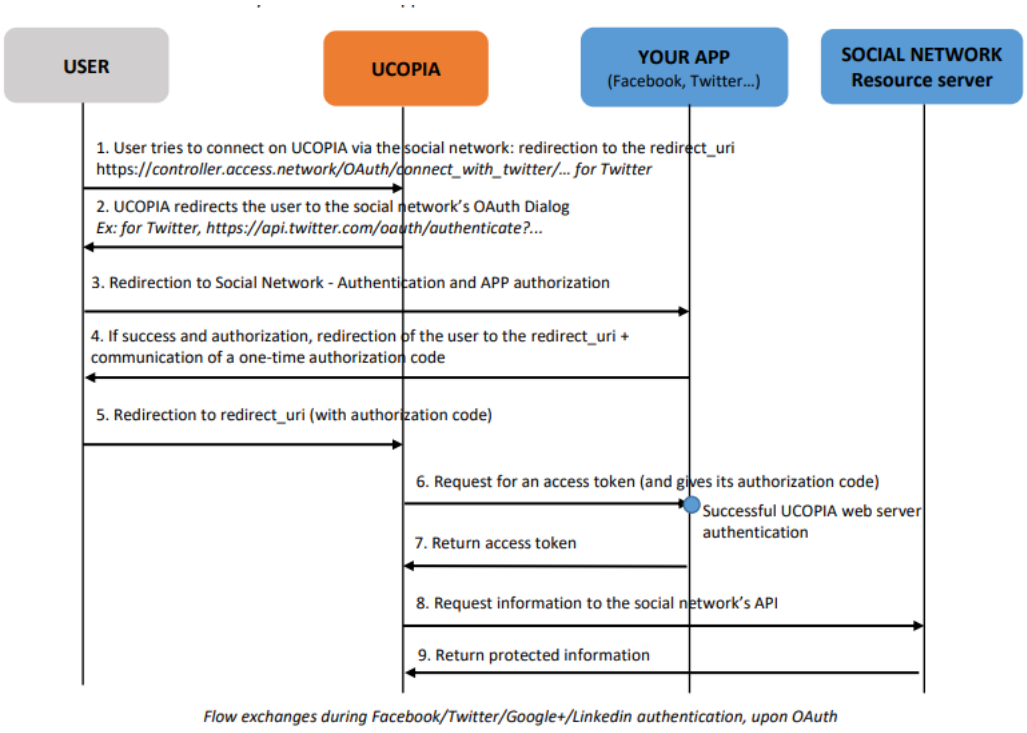

Figure 7: Connection through social media

2 University / Office

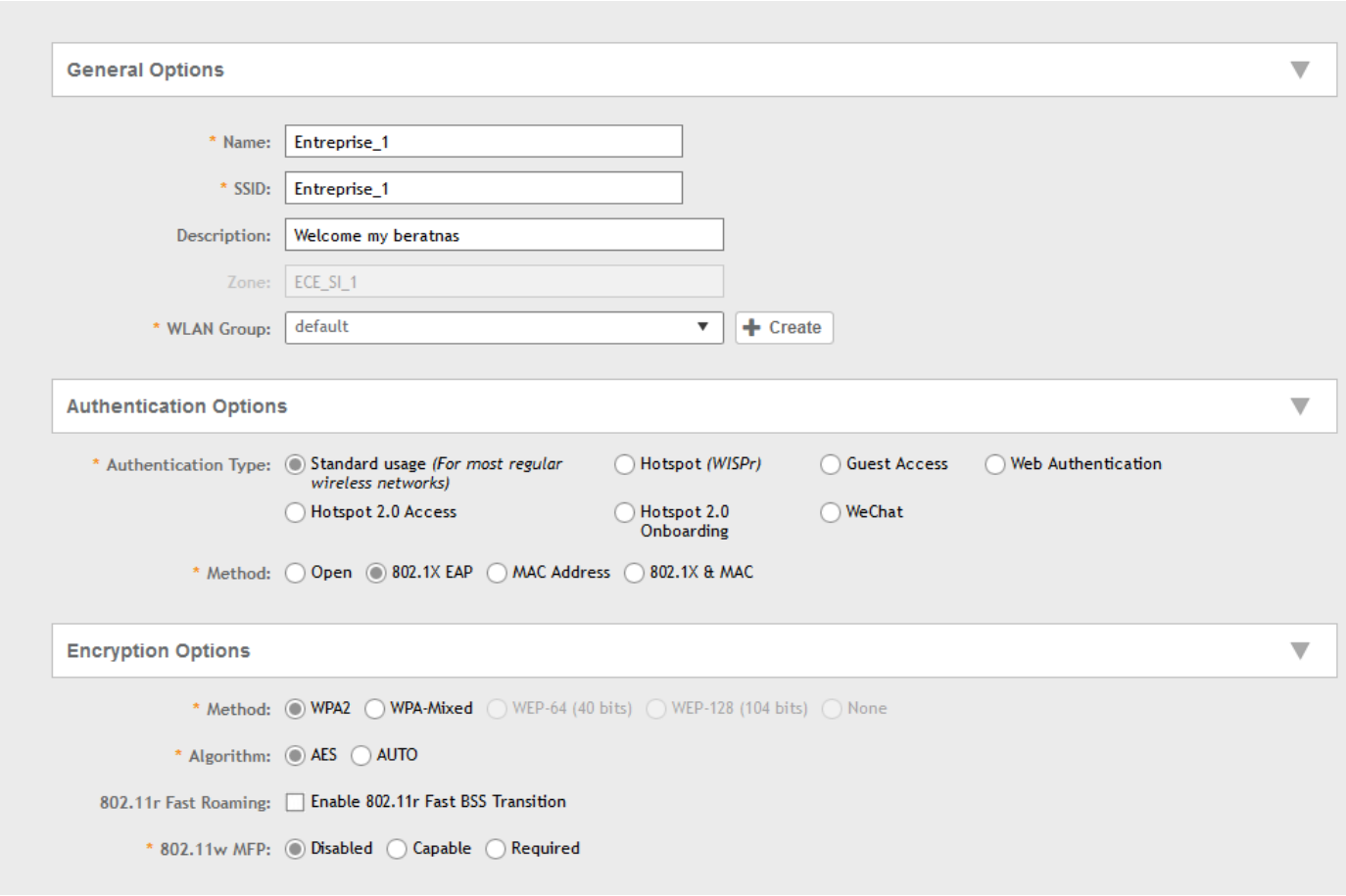

Figure 8: Configuration for University or Office

2.1 Authentication method

Like before we still have a regular case of usage so we are using the standard usage as the authentication type. The main difference is that in universities or offices, we need a more secure network than in Airports. Even though there is a lot of users in this case too (some universities in America can have more than 20000 students for example), it is easier to give a password to users in this case, since they will use the Wi-Fi on daily basis, and it is more common.
For the authentication method we chose to use 802.1X which provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. It encapsulates the Extensible Authentication