# Déploiement du réseau du Château de Justiniac

*à l'occasion de l'Assemblée Générale de la Fédération French Data Network (FFDN) 2018*

**Par Julien Vaubourg**
*julien[at]vaubourg[dot]com*

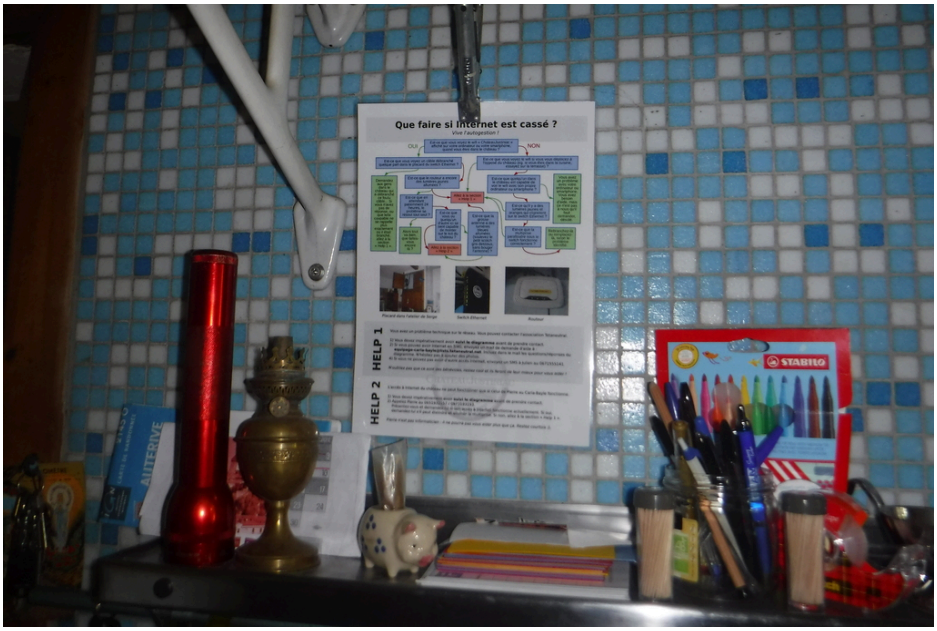
Le 10/03/2019


*Avec la participation de :*

Tetaneutral.net

*Merci en particulier à :*

Fanny, Lou, Sylvain, Bikepunk, Serge et Pierre


Que faire si internet est cassé ?
HELP 1
HELP 2
STABILO

# Table des matières

# 1 Contexte

Ce rapport détaille la mise en œuvre du réseau informatique du Château de Justiniac (Ariège). Ce travail a été réalisé bénévolement, en échange de la mise à disposition du lieu à titre gratuit, pour la tenue de l'assemblée générale (AG) de la Fédération des fournisseurs d'accès à Internet associatifs (aka. Fédération FFDN). Environ 70 personnes ont participé à l'AG 2018 de la Fédération FFDN, qui s'y est déroulée du 5 au 8 mai 2018.

L'objectif de ce rapport est de raconter le plus précisément possible, de la théorie à la pratique, comment :

1. il est possible d'apporter une connexion à Internet à très haut débit [1] dans un lieu qui n'est pas supposé pouvoir en bénéficier ;
2. diffuser un réseau wifi performant dans un grand lieu avec des murs épais comme c'est le cas pour un château, en limitant les moyens financiers sans renier la qualité ;
3. réaliser le tout en utilisant autant que possible des logiciels libres et en collaborant avec une association membre de la Fédération FFDN.

Ce rapport est similaire, tant dans la structure que les objectifs, à celui produit suite à la mise en place du réseau informatique du Château de Millemont [2] (Yvelines), avec les principales différences suivantes :

1. Le Château de Justiniac a été relié à Internet via un pont wifi de 10 km et une connexion VDSL2 distante (contre un double lien 4G à Millemont).
2. Les logiciels libres ont été privilégiés (contre l'utilisation d'un contrôleur propriétaire Ubiquiti Unifi).
3. Le support du réseau est pris en charge par une association de la Fédération FFDN (contre un support privé).

Des vues générales du château sont disponibles dans l'Annexe A.

# 2 Conception du réseau

Le réseau peut être découpé en deux parties principales : le LAN (réseau local équipé de bornes wifi) et le WAN (connexion à Internet).

**Relation entre le LAN et le WAN** Le WAN représente le raccordement à une *source Internet* (eg. ADSL par la ligne téléphonique) tandis que le LAN du château représente la *plomberie intérieure* (eg. câblage et antennes wifi dans le bâtiment), qui permet de rendre l'accès Internet disponible partout dans la maison. La source d'approvisionnement est donc connectée au tuyau principal de la maison, mais elle peut être remplacée par une autre source, sans avoir à modifier le réseau d'alimentation de la maison. Ainsi, tout comme il est possible de passer de l'eau d'un puit à l'eau du service public en déviant simplement un seul tuyau et sans toucher aux robinets de la maison, il est possible de passer d'un Internet par ADSL à un Internet par fibre optique (ou autre technologie) en modifiant seulement un branchement et sans toucher aux bornes wifi de la maison. Les parties WAN et LAN du réseau du château sont donc interconnectées mais indépendantes.

## 2.1 Partie WAN

### 2.1.1 Méthode de raccordement à Internet

La connexion ADSL déjà en activité du château permettait d'obtenir un débit descendant de quelques Mbps, supposé être insuffisant pour réunir 70 informaticien·nes dans un même lieu [3].

1. À partir de 30 Mbps d'après l'ARCEP.
2. https://julien.vaubourg.com/files/cr_millemont.pdf
3. https://ma.juii.net/blog/wifi-for-a-conference

Aucun opérateur ne semble pouvoir proposer un meilleur débit ADSL, et le lieu ne peut bénéficier ni de VDSL ni de fibre optique [4]. Avant d'envisager une solution contraignante comme la 4G (qui semble compromise par avance [5]), il peut être intéressant de chercher un lieu environnant qui est éligible à une meilleure connexion à Internet, puis d'étudier si ce lieu pourrait être raccordé au château.

Le principe général de la méthode de raccordement est illustré par la Fig 1.

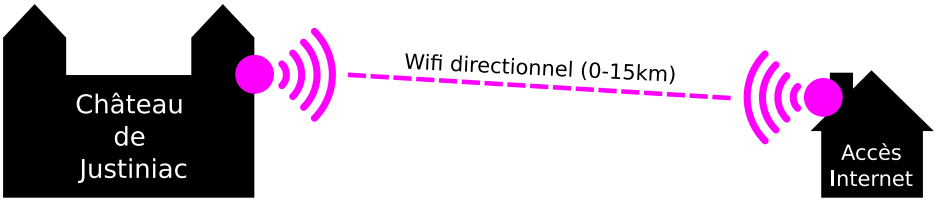



FIGURE 1 – Principe général d'un pont wifi, pour connecter un lieu équipé d'une connexion à Internet à un lieu qui n'en dispose pas (ie. le Château de Justiniac sur le schéma).

Cette méthode implique la mise en place d'un pont sans-fil entre le château et le lieu qui dispose du bon accès à Internet, qui a les caractéristiques suivantes :

**Une paire d'antennes** Créer le pont wifi consiste simplement à accrocher une antenne à l'extérieur (ou derrière une vitre) de chaque lieu, et de les faire se regarder.

**Simplement du wifi** La technologie sans-fil utilisée est le wifi : le même que celui utilisé dans les maisons. Il n'y a pas d'autorisation à demander et n'importe qui peut librement mettre en place ce type de pont wifi, tant que la puissance d'émission des antennes n'est pas trop forte. Une fois la puissance maximale dépassée, il faut être en possession d'un certificat de radioamateur pour être dans la légalité. Cette puissance limite est difficile à calculer : le plus simple est de retenir que pour un pont d'environ 10 km de distance, la puissance nécessaire reste sous le seuil légal, et que cette distance couvre la plupart des besoins.

**Wifi directionnel** À l'inverse du wifi dans les maisons, celui émis par les antennes du pont n'est pas envoyé dans toutes les directions (il n'est donc pas omnidirectionnel) : il est envoyé dans une seule direction (il est donc directionnel, avec un angle qui ne dépasse pas les 120°, pour les antennes les plus larges) pour concentrer toute la puissance du signal et lui faire parcourir jusqu'à plusieurs dizaines de kilomètres.

**Bande 5 Ghz** Deux bandes de fréquences sont légalement disponibles lorsqu'on veut émettre en wifi, quel que soit l'usage : la bande 2.4 Ghz et la bande 5 Ghz. Bien que les fréquences plus basses de la bande 2.4 Ghz soient plus à même de traverser la matière (murs, arbres, etc) que celles plus hautes de la bande 5 Ghz, cette dernière est généralement utilisée pour les ponts wifi. En effet, les appareils communiquant sur le 2.4 Ghz sont actuellement bien plus répandus (ordinateurs, smartphones, mais aussi portes de garage, babyphones et autres objets connectés) et rayonnent largement en-dehors des maisons. Cette surutilisation des fréquences implique des parasitages fréquents dans les communications, et donc des réémissions de paquets TCP/IP et donc finalement une réduction du débit effectif. Pour cette raison, et parce que la bande 5 Ghz permet également de répartir les appareils sur un plus grand nombre de canaux, il est actuellement mieux avisé de survoler les habitations avec des signaux longue distance en 5 Ghz plutôt qu'en 2.4 Ghz.

**Vue dégagée** Puisque les fréquences hautes du wifi 5 Ghz ne traversent pas bien la matière, les deux antennes doivent pouvoir se voir en vision directe, sans obstacle (autres bâtiments, collines ou forêts) entre les deux. Plus la distance entre les deux antennes est grande, moins les ondes n'ont de puissance en bout de course, moins elles traversent la matière, plus cette contrainte s'applique. Ainsi, un pont wifi 5 Ghz de quelques centaines de mètres pourra supporter de traverser un bosquet, mais ne permettra pas de connecter les deux antennes dans ces conditions sur plusieurs kilomètres.

**Commutation de paquets** D'un point de vue topologie réseau, les antennes wifi sont équivalentes à des switchs (commutation de paquets entre l'interface filaire et l'interface wifi). Le lien wifi est donc un lien de couche 2, équivalent à un câble Ethernet cuivré ou un segment de fibre optique, qui permet d'agrandir un réseau IP existant [6]. On s'interdit évidemment de faire du NAT sur les antennes, dont la lourdeur et les

4. Un site parmi d'autres pour tester : `https://www.eligibilite-adsl.com`
5. Aucune antenne 4G à proximité n'est référencée : `https://www.couverture-mobile.fr/#lat=4320758&lng=149309&z=16`
6. À noter que pour que l'analogie du câble soit parfaitement vraie, il faudrait également que les deux antennes supportent la

inconvénients ne sont pas justifiés dans notre cas.

Les études préliminaires pour la mise en place de cette solution de raccordement à Internet sont généralement, par ordre chronologique :

1. Référencer les zones géographiques éligibles au très haut débit (aka. THD, ie. VDSL ou fibre optique), à proximité du château.
2. Sélectionner les villes cette liste qui sont à vue directe du château, en y repérant les bâtiments particulièrement bien exposés (d'abord de façon théorique, puis en allant sur le terrain).
3. Nouer du lien social avec les locataires ou propriétaires de ces bâtiments, de façon à pouvoir dénicher la bonne personne ou le bon organisme avec lequel on pourra « contractualiser » l'installation de l'antenne sur le bâtiment. Il faut également confirmer la possibilité d'avoir du THD performant, à l'usage.

Les sections suivantes détaillent ces étapes, dans le cadre du raccordement du Château de Justiniac.

### 2.1.2 Référencer les lieux éligibles au THD

Le Plan France Très Haut Débit de l'Agence Numérique a permis la mise à disposition d'un observatoire en ligne [7] de la couverture française du THD. Il s'agit d'une application web de cartographie, qui délimite les zones géographiques en fonction des débits maximums auxquels les habitations sont supposées pouvoir souscrire. La Figure 2 permet de déterminer où sont situées les zones éligibles au THD, à proximité de Justiniac.

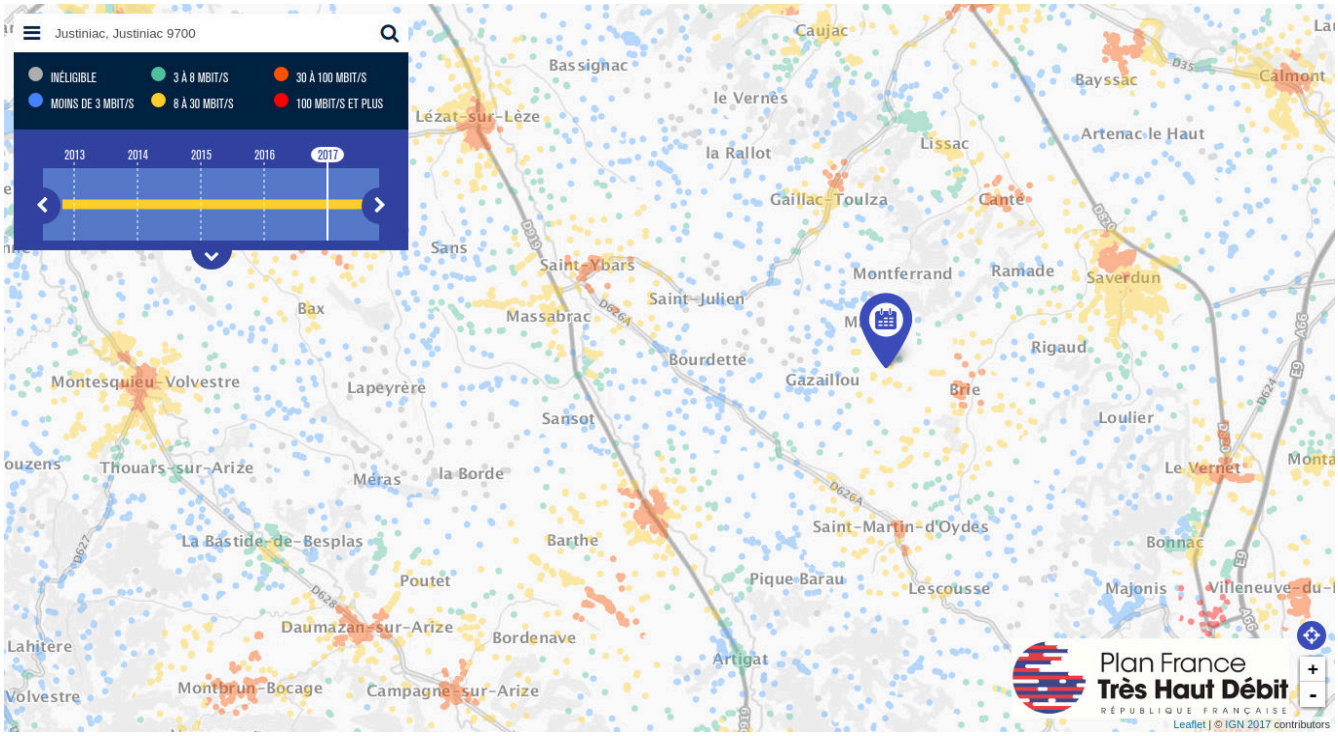



FIGURE 2 – Capture d'écran du site de l'Observatoire de France THD, pour la région de Justiniac (2018).

On constate dans un premier temps qu'il n'y a pas de THD qui dépasse les 100 Mbps (en rouge) dans la région. Les zones les plus avantagées sont en orange, et proposent donc un débit estimé entre 30 et 100 Mbps. En général, ce type de zone correspond surtout aux habitations éligibles au VDSL2.

technologie WDS (cf. https://en.wikipedia.org/wiki/Wireless_distribution_system), pour leur éviter de devoir réécrire les adresses MAC des trames qui doivent passer dans le lien wifi (cf. https://www.excentis.com/blog/operation-wi-fi-bridges et https://oldwiki.archive.openwrt.org/doc/howto/clientmode).

7. https://observatoire.francethd.fr

Comme l'ADSL2+, le VDSL2 permet de déployer des accès à Internet sans déployer de câble dédié, en réutilisant les installations téléphoniques existantes (aka. paires cuivre). Mais contrairement à l'ADSL2+ qui culmine théoriquement autour des 20 Mbps, le VDSL2 peut théoriquement proposer des débits jusqu'à 100 ou 200 Mbps. En pratique, en France, on constate surtout des débits réels qui stagnent plutôt autour des 30 Mbps réels. Ce type de débit entre tout de même dans la catégorie THD d'après l'ARCEP, et sont déjà largement confortables, pour la plupart des usages. Pour qu'une habitation soit éligible au VDSL2, il faut que le NRA (Nœud de Raccordement d'Abonnés – un bâtiment qui peut aller de la cabane de rue en béton à l'immeuble complet selon les villes) auquel sa ligne téléphonique est relié, soit équipé d'un DSLAM (un équipement informatique spécialisé) compatible VDSL2 avec un opérateur grand public qui propose des offres dessus. Pour que l'habitation bénéficie ensuite d'un débit réellement supérieur aux offres ADSL2+, il faut qu'elle se situe à moins d'un kilomètre de son NRA.

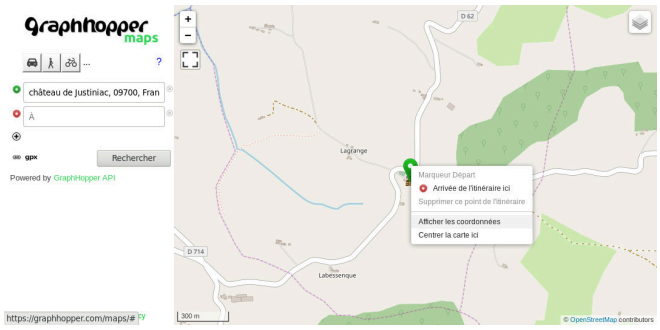
En visionnant la Figure 2, on se demande bien comment l'Agence Numérique pourra respecter son engagement d'une couverture à 100% du territoire français avec du THD d'ici à 2020. Néanmoins, il existe bien des zones éligibles au THD à proximité du château : Brie, Saint-Ybars, Saint-Martin-d'Oydes, Saverdun, etc. Nous pouvons donc passer à l'étape suivante.

### 2.1.3 Sélectionner les lieux qui sont à vue directe avec le château

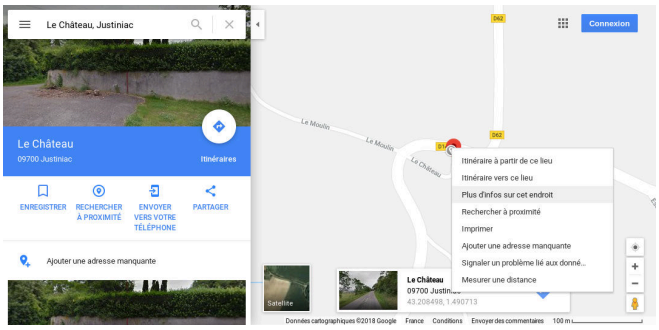
Pour pouvoir déployer le lien wifi entre les château et l'un des lieux éligibles au THD, il faut que l'un et l'autre puissent se voir à vue directe. Concrètement, il faudrait que depuis l'un des deux lieux, il soit possible de voir l'autre lieu, en utilisant une paire de jumelles ou un téléobjectif.

**Topologie du terrain** Il est inutile de faire le test des jumelles si la topologie du terrain permet de déterminer qu'il est impossible que les deux lieux se voient. Par exemple, parce qu'il y a des collines entre les deux lieux, que même des mâts de 10 mètres sur les toits ne permettraient pas de surplomber. Pour ça, il existe l'outil de cartographie web HeyWhatsThat [8]. Le site n'est absolument pas ergonomique, en plus d'être légèrement austère, mais il reste un allié indispensable des *wifiistes*. Le principe est simple : toutes les zones géographiques qui sont théoriquement visibles depuis un lieu donné, sont colorées en rouge sur une carte Google Maps.

**Utiliser HeyWhatsThat** Avant de créer un nouveau panorama HeyWhatsThat, il est nécessaire de connaître les coordonnées GPS du château. Une telle information peut simplement être trouvée avec un service en ligne comme GraphHopper [9], comme illustré sur la Figure 3.




(a) En utilisant le service libre GraphHopper.




(b) Ou en utilisant Google Maps (utiliser Chromium pour pouvoir copier-coller le texte des coordonnées).

FIGURE 3 – Déterminer les coordonnées GPS d'un lieu, à partir de son adresse.

8. https://heywhatsthat.com
9. https://graphhopper.com/maps/

Cliquer ensuite sur l'onglet *New panorama* de HeyWhatsThat, et reporter les deux coordonnées dans les champs *Latitude* et *Longitude* (il serait aussi possible d'utiliser directement le champ *Address* sans saisir les coordonnées, mais le résultat est souvent plus aléatoire). Ignorer la partie concernant le *highest nearby spot* et saisir la hauteur maximum approximative du bâtiment, en considérant en plus l'installation d'un mât sur le toit, dans le champ *Elevation* (vérifier que le site est bien en système métrique, en cochant la bonne case, en bas à gauche de la carte). Enfin, entrer un titre pour le panorama, correspondant par exemple au nom du lieu des coordonnées. Un exemple pour le château de Justiniac est proposé dans la Figure 4.

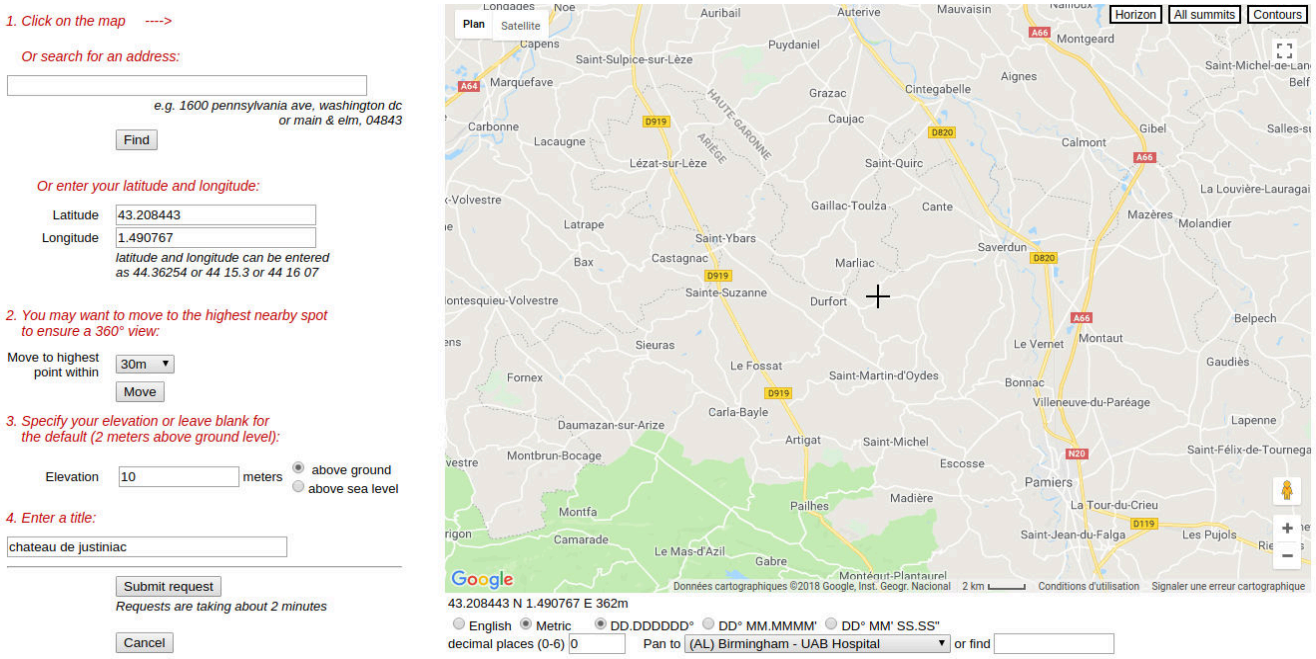



FIGURE 4 – Création d'un nouveau panorama HeyWhatsThat pour le Château de Justiniac.

Une fois le panorama créé, HeyWhatsThat donne accès à deux types d'analyse du terrain : la vue et le profil. Sur la vue, les zones rouges correspondent aux zones géographiques qui sont théoriquement visibles depuis le château, en se positionnant à la hauteur correspondant à l'élévation indiquée. Un exemple de vue est présenté dans la Figure 5. On constate qu'à 10 mètres de haut, les zones que peut voir le château sont en réalité très morcelées, ce qui est logique étant donnée la vue très vallonnée qu'on peut constater depuis la terrasse ou le toit. On constate également que la plupart des zones THD fournies par l'Observatoire, ne sont pas à vue du château... ni Brie, ni Saint-Ybars, ni Saint-Martin-d'Oydes et à peine un morceau de Saverdun. Par contre, un village qui est beaucoup plus éloigné des autres est présent à la fois sur la carte de l'Observatoire et la vue HeyWhatsThat : il s'agit du Carla-Bayle (en bas à gauche de la vue).

