LAFORGE Samuel

LEGER Lucas

**Case Study – IT Infrastructure**

**LaserLog© – Headquarter Renewal**

# Summary :

In this report we will study the case of a company called LaserLog©. LaserLog© is a global logistics company for companies in Europe and the Middle East. Today the company has decided to move its headquarters to the Paris region and has called on our company to manage the renewal of their network infrastructure as well as the management of their security and maintenance in operational conditions.

We will propose a network infrastructure from the plans to the realization and implementation. This infrastructure will be totally redundant from the arrival of the fiber to the user's station in order to have a highly available network. The equipment installed as well as their additional options will allow to have a fully secured network. One of the risks that could occur would be that an equipment fails like a switch for example and that we lose all the stations attached to it.

# Technical infrastructure solutions :

## Proposed architecture

To begin the presentation of the proposed architecture we will define the different arrivals of the optical fiber on the site. The fiber will be a multimode fiber and our solution will be a secured level 3 connection. The level 3 connection is the fact that the optical fiber leaves from two different operator connection nodes and arrives on the site by two different places. this system allows a maximum security of the internet arrival

Our proposal in terms of offer will be the following :

A need for two optical fibers (one main fiber + one backup fiber) :

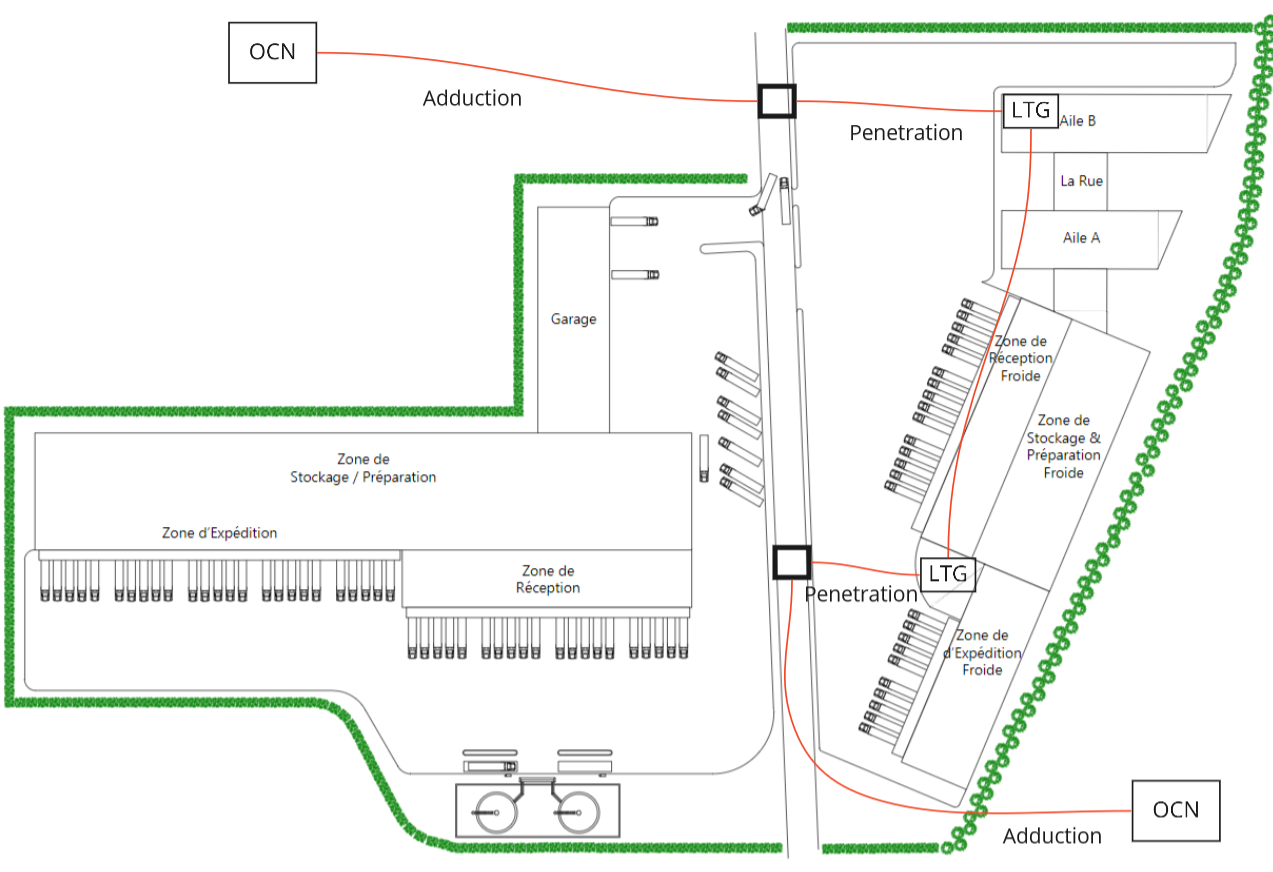
The first fiber will be a 5Gbps FTTO with additional options of a guaranteed and symmetrical throughput and a guaranteed recovery time of 8 hours

The second fiber will be a 5Gbps FTTO with an additional option of a guaranteed and symmetrical throughput and a best effort recovery time guarantee