Protocol (EAP) which is used to authenticate each user personally. It is the protocol used at ECE Paris to log students and teachers.

2.2 Encryption method

For the encryption method we used what is supported and the most secure, it being the WPA2 method with AES as the algorithm.

2.3 Network components

We have same 2 physical components than before in our network, and in this case we also have an authentication server. On it is the credentials and we'll need to use the RADIUS protocol to access them. This server is firstly on the UCOPIA authenticator and secondly on a distant server (**5.39.109.250**).

2.4 Schema of the connection

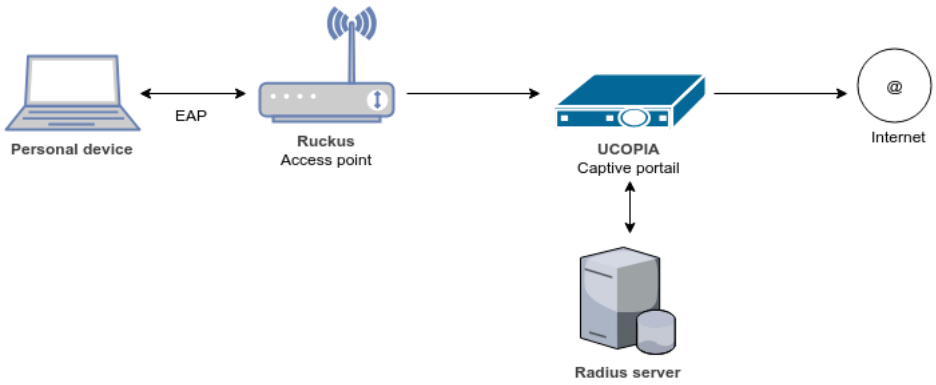

Figure 9: Diagram of an university Wi-Fi

2.5 Secure the network

The Ruckus radius server allows us to simplify the security clearances without even having to use LDAP.