À l'aide d'un simple clic gauche quelque part sur la carte, HeyWhatsThat calcule le profil de terrain (sur la partie supérieure de la page) entre le château et l'endroit choisi. La ligne du dessus correspond à la ligne de vue qu'on devrait avoir depuis le château, en regardant dans cette direction, à 10 mètres de haut depuis le sol du château. Un exemple est donné en Figure 6, en choisissant le Carla-Bayle comme point distant. On constate que la vue surplombe effectivement toutes les collines, et que le château et le Carla-Bayle devraient pouvoir se voir. Dans les paramètres du profil, le *far end elevation* a été positionné sur *+4*, pour demander à HeyWhatsThat de considérer que ce qu'on souhaite voir au Carla-Bayle se situe à quatre mètres au-dessus du sol (ie. une antenne sur un balcon).

Le profil permet également de constater que le Carla-Bayle est à environ 10 km du château. C'est une bonne distance pour un pont wifi, qui permet de garder de bonnes performance en utilisant du matériel abordable (15 km maximum). La Figure 7 permet de confirmer la distance à vol d'oiseau entre le château et le rempart Nord du Carla-Bayle.

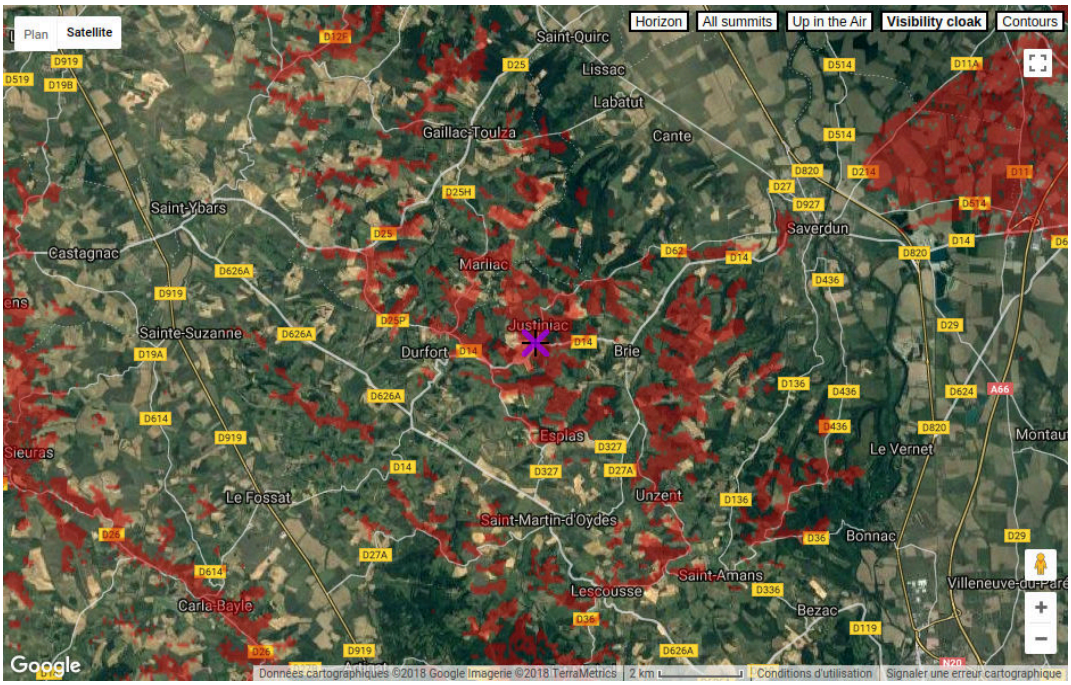



FIGURE 5 – Vue HeyWhatsThat : les zones rouges correspondent aux zones géographiques théoriquement visibles depuis le château.

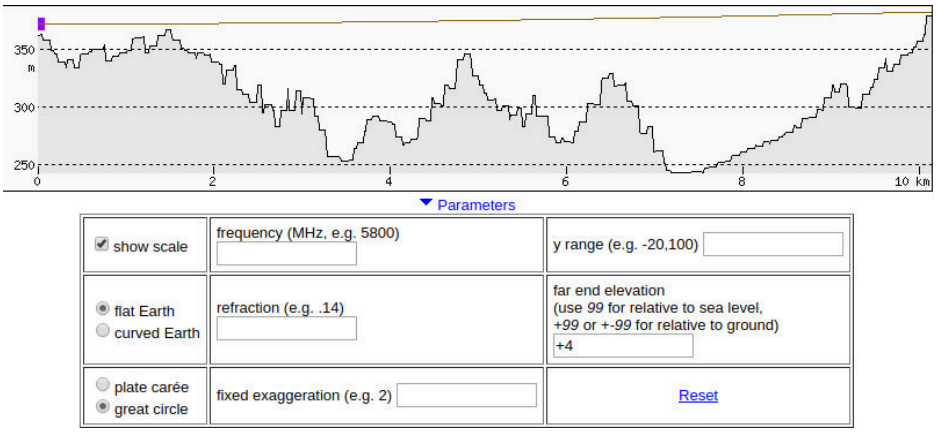



FIGURE 6 – Profil HeyWhatsThat, entre le château et le Carla-Bayle : la ligne du dessus correspond théoriquement à la ligne de vue depuis le château.

**Limites de l'étude cartographique** Toutes les informations données par HeyWhatsThat concernent la topologie des terrains, en considérant qu'ils sont nus, et qu'il n'y a donc ni arbres ni bâtiments. Il est peu probable qu'on puisse voir un lieu que HeyWhatsThat considère comme non-visible, par contre il y a un gros risque de ne pas pouvoir voir un lieu que HeyWhatsThat considère comme visible, notamment – dans notre cas – à cause des bois et forêts. Une fois le repérage cartographique terminé, il faut donc prendre une voiture et une paire de jumelles, et visiter tous les endroits qui sont censés être visibles et qui pourraient aider à créer le pont wifi.

**Ne pas oublier les ami·es du château** Dans l'étude réalisée pour le Château de Justiniac, le Carla-Bayle n'a pas été le choix le plus évident, étant donnée la distance à laquelle il se trouve comparé aux autres lieux potentiellement


FIGURE 7 – Distance à vol d'oiseau entre deux points géographiques, avec Google Maps. Le calcul est également faisable avec FranceTopo.fr, mais d'une façon étonnamment plus compliquée.

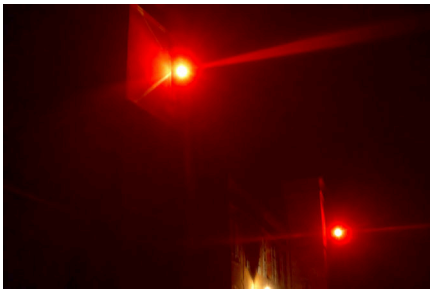
intéressants. Un troisième paramètre était initialement également entré en ligne de compte : il est possible de faire l'économie de l'étape suivante (nouer du lien social), si le point distant choisi correspond à un village dans lequel des gens déjà connus résident. Le propriétaire du Château de Justiniac possède le lieu depuis 30 ans et connaît beaucoup de gens aux alentours, qui seraient potentiellement ravis de participer à l'amélioration de la connectivité du château. Dès lors, il est intéressant de référencer l'ensemble des sympathisant·es du lieu, en les plaçant sur une carte. Cette nouvelle carte est ensuite à recouper avec celle de l'Observatoire et celle de HeyWhatsThat, pour déterminer si le lieu parfait existe.

**Pourquoi pas un saut supplémentaire** Plusieurs études sur le terrain ont également été réalisées, pour essayer de relier le château à des villages plus proches que le Carla-Bayle, dans lesquels des gens déjà identifiés habitent. Par exemple, un ami de longue date du château habite à Esplas, qui se situe entre Justiniac et Saint-Martin-d'Oydes, et sa maison est visible à l'œil nu depuis la terrasse du château. Un autre profil HeyWhatsThat permet de constater que Saint-Martin-d'Oydes (qui bénéficie de THD d'après l'Observatoire) devrait être visible depuis Esplas. Ainsi, il aurait été possible de créer un premier pont wifi entre le château et l'ami d'Esplas, puis un second entre cet ami et une habitation de Saint-Martin-d'Oydes. L'utilisation d'un tel relais (ou rebond) peut permettre de sauver la situation, en offrant potentiellement énormément de nouvelles possibilités d'interconnexion. Dans ce cas, l'étude de terrain s'est soldée par un échec, puisque les arbres ne permettent absolument pas de voir les habitations de Saint-Martin-d'Oydes depuis Esplas.

Après une visite au Carla-Bayle et la découverte d'un panoramique à couper le souffle dans ce village rempli d'artistes, il a été décidé de concentrer tous les efforts sur cette solution. Il ne reste plus qu'une dernière chose à faire : être sûr à 100% que le château et le Carla-Bayle peuvent bien se voir sans aucun obstacle, grâce au terrain favorable et la vue dégagée. Cette partie de l'histoire est racontée dans la Figure 8, complétée par la Figure 9.

(a) Que ce soit à l'œil nu ou avec des jumelles, à 10 km de distance et malgré la vue panoramique et la boussole, il a été impossible de réussir à localiser le château depuis le Carla-Bayle.

(b) Des spots lumineux de 400 W équipés de filtres rouges ont été positionnés sur les deux tours du château, en direction du Carla-Bayle.



(c) De nuit, grâce à cette installation, il a été possible de localiser le château grâce aux deux petits points rouges visibles à l'horizon. Une personne au téléphone éteignait et allumait les spots, pour confirmer qu'il s'agissait bien de ceux du château.

(d) Une fois le château localisé, un photographe a été appelé en renfort pour obtenir une vue du château.

(e) Un Nikon D800 avec capteur 35 millions de pixels équipé d'un téléobjectif zoom 70/200 millimètres avec doubleur (140/400 millimètres) a été utilisé pour cette opération.

(f) Après un traitement numérique sur les couleurs effectué par le photographe, l'orientation du château est bien visible et le dégagement dans les arbres aussi.

FIGURE 8 – Étude de faisabilité du pont wifi entre le château et le Carla-Bayle.

Ultime vérification : un mail a été envoyé à la mairie du Carla-Bayle, pour avoir une confirmation des débits VDSL2 réels qui sont accessibles au village. Étonnamment, le mail est arrivé dans les mains d'une personne qui connaissait parfaitement le sujet et qui a répondu le lendemain. La mairie elle-même disposerait d'un débit de 50 à 60 Mbps en VDSL2, grâce au NRA raccordé en fibre optique dans le village. Le déploiement de la fibre optique chez les particuliers est prévu entre la fin 2017 et 2025.

Le lieu étant choisi, il reste désormais à trouver la bonne personne au Carla-Bayle, qui est bien située par rapport au panoramique, et qui accepte de collaborer. C'est l'objet de la dernière étape : nouer du lien social, pour trouver la source de la connexion Internet VDSL2 sur laquelle raccorder le pont wifi.

### 2.1.4 Nouer du lien social pour trouver la source

Il aura fallu plusieurs mois pour trouver la bonne personne au Carla-Bayle.


FIGURE 9 – Localisation du château depuis la vue du Carla-Bayle, de nuit grâce aux spots rouges.

**Les Connaissances** Les premières tentatives ont consisté à exploiter le réseau de personnes qui gravitent autour du Château de Justiniac : « Connais-tu quelqu'un qui habite au Carla-Bayle ? ». Plusieurs visites, appels téléphoniques et mails ont été envoyés dans ce sens, en contactant des habitant·es « *de la part de* ». Malheureusement, aucune de ces personnes ne s'est révélée être la perle rare. Le Carla-Bayle est un village d'artistes, qui vit surtout l'été de ses nombreuses galeries d'art. Beaucoup de résident·es n'y passent qu'une partie de l'année, et certain·es vont jusqu'à couper l'électricité l'hiver. D'autres n'étaient tout simplement pas intéressés pour prendre du temps pour collaborer sur ce projet. Une partie de ces personnes n'a peut-être également pas donné suite à cause de l'utilisation d'une technologie impliquant l'émission d'ondes : la population-type de ce village a probablement augmenté les chances de croiser des personnes mal à l'aise avec cette problématique.

**Le Bar du village** La seconde vague de tentatives a consisté à aller directement à la rencontre des habitant·es du Carla, dans un premier temps en utilisant les lieux de passage. Une annonce papier a été déposée dans un café-épicerie bio très populaire dans le village. L'annonce, accrochée sur le bar, proposait de prendre contact pour obtenir un super accès à Internet pas cher, en participant à un projet militant et à but non-lucratif. Il n'y a eu aucun retour suite à cette initiative.

**La Jeune fille de la galerie** L'initiative suivante a consisté à se rapprocher d'une des galeries d'art présente en plein milieu du village. En sympathisant avec la personne en charge d'accueillir les visiteurs, le gros lot aurait pu être décroché : elle connaissait l'association Tetaneutral.net, membre de la Fédération FDN, parce que des ami·es en colocation utilisent un accès Internet fourni par cette association. Cette personne résidait en plein milieu du rempart Nord, avec une vue en direction de Justiniac. Malheureusement, elle travaillait ici en service civique, et allait donc rendre son appartement dans les mois suivants. Également amatrice du THSF (événement annuel du milieu hacker sur Toulouse), elle était motivée pour aider, et a donc organisé une rencontre avec son voisin. Cette rencontre s'est malheureusement révélée infructueuse, notamment parce que le voisin en question ne voulait pas entendre parler de Orange, qui était pourtant le meilleur opérateur pour ouvrir une ligne VDSL2 chez lui. Ironie du sort, son souci était donc de garder un Internet « éthique » avec sa ligne ADSL Free, plutôt que d'accepter l'ouverture d'une ligne Orange, qui représentait pour lui le plus infréquentable des opérateurs. Il n'a pas été possible de le convaincre que notre souci était précisément de faire de l'Internet plus éthique. Notre interlocutrice a été régulièrement tenu au courant des avancées par la suite, de façon à ce qu'elle n'oublie pas d'en parler autour d'elle.

**L'Artiste et sa femme** Peu avant Noël, la situation devenait inquiétante : tous les filons à disposition semblaient épuisés, alors que le Carla-Bayle restait pourtant la meilleure option. Les nouvelles initiatives ont donc consisté à vagabonder dans le village les jours de beau temps, et faire du porte-à-porte pour entrer en contact avec des personnes au hasard, sur le rempart Nord. Bien que la plupart des maisons soient désertes en hiver, le beau temps a permis de repérer quelqu'un par sa fenêtre ouverte. Cette personne était également locataire pour une courte durée et ne pouvait pas s'engager, mais elle connaissait un artiste dans la rue de derrière, qui serait potentiellement intéressé. L'accueil chez cet artiste fut chaleureux : en trente minutes, il était convaincu, il avait accepté de collaborer, la fenêtre où accrocher l'antenne était identifiée, la prise téléphonique avait été située, et il y avait même un accord pour les passages de câbles. Après échange de contacts pour la suite des opérations, et alors que nous nous apprêtions à nous dire au revoir, sa femme est entrée en scène. Après une rapide présentation des motivations de ma présence ici, elle s'est empressée de demander à son mari ce qu'il faisait, en lui faisant remarquer qu'ils avaient déjà eu bien des problèmes avec leur accès à Internet, et qu'il n'était pas question de recommencer. Cette angoisse a pu être calmée en lui faisant remarquer que, justement, elle n'aurait plus avoir à discuter avec un FAI commercial, et que ça serait désormais notre travail de maintenir la ligne fonctionnelle. Puis la question fatale est arrivée : « Mais votre antenne, là, ça fait des ondes ? ». Par expérience, il est inutile de continuer quand ce débat est posé sur la table. La problématique des ondes est de l'ordre de la croyance (dans les deux sens, puisque personne ne peut affirmer ni la nocivité ni la totale bénignité de l'effet des ondes radio sur le corps humain), et les chiffres n'y changent donc pas grand chose. Nous avons convenu qu'elle recevrait par mail des études permettant de resituer l'importance des ondes wifi par rapport à d'autres types d'ondes du quotidien [10], mais il semblait déjà acquis que c'était un coup dans l'eau. Avant de partir, en désespoir de cause, je demande à l'artiste le nom d'une autre personne du village à aller voir... Sa recommandation se révélera finalement être la clé pour nous ouvrir les portes du VDSL2 du Carla.

**Le Wifi et la villa de Juppé** Ce nouveau nom écrit sur le papier que je tiens dans mes mains fébriles semble être l'espoir qu'il n'était plus autorisé de nourrir. L'homme conseillé par l'artiste a pris l'initiative il y a quelques années d'installer rien de moins qu'un réseau wifi à l'intérieur du village, de façon à permettre aux galeries qui n'ouvrent que l'été de se dispenser de payer un abonnement Internet pour toute l'année. La première visite à l'improviste est un échec : sa copine me fait savoir qu'il a actuellement la gastro et qu'il n'est donc pas disponible. Des contacts sont donnés pour demander de prévenir quand je peux repasser, et Noël se passe ainsi avec la certitude que le problème du Carla est en passe de se résoudre. Pour autant, il n'y aura aucun retour de leur part. Ce sera une seconde visite à l'improviste en janvier, qui permettra de finalement accéder à l'homme-clé. J'apprends à cette occasion, que le Carla-Bayle bénéficierait d'un des meilleurs accès à Internet de la région parce que Alain Juppé aurait eu une villa dans le coin, et qu'il aurait donc fait en sorte d'inaugurer un NRA au milieu du village – information que je n'ai pas vérifiée. Concernant le réseau wifi du village pour les galeries, ça aurait été un échec et une source de conflits : la consigne qu'il avait passé était de limiter l'accès à Internet à un usage de base, pour que tout le monde (y compris lui) puisse bénéficier d'un accès à Internet correct. YouTube semblant être passé dans les usages de base d'Internet, sa connexion ADSL était saturée, et l'absence de montage légal lié à son installation – uniquement constitué de relais wifi de sa box – posait des questions. Néanmoins, je comprends que je fais face à la personne qui dépanne

10. Le lien suivant lui a notamment été transmis : https://www.ilico.org/2014/03/pour_etre_sur_la_meme_longueur_d_ondes_sur_le_reseau_wifi_de_chanteix/

un peu tout le monde au Carla, dès lors qu'il y a un problème informatique. Notre homme étant de nature très militante, il connaît également Tetaneutral.net et affirme pouvoir me trouver les bonnes personnes.

**Le Millionnaire et le voisin** Il me propose d'aller voir deux personnes qui vivent sur le rempart Nord : un millionnaire et une autre personne moins aisée financièrement. Puisque l'arrangement que je compte proposer à l'heureux élu est avantageux pour lui sur le plan financier, je choisis de privilégier la seconde personne. En nous dirigeant vers son appartement, je comprends ce qui est en train de se passer : me voici de retour devant la porte du voisin de la Jeune fille de la galerie, qui refusait d'entendre parler d'un accès VDSL2 de Orange, plusieurs semaines après. À ma grande surprise, les choses se sont déroulées de façon différente, puisqu'il aura suffit à son *conseiller informatique* de lui dire clairement et sans détour que ce que je proposais était tout à son avantage et qu'il devrait juste accepter, pour que j'obtienne un accord ferme.

Parfois, le discours et les arguments n'ont aucun effet, tant qu'ils ne sortent pas de la bouche de la bonne personne. Peu importe, la source où puiser la connexion Internet est identifiée, l'installation du pont wifi peut démarrer, en parallèle de l'ouverture de la ligne VDSL2.

### 2.1.5 Ouverture de la ligne VDSL2

La ligne VDSL2 du Carla-Bayle est ouverte au nom du locataire, en utilisant l'IBAN du compte en banque de Tetaneutral.net.

**Orange** L'opérateur Orange a été choisi en fonction des retours de quelques habitant·es du Carla-Bayle, qui ont estimé que c'était celui qui leur avait posé le moins de problèmes. Un forfait Livebox Play avec mobiles illimités est soucrit, afin de permettre au locataire de garder la possibilité d'utiliser son téléphone fixe sans contrainte. Les numéros spéciaux et le service Internet+ ont été désactivés depuis le compte Orange, pour éviter les surfacturations pour l'association.

**Migration** L'obtention du numéro RIO de la ligne téléphonique actuelle du Carla-Bayle a demandé de la patience, à cause des difficultés du locataire à retranscrire les informations données au 3179 [11]. Par contre, la souscription au forfait Orange avec un IBAN qui ne porte pas le nom du locataire n'a pas posé de problème. De la même façon, le fait que de fausses informations (date de naissance, lieu de naissance, profession) aient été fournies à Orange lors de la souscription n'a levé aucun voyant rouge chez eux. En définitive, Orange a accepté d'écraser un accès ADSL existant en n'ayant aucune garantie de la provenance de l'appel, et en utilisant un IBAN qui aurait pu être trouvé sur le web. Cette absence de contrôles s'est révélée pratique pour ouvrir la ligne à la place du locataire, mais peut légitimement interroger.

**Incidents** Une fois la Livebox reçue, le locataire s'est emporté contre Orange, en se plaignant qu'elle ne fonctionnait pas et en affirmant qu'il n'avait pas fait d'erreur d'installation. Un passage chez lui a permis de comprendre que le câble Ethernet de son ordinateur fixe avait été branché sur le port fibre de la Livebox. Un seul autre incident a eu lieu peu de temps après l'ouverture de la ligne, à cause d'un technicien sous-traitant de Orange qui a fait une erreur dans le NRA en voulant raccorder un autre client. Le service client de Orange s'est révélé étonnamment efficace à cette occasion.

### 2.1.6 Mise en place du pont wifi

Comme expliqué dans la Section 2.1.1, mettre en place le pont wifi consiste simplement à accrocher une antenne sur chaque bâtiment. Une antenne émet un SSID wifi (comme n'importe quel routeur ou box wifi), tandis que l'autre va simplement se connecter dessus (comme n'importe quel client wifi, de type ordinateur ou smartphone). La seule différence avec un simple duo routeur-ordinateur, c'est que les deux antennes doivent se regarder, et donc être

11. Le script Python fournit sur Wikipédia est pratique pour le tester avant d'appeler Orange : `https://fr.wikipedia.org/wiki/Relev%C3%A9_d'identit%C3%A9_op%C3%A9rateur#Cl%C3%A9_de_contr%C3%B4le_(CCC)`

pointée chacune dans la direction de l'autre. Comme expliqué dans les sections précédentes, on veillera également à ce que la vue soit parfaitement dégagée [12] entre les deux antennes.

**Pont wifi nu** La façon la plus simple de mettre en place le concept général de pont wifi présenté précédemment dans la Figure 1, est de suivre la topologie proposée par la Figure 10. Dans cet exemple, le routeur de la maison (ici une Livebox Orange, qui sert également de modem VDSL2) est directement utilisé pour fournir les adresses IP de l'ensemble des équipements du château (DHCP ou NDP). Dans ce cas de figure, tous les équipements du château et de la maison sont sur un seul et même réseau IP, qui correspond au LAN de la maison qui été étendu.

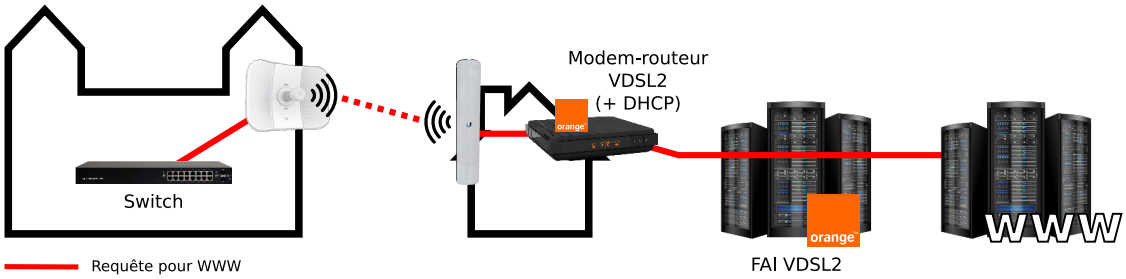


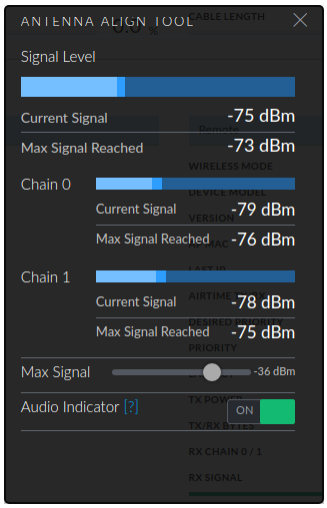

FIGURE 10 – Extension du réseau de la maison jusqu'au château, sans aucun routage supplémentaire. Le serveur du service Internet est ici un serveur web (représenté par *www*, mais il pourrait aussi bien proposer un autre type de service).

Dans cette situation, le réseau du château est uniquement constitué de switchs équipés d'interfaces filaires et sans-fils (ie. switchs, antennes directionnelles pour le pont wifi, et bornes wifi omnidirectionnelles pour la connexion des ordinateurs et smartphones). Par conséquent, il n'y a quasiment aucun effort de configuration à faire pour déployer cette installation : il faut simplement que les antennes du pont wifi se connectent l'une à l'autre. Ensuite, brancher des équipements sur le switch du château en reviendra au même que si ces équipements étaient directement branchés sur les ports RJ45 de la Livebox elle-même.