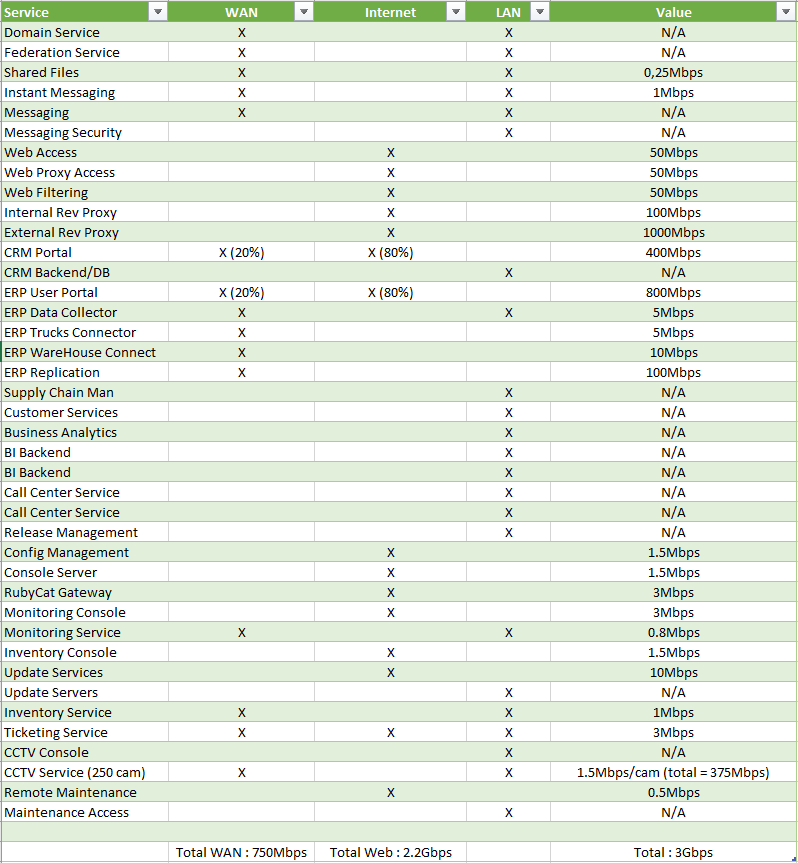
The requirements in terms of access are as follows :

* MPLS WAN access for logistics applications
* WEB access
* Access to Telephony via PABX

The arrival pattern is therefore as follows:

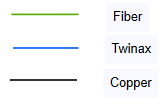


The necessary flow rates on each access have been calculated according to the services provided by the customer :



Now that the fiber optic part has been seen we will continue with the network architecture plans.

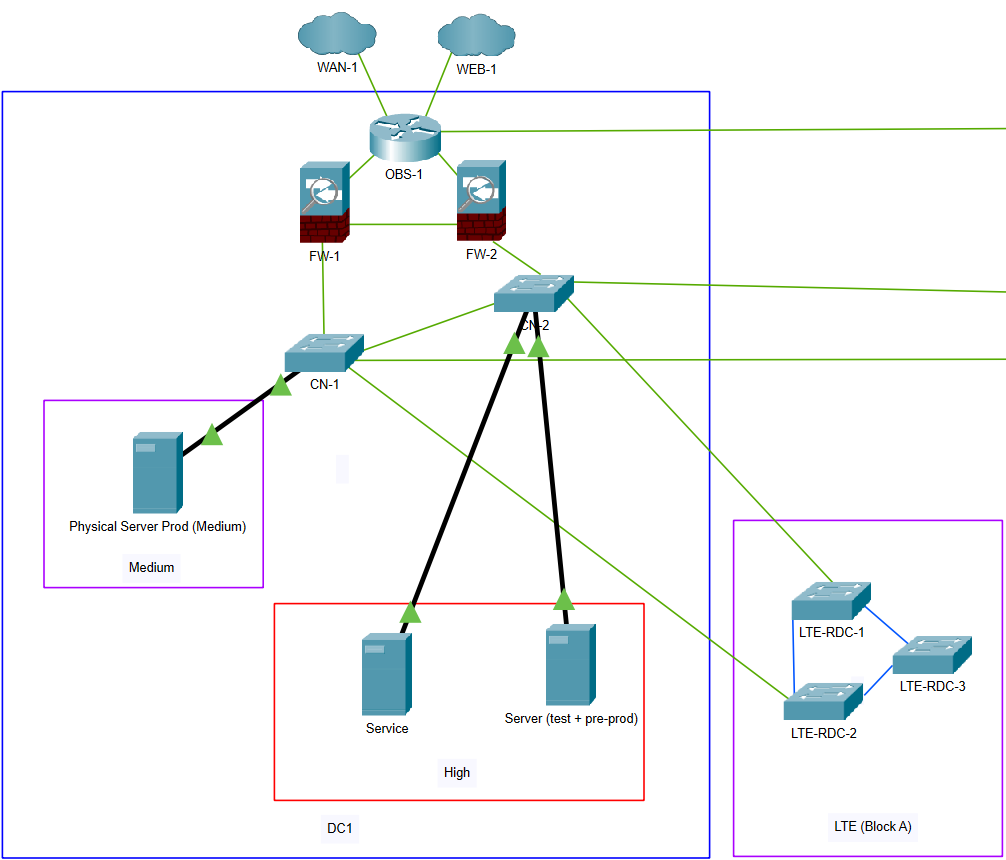
**Network topology legend :**



**First Datacenter :** The first datacenter will have an OBS router and will be composed of redundant firewalls and switches to ensure network continuity.

For the servers we will have in this data center a physical server which will contain in a virtual way all the services considered with a criticality known as "Medium" as well as a physical server which will also contain in a virtual way all the environments of "test" and "pre-production" for the services of "high" criticality and a physical server which will contain a service of "high" criticality