We can use a Remote Authentication Dial In User Service (RADIUS) server to secure the following types of access to the Ruckus Layer 2 Switch or Layer 3 Switch:

- Telnet access
- SSH access
- Web management access
- TLS support
- Access to the Privileged EXEC level and CONFIG levels of the CLI

2.6 Control the access to the resources

When RADIUS authentication is implemented, the Ruckus device consults a RADIUS server to verify usernames and passwords. We can optionally configure RADIUS authorization, in which the Ruckus device consults a list of commands supplied by the RADIUS server to determine whether a user can issue the entered command.

RADIUS accounting causes the Ruckus device to log information on a RADIUS accounting server when specified events occur on the device.

Each authenticated user has:

- a privilege level
- A list of commands
- Whether the user is allowed or denied usage of the commands

The last two attributes are used with RADIUS authorization, if configured.
The user is authenticated, and the information supplied in the Access-Accept packet for the user is stored on the Ruckus device. The user is granted the specified privilege level. And with the RADIUS authorization, the user is allowed or denied usage of the commands in the list.

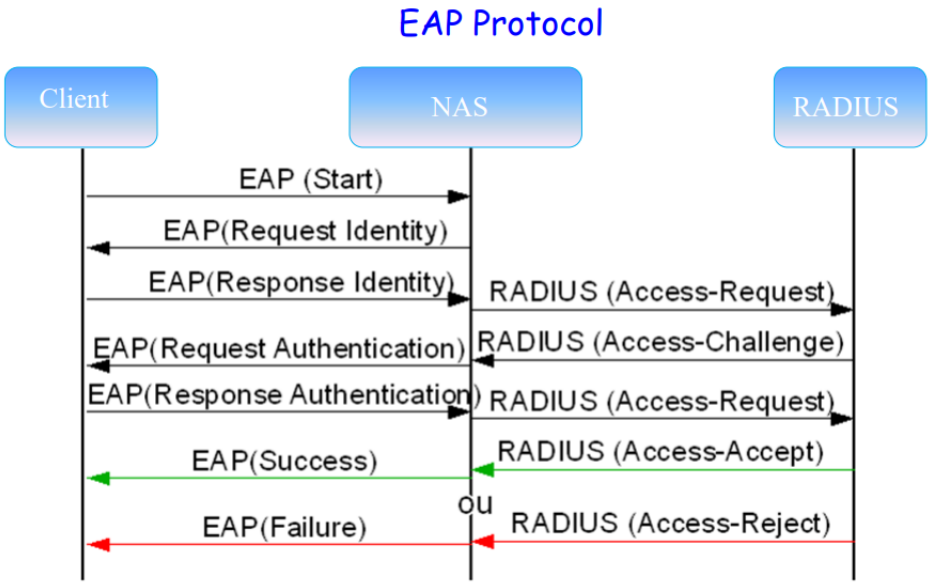

Figure 10: Sequence diagram of connection via Radius

802.1X and WPA2 enterprise use EAP to handle authentication request and Radius to handle secure communication between the access point (or Network Access Service as on the diagram) and the authenticator. EAP protocol follows several steps :

- EAP (start) : the user tries to connect to the access point : it sends a request to access to the NAS.
- The EAP asks hims to indentify himself : he has to give precise information, commonly a login and a password.
- The user provides the requested information.
- NAS sends the hashed information with a shared secret to the RADIUS server within the Access request.
- Radius server verifies that it received information from an authorized NAS, and also that the information that he received exists within its database. It is the access challenge.

- Radius servers sends a response. Access accept means that the user passed the challenge and can access to the other network resources. If it is any other response, the authentication failed.

2.7 Set-up

Our credentials for radius are:

- ece_1
- 1463

In order to connect to the internet we had to authenticate ourselves to the network we had to provide information to the WLAN. Unfortunately we couldn't access anything, we could not log in.
That is because nothing was set-up on the web interfaces for the authenticator and authentication server to accept us.
Since 802.1X is secured, it does not give any ip address until the supplicant is logged in. So we don't have any way to connect to the internet, we have to find a work-around.
To do so we connect to an open network like the following.

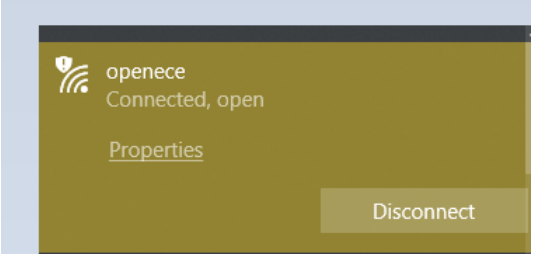

Figure 11: Connection to open network

We then log in with an account and are able to browse the internet. We then go to the set-up page of the access point and of the authenticator. We configure them to allow connections from supplicants by the access point and to transmit them to the authentication server. So we configure the NAS to accept connection from **192.138.100.5**.