Le résultat du test d'alignement de l'antenne du château de la Figure 11a indique un signal évalué à -75 dBm (plus le nombre est proche de zéro, mieux c'est). Le test de débit local (entre les deux LiteBeam) de la Figure 11b indique un taux de transfert maximum de 91.65 Mbps, ce qui dépasse le débit maximum proposé par la connexion VDSL2 du Carla-Bayle. Enfin, le test de débit Internet de la Figure 11c affiche un débit de 83.55 Mbps en download, ce qui correspond à l'ordre de grandeur [13] du débit constaté lorsqu'on se connecte en direct sur l'accès VDSL2 : le pont wifi permet donc de récupérer 100% du débit de la connexion THD du Carla-Bayle (avec une latence correcte de plus ou moins 30 ms, ce qui correspond environ au double de celle constatée en étant en direct sur le VDSL2).

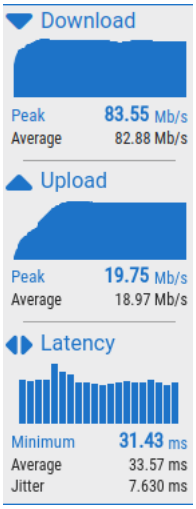
Ce montage est parfait pour tester le bon fonctionnement du pont wifi, ou pour étendre un réseau entre deux bâtiments qui appartiennent à la même personne ou organisation. Ou bien pour partager une connexion à Internet entre deux personnes qui se connaissent et qui se font confiance. Car, dans cette configuration, il n'y a qu'un seul et unique responsable légal pour l'ensemble du trafic Internet : la personne qui a ouvert la ligne VDSL2 chez Orange, et qui habite dans la maison. Si d'autres habitations venaient à se relier au pont wifi de la maison, pour faire comme le château, le propriétaire de la ligne doit donc faire confiance à tous les propriétaires et les visiteurs qu'ils accueillent, qui utilisent sa connexion à Internet, avec ses adresses IP. Pour répartir la responsabilité légale des usages qui sont fait avec la ligne Internet de la maison, il est donc indispensable que chaque habitation reliée au pont wifi dispose de ses propres adresses IPv6 et IPv4 publiques. Puisque Orange ne propose pas ce service, il faut faire intervenir un autre FAI, capable de fournir ces adresses IP différenciées. C'est le cas de la plupart des FAI de la Fédération FFDN.

12. À noter que l'eau ne perturbe pas le signal wifi : ainsi, une grosse pluie ou un épais brouillard ne devrait pas altérer la connexion.
13. Les tests de débit Internet comme `https://www.speedtest.net` sont toujours très variables, dans la mesure où les conditions de test ne peuvent jamais être les mêmes d'un instant $t$ à un autre. Par conséquent, les valeurs obtenues doivent surtout être interprétées comme des ordres de grandeur et non comme des valeurs absolues.




(a) Test d'alignement de la LiteBeam du château.


(b) Test de débit local entre les deux LiteBeam.




(c) Test de débit Internet au château, directement connecté à la LiteBeam.

FIGURE 11 – Test d'alignement et de débit pour le pont wifi entre les deux LiteBeam.

**FFDN et ses tunnels** Les FAI FFDN sont des associations à but non-lucratif qui proposent des solutions généralement de qualité professionnelle, associées à des avantages techniques inédits et une éthique qui se veut exemplaire :

**Adresses IPv6** Un range complet d'adresses IPv6 publiques est délégué aux abonné·es.
**Adresses IPv4** Une ou plusieurs adresses IPv4 publiques peuvent être proposées.
**Vie privée** Les FAI de la Fédération FFDN s'engagent à strictement respecter la vie privée des abonné·es et à ne pas regarder le contenu des flux Internet transportés.
**Neutralité du Net** Ils s'engagent également à respecter la Neutralité du Net, c'est-à-dire à servir tous les contenus qui sont présents sur Internet, sans censure ni priorisation d'un type de contenu par rapport à l'autre.
**Autohébergement** Les IP publiques sont fixes et l'intégralité des ports sont accessibles, permettant d'héberger des serveurs sans contraintes derrière n'importe lequel de leurs accès.

L'idéal serait donc de remplacer la ligne Orange du Carla-Bayle par une ligne opérée par un FAI FFDN. Très peu de FAI FFDN sont parvenus à pouvoir proposer des offres pour des lignes de type VDSL2, et elles sont généralement hors de prix, pour des retombées financières très limitées pour l'association [14]. La solution alternative est de profiter directement des prix attractifs que proposent les gros FAI comme Orange, en utilisant les lignes qu'ils ouvrent, pour ensuite les « convertir » en ligne FFDN. Cette solution implique l'utilisation d'un tunnel VPN, tel que décrit ci-dessous.

**Que fait un VPN** Utiliser un service Internet (eg. afficher une page web, discuter sur Snapchat, faire un transfert FTP) consiste à échanger des demandes et des réponses avec un équipement du FAI qui opère la ligne Internet sur laquelle on est connecté. Pour répondre aux demandes adressées, ce dernier doit – plus ou moins directement – lui-même échanger des demandes et des réponses avec l'équipement qui gère ce service (resp. le serveur web, le serveur Snapchat, le serveur FTP). Lorsqu'on utilise un tunnel VPN, toutes les demandes et réponses passent par un intermédiaire, comme si elles étaient transportées dans des enveloppes. Dans ce cas, le FAI qui gère la ligne se

14. Cette situation s'explique notamment par les tarifs exagérés qui sont proposés par les intermédiaires aux petites structures. Pour mieux comprendre comment fonctionne un FAI comme ceux de la Fédération FFDN, voir `https://julien.vaubourg.com/files/internet-is-coming-1.mp4`.

contente uniquement de transporter des enveloppes depuis et à destination d'un serveur VPN, sans en connaître le contenu. C'est le FAI qui gère le serveur VPN qui s'occupe ensuite lui-même de traiter les demandes qui sont dans ces enveloppes. Les seules IP qui seront connues par les services Internet distants sont celles qui ont été attribuées à l'abonné·e par le FAI du VPN. Le principe est similaire à celui d'un proxy, à un niveau différent. D'un point de vue topologie Internet, on peut alors considérer que le FAI de la ligne devient un simple transitaire supplémentaire pour le FAI du VPN[15].

**Pont wifi avec VPN** Le montage qui permet de répondre à la problématique de la répartition de la responsabilité légale est illustré par la Figure 12. Un nouvel équipement est ajouté dans la maison, pour faire office de passerelle VPN (client). La passerelle utilise la connexion VDSL2 pour ouvrir un seul et unique tunnel VPN avec un serveur FFDN situé sur Internet. Une fois ce tunnel ouvert, tout le trafic Internet en provenance et à destination des équipements qui sont derrière l'antenne de la maison transite à l'intérieur (ie. tout ce qui passe dans le tuyau vert du schéma voyage dans des enveloppes au travers d'Internet). Orange (FAI de la ligne VDSL2) ne voit donc qu'une seule et unique session transiter par son infrastructure, à destination d'un serveur FFDN (FAI du VPN). Si le tunnel VPN est chiffré (ie. le contenu des enveloppes est écrit dans une langue que seul le FAI FFDN peut comprendre), il devient techniquement impossible pour Orange de connaître la nature de ce qu'il transporte. Les IP utilisées sur Internet pour communiquer avec le serveur du service étant celles du FAI FFDN, le ou la propriétaire de la ligne VDSL2 ne prend aucun risque légal en « partageant » son accès Orange : le risque juridique est partagé et chaque foyer est responsable de ce qui a été consulté avec ses IP.

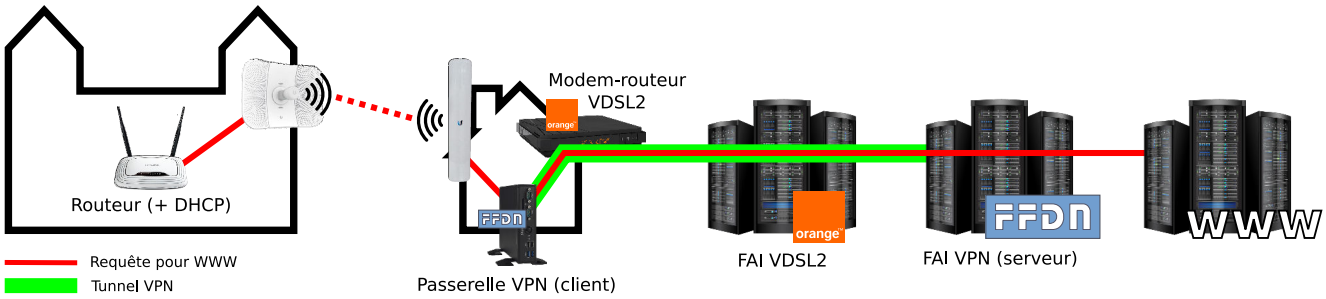



FIGURE 12 – Mise à disposition d'une connexion Internet dédiée au château, à l'aide d'un tunnel VPN proposé par l'un des FAI de la Fédération FFDN. Chaque FAI membre de la Fédération dispose de ses propres serveurs.

D'un point de vue pratique – dans notre cas – le FAI FFDN fournit à l'abonné·e un routeur à installer à son domicile, qui est configuré à la « livraison » avec l'IPv4 et le range IPv6 qui sont attribués à l'abonné·e. Le routeur est relié à sa passerelle VPN de référence via les antennes directionnelles, et les routes sur les serveurs du FAI FFDN permettent de faire communiquer les IP publiques avec le reste d'Internet.

D'un point de vue paquets IP, les PC connectés au wifi du château bénéficient d'une IPv6 publique et d'une IPv4 privée, dont les paquets passent tous dans le même tunnel VPN, comme illustré par la Figure 13.

D'un point de vue réseaux IP, le WAN est donc désormais lui-même composé de plusieurs LAN interconnectés. Pour comprendre les interactions entre les différents réseaux, la Figure 14 propose une représentation imagée des différents LAN avec les équipements qui routent à leurs intersections. Les tests de débit Internet finaux ne varient pas, selon que la passerelle VPN est utilisée ou non pour se connecter (la machine cliente utilisée est donc assez puissante pour ne pas agir comme goulot d'étranglement).

Des photos de l'installation des équipements de la maison du VDSL2 sont disponibles dans la Figure 15, et des photos de l'installation de l'antenne du château sont disponibles dans la Figure 16.

15. Voir `https://julien.vaubourg.com/files/internet-is-coming-1.mp4` pour comprendre la notion de transit chez un FAI.

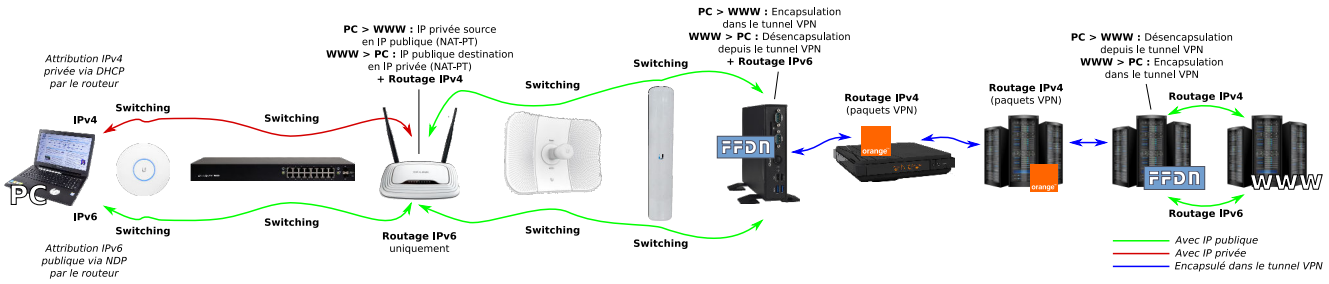



FIGURE 13 – Routage et switching des paquets IPv6 et IPv4 entre un PC du château et un service Internet WWW, via le tunnel FFDN (lui-même monté en IPv4 via la connexion de Orange). Un montage en IPv6 aurait été plus intéressant, si Orange et Tetaneutral.net permettaient ce choix.

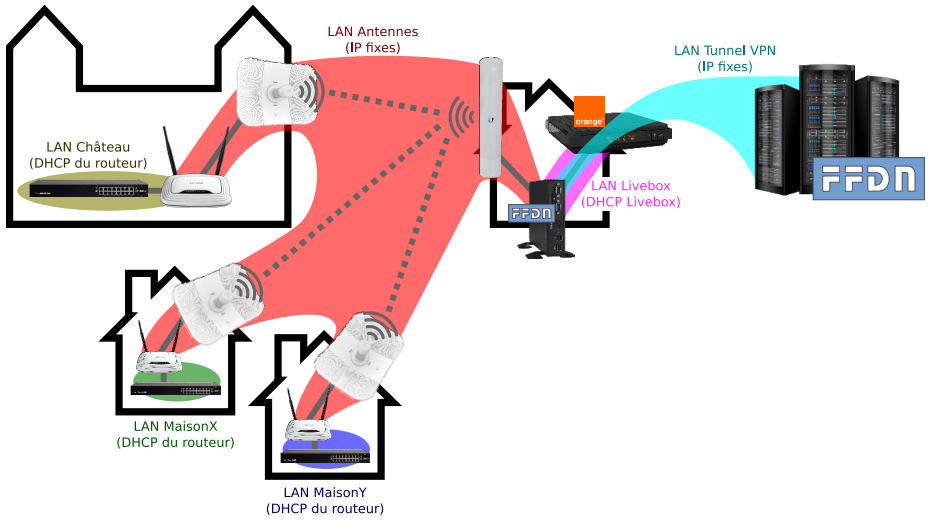



FIGURE 14 – Représentation imagée des réseaux (1 bulle colorée = 1 LAN), avec le château ainsi que 2 autres maisons voisines (MaisonX et MaisonY) qui se connectent à Internet via le tunnel FFDN.

(a) Matériel chez l'habitant : le Shuttle (passerelle VPN) est posé sur la Livebox. Il est connecté à la fois à la Livebox et à la LiteBeam (antenne directionnelle) à l'extérieur.

(b) LiteBeam 120 (antenne directionnelle ouverte à 120°) en direction du château.

(c) Malgré sa puissance, ce modèle de LiteBeam reste discret pour le voisinage, en évitant d'avoir une forme de parabole imposante.

FIGURE 15 – Équipements au Carla-Bayle.

(a) Le seul accès au toit du château se fait par la Tour du Hibou, par une petite fenêtre. Les antennes sont fixées de l'autre côté du toit.

(b) Des bénévoles de Tetaneutral.net sont venus aider pour le montage du lien WAN. L'antenne du WAN ainsi que le mât appartiennent à Tetaneutral.net.

(c) Le propriétaire du château était également présent lorsque l'antenne du WAN a été posée, et a proposé de lui-même fixer le mât à la cheminée.

(d) La grosse antenne (directionnelle) est une LiteBeam AC qui pointe vers le Carla-Bayle. La petite rectangulaire est une NanoStation M5 (cf. Section 2.2.3 de la partie LAN pour comprendre son utilité).

(e) Les antennes sont placées côté Sud du château, qui est la plus belle façade du lieu. Les câbles ont été au maximum camouflés derrière le mât.

(f) Le toit est un peu raide, mais se pratique bien par temps sec, et permet donc de laisser les antennes facilement accessibles.

(g) Les antennes ne sont pas visibles depuis la terrasse (demande du propriétaire), mais peuvent être aperçues en s'éloignant dans le parc. Un mât moins imposant aurait été plus approprié.

(h) À 10 km de distance, c'est très difficile de voir le Carla-Bayle à l'œil nu comme avec des jumelles.

FIGURE 16 – Déploiement des antennes sur le toit du château.

### 2.1.7 Matériel utilisé

Le matériel utilisé pour la mise en place du WAN est listé dans le Tableau 17. Le choix du matériel est arbitraire : Ubiquiti est une marque reconnue qui fait des produits wifi de qualité et à des prix abordables, mais, pour ces antennes, le système d'exploitation n'est pas libre (bien qu'étant basé sur une distribution GNU/Linux). Ce constructeur est actuellement celui qui est le plus largement utilisé au sein des FAI FFDN, pour le montage des ponts wifi.

| Illustration | Produit | Description | Nb | Prix TTC x1 | Propriétaire |
|---|---|---|---|---|---|
|  | Serveur Shuttle DS68U | *Passerelle VPN (client OpenVPN + routage entre le réseau des antennes directionnelles et le tunnel VPN)*<br><br>2 x Intel Celeron 3855U 1.6G / 8Go RAM / 2 x 1Gbps LAN<br>https://www.ldlc.com/fiche/PB00217069.html | 1 | 249.95€ | TTNN |
|  | Ubiquiti LiteBeam LBE-5AC-23 | *Antenne directionnelle pour le pont wifi entre le château et le Carla-Bayle (côté château) – Firmware d'origine*<br><br>Outdoor / 5Ghz AC / 23dBi / +30km / PoE passif 24V / 1 x 100Mbps LAN<br>https://www.eurodk.com/en/products/directional-c/litebeam-ac-23dbi | 1 | 52.44€ | TTNN |
|  | Ubiquiti LiteBeam LBE-5AC-16-120 | *Antenne directionnelle 120° pour le pont wifi entre le château et le Carla-Bayle (côté Carla-Bayle) – Firmware d'origine*<br><br>Outdoor / 5Ghz AC / 16dBi / +30km / PoE passif 24V / 1 x 100Mbps LAN<br>https://www.eurodk.com/en/products/base-stations/litebeam-ac-16dbi-120deg | 1 | 76.57€ | TTNN |
|  | Forfait Orange Livebox Play | *Abonnement VDSL2 au Carla-Bayle*<br><br>Livebox 4 / Illimité fixes et mobiles / Sans décodeur TV<br>https://boutique.orange.fr/internet/offres-adsl/play | 1 | 42.99€ / mois | Locataire Carla-Bayle (payé par TTNN) |
|  | Abonnement Accès Internet TTNN | *Abonnement pour accéder à Internet via les services de TTNN*<br><br>Adhésion à l'association obligatoire<br>https://tetaneutral.net/adherer/ | 1 | Prix libre / mois | Château + Locataire Carla-Bayle |

Tableau 17 – Prix TTC pour la partie WAN : total de 378.96€ + 42.99€ / mois pour TTNN, et une adhésion+abonnement TTNN à prix libre pour le château et le locataire du Carla-Bayle.

## 2.2 Partie LAN

### 2.2.1 Zones à couvrir

Le château dispose d'un rez-de-chaussée et de deux étages, ainsi que d'une cour intérieure et d'un parc. Les zones à couvrir en wifi (ie. où il serait souhaitable de pouvoir connecter facilement son ordinateur ou smartphone à un wifi performant) sont indiquées en rouge sur les plans de la Figure 18. Les extérieurs à proximité du château sont donc également à couvrir, et le second étage ne dispose que d'une seule chambre habitée.

**70% minimum** Pour ce déploiement, on considère arbitrairement qu'une zone est suffisamment couverte dès lors qu'un ordinateur ou un smartphone affiche une réception d'au moins 70% du signal wifi (2.4 Ghz). Concrètement, le niveau de réception du wifi est généralement intimement lié au débit Internet dont bénéficiera l'équipement qui se connecte : 70% du signal wifi présage donc un accès à environ 70% du débit maximal de la connexion Internet, soit 70 Mbps pour une connexion à 100 Mbps. En-dessous de 50% du signal wifi, certains équipements peuvent avoir du mal à se connecter ou perdent régulièrement la connexion au wifi.

**Différents signaux pour un même wifi** Les bornes wifi qui sont déployées sont dual-band, c'est-à-dire qu'elles proposent de se connecter soit à un signal qui utilise une fréquence incluse dans la bande 2.4 Ghz, soit à un signal qui utilise une fréquence de la bande 5 Ghz. La principale différence entre les deux bandes est que la bande 5

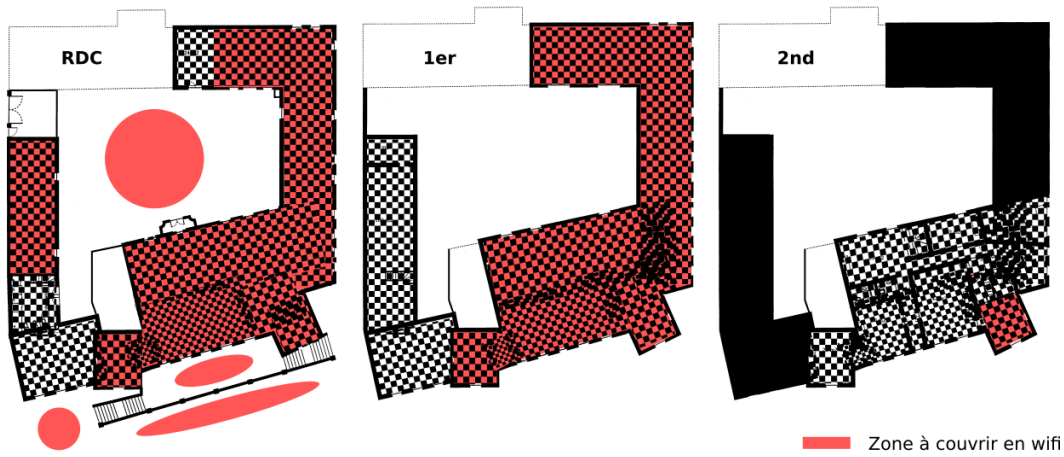



FIGURE 18 – Zones du château à couvrir en wifi (le détail des plans est brouillé par des damiers).

Ghz traverse moins bien les murs, et est généralement moins utilisée (et donc moins polluée, donc plus fiable). Cette notion a été développée plus en détail dans la Section 2.1.1 de la partie WAN. Généralement, les systèmes d'exploitation des ordinateurs n'affichent à l'utilisateur ou l'utilisatrice qu'un seul et unique signal wifi, qu'il soit émis en 2.4 Ghz, 5 Ghz, ou depuis des bornes différentes, dès lors que tous les signaux proposent le même nom de réseau wifi (SSID) : seul le signal le plus puissant parmi tous ceux captés sera affiché. Des gestionnaires réseau comme *wicd-curses* (GNU/Linux) proposent de différencier les différents signaux, en fonction de leur fréquence et de leur borne d'émission (BSSID).

**Systèmes chaotiques** Pour s'assurer qu'il y aura toujours un signal wifi à 70% partout dans les zones à couvrir, il est nécessaire de multiplier les bornes wifi, en les accrochant un peu partout dans le château, sur les murs et plafonds. Toutefois, chaque installation de borne a un coût (prix du matériel, temps de travail et aussi impact esthétique sur le lieu), il ne serait donc pas raisonnable d'en installer une dans chacune pièce. Ainsi, le plan d'installation des bornes wifi nécessite de réussir à déterminer à l'avance, en fonction des plans et de la visite du lieu, quel est le nombre minimum de bornes à installer et où il est le plus judicieux de les placer, pour idéalement avoir à chaque endroit du château exactement un et un seul signal wifi qui atteint ou dépasse les 70% de réception.

La difficulté de cette étude réside dans le fait que la propagation des ondes wifi est proche d'un système chaotique : les ondes peuvent rebondir sur un nombre indéterminé d'obstacles (murs, meubles, humains, etc.), avant d'être totalement absorbées par un obstacle particulier ou de perdre toute leur puissance. Si les ondes rebondissent beaucoup, avec de la chance, elles pourront passer la porte d'un mur très épais et donc permettre à un équipement dans la salle d'à côté de se connecter au wifi... ou bien les rebonds ne les mèneront jamais jusque là... ou bien elles ne passeront la porte que lorsqu'un meuble sera dans une position particulière. Ainsi, pour déterminer précisément le niveau de réception du wifi dans une salle en fonction du placement d'une borne dans une autre salle, il faudra connaître la disposition exacte de tous les éléments, ainsi que la composition et l'épaisseur exacte de tous les meubles, murs, sols et plafonds et déterminer leur taux d'atténuation, pour enfin pouvoir modéliser et simuler le système complexe correspondant.

En réalité, pour ces raisons, ce type d'étude n'est pas réalisable : le taux de réception wifi est donc estimé grossièrement en fonction de l'épaisseur des murs et plafonds, et en fonction de la présence de matériaux métalliques (très forte atténuation à cause la réflexion) ou non à l'intérieur. Ces estimations sont ensuite complétées avec des tests sur le terrain, à l'aide d'une borne wifi portative.

Chacune des bornes doit être reliée à un câble : cette contrainte influence également le choix de leur emplacement.

### 2.2.2 Câblage et placement des bornes

Ironiquement, la mise en place d'une infrastructure permettant de se connecter à Internet en mode sans-fil, demande de déployer beaucoup de fil. Chaque borne wifi du château doit être reliée par un câble Ethernet à un switch du château.

**Pourquoi utiliser des antennes câblées ?** Pour étendre un réseau wifi domestique à l'intégralité d'une maison ou pour l'amener jusqu'à un jardin, les particuliers utilisent généralement des bornes relais wifi, diponibles en grandes surfaces. Ces relais se contentent de capter un signal wifi un peu faible, et de le réamplifier en le réémettant lui-même. Utilisés en cascade, ils peuvent ainsi théoriquement permettre de couvrir de grandes surfaces. Cette technique présente l'immense avantage de ne pas avoir à relier les différents équipements entre eux par des câbles, et donc de ne nécessiter aucun travaux dans la maison. Toutefois, des inconvénients non-négligeables sont également au rendez-vous : le débit effectif de la connexion Internet chute à chaque passage de relais (et rend donc la qualité du service très hétérogène), il suffit qu'un des relais soit en panne pour que tous les autres soient déconnectés [16], le signal de la borne la plus proche est parfois impossible à réémettre parce qu'il est totalement absorbé par un mur, et enfin chaque borne relais doit malgré tout être raccordée à un câble électrique.