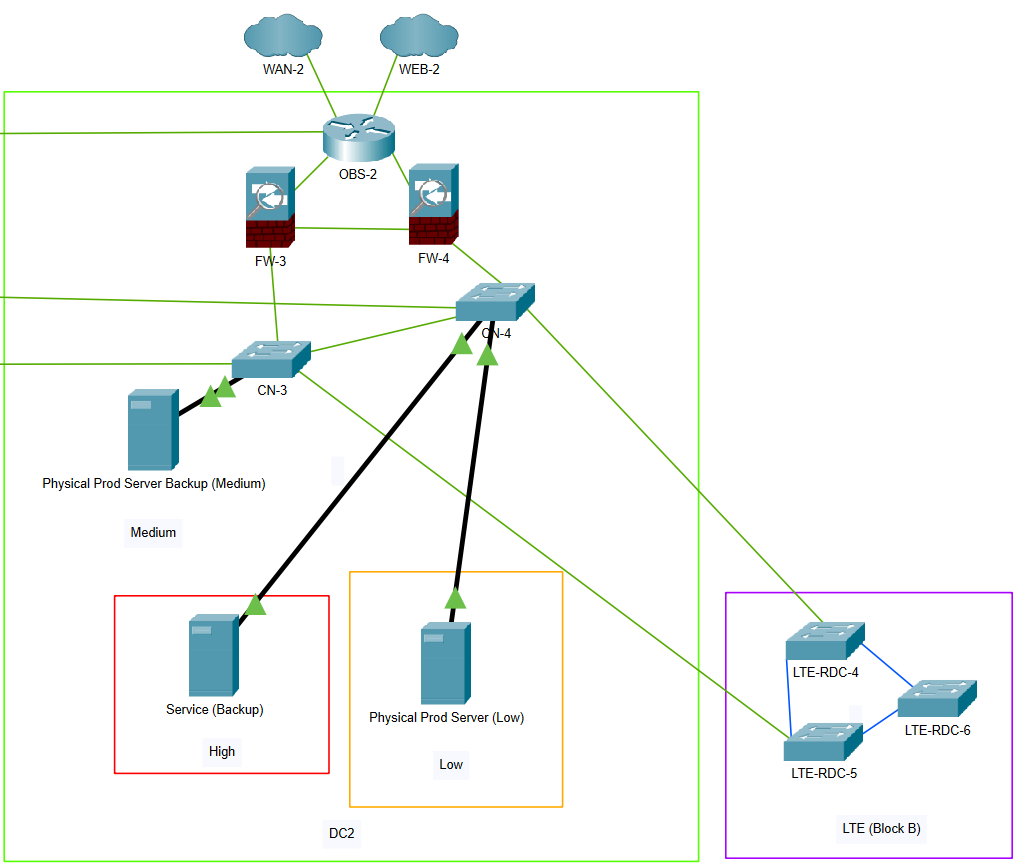
The core network switches of this data center will be connected and redundant on all the switches of each floor technical room which will manage the connections of the stations of the Block A



**Second Datacenter :** The second data center will have a backup OBS router and will be composed of firewalls and redundant switches to ensure network continuity.

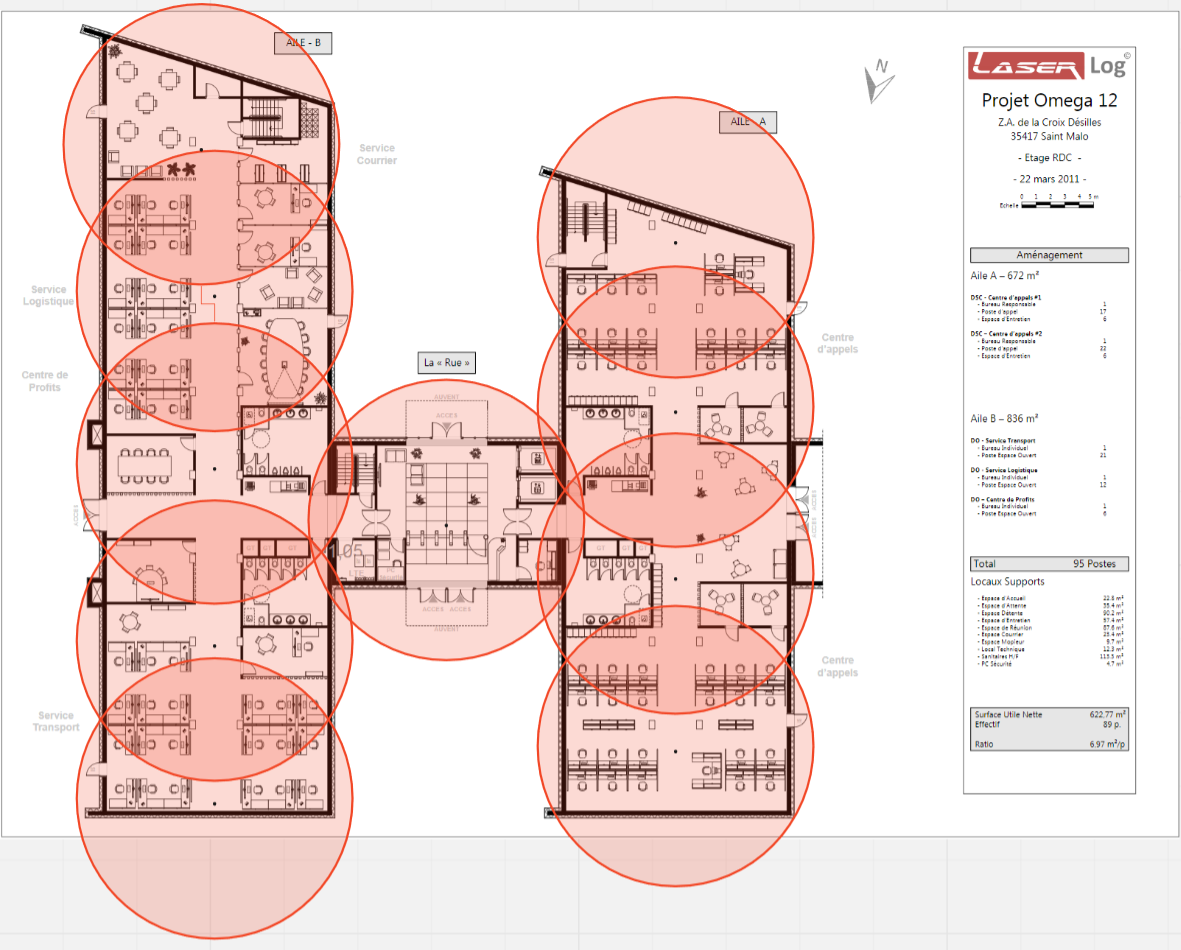
Concerning the servers, we will have in this data center a physical backup server that will contain virtually all the services considered with a criticality called "Medium" as well as a physical server that will also contain virtually all the services with a "low" criticality and a physical backup server that will contain a "high" criticality service.