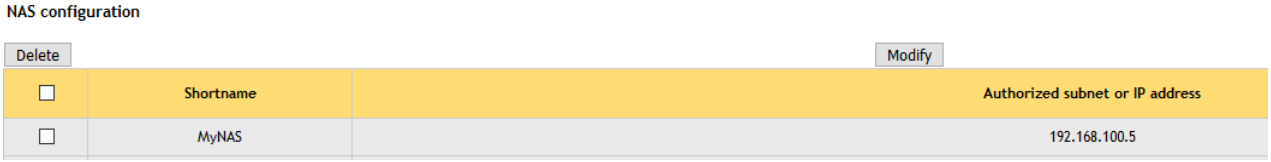

Figure 12: NAS configuration

We also configure the authentication server to accept traffic coming from our NAS. We have to set them up because by default they blacklist everything for improved security.
Once this is done everything should work fine. We click on our WLAN, we enter our credentials and try to connect. When we do so we to a RADIUS Access-Request and it responds by

RADIUS Access-Challenge. If we have invalid credentials then we cannot access the service (RADIUS Access-Reject), if we have valid credentials then we are logged in (RADIUS Access-Accept).

41	14.682453	91.199.6.240	172.32.0.11	RADIUS	384	Access-Request id=163
42	14.831723	172.32.0.11	91.199.6.240	RADIUS	321	Access-Accept id=163
43	15.584198	91.199.6.240	172.32.0.11	RADIUS	363	Access-Request id=128
44	15.658374	172.32.0.11	91.199.6.240	RADIUS	106	Access-Challenge id=128
45	15.674574	91.199.6.240	172.32.0.11	RADIUS	534	Access-Request id=129
46	15.803256	172.32.0.11	91.199.6.240	RADIUS	1132	Access-Challenge id=129
47	15.818307	91.199.6.240	172.32.0.11	RADIUS	379	Access-Request id=130
48	15.889106	172.32.0.11	91.199.6.240	RADIUS	1128	Access-Challenge id=130
49	15.904303	91.199.6.240	172.32.0.11	RADIUS	379	Access-Request id=131
50	15.977602	172.32.0.11	91.199.6.240	RADIUS	1128	Access-Challenge id=131
51	16.003968	91.199.6.240	172.32.0.11	RADIUS	379	Access-Request id=132
52	16.068996	172.32.0.11	91.199.6.240	RADIUS	1128	Access-Challenge id=132
53	16.085090	91.199.6.240	172.32.0.11	RADIUS	379	Access-Request id=133
54	16.159385	172.32.0.11	91.199.6.240	RADIUS	844	Access-Challenge id=133
55	17.852618	91.199.6.240	172.32.0.11	RADIUS	517	Access-Request id=134
56	17.928289	172.32.0.11	91.199.6.240	RADIUS	165	Access-Challenge id=134
57	17.942143	91.199.6.240	172.32.0.11	RADIUS	379	Access-Request id=135
58	18.020222	172.32.0.11	91.199.6.240	RADIUS	143	Access-Challenge id=135
59	18.041158	91.199.6.240	172.32.0.11	RADIUS	416	Access-Request id=136
60	18.168683	172.32.0.11	91.199.6.240	RADIUS	159	Access-Challenge id=136
61	18.183998	91.199.6.240	172.32.0.11	RADIUS	464	Access-Request id=137
62	18.319501	172.32.0.11	91.199.6.240	RADIUS	143	Access-Challenge id=137
63	18.334056	91.199.6.240	172.32.0.11	RADIUS	416	Access-Request id=138
64	19.334416	172.32.0.11	91.199.6.240	RADIUS	86	Access-Reject id=138

Figure 13: RADIUS

Since our credentials are correct we are connected to the secure University / Office network and now we can go on the internet (almost freely).

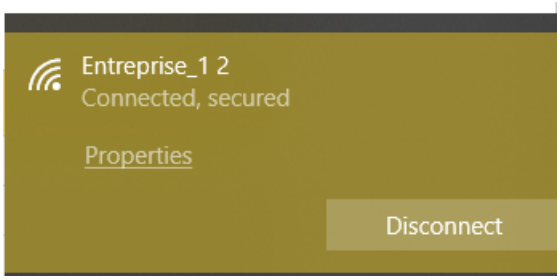

Figure 14: Proof ability to connect

3 Sources

- https://en.wikipedia.org/wiki/IEEE_802.1X
- https://en.wikipedia.org/wiki/RADIUS
- Wi-Fi Security course, 3rd Edition, Dr. Abbas Hatoum