Pour ces raisons, l'utilisation de bornes relais n'a pas été retenue pour ce projet. Chaque borne wifi restera indépendante et toutes offriront la même meilleure qualité de service possible, en étant directement câblées sur un switch et en utilisant la technologie PoE (Power Over Ethernet) pour les alimenter électriquement (ie. le switch fournit également l'électricité à la borne via l'unique câble Ethernet qui les relie).

**Déploiement vertical** Comme la plupart des châteaux de ce type, les nombreux murs en pierre sont épais et laissent très mal se propager les ondes wifi. Par contre, les plafonds sont plutôt fins, en bois / plâtre et parfois chaux, et dépourvus de matériaux métalliques. Ainsi, une borne wifi au premier étage pourra facilement servir en même temps pour les étages inférieurs et supérieurs, tandis qu'elle pourra ne pas être suffisante pour couvrir la pièce juste à côté d'elle. La répartition des bornes wifi doit donc être pensée en fonction de l'environnement vertical plutôt que horizontal.

**Invisibilisation** Un château ne dispose d'aucune solution facile pour câcher des câbles : ni faux-plafonds, ni colonnes sèches, ni double-murs. Ainsi, déployer des bornes wifi partout dans le château consiste surtout à réussir à câbler tout le château sans dénaturer le charme et l'authenticité du lieu.

Pour y parvenir, les différents atouts du lieu doivent être exploités :

— Dans notre cas, le deuxième étage du château est en grande partie utilisé comme grenier. La structure métallique imposante qui le traverse à moins d'un mètre du sol indique qu'il ne pourra probablement jamais être utilisé pour autre chose. Ce grand grenier sans murs intérieurs est une aubaine : il permet de déployer de grandes longueurs de câbles sans se soucier de l'esthétique, et d'atteindre toutes les pièces du premier étage du bâtiment principal directement depuis les plafonds. Un tuyau de VMC traverse même tout le château à la verticale, du rez-de-chaussée jusqu'au grenier d'où il tire son air frais.
— Dans ce type de château, on trouve généralement de grands placards permanents, qui sont placés de façon opportuniste à peu près à chaque fois que la forme d'un mur offre une enclave. Ces placards intégrés à la structure, qui ne changeront jamais de place, sont idéals pour faire office de colonnes sèches, pour traverser des étages entiers à la verticale.
— Parfois, on trouve quelques centimètres d'air (éventuellement comblés avec de la laine de roche) sous les planchers en chêne. La vestuté du bâtiment, de façon générale, facilite les occasions de trouver des ouvertures déjà existantes dans ces planchers.
— Enfin, les restaurations les plus récentes offrent quelques fois des morceaux de faux plafonds (eg. pour les arrivées de VMC des salles de bain), avec – parfois – une trappe d'accès. Leur emplacement peut être déterminant pour le choix du placement des bornes wifi, étant donné le confort qu'ils apportent à l'installation.

De nombreuses photos des passages des câbles sont disponibles dans l'Annexe B.

16. L'utilisation d'un maillage de type mesh pourrait éliminer cette contrainte, mais le niveau de technicité de l'installation finale augurerait alors d'autres problèmes complexes à résoudre.

**Concevoir le plan wifi** Les étapes pour concevoir le plan de placement des bornes wifi pourraient être résumées ainsi :

1. Récupérer des plans du château et (parfois) les mettre à jour.
2. Placer les bornes sur les plans de façon idéale en essayant d'en mettre le moins possible, en considérant systématiquement qu'un simple plafond ou un mur en placo-plâtre permettront de couvrir les espaces adjacents, mais qu'un mur porteur bloquera le signal. Certaines pièces sont également plus importantes que d'autres (eg. un salon, un bureau ou encore la cuisine, qui est souvent un lieu de vie central), et méritent probablement d'être directement équipées pour un confort maximum.
3. Étudier sur le terrain les contraintes fortes, comme les salles particulièrement jolies à ne pas dénaturer, les grandes pièces métalliques (forte atténuation du signal), ou encore les néons (fortes perturbations électromagnétiques).
4. Étudier également sur le terrain les atouts du lieu, comme ceux décrits plus haut. Repérer les placards qui pourraient servir de locaux techniques (installation des équipements réseau tels que les switchs ou le routeur).
5. Revenir aux plans, et adapter le placement des bornes en fonction des observations de terrain. Déterminer également le nombre et la localisation des locaux techniques, en fonction des contraintes et des facilités de cablâge repérées.
6. De nouveau sur le terrain, effectuer des tests de niveau de réception à l'aide d'une borne wifi portative et d'un smartphone ou un ordinateur, de façon à vérifier s'il est effectivement possible de capter le signal d'une pièce adjacente dans les pièces qui ne seront pas équipées. Ce type de test a par exemple été utile pour découvrir qu'un énorme four à pain (qui n'est plus en service) bloque le signal de façon inattendue, et impose donc l'ajout d'une borne supplémentaire.
7. Corriger de nouveau les plans si nécessaire.

Le plan de placement des équipements pour le Château de Justiniac est disponible dans la Figure 19. Un seul local technique (un seul switch), situé dans un placard permanent, a été utilisé. Dans ce cas, la couverture wifi est plutôt très serrée.

### 2.2.3 Extension du LAN

Les circassien·nes de la compagnie de cirque moderne « Les Têtes en l'air » vivent en caravanes sur un terrain du château, à moins de 200 mètres du bâtiment principal. Ils disposaient de leur propre accès à Internet par ADSL, coûteux et très lent. Pour résoudre ce problème, un atelier pratique a été proposé lors de l'AG FFDN 2018 qui s'est déroulée à Justiniac : étendre le LAN du château pour faire directement profiter à nos ami·es du cirque de l'accès à Internet du château.

Plutôt que de tendre un câble au milieu des bois, un second pont wifi peut être mis en place depuis le toit du château. La Figure 20a propose le tracé du pont wifi à réaliser, tandis que la Figure 20b montre la vue qui est disponible depuis le toit du château vers les caravanes. Le hangar à proximité des caravanes est difficilement visible depuis le château, ce qui pourrait être un problème critique dans le cas d'un pont wifi longue distance (cf. conditions pour la mise en place d'un pont wifi à la Section 2.1.1 de la partie WAN). Cependant, avec une distance de moins de 200 mètres, le signal wifi reste assez puissant en bout de course pour être capable de traverser des obstacles relativement fins comme la cime des arbres. L'expérience vaut le coup d'être tentée.

L'atelier a été animé par Spyou, fidèle contributeur FFDN et particulièrement actif dans SCANI[17], une coopérative d'intérêt collectif correspondante de la Fédération. Cet atelier a été l'occasion pour les participant·es de comprendre les quelques aspects théoriques liés aux ponts wifi, d'apprendre à sertir des câbles RJ45 et de configurer des antennes directionnelles, le tout en rendant service à des voisins.

Le résultat du test d'alignement de l'antenne du château de la Figure 21a indique un signal évalué à environ -78 dBm. Le signal a tendance à varier fréquemment en fonction du mouvement des arbres avec le vent, mais reste toujours correct (il sera encore meilleur en hiver quand les feuilles seront tombées). Le test de débit local (entre les deux NanoStation) de la Figure 21b indique un taux de transfert maximum de 26 Mbps, ce qui est proche du

17. https://www.scani.fr

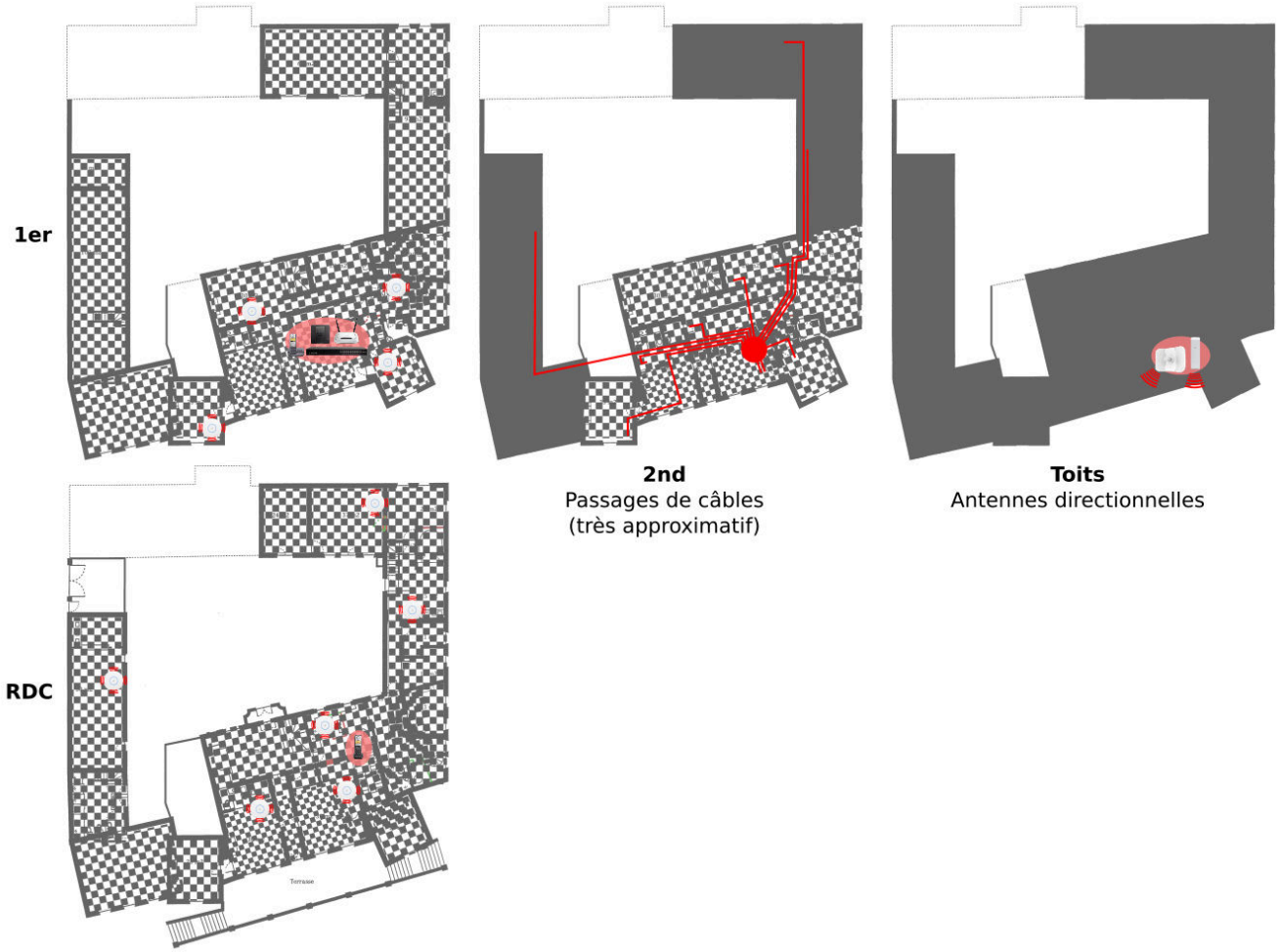



FIGURE 19 – Disposition des équipements dans le château (le détail des plans est brouillé par des damiers).

débit maximum constaté au château. Enfin, le test de débit Internet de la Figure 21c affiche un débit de 13 Mbps en download : le pont wifi vers le cirque permet donc de récupérer un très bon débit, avec une latence toujours correcte de 48 ms.

Un grand merci aux bénévoles qui ont participé à cet atelier durant l'AG, et aux associations SCANI et Tetaneutral.net, qui ont généreusement offert le matériel nécessaire au montage de cette extension du LAN. Des photos des installations sont disponibles dans la Figure 22.

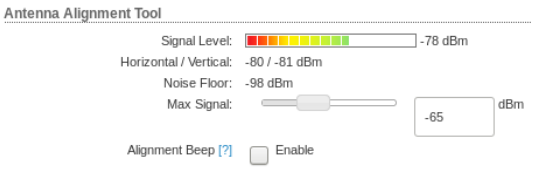
### 2.2.4 Matériel utilisé

Le matériel utilisé pour la mise en place du LAN complet est listé dans le Tableau 23. Le routeur TP-Link et les antennes AC Lite ont pu bénéficier d'un système d'exploitation libre.

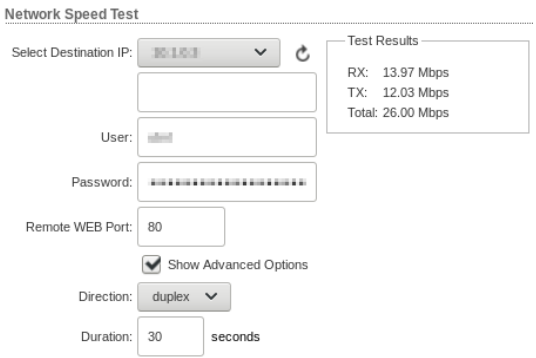
(a) Tracé du pont wifi vers les caravanes du cirque (environ 120m).

(b) Vu depuis le château, le hangar rouge qui est juste devant les caravanes est en grande partie camouflé par les arbres.

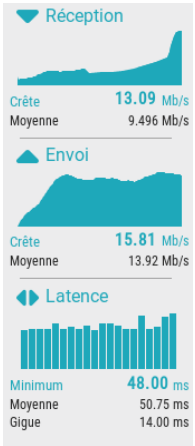
FIGURE 20 – Situation des caravanes par rapport au château, pour l'extension du LAN du château.




(a) Test d'alignement de la NanoStation du château.




(b) Test de débit local entre les deux NanoStation.




(c) Test de débit Internet au cirque, connecté à la borne wifi.

FIGURE 21 – Test d'alignement et de débit pour le pont wifi entre les deux NanoStation.

(a) Une antenne NanoStation M5 qui pointe vers le hangar rouge a été ajoutée sur le mât de l'antenne du WAN. Elle permet d'agrandir le LAN jusqu'aux caravanes du cirque qui sont stationnées sur un terrain du château.

(b) Spyou, sur son ordinateur, a accepté d'animer un atelier durant l'AG FFDN, pour apprendre aux bénévoles présent·es à monter un pont wifi. Les deux NanoStation ont été offertes par SCANI.

(c) L'antenne utilisée pour la réception est une NanoStation Loco M5, positionnée sur le hangar rouge.

(d) Elle est fixée en haut de la gouttière du hangar rouge, positionné entre les caravanes du cirque et le château.

(e) Passage du câble de l'antenne vers l'intérieur du hangar, au travers les planches de bois.

(f) Passage du câble dans le grenier de l'extrémité du hangar.

(g) Passage vers l'intérieur de la partie fermée du hangar, en suivant une gaine de câbles électriques.

(h) L'antenne est alimentée électriquement à l'aide d'un injecteur PoE.

(i) Routeur/borne wifi (configuré en bridge) offert par Tetaneutral.net, permettant de recevoir directement des IP du château. Le réseau wifi porte directement le nom de la compagnie de cirque et permet aux caravanes à proximité de se connecter à Internet.

FIGURE 22 – Déploiement de l'extension du LAN vers les caravanes du cirque.

| Illustration | Produit | Description | Nb | Prix TTC x1 | Propriétaire |
|---|---|---|---|---|---|
|  | Routeur TP-Link TL-WR841ND | *Routeur IPv6/IPv4 du château avec NAT-PT IPv4 et DHCP/NDP – Flashé en OpenWrt image TTNN*<br><br>CPU ?? / 5 x 100Mbps LAN / Wifi désactivé (antennes inutiles)<br>https://www.materiel.net/routeur-adsl/tp-link-tl-wr841n-v8-94778.html | 1 | 19.90€ | TTNN |
|  | Ubiquiti EdgeSwitch ES-16-150W | *Switch PoE du château – Firmware d'origine*<br><br>16 x port PoE 1Gbps / 2 x port 1Gbps SFP<br>https://www.eurodk.com/en/products/ubnt-switches/edgeswitch-16-150w | 1 | 279€ | Château |
|  | Ubiquiti UniFi AC Lite UAP-AC-LITE (pack de 5) | *Points d'accès wifi omnidirectionnels du château – Flashé OpenWrt image custom*<br><br>Indoor / 2.4+5Ghz AC / 2 x 3dBi / PoE passif 24V / 1 x 1Gbps LAN<br>https://www.eurodk.com/en/products/unifi/unifi-ac-lite-5-pack | 2 | 345.08€ | Château |
|  | Ubiquiti NanoStation M5 | *Antenne directionnelle 60° pour le pont wifi entre le château et les caravanes du cirque (côté château) – Firmware d'origine*<br><br>Outdoor / 5Ghz N / 16dBi / +15km / PoE passif 24V / 2 x 100Mbps LAN<br>https://www.eurodk.com/en/products/nanostations/nanostation-m5 | 1 | 75€ | Château (cadeau SCANI) |
|  | Ubiquiti NanoStation Loco M5 | *Antenne directionnelle 60° pour le pont wifi entre le château et les caravanes du cirque (côté cirque) – Firmware d'origine*<br><br>Outdoor / 5Ghz N / 13dBi / +10km / PoE passif 24V / 1 x 100Mbps LAN<br>https://www.eurodk.com/en/products/nanostations/nanostation-loco-m5 | 1 | 56.64€ | Château (cadeau SCANI) |
|  | Routeur Netis WF2710 | *Point d'accès wifi omnidirectionnel du cirque – Firmware d'origine*<br><br>Indoor / 2.4+5Ghz AC / 3 x 5dBi / Utilisé en mode bridge<br>https://www.laboutiquedunet.com/p-NET00371/Routeur-NETIS-AC750-Wireless-Dual-Band-WF2710.html | 1 | 41.80€ | Château (cadeau TTNN) |
|  | Ubiquiti ToughCable Carrier | *Rouleau de câble Ethernet*<br><br>Blindé SFTP / Cat5e ready Cat6 / Outdoor / 300m / Noir<br>https://www.eurodk.com/en/products/outdoor-cables/toughcable-carrier | 1 | 178.31€ | Château |
|  | Ubiquiti ToughCable Connectors | *Connecteurs RJ45*<br><br>Blindage / Cat6 / 100 unités<br>https://www.eurodk.com/en/products/connectors/toughcable-connectors | 1 | 47.20€ | Château |
|  | Network Tools Kit (4 Tools) | *Trousse à outils pour sertir les câbles RJ45*<br><br>Pince à sertir RJ45+RJ11 / Pince à dénuder / Pince pour prises murales / Testeur de câble<br>https://www.eurodk.com/en/products/ethernet-tools/network-tools-kit-4-tools | 1 | 19.36€ | Julien |

TABLEAU 23 – Prix TTC pour la partie LAN : total de 1407.37€ (dont 212.7€ de prêts et dons).

## 2.3 Téléphonie

Avant l'installation du nouveau lien Internet via le pont wifi du Carla-Bayle, le château utilisait une connexion ADSL qui lui permettait pour le même prix d'avoir également accès à un service de téléphonie IP avec appels illimités vers les téléphones fixes (France + une centaine de pays) et les téléphones mobiles (France uniquement). Le château étant un lieu de passage de gens du monde entier, qui ne disposent généralement pas de forfaits mobiles français, le téléphone fixe illimité du château est particulièrement utile. De plus, la réception téléphonique est très mauvaise pour les mobiles. Enfin, avoir un forfait illimité permet de ne pas avoir à surveiller les usages, qui sont relativement incontrôlables.

**Forfait OVH** La solution utilisée pour reproduire ce service avec la nouvelle connexion à Internet, a été de souscrire à un forfait VoIP chez OVH. L'offre découverte permet d'avoir accès à l'illimité pour les téléphones fixes, tandis qu'une option supplémentaire permet d'avoir également les mobiles français illimités. Contrairement au service qui était fourni avec l'ADSL, ce forfait a l'avantage d'inclure la Suisse dans l'illimité pour les téléphones fixes, ce qui est particulièrement utile pour contacter le propriétaire du château qui vit dans ce pays. La Figure 24 présente le guide d'utilisation cartonné à destination des habitant·es du château, pour les aider à maîtriser les frais téléphoniques.

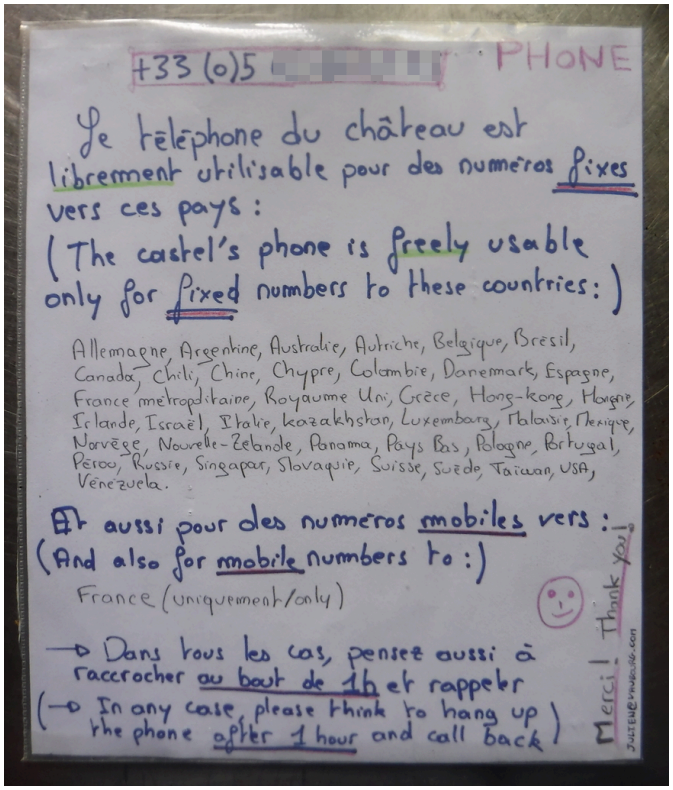



FIGURE 24 – Guide d'utilisation cartonné du téléphone OVH, avec les tarifs par pays et type d'appel.

**Passerelle VoIP** Le matériel utilisé (cf. Figure 25) est un Cisco SPA112, qui est mis à disposition gratuitement contre caution, par OVH. Ce routeur VoIP permet de connecter directement des téléphones standards en RJ11, et donc de réutiliser les téléphones Gigaset qui étaient déjà utilisés auparavant. De plus, OVH livre le matériel préconfiguré : il suffit donc de le relier au réseau en filaire et de brancher les téléphones, pour que le service téléphonique soit opérationnel.

| Illustration | Produit | Description | Nb | Prix TTC x1 | Propriétaire |
|---|---|---|---|---|---|
|  | Forfait OVH SIP Découverte | *Abonnement VoIP pour le téléphone fixe du château*<br><br>Illimités fixes et mobiles / Adaptateur IP Cisco SPA112<br>https://www.ovhtelecom.fr/order/voip/#/legacy/telephony/voip/phones?choice=individual | 1 | 13.19€ / mois + 60€ caution | Château |
|  | Siemens Gigaset A400 Duo | *Téléphones fixes du château*<br><br>Combiné principal (avec répondeur) en RJ11 et secondaire connecté au principal en radio<br>https://boutiquepro.orange.fr/equipements-siemens-gigaset-a400-duo.html | 1 | 40€ | Château (récupération) |

Tableau 25 – Prix TTC pour la téléphonie.

**Numéro de téléphone** Le numéro de la ligne est un numéro de téléphone OVH par défaut. Une fois la ligne activée, il est possible de demander une portabilité du numéro (environ 15 jours), en renseignant le numéro RIO correspondant à la ligne téléphonique de la box ADSL (il suffit d'appeler le 3179 depuis cette ligne pour l'obtenir). Depuis le compte OVH, il est également possible de désactiver la possibilité d'appeler des numéros spéciaux.

### 2.4 Topologie finale

La vue d'ensemble de tous les équipements utilisés ainsi que la façon dont ils sont interconnectés est représentée par le schéma de topologie réseau de la Figure 26. Les notions de Access/Trunk sont expliquées dans la première partie de la section suivante, qui présente la notion de VLAN de management.

## 3 Configuration du matériel

Toutes les configurations et quelques scripts sont regroupés dans les annexes à partir de la page 61. Leur fonctionnement interne est documenté autant que possible directement sous la forme de commentaires, et leur utilisation est présentée ci-dessous. Les références exactes des équipements utilisés ont été listées dans les Figures 17 (WAN page 23), 23 (LAN page 30) et 25 (téléphonie page 32).

### 3.1 Avec VLAN de management... ou non

Le schéma de la topologie du réseau présenté dans la Figure 26 introduit les concepts de Trunk et Access, qui sont liés à la notion de VLAN.