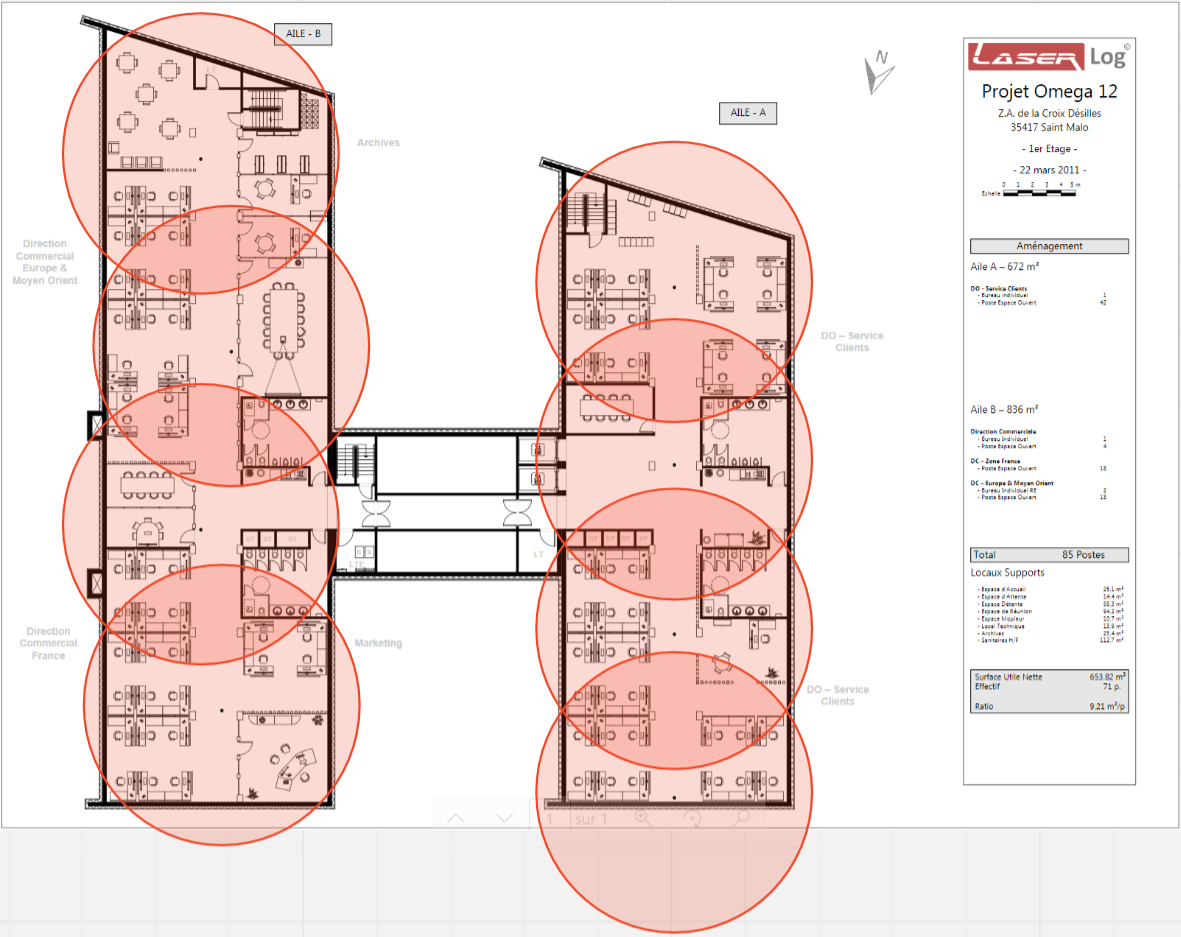
The core network switches of this data center will be connected and redundant on all the switches of each floor of the technical room which will manage the connections of the stations of Block B.