**Principe général** Les VLAN sont de simples identifiants qui servent à marquer (*tagger*) les trames Ethernet, de façon à permettre (principalement) aux switchs de les trier et de les acheminer uniquement à certains de ses ports physiques. En règle générale, un numéro de VLAN (niveau 2) est associé à un réseau IP particulier (niveau 3 – en regroupant dans le même VLAN les réseaux IPv6 et IPv4 qui vont de pair). Lorsqu'un même switch est utilisé pour transmettre les trames de plusieurs réseaux IP différents, les VLAN lui permettent de séparer correctement les domaines de broadcast : ainsi, une machine qui est supposée être sur le réseau A ne recevra pas les trames de broadcast qui concernent le réseau B. Cette étanchéisation a donc principalement pour but d'alléger le trafic sur les liens pour éviter les congestions du réseau, et de résoudre certains problèmes comme les conflits entre serveurs DHCP/NDP.

**Trunk et Access** Le numéro de VLAN d'une trame peut être inscrit et effacé de ses entêtes soit par le port du switch lui-même, soit par l'interface réseau de la machine qui est en face. Si c'est à la charge de la machine en face

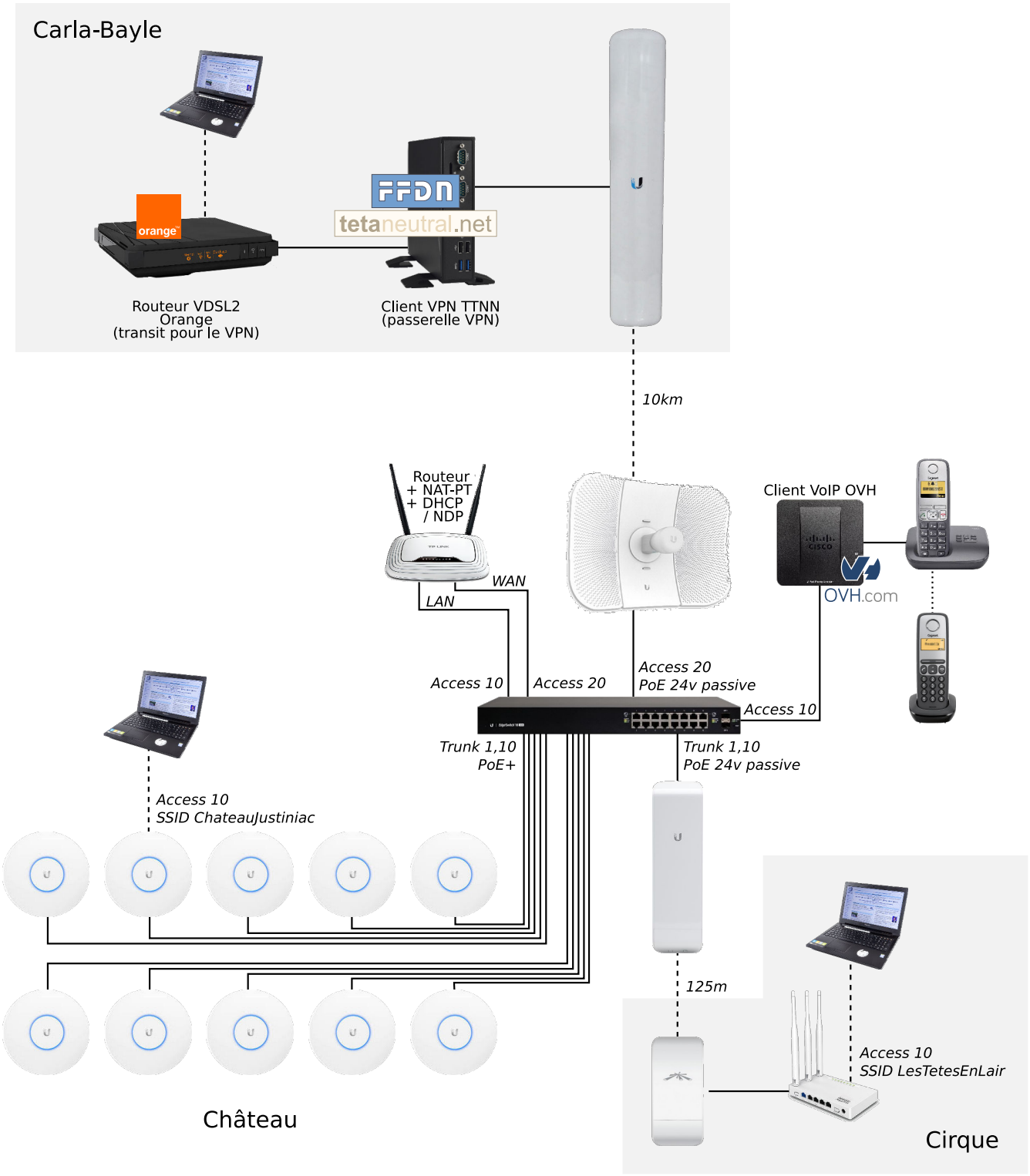



FIGURE 26 – Topologie réseau (les Access/Trunk ne sont utiles que pour la version avec VLAN de management, qui n'a pas été laissée en production – seul le Access 20 subsiste).

de positionner elle-même le numéro de VLAN de ses trames, on parlera d'un lien Trunk [18]. Dans ce cas, le switch se limitera à vérifier si les trames reçues portent bien un des numéros de VLAN présents dans la liste qui a été préconfigurée pour son port, et à éventuellement ajouter un numéro de VLAN par défaut lorsque des trames sans VLAN arrivent (ou simplement les refuser). Les liens Trunk permettent donc d'accepter des trames de différents VLAN sur un même port : ils sont donc particulièrement utilisés pour relier les différents switchs (*backbones*) entre eux, généralement via leurs ports à très haut débit (eg. GBIC/SFP). Dans le cas d'un port physique de switch ou d'une interface réseau configurée en VLAN Access, les trames qui arrivent ne sont pas supposées être déjà marquées par un numéro de VLAN. C'est l'équipement qui reçoit qui marque les trames, avec un numéro de VLAN préconfiguré (le VLAN natif chez Ubiquiti) et qui dépend donc uniquement de comment est reliée la machine cliente à l'équipement (ie. sur quel réseau wifi, ou depuis quel port physique). Les VLAN Access concernent donc généralement plutôt les accès des machines en périphérie du réseau, telles que les ordinateurs/smartphones des clients, serveurs, imprimantes, etc, qui n'ont pas à gérer ces informations elles-mêmes ni même à en avoir connaissance.

**Dans le cadre de la sécurité** En permettant de réduire le volume du trafic parasite à destination et en provenance des machines clientes, les VLAN sont devenus incontournables dans les stratégies de défense en profondeur [19]. Ils ne peuvent effectivement pas prétendre assurer la sécurité du réseau à eux-seuls (ce sont de simples numéros transmis en clair sans aucun contrôle d'authentification ni d'intégrité), mais permettent néanmoins d'ajouter une contrainte supplémentaire dans le cadre d'une éventuelle attaque, tout en gardant le réseau plus propre et donc plus simple à contrôler.

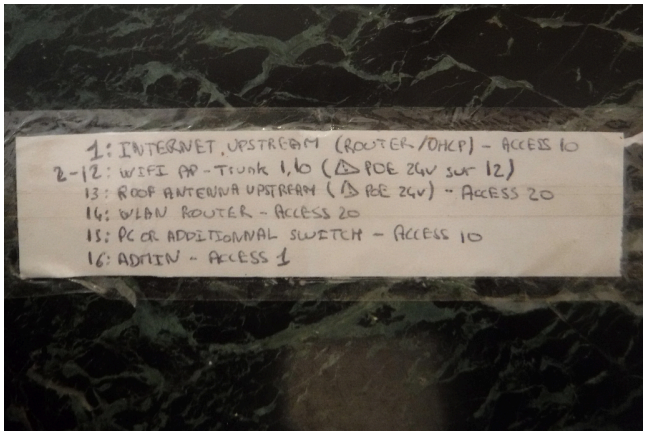
**VLAN de management** L'utilisation d'un VLAN dédié aux opérations de management (VLAN 1 sur le schéma de topologie) est généralement associée aux bonnes pratiques de base lorsqu'on crée un réseau avec plusieurs équipements actifs. L'idée sous-jacente est de ne permettre d'accéder aux interfaces de configuration des équipements actifs (switchs, routeurs, bornes wifi, etc) que depuis un réseau IP spécial, qui n'est pas routé avec les réseaux IP dans lesquels sont placées les machines clientes. Ainsi, un·e attaquant·e qui profiterait d'un accès temporaire au réseau wifi du château, n'aurait pas de possibilité d'accéder directement aux services d'admin proposés sur les équipements actifs (SSH, Telnet, web, SNMP, etc), et donc plus de difficultés pour tester leur niveau de sécurité. Pour permettre aux admins légitimes de travailler, certains ports physiques du switch doivent permettre d'accéder au réseau avec le VLAN de management, ou bien un second réseau wifi sécurisé et non-public doit permettre d'être routé vers le réseau de management. Le contrôle d'accès peut aussi être assuré par la mise en place d'un serveur VPN interne.

**Sécurité versus efficacité** Le réseau du château a dans un premier temps été strictement conçu en implémentant un VLAN de management. Toutefois, comme souvent lorsqu'il s'agit de mesures de sécurité, la mise en place d'un système de VLAN complexifie la compréhension et l'administration du réseau. Dans le futur, la maintenance de ce réseau est supposée être assurée par l'association Tetaneutral.net. Or, durant l'AG FFDN, un membre de l'association a fait remarquer que les bénévoles qui s'occupent des réseaux chez eux ne sont pas formé·es pour utiliser des VLAN, et que la maintenance de ce réseau risque d'être quelque chose de trop différent de ce à quoi illes sont habitué·es.

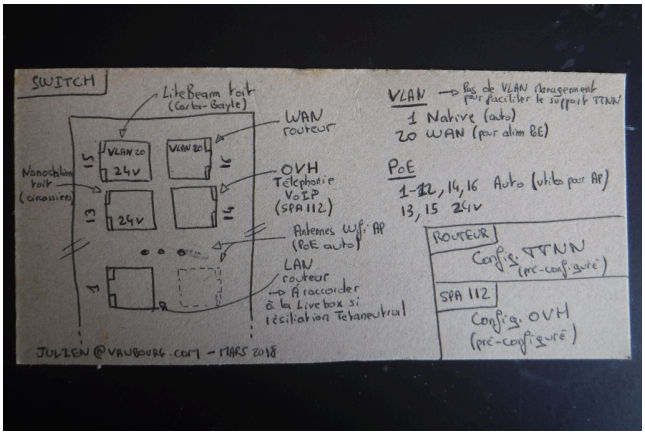
Comme dans toutes associations, le temps des bénévoles est précieux et tout ce qui est mis en place devrait être pensé pour en consommer le moins possible sur le long terme. Bien que l'implémentation du réseau de management dans un VLAN séparé ait demandé du travail supplémentaire, il a été décidé de supprimer tout ce qui avait été mis en place spécifiquement pour son fonctionnement. L'impact de ce recul en matière de sécurité n'est pas suffisamment significatif : sur le principe de l'analyse du modèle de menace [20], un niveau de sécurité supérieur n'est pas nécessaire pour ce réseau, en comparaison avec les conséquences négatives qu'il pourrait avoir à l'avenir sur le bon fonctionnement du service.

18. Bien que ces notions existent chez tous les constructeurs de matériel de réseau informatique, l'appellation Trunk/Access est une invention de Cisco. Chez Ubiquiti ou HP, il serait plus juste de parler de Tagged/Untagged, mais ces appellations sont souvent moins familières. Chez HP par exemple, la notion de Trunk existe malgré tout mais n'a aucun rapport avec les VLAN : il s'agit d'un aggrégat de liens physiques, équivalent à l'EtherChannel de Cisco.
19. https://en.wikipedia.org/wiki/Defense_in_depth_(computing)
20. https://fr.wikipedia.org/wiki/Mod%C3%A8le_de_menace

Les interfaces de management des équipements actifs restent adressées sur des réseaux IP différents de ceux proposés par DHCP/NDP pour les clients, mais sont désormais accessibles depuis n'importe où dans le réseau. Comme illustré dans la Figure 27, l'utilisation des ports du switch devient ainsi beaucoup moins contrainte.




(a) Avant, avec le VLAN de management.




(b) Après, sans le VLAN de management (avec quelques informations supplémentaires).

FIGURE 27 – Étiquettes collées sur le switch en guise de documentation rapide.

**VLAN pour le WAN** La version sans VLAN de management en production équivaut à considérer qu'un VLAN par défaut est utilisé partout. Sur le schéma de topologie de la Figure 26, seul le VLAN 20 persiste dans la version sans VLAN de management, en restant un VLAN différencié. Ce dernier aurait pu être évité en reliant directement l'antenne directionnelle du pont WAN (la parabole) au routeur plutôt que de passer par le switch. Le routeur ne proposant pas de PoE sur ses ports Ethernet, il aurait alors fallu utiliser un adaptateur PoE avec une prise électrique supplémentaire pour alimenter l'antenne. C'est uniquement pour profiter d'un port PoE 24V que le switch a été utilisé dans ce cas, avec un VLAN pour séparer proprement le trafic du WAN (avant le routeur) de celui du LAN (après le routeur).

Les configurations présentées par la suite correspondent au réseau actuellement en production, mais sont (presque) toujours accompagnées de leur version « avec VLAN de management », dans un but purement pédagogique.

## 3.2 Antennes directionnelles

L'utilisation d'équipements Ubiquiti implique une configuration très aisée des antennes, directement depuis leurs interfaces web (les accès SSH sont d'une utilité assez limitée dessus). Le système de ces antennes n'est pas libre (sans possibilité de flashage en OpenWrt), mais leur excellent rapport qualité/prix les ont largement positionnées comme solution préférée de la plupart des associations FFDN, y compris Tetaneutral.net.

**WAN côté Carla-Bayle** Les copies d'écran de la Figure 46 (page 61) permettent de comprendre comment la LiteBeam 120 a été configurée pour créer le pont wifi du WAN côté Carla-Bayle. L'antenne est configurée en *AP PtMP* (Point-to-MultiPoint), de façon à permettre à plusieurs antennes de se connecter dessus. Dans notre cas, il n'y aura que l'antenne directionnelle du château qui se connectera dessus, mais il est possible que ce déploiement serve dans le futur pour fournir un accès à Internet à d'autres maisons qui sont capables de voir le rempart Nord du Carla-Bayle. La connexion est chiffrée en WPA2-AES avec une clée partagée à générer. Au niveau réseau, l'antenne doit être configurée en Bridge et n'a aucune raison de faire du NAT-PT. Son IP de management est fixe, et pour plus de facilité, elle est intégrée au réseau IP de management qu'utilise Tetaneutral.net sur ses autres équipements (routeur

et passerelle VPN – cf. Section 3.4.1). Côté services, le SNMP est configuré de façon à rejoindre la communauté utilisée par Tetaneutral.net pour superviser les équipements réseau dont l'association a la charge.

**WAN côté château** Les copies d'écran de la Figure 47 (page 62) permettent de comprendre comment la LiteBeam a été configurée pour créer le pont wifi du WAN côté château. Cette fois-ci, l'antenne est configurée en *Station PtMP*, de façon à pouvoir se connecter sur l'antenne du Carla-Bayle. Les champs *SSID* et *Clé partagée* doivent strictement correspondre à ce qui a été renseigné sur l'autre antenne. L'antenne est également positionnée en *Bridge*, et son IP de management est dans le même réseau IP que les autres équipements dédiés au WAN. Les deux antennes agissent donc comme des switchs sur le réseau.

**LAN entre le château et le cirque** Les copies d'écran de la Figure 48 (page 63) permettent de comprendre comment les NanoStation ont été configurées pour créer le pont wifi de la section du LAN entre le château et le cirque. Sur le même principe que les antennes du WAN, les deux antennes directionnelles doivent partager le même SSID et la même clé partagée pour le WPA. Cette fois-ci, les antennes ne sont pas en PtMP puisqu'il s'agit d'un pont wifi qui n'a pas vocation à accueillir plus qu'une seule station. Attention pour la version avec VLAN de management : le VLAN numéro 1 n'est pas considéré comme valide par le firmware de l'antenne. Il s'agit plus ou moins d'un bug (rien ne devrait interdire ça), qui est à prendre à considération au moment de choisir le numéro de VLAN de management sur les autres équipements. Comme toutes les antennes, elles sont configurées en mode Bridge, avec cette fois-ci des IP qui appartiennent au réseau IP dédié aux interfaces de management des équipements du LAN.

**Management en IPv4** Les IP de management des antennes sont ici uniquement en IPv4. Bien que quelques fonctionnalités IPv6 soient proposées sur certains matériel Ubiquiti, elles ne sont pas encore suffisamment déployées. Par souci d'homogénéité entre les antennes directionnelles et par souci de cohérence avec la configuration des équipements WAN de Tetaneutral.net, seules les IPv4 sont malheureusement utilisées ici. Un choix différent a été fait pour les bornes wifi à l'intérieur du LAN.

## 3.3 Bornes wifi

### 3.3.1 Choix de OpenWrt

Les bornes wifi sont également de la marque Ubiquiti, pour profiter d'un rapport qualité/prix avantageux. Les UAP-AC-LITE sont vendues environ 350€ TTC en lot de cinq [21] et correspondent au matériel d'entrée de gamme de Ubiquiti pour des antennes omnidirectionnelles. La qualité est néanmoins au rendez-vous, avec toutes les fonctionnalités matérielles modernes qui peuvent être espérées (eg. dual-band, Gigabit, 802.11ac, PoE). Contrairement aux antennes directionnelles, les UAP-AC-LITE peuvent fonctionner avec un firmware libre (flashées en OpenWrt [22]), qui est capable d'exploiter la pleine puissance du matériel (voire même de rendre la borne plus stable [23]).

**Personnalisation du wifi** Utiliser le firmware d'origine des bornes wifi plutôt que OpenWrt aurait permis de bénéficier du confort incontestable du contrôleur UniFi de Ubiquiti. Il aurait été ainsi possible de proposer une interface web ergonomique et pratique aux habitant·es du château, pour leur permettre de personnaliser librement la configuration de leur réseau wifi. En décidant de flasher les bornes en OpenWrt, il est navrant de constater qu'il n'existe pas (jusqu'à preuve du contraire) de contrôleur du même acabit pour changer et pousser la configuration d'une flotte de bornes wifi. Chaque borne doit être configurée manuellement à l'identique, avec le même SSID (nom du réseau wifi), le même mot de passe WPA2, et une IP de management personnalisée. Un simple changement du nom du réseau wifi ou du mot de passe nécessite de passer sur chaque borne, une à une, manuellement ou par l'intermédiaire d'un script.

21. https://www.eurodk.com/en/products/unifi-ac/unifi-ac-lite-5-pack
22. https://openwrt.org/toh/views/toh_available_864?dataflt%5B2%5D=lede%20supported%20current%20rel_%3D17.01.4&dataflt%5B3%5D=device%20type_%3DWiFi%20Router&datasrt=%5Ewlan%205.0ghz
23. https://nicolas314.wordpress.com/2016/05/30/openwrt-on-ubiquiti-ac-lite/

**Robustesse et ouverture** L'absence de contrôleur central peut toutefois permettre de simplifier le réseau. En flashant toutes les bornes en OpenWrt directement avec leur configuration, il devient même possible d'utiliser ensuite le bouton reset des UAP-AC-LITE pour les réinitialiser avec cette configuration. Tous ces équipements totalement indépendants et figés, sans service dynamique de haut niveau à maintenir, rend le réseau très robuste et peu enclin à demander de l'entretien par la suite.

Alors que le nom du réseau wifi « ChateauJustiniac » a peu de raison d'être modifié dans le futur, la nécessité de mise à jour du mot de passe pourrait être plus problématique. La solution qui a été trouvée a le mérite d'être simple : en accord avec le propriétaire, le wifi est disponible uniquement en clair, sans aucune authentification. En plus d'être pratique d'un point de vue technique, cette décision est également politique. Les personnes utilisant le réseau sont invitées à comprendre que le chiffrement du réseau wifi local n'est en rien une garantie de confidentialité de leurs communications (d'autant plus quand le mot de passe est écrit en gros dans la cuisine), et qu'il est nécessaire dans tous les cas pour elles d'utiliser des outils qui proposent un chiffrement de bout-en-bout. Le propriétaire est ravi de la facilité avec laquelle on se connecte sur son réseau, et n'imaginait même pas que ça puisse être possible. La question de l'utilisation éventuellement abusive de la connexion par des voisins ne se pose pas dans ce cas, étant donné l'isolement du château [24].

### 3.3.2 Configuration OpenWrt

La configuration des bornes wifi se résume à quelques fichiers dans le répertoire */etc/config/* du système OpenWrt, ainsi qu'un script personnalisé exécuté à chaque démarrage.

**Interfaces réseau – /etc/config/network** La Configuration 1 (page 64) permet de configurer un simple bridge sur la borne. Cette interface permet de relier les clients wifi au réseau directement au niveau Ethernet. La configuration prévoit également une adresse IPv4 (*10.11.12.13*), désignée comme adresse fallback. Cette adresse est la même sur toutes les bornes wifi, et n'est destinée à être utilisée qu'en cas de secours, en filaire directement avec l'ordinateur d'un·e admin. Lorsque les bornes sont reliées au réseau, il n'est possible de les contacter qu'en IPv6 (cf. explications plus bas). Dans la version avec VLAN de management, cette adresse de fallback est naturellement adressée sur une interface séparée, qui correspond à un VLAN différent. Dans cette configuration il y a deux VLAN en Access (le 1 correspond au réseau de management et le 10 au réseau wifi) et le port physique du switch auquel est relié la borne est configuré en Trunk (avec 1 et 10 dans la liste des VLAN autorisés).

**Diffusion du wifi – /etc/config/wireless** La Configuration 2 (page 64) permet à la borne wifi d'émettre un SSID « ChateauJustiniac ». Les UAP-AC-LITE permettant de faire du dual-band, chaque borne diffuse en réalité deux fois le même SSID, mais sur deux bandes de fréquence différentes (ici *radio0* pour 5 Ghz et *radio1* pour 2.4 Ghz) :

**Fréquences :** Dans le langage Hostapd/MAC80211 (que reprend directement OpenWrt), l'utilisation de 11a comme valeur de *hwmode* signifie une utilisation de la bande 5 Ghz (avec 11g pour le 2.4 Ghz). Dans ces bandes de fréquences (qui sont des intervalles), la fréquence sur laquelle l'antenne doit se positionner est déterminée par l'option *channel*. L'antenne émettra en réalité sur toute une sous-bande de fréquences, qui sera centrée sur ce channel, et dont la largeur est déterminée par l'option *htmode*. Pour proposer du wifi 802.11ac (la norme la plus performante actuellement, qui est supportée par ces bornes), il faut utiliser au minimum une largeur de 80 Mhz, ce qui explique la valeur VHT80 pour radio0 (le 802.11ac ne fonctionne que sur la bande 5 Ghz). Pour la bande 2.4 Ghz, il est possible de choisir une largeur de 20 ou 40 Mhz : la valeur HT20 choisie indique une bande de 20 Mhz, qui permet de laisser la possibilité à de vieux équipements de se connecter sans difficulté, avec plus de canaux disponibles sans superposition (mais avec des débits inférieurs). Le SSID diffusé en 5 Ghz permet donc d'atteindre des débits importants avec des appareils relativement récents, et celui en 2.4 Ghz donne l'assurance que tout le monde peut se connecter au wifi (en 802.11n – ou inférieur – qui est la norme juste avant ac).

24. Les chrétien·nes du coin pourront néanmoins profiter du réseau quand ils s'ennuient à la messe, lorsqu'elle a lieu dans la chapelle qui est attenante au château. Ou bien faire une story snap à la Toussaint en allant loller au cimetière.

**Canaux :** La valeur *auto* pour l'option channel indique que c'est à OpenWrt de choisir automatiquement les canaux à utiliser. Le problème est que OpenWrt n'a pas une implémentation intelligente de cette fonction, puisqu'il semble se contenter de choisir systématiquement le canal 11 en 2.4 Ghz et le canal 36 en 5 Ghz [25], sans se préoccuper du taux actuel d'utilisation de ces canaux. La Figure 28 en est une bonne illustration. Or, il est primordial de faire en sorte de limiter autant que faire se peut le recouvrement des canaux : il ne devrait jamais être possible de capter deux signaux émis par deux bornes différentes, qui utilisent le même numéro de canal. Dans le cas contraire, les deux bornes partageraient alors le débit disponible sur la bande radio, en étant contraintes de se parler en permanence pour s'assurer qu'elles ne transmettent jamais de données simultanément. En réglant la puissance des antennes et en diversifiant les canaux utilisés [26], il est possible de grandement améliorer la qualité des liens wifi, notamment dans le cas où il y a beaucoup d'activité dans le château. Ces réglages, qui doivent se faire borne par borne après les avoir flashées et démarrées, nécessitent une autre étude et un autre plan réseau à réaliser. Cette partie du travail n'est pas encore documentée : elle fera l'objet d'une mise à jour de ce document prochainement [27].

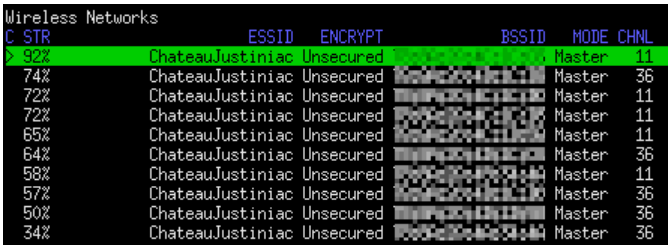



FIGURE 28 – Liste des réseaux wifi disponibles depuis l'entrée du château (avec *wicd-curses*), en laissant l'option *auto* de OpenWrt pour le choix des canaux.