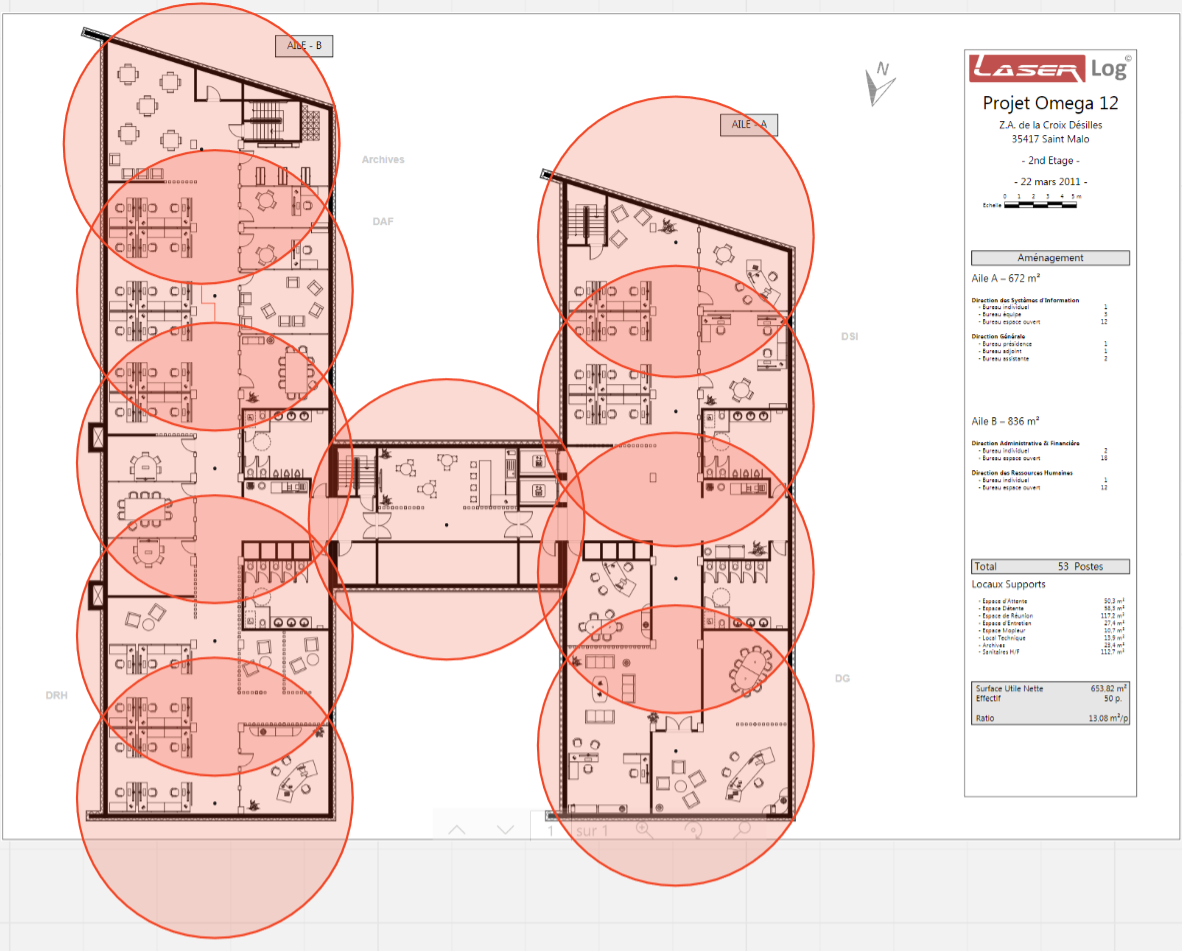


To complete this part of the client's network architecture, we will have to set up Wi-Fi terminals in all the offices and in the entire warehouse area. The architecture will be as follows :

First of all, the plans of the offices with the Wi-Fi terminals from the ground floor to the 2nd floor :







The Wi-Fi hotspots will have to respect some criteria :

* The Wi-Fi hotspots are not overlapped between each stage to avoid interference
* The Wi-Fi hotspots are not located above desks or tables in relaxation areas to avoid any problem with waves emitted on employees or visitors
* The range of the Wi-Fi hotspots overlaps to keep an optimal connection in any area of the building
* The range is also limited on the outside so as not to pick up from outside

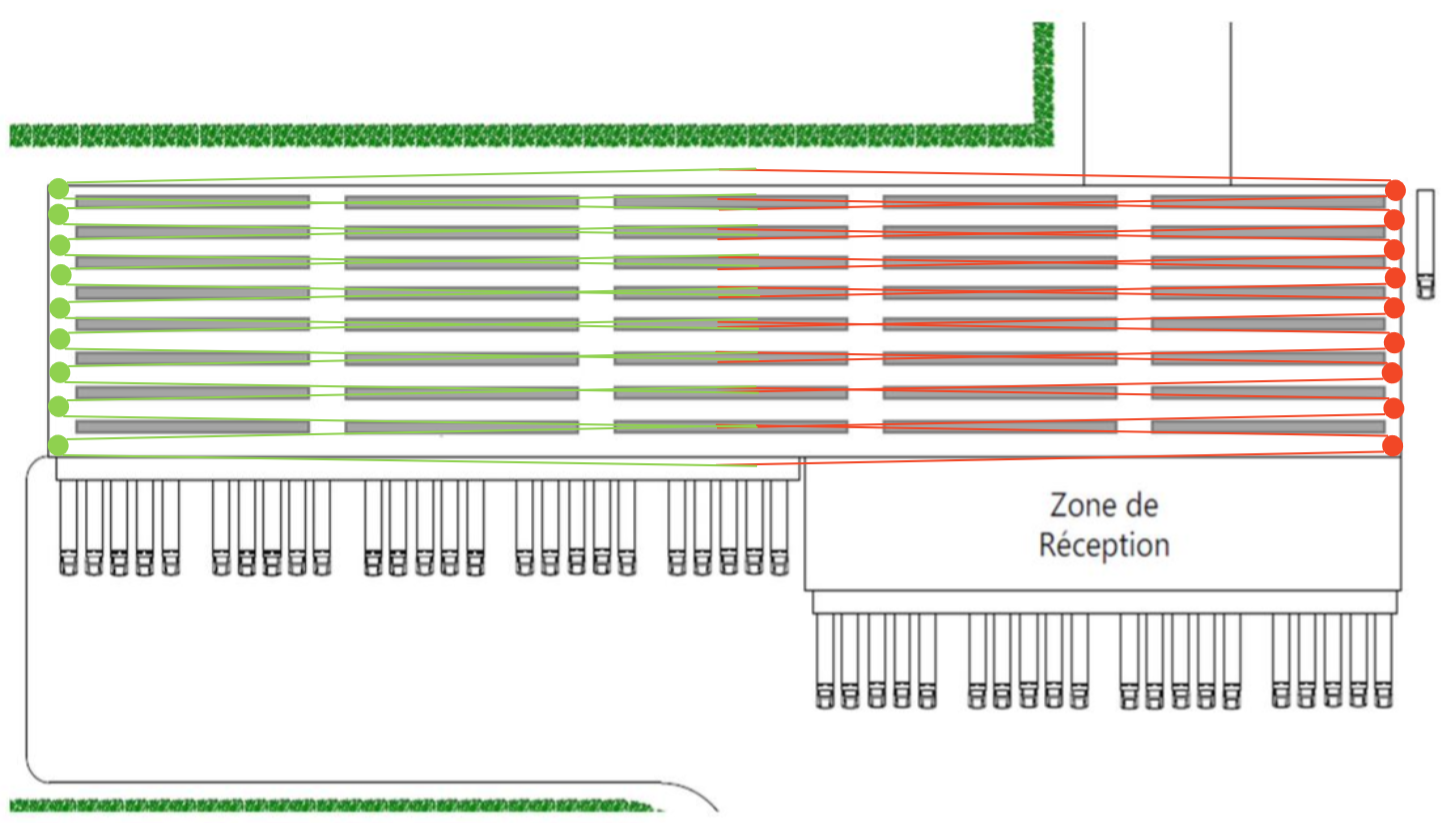
The hotspots will also broadcast two different wireless networks :

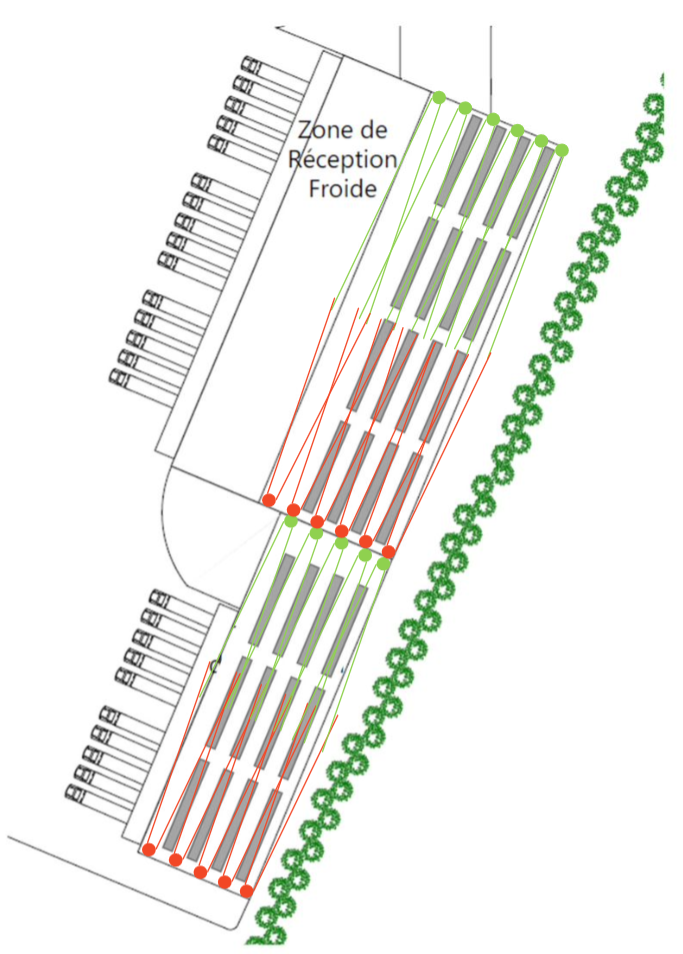
- The first one will be for the guests. It will be on an isolated subnet and cannot access to the data on the servers.

- The second one will be for employees only and are on the regular subnet as the wired network.

For the warehouse area we will install outdoor terminals with a unidirectional antenna to resist temperature and dust and to ensure internet access in all storage rows

So we thought of the following scheme :





Warehouse Wi-Fi hotspots will have to meet different criteria than those in the office :

* Inclination of the terminals downwards to be defined during the installation in order to have a slight wave crossing with the opposite terminal
* The Wi-Fi terminals will be placed at a height of about 4m to avoid damage to the user’s machines
* The terminals will be connected to two RJ45 sockets which will be connected to two different switches to ensure redundancy in the warehouse

## 2. Presentation of the equipment

Today our customer uses certain brands of equipment for his network infrastructure such as HP for his switches, which he is satisfied with. On the other hand, their Cisco firewall solution does not suit them, particularly because of the non-advanced filtering available in the application. They do not have a Wi-Fi solution and have an electrical backup system used by the refrigeration part of their information system.

Concerning the equipment that we will put in place we can find the following:

Our customer being satisfied with their switches we will keep the same brand. We will have HP FlexFabric 5950 48 port SFP+ Layer 4 core network switches in the general technical rooms and Aruba Instant On 1960 48 port PoE/PoE+ switches for the floor technical rooms.

HPE FlexFabric 5950 Aruba Instant On 1960

Regarding the firewall part, we will set up a new solution for the customer. We will propose him new generation firewalls Sophos XGS 3100 which allow an advanced management of filtering as for example the installation of personalized rules of WEB filtering.