**Clients inactifs :** Les options *disassoc_low_ack* (booléen), *skip_inactivity_poll* (booléen) et *max_inactivity* (secondes) permettent de déconnecter automatiquement tous les clients qui sont soit dans de mauvaises conditions pour communiquer avec la borne (beaucoup d'erreurs détectées dans la communication), soit totalement inactifs (une trame vide est envoyée au bout de 10 secondes pour vérifier leur présence). Le principal intérêt de ces options est de forcer les gestionnaires de réseau des clients à se reconnecter, en choisissant éventuellement une autre borne (avec le même SSID) qui serait dorénavant plus proche d'eux dans le cas où ils seraient mobiles.

**Puissance et distance :** L'option *distance* est supposée indiquer la distance maximale qu'on souhaite qu'il puisse y avoir entre la borne et le client connecté le plus éloigné (en mètres), probablement en supposant qu'il n'y aucun obstacle. L'option *txpower* correspond à la puissance d'émission de l'antenne en dBm (donc indirectement en milliwatts [28]). Les valeurs choisies ici sont simplement inspirées de configurations trouvées sur Internet pour ce type de borne.

**Accès SSH – /etc/config/firewall** Ce fichier a été modifié par rapport à celui d'origine uniquement dans la version du réseau avec VLAN de management. La Configuration 3 (page 65) permet de configurer le pare-feu de façon à ce que l'accès SSH à la borne ne soit possible que depuis le VLAN du réseau de management. Cette limitation aurait dû être supportée par Dropbear lui-même sans avoir à utiliser le pare-feu, en modifiant simplement sa configuration pour qu'il ne fasse écouter le serveur SSH que sur l'interface du VLAN de management. Malheureusement, Dropbear est buggué et n'est plus capable de faire écouter le serveur SSH sur les adresses IPv6 dès lors qu'on lui impose un nom d'interface. La solution avec pare-feu fonctionne, mais elle est légèrement plus lourde, notamment parce qu'il y a nécessité d'activer conntrack pour suivre les sessions [29].

25. D'autres systèmes comme UniFi, qui pourtant utilise un contrôleur central, ne sont pas beaucoup plus intelligents.
26. Choix des canaux : `https://lafibre.info/wifi/quel-canal-wi-fi-choisir-pour-optimiser-son-debit`
27. Mise à jour du 26/11/2019 : je travaille dessus :)
28. `https://www.adriangranados.com/blog/dbm-to-percent-conversion`
29. Ce dernier semble également subir un bug : le OUTPUT en IPv6 doit être positionné à ACCEPT pour laisser sortir les paquets de la session alors que ça n'est pas le cas en IPv4.

**Adresse IP, roaming et lumières – /etc/rc.local** La Configuration 4 (page 66) est un script Bash qui est exécuté à chaque démarrage de la borne wifi. Son principal rôle est de personnaliser la configuration des bornes lors de leur tout premier démarrage, alors que la même image OpenWrt a été déployée sur chacune d'entre elles.

**Fonction *set_management_addr()*** Permet de définir l'adresse IP de management de la borne, qui servira pour se connecter dessus en SSH, ou simplement pour la pinguer pour vérifier si elle est correctement branchée. Les bornes n'ont qu'une seule adresse IP accessible depuis le réseau : une adresse IPv6 de lien local. Pour générer l'adresse de la borne, un « AP ID » est calculé à partir de l'adresse MAC de son interface filaire (elle est hashée en capitales avec MD5 et seules les 4 premiers caractères du hash sont utilisés pour définir l'identifiant). Le AP ID est simplement collé au préfixe *fe80:* : et l'adresse /64 ainsi produite est assignée de façon permanente à l'interface du bridge (ou à l'interface de management dans le cas d'un réseau avec VLAN de management).

**Fonction *set_ap_roaming()*** Permet de définir des options spécifiques au roaming dans la configuration wireless [30] [31]. Grâce à cette configuration, les clients qui supportent le protocole 802.11r pourront passer d'une borne à l'autre sans déconnexion, s'ils sont mobiles dans le château. Pour activer cette fonctionnalité, il est nécessaire que chaque borne connaisse la liste de toutes les adresses MAC (BSSID) de toutes les bornes wifi qui partagent le même nom de wifi (SSID). Cette liste doit donc être écrite en dur dans le script, qui est lui-même compilé dans l'image OpenWrt qui sert à flasher toutes les bornes. Si une borne wifi devait être ajoutée dans le futur, il faudrait donc mettre à jour la liste et reflasher toutes les bornes (ou mettre à jour leur configuration en SSH, avec le risque qu'un reset supprime la nouvelle entrée).

**Fonction *turnoff_leds()*** Permet d'éteindre toutes les lumières produites par la borne, lorsqu'elle est en fonctionnement. Dans le cas du tout premier démarrage de la borne, la borne s'allumera brièvement en bleu (ligne 68) : c'est un repère visuel qui permet de savoir que le script a fonctionné et que la configuration du premier démarrage a bien été appliquée.

### 3.3.3 Image OpenWrt

Afin de flasher directement les bornes wifi avec les fichiers et scripts personnalisés, il est possible de compiler une image OpenWrt sur-mesure qui les intègre par défaut.

**Container** L'usage d'un container pour la compilation d'une image OpenWrt n'est pas nécessaire, mais permet simplement de garder l'ordinateur de l'admin propre, sans logiciels ou bibliothèque qui ne seraient utiles que pour cet usage spécifique. Un simple container LXC avec une Debian Stable est suffisant :

```
$ sudo lxc-create -n openwrt -t debian
$ sudo lxc-start -n openwrt
```

**Image Builder** Le projet OpenWrt (qui a récemment fusionné avec le projet LEDE, qui était autrefois un fork) met à disposition un Image Builder, qui est un simple dossier avec tous les scripts et fichiers nécessaires pour construire une image OpenWrt complète depuis ses sources. Il est disponible dans le dépôt officiel *ar71xx*, correspondant à l'architecture matérielle des UAP-AC-LITE [32] :

```
$ cd /var/lib/lxc/openwrt/rootfs/root/
$ wget https://downloads.lede-project.org/releases/17.01.4/targets/ar71xx/generic/\
lede-imagebuilder-17.01.4-ar71xx-generic.Linux-x86_64.tar.xz
$ tar xf lede-imagebuilder-*.tar.gz
```

30. https://www.reddit.com/r/openwrt/comments/515oea/finally_got_80211r_roaming_working/
31. https://gist.github.com/lg/998d3e908d547bd9972a6bb604df377b
32. https://downloads.openwrt.org/snapshots/targets/ar71xx/generic/

**Environnement de compilation** Une fois les outils de compilation installés dans le container, il reste à importer tous les fichiers de configuration et scripts personnalisés dans l'environnement de compilation, et à compiler en une seule ligne de commande.

Installer les outils et bibliothèques pour la compilation :

```
$ sudo lxc-attach -n openwrt
LXC# apt-get install build-essential libncurses5-dev zlib1g-dev gawk git gettext \
  libssl-dev xsltproc wget unzip python
```

Copier les fichiers de configuration de la Section 3.3.2 dans un répertoire *files/* à la racine du dossier de l'Image Builder, de façon à obtenir :

```
LXC# cd /root/lede-imagebuilder-17.01.4-ar71xx-generic.Linux-x86_64/
LXC# find files/ -type f -exec stat -c '%n (%a)' {} \;
files/etc/rc.local (644)
files/etc/shadow (600)
files/etc/config/network (644)
files/etc/config/wireless (644)
files/etc/dropbear/authorized_keys (600)
```

Comme illustré par le résultat de la commande *find* dans le code précédent, les fichiers doivent être rangés dans le dossier *files/* comme s'ils étaient à la racine du système OpenWrt, avec les sous-dossiers correspondants (en respectant les droits des fichiers tels qu'ils sont précisés entre parenthèses).

Les deux fichiers qui ne sont pas fournis dans la Section 3.3.2 (*shadow* et *authorized_keys*) servent à définir le mot de passe root des bornes et les clés SSH qui pourront se connecter en root. Les autres utilisateurs Unix référencés par défaut sur OpenWrt sont :

```
# cat /etc/shadow
root:<ROOT_HASH>:17611:0:99999:7:::
daemon:*:0:0:99999:7:::
ftp:*:0:0:99999:7:::
network:*:0:0:99999:7:::
nobody:*:0:0:99999:7:::
dnsmasq:x:0:0:99999:7:::
```

**Compilation** Pour compiler l'image personnalisée[33], il suffit de préciser le type de matériel qui sera utilisé (*PROFILE*), les fichiers personnalisés à ajouter ou remplacer (*FILES*) et une liste relative de paquets à installer ou désinstaller (si le nom du paquet est préfixé par un symbole moins, alors il est supprimé de la configuration OpenWrt par défaut, sinon il est ajouté) :

```
LXC# cd /root/lede-imagebuilder-17.01.4-ar71xx-generic.Linux-x86_64/
LXC# make image PROFILE=ubnt-unifiac-lite FILES=files/ PACKAGES='-ppp \
  -ppp-mod-pppoe -dnsmasq -odhcpd -odhcp6c -firewall -kmod-ipt-nat \
  -kmod-nf-nat -iptables -ip6tables -kmod-ip6tables -kmod-ipt-conntrack \
  -kmod-nf-ipt6 -kmod-nf-conntrack6 -kmod-nf-conntrack -wpad-mini wpad' \
  EXTRA_IMAGE_NAME=justiniac
```

33. Documentation : https://openwrt.org/docs/guide-user/additional-software/imagebuilder

Dans cette commande de compilation, un maximum de paquets OpenWrt installés par défaut sont supprimés, pour alléger au maximum le système de la borne (bien que cet effort n'ait probablement pas un impact très significatif sur ses performances finales). Le paquet *wpad-mini* est remplacé par *wpad* pour profiter du support du 802.11r (ie. le roaming – cf. fichier */etc/rc.local* de la Section 3.3.2). Pour connaître la liste des paquets installés par défaut, une solution simple est de démarrer sur une image OpenWrt standard (un lien est proposé dans la section suivante) et d'exécuter :

```
# opkg list-installed | awk '{print $1}' | sed ':M;N;$!bM;s#\n# #g'
```

Dans le cas d'un réseau avec VLAN de management, plus de paquets sont nécessaires sur les bornes, notamment à cause de l'utilisation du pare-feu :

```
LXC# make image PROFILE=ubnt-unifiac-lite FILES=files/ PACKAGES='-ppp \
  -ppp-mod-pppoe -dnsmasq -odhcpd -odhcp6c -wpad-mini wpad' \
  EXTRA_IMAGE_NAME=justiniac
```

Si la compilation ne rencontre pas de problème, l'image personnalisée est générée dans son répertoire d'architecture :

```
3.2M    /var/lib/lxc/openwrt/rootfs/root/lede-imagebuilder-17.01.4-ar71xx-gene
ric.Linux-x86_64/bin/targets/ar71xx/generic/lede-17.01.4-justiniac-ar71xx-gene
ric-ubnt-unifiac-lite-squashfs-sysupgrade.bin
```

Elle peut désormais être directement installée comme mise à jour UniFi ou OpenWrt, sur des bornes UAP-AC-LITE.

### 3.3.4 Installation de OpenWrt

**Script maison** Cette section suppose l'utilisation du script disponible dans la Configuration 5 (page 67). Pour l'utiliser, il est nécessaire de mettre à jour les constantes *DEV_WIFI* et *DEV_WIRE* en tête du script, avec le nom des interfaces réseau wifi et filaire de l'ordinateur de l'admin.

**Signature RSA** Depuis la version 3.4.14 du système UniFi, Ubiquiti protège ces équipements contre l'installation de firmwares tiers [34]. Il devient donc impossible d'installer une version de OpenWrt qui n'intègre pas une signature RSA produite par Ubiquiti. La première chose à faire est donc de downgrader la version de UniFi, pour revenir à une version qui autorisait encore d'installer une nouvelle version du firmware sans signature valide. Ces versions ne sont plus trouvables sur le site officiel [35] et nécessitent donc d'être téléchargées depuis un serveur tiers [36].

Le chemin local vers le fichier du firmware UniFi qui servira au downgrade est à renseigner dans la constante *PATH_FW_UNIFI* en tête du script. La borne doit être branchée directement en filaire à l'ordinateur de l'admin. Son adresse IPv6 de lien local sera automatiquement détectée par *scan6*, et utilisée pour la liaison SSH. Il est préférable de faire d'abord un reset physique de la borne (au trombone, jusqu'à ce qu'elle s'allume en bleu puis clignote rapidement en blanc), si elle n'est pas neuve.

Downgrader la version UniFi de la borne :

```
$ ./flash_uap.sh unifi-unifi
```

34. https://blog.cavebeat.org/2018/01/install-openwrt-lede-17-01-4-on-ubiquiti-uap-ac-lite/
35. https://www.ubnt.com/download/unifi
36. Firmware UniFi v3.4.7 : https://julien.vaubourg.com/pro/fw-unifi-3.4.7.bin

**Passage à OpenWrt** Avant de procéder à l'installation, il est préférable de vérifier que la version active de UniFi est bien celle qui est suffisamment ancienne pour pouvoir installer OpenWrt par-dessus. Il suffit se connecter en SSH sur la borne avec l'IP *192.168.1.20* (ou l'IPv6 qui apparaît dans la trace du script précédent) et les identifiants ubnt/ubnt. Selon la version installée, vous devriez obtenir un prompt du type *BZ.v3.4.7#* avec une version inférieure à 3.4.14.

Le chemin local vers le fichier du firmware OpenWrt qui servira à l'installation est à renseigner dans la constante *PATH_FW_OPENWRT*. Il est préférable d'utiliser une version non-personnalisée de OpenWrt pour cette première installation, pour ne pas risquer de confondre un échec du flashage avec une erreur dans un script de démarrage. Une image OpenWrt standard compatible avec les bornes UAP-AC-LITE est disponible dans les dépôts officiels [37] [38].

Installer OpenWrt pour la première fois sur la borne :

```
$ ./flash_uap.sh unifi-openwrt
```

**Version personnalisée** Pour vérifier que OpenWrt a bien été installé sur la borne, il suffit de se connecter en SSH avec l'IP *192.168.1.1* (ou l'IPv6 de lien local) et l'utilisateur root (sans mot de passe). Il est déconseillé de flasher une borne avec une image qui contient des fichiers personnalisés, sans les avoir testés avant en les poussant en SSH sur un OpenWrt déjà installé. En effet, si une erreur de configuration ou un script défaillant empêche de se connecter en SSH après une nouvelle installation, il n'y a pas de solution pour revenir en arrière, puisqu'un reset physique au trombone réinitialisera toujours la dernière image installée (la borne devra alors être renvoyée chez Ubiquiti, s'ils acceptent de faire fonctionner la garantie).

Le chemin local vers le fichier du firmware OpenWrt personnalisé qui servira à l'installation est à renseigner dans la constante *PATH_FW_OPENWRT*.

Mettre à jour OpenWrt avec une image personnalisée :

```
$ ./flash_uap.sh openwrt-openwrt
```

Pour l'installation sur les autres bornes, une fois les fichiers personnalisés testés, la commande *unifi-openwrt* peut directement être utilisée avec l'image personnalisée.

**Premier démarrage personnalisé** Comme indiqué dans la Section 3.3.2, la borne est supposée s'allumer brièvement en bleu lors de son premier démarrage, avant l'extinction de toutes les lumières. Cette étape permet de valider que le script personnalisé de démarrage a bien été exécuté. Dès lors, il est possible de contacter la borne en utilisant son adresse IPv6 de lien local avec son AP ID. Lors de la mise à jour du firmware UniFi, le script a inscrit l'adresse MAC de la borne avec son AP ID (4 caractères hexadécimaux) à la fin du fichier */tmp/ap_macs* (constante *PATH_AP_MACS*), sur l'ordinateur de l'admin. Il faut penser à récupérer ce fichier, après avoir flashé toutes les bornes à la suite.

Pour vérifier l'installation de l'image OpenWrt personnalisée :

```
$ ./flash_uap.sh ping <AP_ID>
```

Pour se connecter en SSH sur la borne (root sans mot de passe) :

```
$ ./flash_uap.sh sshwired <AP_ID>
```

37. https://pwassi.privatedns.org/openwrt/unifiac/
38. https://downloads.openwrt.org/snapshots/targets/ar71xx/generic/ > ubnt-unifiac-lite-squashfs-sysupgrade.bin

### 3.3.5 Personnalisation esthétique

Les UAP-AC-LITE sont livrées avec le gros U de Ubiquiti imprimé au centre de la borne.

Le logo n'est pas très esthétique (d'autant plus quand la borne n'est pas dans le bon sens), et il n'y a pas de raison d'afficher la pub d'une entreprise un peu partout dans le château. Pour cette raison, une trentaine de stickers ont été imprimés au diamètre 57 mm de façon à intégralement recouvrir le rond central des bornes. Le graphisme a été réalisé avec Inkscape [39] et les stickers ont été imprimés à la PAO de l'Université de Lorraine en qualité vinyle pour l'extérieur. Le sticker est visible à différents endroits du réseau, comme illustré par la Figure 29.

Comme expliqué dans la Section 3.3.2, les lumières autour de l'anneau central ont été désactivées logiciellement. Ce choix a été fait autant pour éviter les nuisances lumineuses dans le château que pour éviter de paniquer les personnes qui pourraient être suspicieuses vis-à-vis des ondes. Pour ces mêmes personnes, le graphisme retenu ne représente aucune onde autour du château dessiné, bien qu'il soit clairement écrit qu'il s'agit de wifi.

Le château est représenté de façon simpliste depuis le côté Sud, avec la terrasse stylisée en un seul trait rouge, avec la porte d'entrée au centre. La terre qui surplombe le château est censée représenter la possibilité de communiquer avec le monde entier, bien que des retours aient montré qu'il y avait une incompréhension du pourquoi l'Europe est présente sur le logo... La symbolique du sticker n'est donc pas totalement maîtrisée, mais les témoignages précisent aussi qu'il a au moins le mérite de pouvoir être réutilisable le jour où le château souhaitera commercialiser des bouteilles de vin.

## 3.4 Routage et switching

Les adresses IP ont été anonymisées avec des *X*, parfois remplacés par des *Y* lorsque l'anonymisation rend deux adresses malencontreusement identiques.

### 3.4.1 Routeur du château

Le routeur du château est fourni préconfiguré par Tetaneutral.net, qui en garde la propriété. Il s'agit d'un TP-Link TL-WR841ND qui inclus un switch Ethernet de quatre ports, un port Ethernet supplémentaire et deux antennes wifi. Il a la particularité de pouvoir être flashé en OpenWrt et est à ce titre équipé d'un système LEDE Reboot.

Le wifi a été désactivé pour ce déploiement, et le switch intégré est utilisé uniquement pour relier le routeur au switch principal du château. Le fichier */etc/config/network* utilisé par OpenWrt pour le paramétrer est disponible dans la Configuration 6 (page 68).

D'un point de vue configuration IP, seules deux interfaces sont utilisées :

**Interface br-lan :** Il s'agit d'une interface virtuelle qui permet d'utiliser l'interface physique du switch intégré (*eth0*) comme un bridge. Ainsi, un paquet envoyé via cette interface sera envoyé sur le bon port du switch, en fonction de l'algorithme de son driver. Dans notre cas, il n'y qu'un seul câble branché entre l'un des ports de ce switch intégré et le port « upstream » du switch principal du château. Cette interface dispose de deux IP : la première IPv6 (*2a03:XXXX:XXXX:XX01::1/64*) du range public dédié au château (/56) utilisé par le NDP pour attribuer des IPv6 aux machines du LAN, ainsi que la première IPv4 (*192.168.XXX.XXX.1/24*) du range privé utilisé par le DHCP pour attribuer des IPv4 aux machines du LAN.

**Interface eth1 :** Il s'agit du port Ethernet isolé sur le routeur, qui sert à connecter le WAN. Dans notre cas, c'est l'antenne directionnelle qui pointe vers le Carla-Bayle (et donc indirectement la passerelle VPN) qui est reliée à ce port (en réalité via le switch principal du château pour bénéficier du PoE, comme expliqué dans la Section 3.1). Cette interface dispose principalement de trois IP : une IPv6 d'interconnexion (*2a03:XXXX:XXXX:XX00::1/56*) [40] du range public dédié au château (/56), une IPv6 de lien local imposée (*fe80::XXXX*/64) ainsi que la seule et unique IPv4 publique dédiée au château (*89.XXX.XXX.XXX/32*).

39. Fichier source : `https://julien.vaubourg.com/justiniac/sticker.svg`

40. Tetaneutral.net a fait le choix de l'adresser dans un /56 qui contient le /64 du sous-range IPv6 utilisé par le NDP sur le LAN, sans pour autant utiliser des IP du même /64 (*XX00* vs *XX01*). Cette configuration fonctionne parce que le sytème utilisera toujours la route la plus spécifique, mais il aurait été plus propre de réduire le scope de l'IP d'interconnexion au /64 plutôt que /56.


(a) Sticker « ChateauJustiniac », destiné à recouvrir le logo Ubiquiti des bornes UAP-AC-LITE.

(b) Borne wifi du château.

(c) Sur le switch central.

(d) Sur l'antenne du cirque.

(e) Sur le mât des câbles du grenier.

(f) Les stickers restants ont été distribués à des proches du château en tant que collectors.

FIGURE 29 – Sticker « ChateauJustiniac » pour les bornes wifi et autres emplacements.

Ensuite, seules les routes par défaut ont besoin d'être configurées :

**Routes IPv6 :** Route par défaut vers une IPv6 de lien local imposée (*fe80::YYYY*/64 au travers de *eth1*) attribuée à la passerelle VPN.

**Routes IPv4 :** Route par défaut vers une IPv4 publique attribuée à la passerelle VPN (*91.XXX.XXX.XXX/32*).

**Goulot d'étranglement** La puissance du TP-Link semble limitée, et est probablement responsable d'une limitation du débit maximum qu'il est possible d'atteindre sur le réseau wifi en aval. Remplacer ce routeur avec un matériel plus puissant dans le futur pourrait être approprié.

La compréhension de la configuration IP de la passerelle VPN présentée ci-dessous permet de mieux comprendre l'utilité des différentes IP du routeur.

### 3.4.2 Passerelle VPN

Le Shuttle utilisé pour la passerelle VPN est un simple ordinateur qui accueille une Debian Stable. Conformément aux habitudes de Tetaneutral.net, toute la configuration réseau est écrite dans le fichier */etc/rc.local*, dont les commandes sont exécutées en root au démarrage. Cette façon de faire permet de rapidement interchanger les machines en n'ayant qu'un seul fichier à recopier, et d'éviter les nombreux bugs ou incohérences du fichier */etc/-network/interfaces* qui est d'ordinaire utilisé pour configurer les interfaces réseau.

Le fichier */etc/rc.local* utilisé sur la passerelle VPN est disponible dans la Configuration 7 (page 69). Le fichier a été commenté dans le cadre de cette documentation, et son fonctionnement est résumé ci-dessous de façon plus littéraire.

Parmi les interfaces réseau disponibles, celles qui sont utiles sont :

— **Interface eth0 :** Il s'agit du port Ethernet physique sur lequel est branché la box Internet de l'appartement du Carla-Bayle. Sa seule IP est donc une IPv4 privée (*192.168.YYY.YYY/24*) attribuée en DHCP par la Livebox (qui ne semble pas proposer d'IPv6 et impose donc un montage du VPN en IPv4).

— **Interface eth1 :** Il s'agit du second port Ethernet physique du Shuttle, sur lequel est branché l'antenne directionnelle du Carla-Bayle, qui pointe directement sur celle du château. Cette interface dispose de beaucoup d'IP : une IPv6 de lien local imposée (*fe80::YYYY/64*, qui correspond à la route par défaut du routeur), une IPv4 privée (*172.XXX.XXX.1/24*) du même range que les deux antennes directionnelles (le routeur VPN chez Tetaneural.net possède aussi une IP de ce range, pour avoir accès aux interfaces de gestion des antennes à distance via le VPN, eg. pour les échanges SNMP pour la supervision), ainsi que deux adresses IPv4 publiques (*89.YYY.YYY.YYY/32* et *91.XXX.XXX.XXX/32*) dont l'une des deux sert de route par défaut pour le routeur du château.
Ces deux adresses IPv4 sont publiques et appartiennent à Tetaneutral.net mais ne sont pas uniques sur Internet : l'association les utilise sur toutes les passerelles VPN déployées sur leur réseau, de façon à pouvoir faire pointer l'antenne directionnelle d'une maison vers n'importe quel déploiement (et donc n'importe quelle passerelle VPN) sans avoir à s'inquiéter de la configuration du routeur. C'est une façon de faire qui fonctionne parce que les IP ne sont utilisées que pour faire de l'interconnexion locale, mais il aurait été plus propre de choisir des IPv4 privées qui sont prévues à cet effet. L'une des deux IPv4 n'est pas utilisée dans ce déploiement, et devrait à terme disparaître de toutes les passerelles VPN de l'association.

— **Interface tuncar :** Il s'agit de l'interface virtuelle créée par le client VPN qui tourne sur la passerelle. L'interface ne dispose que d'une seule IPv4 privée (*10.XXX.XXX.2/24*) qui est utilisée pour faire le pont entre le client VPN et le routeur VPN, au travers du tunnel, installé sur un serveur Tetaneutral.net.

**Routes** D'un point de vue routes, la particularité de cette configuration est d'utiliser une table de routage virtuelle (numéro 25 dans la configuration, mais c'est un choix totalement arbitraire). L'utilisation d'une table de routage virtuelle suppose l'utilisation de rules qui forcent le noyau à consulter cette table de routage plutôt que celle par défaut, selon la provenance ou la destination du paquet traité.

Globalement, tout ce qui est supposé passer via le tunnel VPN doit utiliser la table de routage virtuelle, tandis que tout ce qui doit passer directement par la Livebox (ie. uniquement les paquets encapsulés du tunnel VPN lui-même) doit utiliser la table de routage par défaut.

Ainsi, la table de routage par défaut ne contient logiquement que la route IPv4 par défaut récupérée par le DHCP de la Livebox (vers *192.168.YYY.1*). Dans la table virtuelle, en IPv6 comme en IPv4, une route par défaut indique de passer directement par l'interface *tuncar* du tunnel VPN (sans IP de prochain saut précisée, ce qui est logiquement souvent le cas avec un tunnel de type TUN). Les routes définies dans la table virtuelle sont :

**IPv6 :** Le range IPv6 *2a03:XXXX:XXXX:XXXX::/56* dédié au château est accessible via l'adresse de lien local du routeur (*fe80::XXXX*/64 au travers de *eth1*). Une adresse de prochain saut est précisée explicitement (plutôt que d'indiquer uniquement de passer par *eth1*) parce qu'il n'est pas possible de savoir si les adresses sont directement accessibles par le lien ou non (le range pourrait être ensuite découpé côté château et donner lieu à du routage en plusieurs sauts).

**IPv4 :** Les IPv4 privées du range des adresses des interfaces de management des antennes (*172.XXX.XXX.0/24*) sont accessibles directement via *eth1* (ie. l'antenne directionnelle, sans IP de prochain saut précisée parce qu'il n'y a pas d'autre intermédiaire [41]). La seule et unique adresse IPv4 publique dédiée au château fait également l'objet d'une route, directement par *eth1* (il n'y a pas de prochain saut, puisqu'on sait que c'est directement au routeur du château qu'elle sera adressée, et qu'il utilisera obligatoirement de la réécriture d'adresses avec du NAT-PT pour adresser les machines clientes sur son réseau).

**Accès à distance** Pour pouvoir dépanner le réseau du château y compris lorsque le tunnel VPN est tombé, il est nécessaire de pouvoir accéder au routeur via le Shuttle de la passerelle VPN. L'adresse IP privée de la passerelle VPN sur le réseau de la Livebox (*192.168.YYY.YYY/24*) doit être fixée manuellement via la Livebox, et une redirection de port pour le port SSH de la passerelle VPN doit être mise en place pour cette IP. Puisque Orange utilise des IPv4 dynamiques, un client de type DynDns (paquet *ddclient*) doit être installé sur la passerelle VPN. Un simple sous-domaine chez OVH permet d'obtenir gratuitement un accès DynHost, utilisable par DDclient, dont la configuration sera alors (*/etc/ddclient.conf*) :

```
protocol=dyndns2
use=web, web=checkip.dyndns.com
server=www.ovh.com
login=<OVH_DYNHOST_ID>
password=<OVH_DYNHOST_PWD>
<OVH_DOMAIN>
```

Pour accéder au routeur de l'extérieur, le client SSH peut alors utiliser la configuration suivante (le paquet *netcat-openbsd* doit être installé sur la passerelle VPN pour pouvoir utiliser *nc* avec une adresse IPv6) :

```
Host justiniac-shuttle
  HostName <OVH_DOMAIN>
  port <PORT_SHUTTLE>
  ForwardAgent yes
  User root

Host justiniac-router
  Hostname fe80::XXXX%%eth1
  port <PORT_ROUTER>
  ForwardAgent yes
  User root
  ProxyCommand ssh justiniac-shuttle nc %h %p
```

**Redémarrages** Le BIOS peut être configuré pour que la machine démarre automatiquement lorsque son alimentation a été coupée brutalement. Il suffit pour cela de choisir l'option *Power On* dans le menu *Power-On after Power-Fail* de la section *Advanced*. Cette option est utile pour ne pas avoir à intervenir en cas de coupure électrique dans l'appartement.

### 3.4.3 Switch principal

Le seul et unique switch du château est un EdgeSwitch Ubiquiti de 16 ports, qui utilise son système d'origine (il ne peut pas être flashé en OpenWrt) sans toutefois utiliser les fonctionnalités propres à Ubiquiti. Sa configuration est relativement basique, en particulier dans sa version sans VLAN de management.

41. La route vers le réseau *172.XXX.XXX.0/24* qui a été calculée par le noyau quand l'adresse *172.XXX.XXX.1/24* a été définie pour *eth1* a été ajoutée dans la table de routage par défaut, et non dans la table virtuelle, ce pourquoi il est nécessaire de la préciser manuellement ici.

**Mise à jour** La première chose à faire est de mettre à jour le système de l'EdgeSwitch. Le plus simple pour cela est de suivre la documentation Ubiquiti [42], qui explique où télécharger le firmware et comment l'uploader manuellement via l'interface web du switch. Pour accéder à l'interface web, il faut contacter le switch à l'adresse *192.168.1.2* et utiliser les identifiants ubnt/ubnt.

**Changement d'IPv4** Une fois la mise à jour terminée, il est nécessaire de changer l'IPv4 par défaut. Pour cela, aller dans le menu *System > Connectivity > IPv4* de sélectionner *None* pour l'option *Network Configuration Protocol*, afin d'interdire au switch de récupérer une IPv4 par DHCP. Une IP fixe de type *10.YYY.YYY.1/24* peut alors être définie. Cette IP sert simplement de backup IPv4, puisque l'IPv6 de lien local automatiquement générée permet par défaut d'accéder à l'administration SSH sans configuration supplémentaire.

**Activation SSH** La dernière chose à faire via l'interface web est d'activer SSH, afin de pouvoir ensuite la désactiver. Aller dans le menu *System > Management Access > SSH* et cliquer sur la petite roue à droite de RSA/DSA, afin de générer la clé SSH privée du switch. Passer l'option *SSH Admin Mode* à *Enable* et en profiter pour décocher *SSH Version 1*. Tous les changements de configuration peuvent maintenant être appliqués en cliquant sur le bouton *Save Configuration* en haut à droite.

**Mot de passe** Il est désormais possible de se connecter en SSH pour changer le mot de passe de l'utilisateur ubnt : *ssh ubnt@10.YYY.YYY.1*. Utiliser simplement la commande *password* dans le prompt proposé [43], pour pouvoir ensuite saisir le mot de passe actuel (ubnt) et le nouveau mot de passe. Il est désormais possible de désactiver l'administration par HTTP et Telnet, pour se concentrer uniquement sur la CLI via SSH :

```
(UBNT EdgeSwitch) >enable
(UBNT EdgeSwitch) #no ip http server
(UBNT EdgeSwitch) #no ip telnet server enable
(UBNT EdgeSwitch) #write memory
```

**Configuration des ports** Les Configurations 8 et 9 (page 70) permettent de comprendre comment le switch a été configuré. Conformément à ce qui a été dit auparavant dans ce document, tous les ports utilisent le VLAN par défaut, à l'exception des ports 15 et 16 qui utilisent un VLAN différencié. Ces deux ports permettent d'isoler un « mini-switch » qui sert uniquement à relier l'antenne directionnelle du toit (vers le Carla-Bayle) avec le routeur du château, en profitant de l'alimentation de l'antenne par le PoE du switch (*passive24v*). Le port 13 est également alimenté en PoE 24V pour alimenter l'antenne directionnelle du toit qui pointe vers le cirque, mais qui rejoint directement le LAN. Les autres ports détectent par défaut automatiquement si le PoE+ (802.3af/at) est nécessaire ou non, pour alimenter les bornes wifi. Les Configurations 10 et 11 (page 71) permettent de comprendre la configuration du switch dans sa version avec VLAN de management (VLAN 1 – cf. topologie de la Figure 26 page 33 pour visualiser les différents VLAN).

### 3.4.4 Borne wifi du cirque

La borne wifi du cirque est un modem-routeur-wifi configuré en simple bridge wifi, pour émettre le réseau « LesTetesEnLair » permettant aux occupant·es des caravanes de se connecter directement au LAN du château, de façon à pouvoir bénéficier de la connexion à Internet. Il ne peut pas être flashé en OpenWrt. Une autre borne UAP-AC-LITE avec un adaptateur PoE aurait été plus appropriée, mais le budget pour cette partie du LAN n'a pas été prévu dans le déploiement initial.

**Configuration** Le passage en mode bridge peut se faire via l'interface web, dans le menu *Network > Operation Mode*, où l'adresse IPv4 d'administration peut aussi être changée. Le SSID peut être modifié via les menus *Wireless 2.4G/5G*.

42. https://help.ubnt.com/hc/en-us/articles/219467028-EdgeSwitch-Firmware-Upgrade-#1
43. Documentation CLI : https://dl.ubnt.com/guides/edgemax/EdgeSwitch_CLI_Command_Reference_UG.pdf

**Faux contact** Le câble électrique souffre d'un faux contact. Il serait donc approprié dans le futur de remplacer ce matériel, par exemple par un simple TP-Link flashé en OpenWrt.

## 3.5 Vue d'ensemble IP

La Figure 30 propose une vue d'ensemble de la configuration IP des principaux équipements. La route par défaut en IPv6 du PC correspond à l'adresse de lien local automatiquement générée pour l'interface *br-lan* du routeur (conformément aux spécifications de NDP [44]).

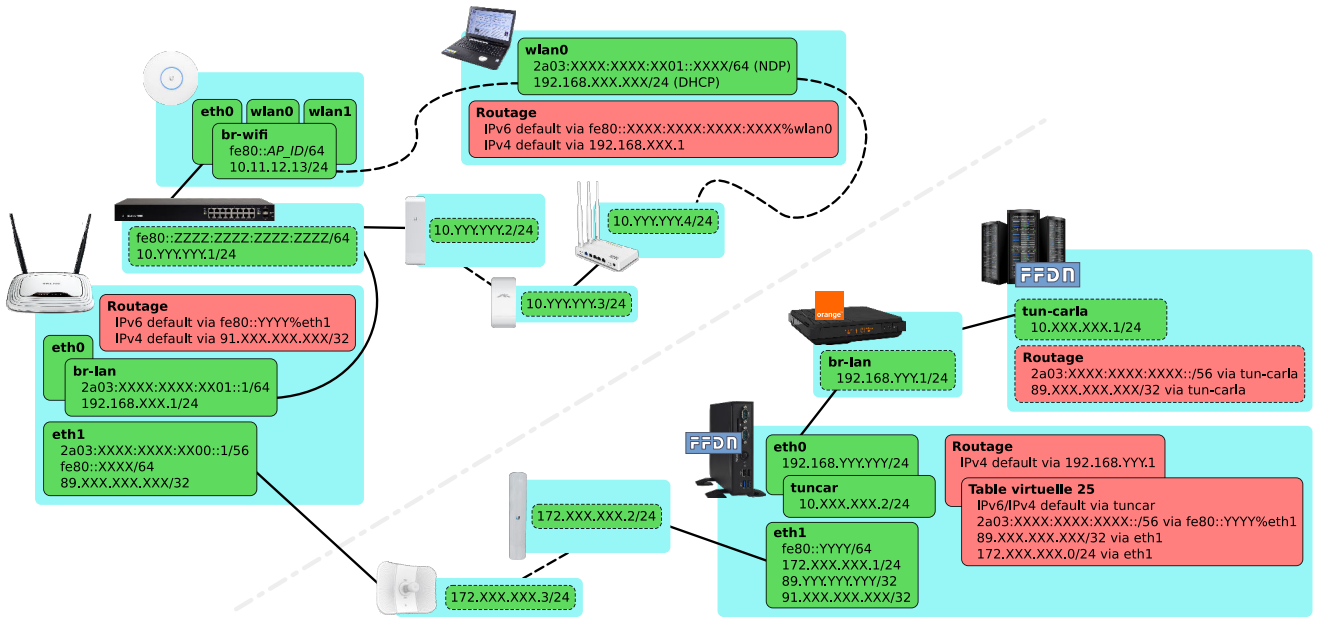



FIGURE 30 – Configuration IP des principaux équipements. Les routes et IP générées automatiquement par le noyau sont ignorées (sauf l'IPv6 de lien local du switch qui est utilisée pour y accéder en SSH), et les boîtes en pointillés sont potentiellement incomplètes.

# 4 Conclusion

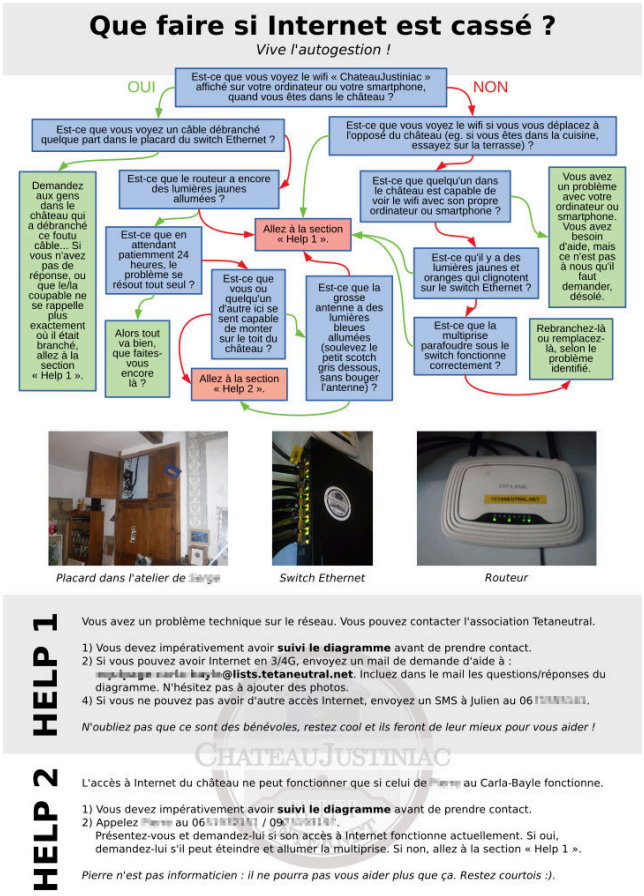
Le Château de Justiniac bénéficie désormais du meilleur accès à Internet de ses environs, avec des débits qui ne sont pas très éloignés de ce que proposent certains abonnements fibrés.

Son accès offre également beaucoup plus de garanties en matière de respect de la vie privée et de la Neutralité du Net, tout en supportant financièrement une association militante de Toulouse. Financièrement parlant, le château paie moins cher qu'avant pour son accès à Internet (y compris en incluant le coût de la ligne VoIP illimitée), pour un meilleur débit, une meilleure éthique et un support plus humain. Le locataire de l'appartement du Carla-Bayle s'y retrouve également, puisqu'il dispose désormais du meilleur accès à Internet qu'il peut avoir, tout en payant moins cher que pour l'accès qu'il utilisait auparavant. Enfin, l'association Tetaneutral.net elle-même ne perd pas d'argent, et commencera à en gagner sur ce déploiement dès lors qu'une autre maison sera connectée à l'antenne du Carla-Bayle.

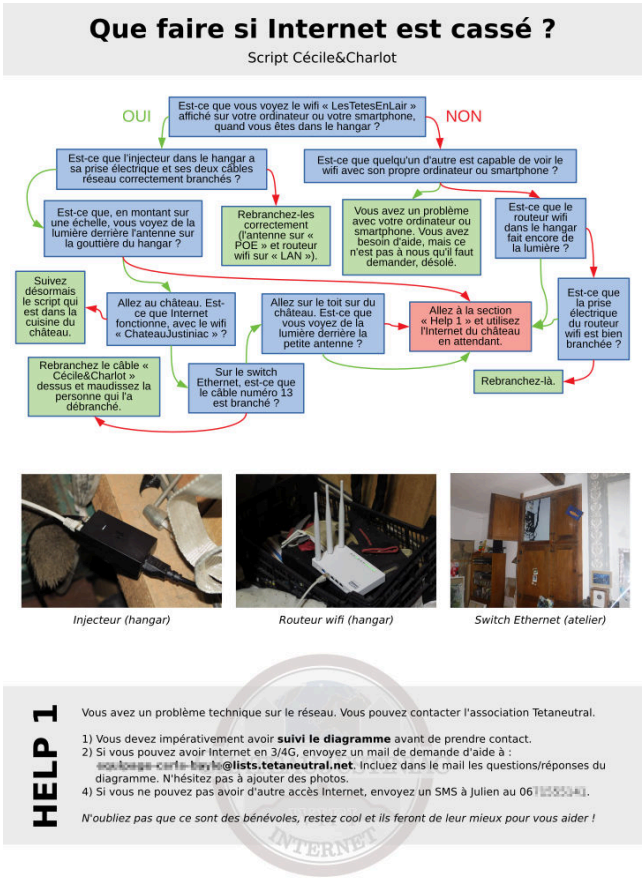
Le réseau wifi du château, qui auparavant était surtout utilisé péniblement depuis la cuisine, est désormais disponible partout, avec une bonne réception. Une vidéo peut désormais être streamée sans interruption, en se déplaçant du potager à la chapelle, en traversant tout le château et ses dépendances.

44. https://tools.ietf.org/html/rfc4861

Il n'y a eu qu'une seule interruption significative de la connexion à Internet depuis maintenant quasiment un an : le propriétaire, qui était présent à ce moment-là, a suivi l'un des panneaux « Que faire si Internet est cassé ? » (cf. Figure 31) qui ont été mis à disposition au château, et a été capable de résoudre le problème par lui-même [45], sans même avoir à contacter Tetaneutral.net.




(a) Panneau à destination du château.




(b) Panneau à destination des caravanes du cirque.

FIGURE 31 – Panneaux plastifiés pour l'aide à la détection des pannes, à disposition des habitant·es du château.

L'AG de la Fédération FFDN au Château de Justiniac a été globalement une réussite, et l'utilisabilité du wifi n'a pas été un sujet, signe qu'il a parfaitement fait son travail. Quelques photos de l'AG sont disponibles dans la Figure 33 de l'Annexe A et les compte-rendus des ateliers sont disponibles sur le wiki FFDN [46].

45. Il est arrivé à la section « Help 2 » et a demandé au locataire du Carla-Bayle d'éteindre et rallumer la multiprise.
46. https://www.ffdn.org/wiki/doku.php?id=evenements:ag2018

# A Illustrations générales

(a) Le château est à la campagne et dispose de grands terrains en fermage.

(b) Vue du château depuis le Sud.

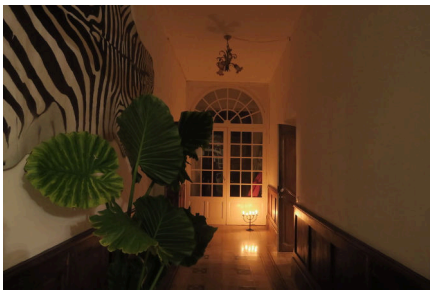
(c) Vue depuis le Sud-Ouest.

(d) Vue depuis le Sud-Est.

(e) Vue depuis le Nord (façade en direction de Toulouse).

(f) Grande terrasse côté Sud.

(g) Vue sur les vallées et les Pyrénées, depuis la terrasse.



(h) Vue intérieure, vers la terrasse (non, ce n'est pas une vraie peau de zèbre).

(i) Billard rocambole (aussi appelé billard français) dans l'entrée du château.

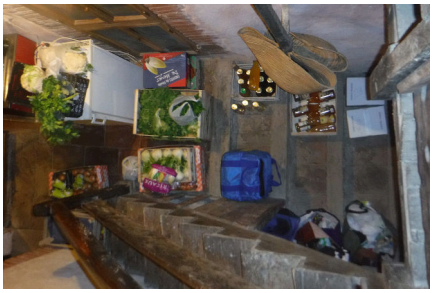
(j) La cuisine, principal lieu de vie des occupant·es durant l'hiver.

(k) Salle à Manger.

(l) Les nombreuses chambres du château permettent d'accueillir beaucoup de personnes de passage.

FIGURE 32 – Vues générales du château.


(a) Fière bannière FFDN.

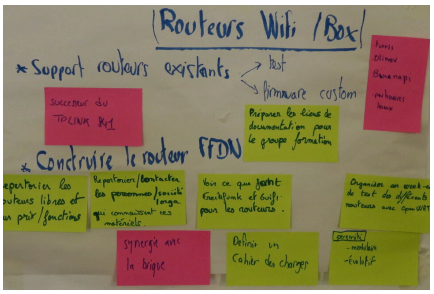


(b) Arrière-cuisine


(c) Téléphone du château en autogestion durant l'événement, pour gérer les arrivées.

(d) Grande salle de travail, également utilisée pour les repas en cas de mauvais temps.


(e) Certains temps étaient collectifs...




(f) ... tandis que d'autres étaient séparés en groupes de travail.

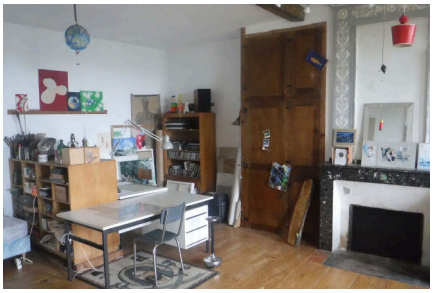
(g) Camping sur le terrain du château.

(h) Un peu moins de la moitié des $\tilde{7}0$ participant·es a choisi de dormir sous tente.

(i) Soirée au château.

FIGURE 33 – Photos de l'AG 2018 de la Fédération FFDN au Château de Justiniac. La politique concernant le respect de la vie privée est très stricte, et ne permet pas la diffusion de photos avec des gens reconnaissables dessus.

# B Passages de câbles



(a) L'Atelier du 1er étage accueille les équipements du cœur de réseau en haut du placard permanent en bois.

(b) 11 câbles (LAN et WAN) partent vers le plafond, et 1 seul part vers le sol (borne wifi de la Salle à Manger). Équipements de haut en bas : client VoIP en noir et routeur en blanc, switch PoE, multiprise parafoudre.

(c) Sortie des câbles dans le grenier, au-dessus du placard.

(d) À droite, 2 câbles alimentent les antennes (upstream et pont vers le cirque) sur le toit.

(e) À gauche, les câbles longent les poutres métalliques pour aller alimenter les bornes wifi du château. Le propriétaire ne souhaitait pas qu'il y ait de nouveaux câbles dans le sol, déjà très encombré.

(f) Une dorsale de câbles traverse le grenier en hauteur.

(g) Le système de poutres permet de facilement amener les câbles partout dans le grenier.

(h) Les retours au sol pour traverser les plafonds sont matérialisés par des poteaux en bois.

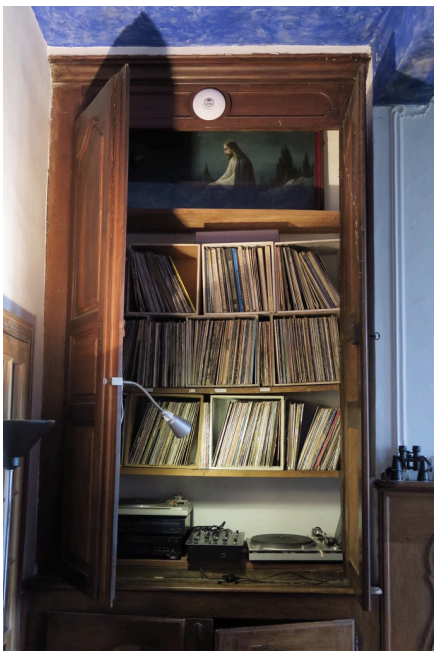
(i) Le grenier est un espace relativement dangereux pour travailler : le sol constitué de planches mal-disposées réserves quelques mauvaises surprises (ici, un trou qui mène directement au-dessus d'un placard de chambre, dans lequel ma jambe est passée).

FIGURE 34 – Cœur de réseau et irrigation des câbles par le grenier.

(a) Percée dans le sol du placard qui switch (au-dessus). C'est le seul câble qui ne passe pas par le grenier.

(b) Départ depuis le sol de l'Atelier du 1er étage.

(c) Passage dans le haut de l'armoire à vinyles de la Salle à Manger.



(d) Antenne de la Salle à Manger.

FIGURE 35 – Passage de câble de la borne de la Salle à Manger.

(a) La Tour du Hibou (parce qu'une famille de hiboux a longtemps vécu au dernier étage). La Chambre de Maxie est au 1er (avec les volets).

(b) Départ depuis le grenier, en partant vers la Tour du Hibou, tout à gauche de la fenêtre.

(c) Passage du grenier à la Tour du Hibou.

(d) Passage dans la Tour du Hibou

(e) Passage vers la Chambre de Maxie, par le sol.