Fw Sophos XGS 3100

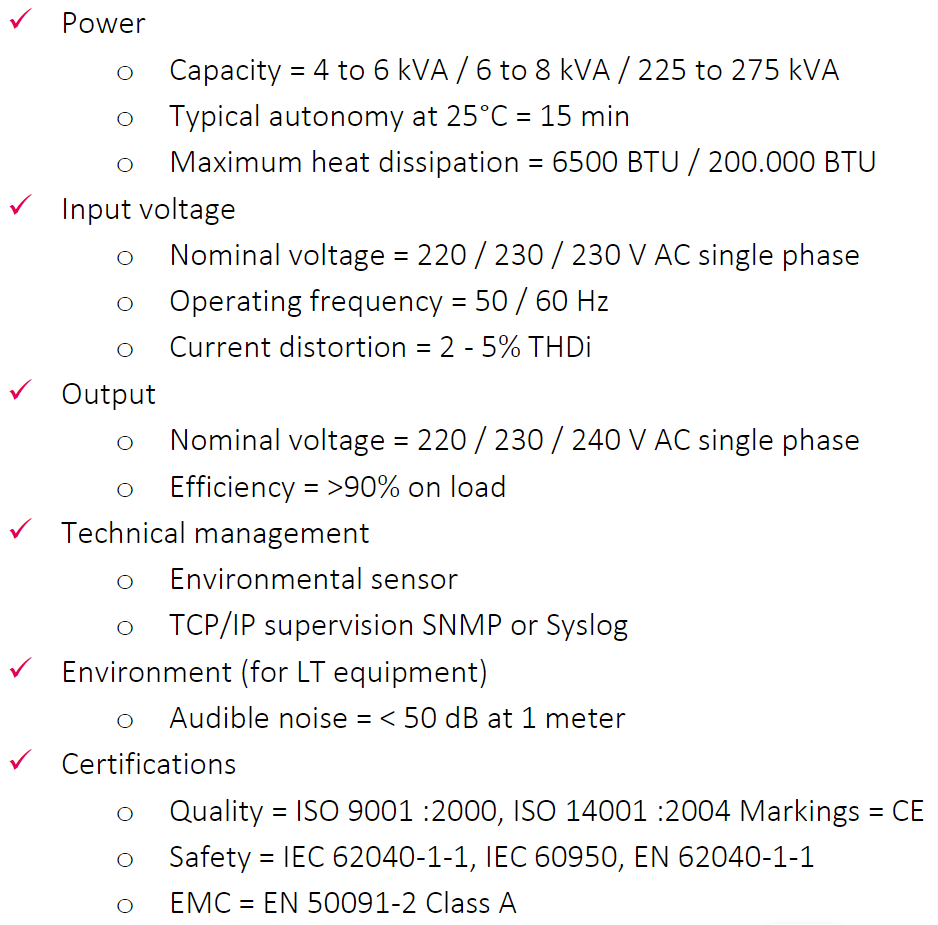
In terms of Wi-Fi terminals, we will use D-Link terminals model DAP-X2810 for the office. These terminals have two RJ45 ports accepting PoE. In addition, these terminals have a range of more than 10m which will cover all the offices without needing to place too many terminals.

D-Link DAP-X2810

The terminals that we will install will be StarTech Outdoor 1T1R accompagnied by Yagi unidirectionnel antennas with a 200m maximum range.

StarTech Outdoor 1T1R Antenna Yagi

For the security of the information system we will leave it linked to the current electrical backup system

The air conditioning units will be selected according to the following criteria:

Total BTU for the datacenters are about to 3719.54 BTU/hr.

Total BTU for the LTE are about to 4098BTU/hr.

Client’s servers will be an additionnal part of the BTU.

The CABLOFIL cable trays will pass through false ceilings as follows

- 1 path for the low voltage (distance of at least 30cm if there is a parallel path with strong currents)

- 1 path for high voltage (distance of at least 30cm if there is a parallel path with other high voltage)

- 1 path for air-conditioning (distance of at least 30cm if there is a parallel path with strong currents)

The IRO tubes or ICTA conduits of appropriate diameter will pass through the cable trays (cable fixing every 1m).

The computer cabinets will be 42U size and Access Multiple type from EFIRACK or TE 7000 type from RITTAL or equivalent.

The RJ45 cables for connecting the switches to the stations on each floor will be at least 6a cables.

## 3. Project governance

In the first step we will have to communicate with the Internet Access Supplier and the Electrical Engineer to have every informations that we need.

We’ll also have to get access to the configuration files of the existing network equipments in order to have a similar configuration for our new equipments.

After the reception of all these informations, we will start the deployment of all the equipments in our offices.

First, we will make the entire configuration manually for each model.

Then, all the equipments that we chose have a function to backup the configuration file.

We will be able to incorporate these configuration files to the others same models.

These operations (Firewall configuration, switches configuration, access points configuration in nuclias connect application, …) should take us two days of work.

For the on site deployments, there will be two technicians who will be on site. This will allow us to have the full infrastructure faster and we will be able to test longer before the arrival of all the employees of LaserLog.

First we will deploy all the datacenters equipments. The Internet Access Supplier will have to intervene before us. It will allow us to test the Internet access after the deployment of all the equipments. This operation should take a day of work to be done.

For the second step, we will deploy the equipments for the LTE. We will link every network plugs in the offices to the switches that will be linked to the switches that are in the datacenters. After this we will be able to test de Internet access from the offices. After that we will also be able to make some tests with the users that are on site with their working application. These operations are planned on one day of work.

The third step is the longer. We will deploy all the access points and antennas in the offices and in the warehouses.

We will plug every access point in the false ceiling for the office part. We will test the good configuration and test the Internet access on the wireless network.

For the warehouses, we are going to put the access point on the wall and plug the antennas directly on the AP. The antennas will be directed to the ground to not interfere with the other antenna that will be placed on the wall in front of this antenna.

This step is planned on four days of work.

After all of these operations, the network infrastructure will be complete.

However, we will be available on site for user’s test and potential changes in the configuration during one day.

## 4. Project plan

## 5. Project requirements and constraints

## 6. Service Level Agreements implementation for the project

For the client’s need about the support service that we must provide, we have an agreement on these terms:

The tier 1 service is not in the contract. In fact, it will be managed by the IT department of Laserlog.

The IT department can call us if they need on a specific action.

The tier 2 service is a technical support which needs deep knowledges and cannot be managed by the IT department of Laserlog.

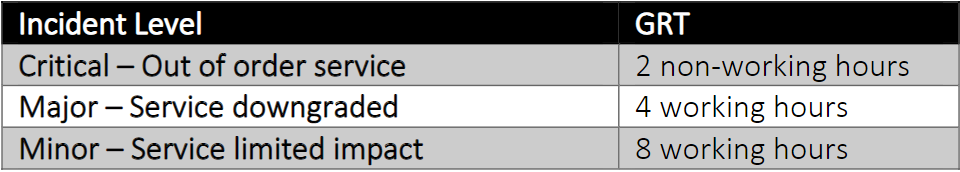
The tier 3 service is managed by expert in each product and service support.

The tier 4 service concern all the askings needing us to have a contact with manufacturers, application’s editors, etc.

Une image contenant table

Description générée automatiquement

The incidents treatment is submitted to the following SLA table:



The criticality of incidents needs to be discussed with the client.

In case of disrespect of the GTR, penalties will be applied.

These penalties percentage represent a reduction on the client’s monthly subscription.

Une image contenant texte

Description générée automatiquement

## 7. Transition and/or reversibility phase terms and conditions

In case of end or breach of contract we are committed to give all the informations that are needed for the proper functioning of the client’s services.

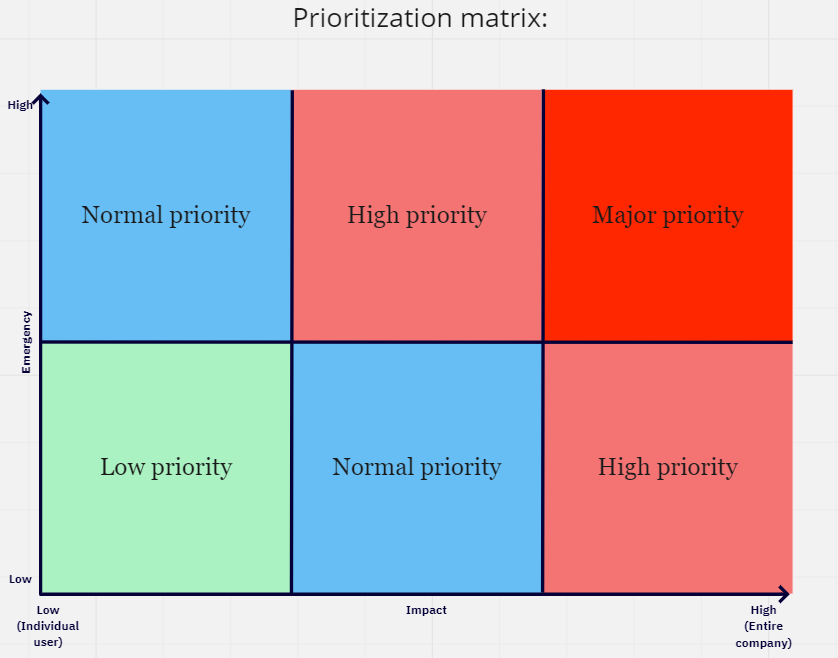
In these cases, we will give the passwords of the equipments, the procedures, the documentations, the configuration files, etc. to the client.

In case of disrespect of these terms we are committed to receive a penalty.

# Management process :

## 1. Incident management process

There is the the prioritization matrix. It allows us to know what kind of incident are critical and need a major priority and what kind needs to be treated as a low priority incident and the intervention has to be planned :



This is a proposal of SLA conditions to define the criticality of each incidents :

Une image contenant texte

Description générée automatiquement

## 2. Monitoring management infrastructure and process

The monitoring fucntionning is ensured by Centreon and Grafana.

Centreon is an open source software that can see with some commands how the system is going on different equipments.

Grafana will allow us to have a more readable interface than the native Centreon interface.

In Centreon, notifications by mail and text messages can be configured. In that case we can provide a 24h/24 monitoring and we are able to take action at every time.

## 3. Backup management infrastructure and process

Every equipment’s configuration files will be manually saved at every change.

To be able to find the logs, we can enable daily backup sent with email on Sophos appliances.

Our retention policy is that we save logs during 3 months. After that time, every logs are deleted.

Switches have less usefull logs. We can output the logs and export it but we cannot back it up every day automatically. We will stay at disposition for the client to give the logs needed in as soon as possible.

## 4. Release and change request management infrastructure and process

Change request are every ticket where user is asking for change, add or deletion on any equipment that will have consequences on the IT services or on the global infrastructure.

It will be treated as a standard ticket.

For the change requests which need us to go on site, an action plan will be made with the client to intervene at the good moment for the users, specifically if it needs an Internet shutdown.

## 5. Problem management infrastructure and process

A problem is declared when an incident is recurring.

It can also be declared when the support service center know that the incident will take place on several sites.

A problem needs to have a definitive solution in order to avoid other incident ticket opening.

Problems are treated as normal ticket with same prioritization as incidents. Problems are directly attributed to Level 2 support.

## 6. Escalation management process

The functional escalation is the transition from a technician to another in the same level.

For example, if a incident is declared with a normal priority on level 1 support but the technician in charge of this incident cannot resolve it, he can transfer the ticket to another technician who is more competent. The incident stay at the same priority level and at the same support level.

The hierarchical escalation is the transition from a support level to another.

For example, if an incident is declared with a normal priority on level 1 support but the technicien in charge of the incident discover that the cause of the problem needs deeper knowledges to be resolve he will transfer the ticket to the level 2 support that has the knowledges and the skills to resolve it.

The support service center is divided in three levels of support :

- The level 1 is mostly for user incident.

- The level 2 is mostly for technical incident and problems.

- The level 3 is here to help the other technicians or to resolve tickets that had been escalated from the other levels.

## 7. Security management infrastructure and process

## 8. Hardware and software maintenance management

To be able to replace the hardware in the faster time after the shutdown, spare equipments will be stored in our offices and in the clients office according to the type of equipment.

## 9. Operation Maintenance Services

# Presentation of the project during the Build and Run phases :

# Organization of the project :

# Detailed planning and approach :

# Roles and responsibilities between the Client and the applicant :

# Detailed Financial Statement :