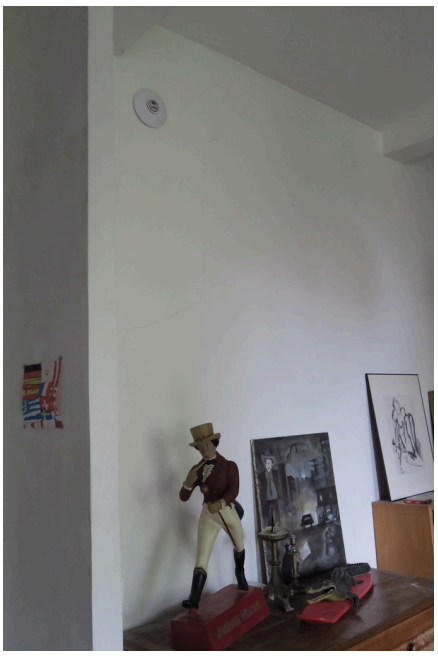

(f) Antenne de la Chambre de Maxie.

FIGURE 36 – Passage de câble de la borne de la Chambre de Maxie.

(a) Départ depuis le grenier, en passant sous le plancher.

(b) Passage par le sous-plafond de la Salle de Bains Bleu le long de la VMC.

(c) Le mur qui mène au Salon peut y être directement percé.



(d) Antenne du Salon.

FIGURE 37 – Passage de câble de la borne du Salon.

(a) Départ depuis le grenier, avec un lot de 3 câbles pour 3 bornes différentes.

(b) Passage à l'intérieur du plancher du grenier, et percée dans le sol à proximité du câble électrique gris.

(c) Passage par le grand placard de la Chambre de l'Appartement du 1er. Le câble de la borne de la Cuisine de l'Appartement du 1er part à droite.

(d) Passage vers le petit placard latéral.

(e) Passage vers la Cuisine de l'Appartement du 1er. Le trou dans le mur porteur était déjà existant.

(f) Antenne de la Cuisine de l'Appartement du 1er, en haut à gauche.

FIGURE 38 – Passage de câble de la borne de la Cuisine du 1er.

(a) Le départ du câble de la borne de la Cuisine de l'Appartement du RDC suit le même chemin que celui pour la Cuisine de l'Appartement du 1er. Il part à gauche.

(b) Passage vers le placard gauche de la cheminée de l'Appartement du 1er.

(c) Passage dans le placard.

(d) Passage vers le Grand Dortoir. Passer à cet endroit du mur permet de percer une partie du mur porteur qui n'est faite que de briques.

(e) Passage dans le Grand Dortoir, via une sorte de meurtrière comblée avec de la brique qui est cachée par un placard.

(f) Traversée du Grand Dortoir le long de la sous-pente.

(g) Les cavaliers ont été peints en noir au marqueur, pour rendre les câbles plus discrets.

(h) Descente le long du mur, derrière la poutre.

(i) Traversée par le sol, sous la moquette.

(j) Passage vers la Cuisine du RDC.

(k) Descente par le plafond de la Cuisine du RDC et poursuite le long du mur à gauche.

(l) Antenne de la Cuisine du RDC.

FIGURE 39 – Passage de câble de la borne de la Cuisine de l'Appartement du RDC.

(a) Le départ du câble de la borne de l'Atelier du RDC suit le même chemin que celui pour la Cuisine de l'Appartement du 1er. Il part à droite.

(b) Passage dans la continuité du Grand Dortoir.

(c) Passage à l'intérieur de la marche qui mène au Petit Dortoir, après un retour au sol sous la moquette.

(d) Passage dans le Petit Dortoir

(e) Passage vers l'Atelier du RDC, par le sol.

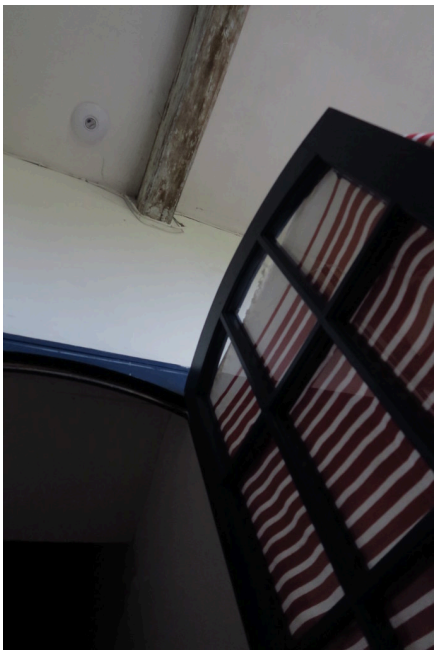
(f) Antenne de l'Atelier du RDC.

FIGURE 40 – Passage de câble de la borne de l'Atelier du RDC.

(a) Départ depuis le grenier, avec une percée dans le sol du petit escalier qui monte à la Chambre de la Tour.

(b) Passage à l'intérieur du plancher de l'entrée de la chambre.

(c) Passage à l'intérieur du plancher de la chambre elle-même (éventré sur la photo).



(d) Antenne de la Bibliothèque, située sous la Chambre de la Tour.

FIGURE 41 – Passage de câble de la borne de la Bibliothèque

(a) Départ depuis le bout du grenier, sous la fenêtre.

(b) Percée dans le mur extérieur (câble au-dessus).

(c) Le câble arrive sur le toit du Préau.

(d) Puis il rentre directement à l'intérieur du grenier du Préau.

(e) Passage à l'intérieur du grenier du Préau. Une grande quantité de mou a été laissée ici en prévision de potentiels futurs travaux dans la Ruine que le câble traverse ensuite.

(f) Passage du grenier du Préau à la Ruine.

(g) Passage de la Ruine vers le grenier de la Salle des Fêtes.

(h) Entrée dans le grenier de la Salle des Fêtes.

(i) Nid d'abeilles à proximité de la percée pour entrer dans le grenier : la perceuse a été utilisée par à-coups en fonction du bruit de la ruche en réaction aux vibrations.

(j) Traversée du grenier le long de la sous-pente à gauche.

(k) Passage vers la Salle des Fêtes, au sol.

(l) Antenne de la Salle des Fêtes.

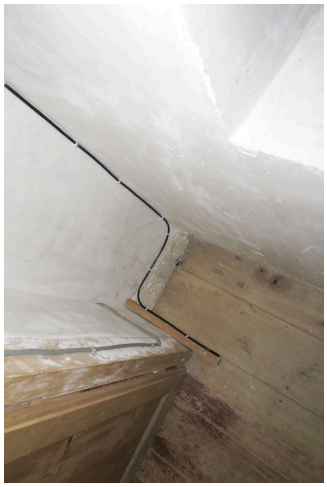
FIGURE 42 – Passage de câble de la borne de la Salle des Fêtes.

(a) Départ depuis le grenier, en partant sous le plancher du grenier.

(b) Passage vers la Chambre de la Cour, en perçant dans le sol.

(c) Passage dans le haut du placard de la Chambre de la Cour, près d'un fil électrique.

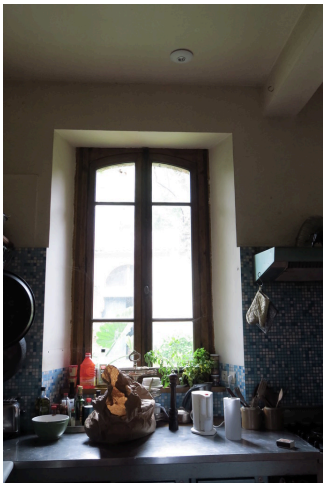
(d) Passage dans la partie supérieure du placard.



(e) Passage dans la partie inférieure.

(f) Passage dans le plancher de la Chambre de la Cour.

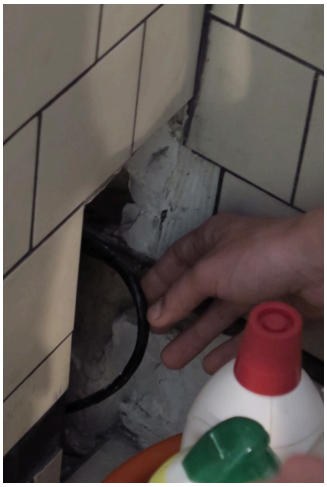
(g) Percée entre le Plafond de la Cuisine et le dessous du plancher de la Chambre de la Cour.



(h) Antenne de la Cuisine, câblée par le plafond.

FIGURE 43 – Passage de câble de la borne de la Cuisine.

(a) Départ depuis le grenier, le long des tuyauteries des salles de bain.



(b) Passage par la Salle de Bain du Châtelain au 1er étage.

(c) Arrivée deux étages en dessous, dans le faux plafond de la salle de bain / cuisine de la Suite.

(d) Percée dans le mur du faux plafond.

(e) Passage vers le Salon Piano.

(f) Antenne du Salon Piano (en haut à droite).

FIGURE 44 – Passage de câble de la borne du Salon Piano.

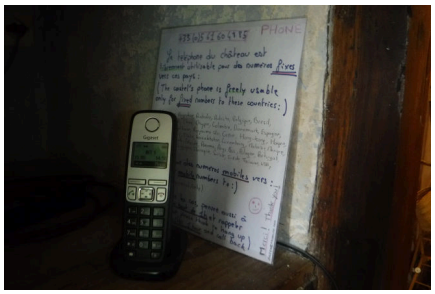

(a) Routeur VoIP Cisco SPA112 préconfiguré par OVH, permettant de relier n'importe quel téléphone analogique au compte VoIP OVH.

(b) Le câble de téléphone RJ11 descends le long du placard du switch en suivant le câble Ethernet de la borne de la Salle à Manger.

(c) Passage vers l'extérieur du placard, long du fil d'alimentation électrique de la multiprise parafoudre.

(d) Passage derrière une étagère, pour atterrir à l'endroit où était située l'ancienne Livebox et son téléphone.

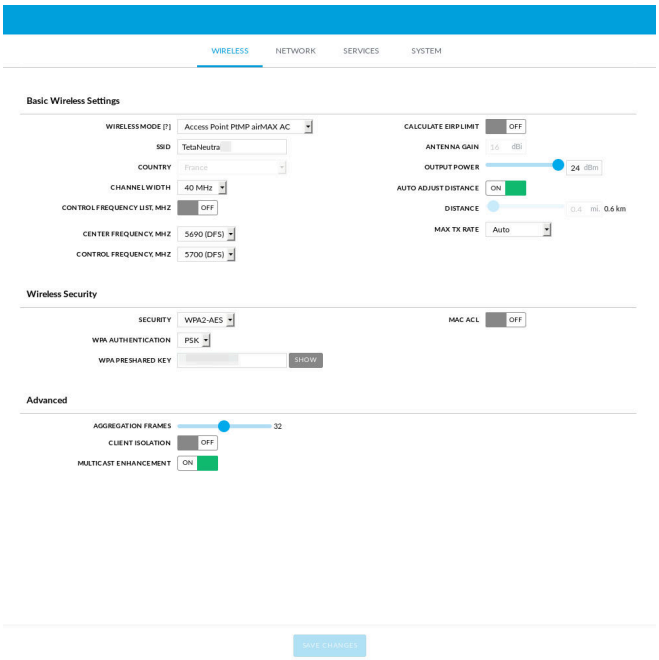
(e) Téléphone analogique Gigaset A400A avec répondeur intégré.



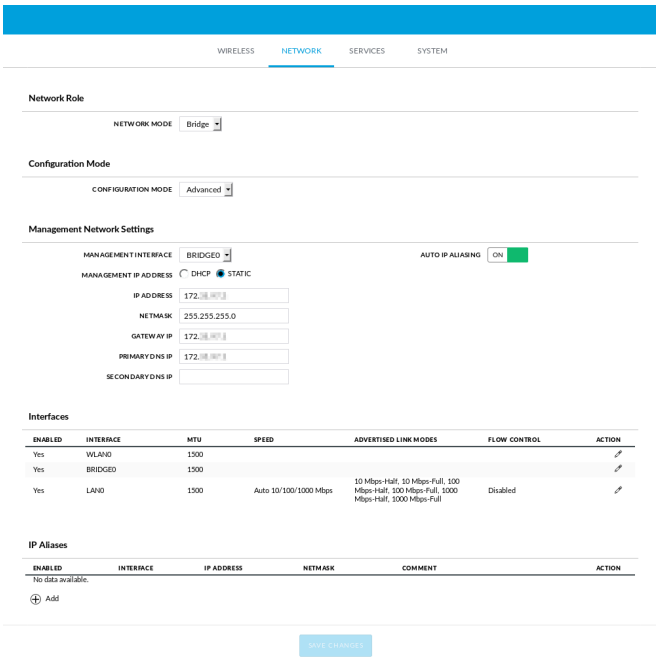
(f) Combiné radio secondaire disponible dans la Cuisine du RDC.

FIGURE 45 – Infrastructure téléphonique.

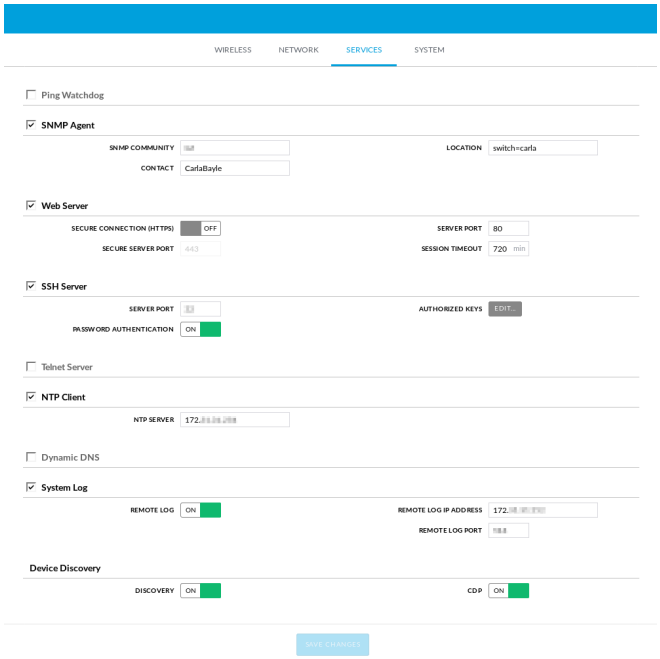
# C Configurations




(a) Section Wireless (AP PtMP – Point-to-MultiPoint – pour pouvoir connecter d'autres adhérent·es TTNN du coin dans le futur).

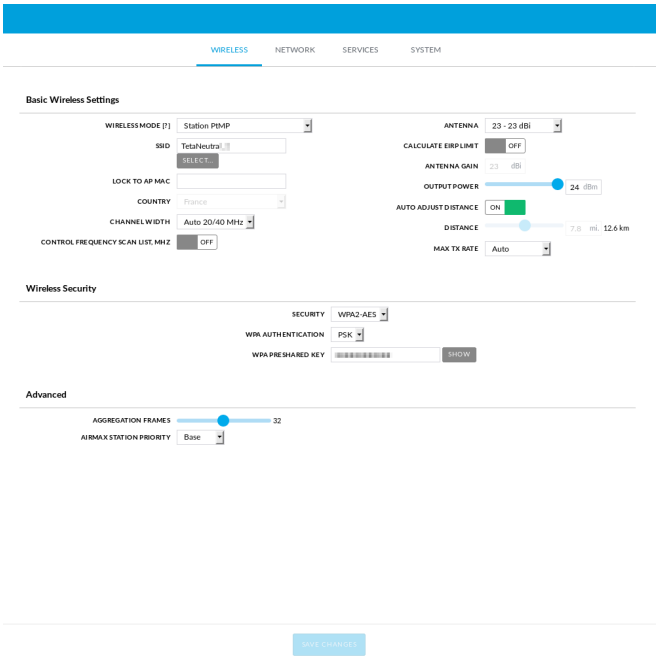



(b) Section Network (mode Bridge).

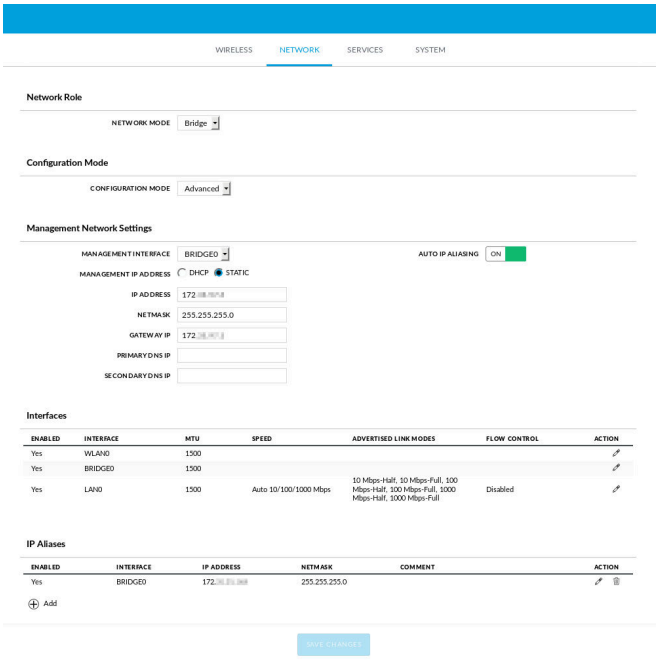



(c) Section Services (supervision SNMP et logging à distance).

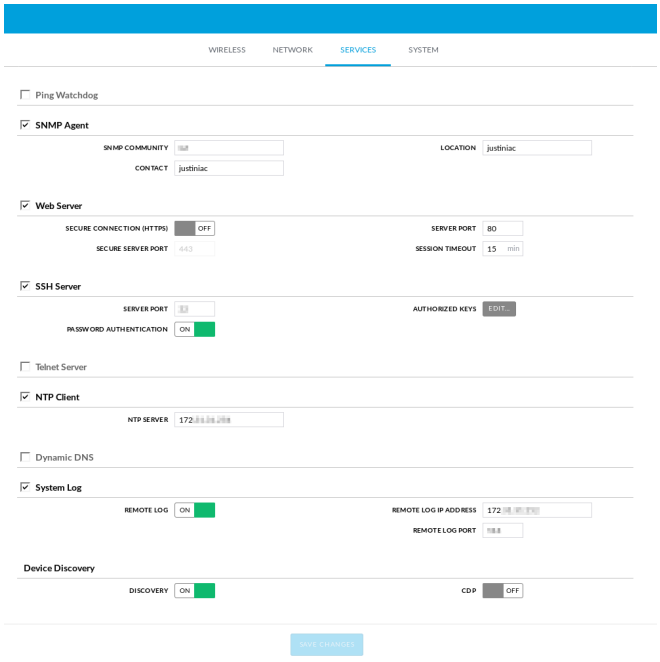
FIGURE 46 – Pont wifi WAN – Configuration de la LiteBeam 120 côté Carla-Bayle.




(a) Section Wireless (Station PtMP).

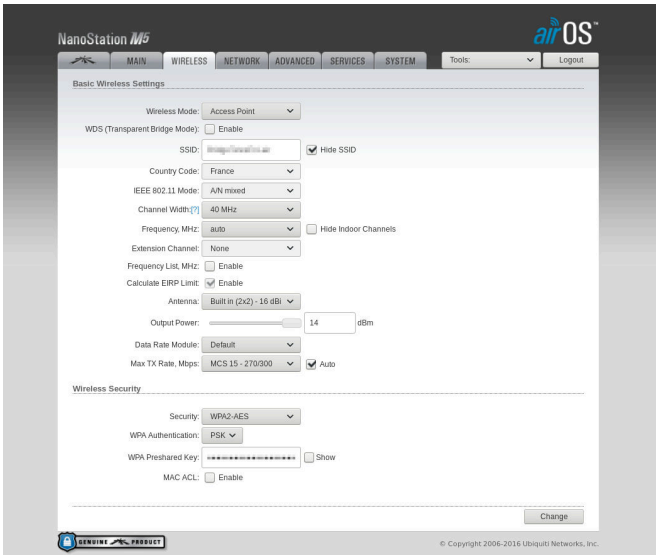



(b) Section Network (mode Bridge).



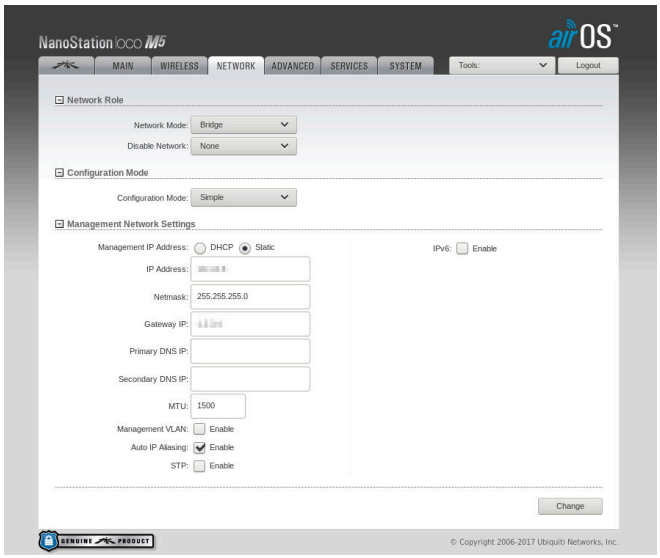

(c) Section Services (supervision SNMP et logging à distance).

FIGURE 47 – Pont wifi WAN – Configuration de la LiteBeam côté château.




(a) Section Wireless de la NanoStation M5 côté château (Access Point).


(b) Section Wireless de la Loco M5 côté cirque (Station).




(c) Section Network (mode Bridge pour les deux antennes).

FIGURE 48 – Pont wifi LAN – Configuration des deux NanoStation (côtés château et cirque).

```
# SANS VLAN DE MANAGEMENT

config interface 'loopback'
  option ifname 'lo'

config interface 'wifi'
  option ifname 'eth0'
  option type 'bridge'
  option proto 'static'
  option ipaddr '10.11.12.13' # fallback
  option netmask '255.255.255.0'
```

```
# AVEC VLAN DE MANAGEMENT

config interface 'loopback'
  option ifname 'lo'

config interface 'management'
  option ifname 'eth0.1'
  option proto 'static'
  option ipaddr '10.11.12.13' # fallback
  option netmask '255.255.255.0'

config interface 'wifi'
  option ifname 'eth0.10'
  option type 'bridge'
```

Configuration 1 – Bornes wifi du LAN – Fichier /etc/config/network pour les UAP-AC-LITE/OpenWrt.

```
config wifi-device 'radio0'
  option type 'mac80211'
  option channel 'auto'
  option hwmode '11a'
  option path 'pci0000:00/0000:00:00.0'
  option htmode 'VHT80'
  option txpower '20'
  option country 'FR'
  option distance '10'

config wifi-iface 'default_radio0'
  option device 'radio0'
  option network 'wifi'
  option mode 'ap'
  option disassoc_low_ack '1'
  option skip_inactivity_poll '1'
  option max_inactivity '10'
  option ssid 'ChateauJustiniac'
  option encryption 'none'

config wifi-device 'radio1'
  option type 'mac80211'
  option channel 'auto'
  option hwmode '11g'
  option path 'platform/qca956x_wmac'
  option htmode 'HT20'
  option txpower '20'
  option country 'FR'
  option distance '10'

config wifi-iface 'default_radio1'
  option device 'radio1'
  option network 'wifi'
  option mode 'ap'
  option disassoc_low_ack '1'
  option skip_inactivity_poll '1'
  option max_inactivity '10'
  option ssid 'ChateauJustiniac'
  option encryption 'none'
```

Configuration 2 – Bornes wifi du LAN – Fichier /etc/config/wireless pour les UAP-AC-LITE/OpenWrt.

```
config defaults
  option input DROP
  option output DROP
  option forward DROP

config zone
  option name management
  list network 'management'
  option input DROP
  option output ACCEPT
  option forward DROP

config rule
  option name Allow-Ping
  option src management
  option proto icmp
  option icmp_type echo-request
  option family ipv4
  option target ACCEPT

config rule
  option name Allow-ICMPv6
  option src management
  option proto icmp
  list icmp_type echo-request
  list icmp_type echo-reply
  list icmp_type destination-unreachable
  list icmp_type packet-too-big
  list icmp_type time-exceeded
  list icmp_type bad-header
  list icmp_type unknown-header-type
  list icmp_type neighbour-solicitation
  list icmp_type neighbour-advertisement
  option family ipv6
  option target ACCEPT

config rule
  option name Allow-SSH
  option src management
  option dest_port 22
  option proto tcp
  option target ACCEPT
```

Configuration 3 – Bornes wifi du LAN – Fichier /etc/config/firewall pour les UAP-AC-LITE/OpenWrt (uniquement pour la version avec VLAN de management).

```
firstboot_file=/root/.firstboot

# BSSID of every AP on the network
mac_aps='
  <MAC_AP1>
  <MAC_AP2>
  <MAC_AP3>
  <MAC_AP4>
  <MAC_AP5>
  <MAC_AP6>
  <MAC_AP7>
  <MAC_AP8>
  <MAC_AP9>
  <MAC_AP10>
'

# Random values, but same on every AP
ieee80211r_pwd=<RANDOM_HASH>
ieee80211r_domain=<RANDOM_STRING>

function turnoff_leds() {
  echo 0 > /sys/class/leds/ubnt\:white\:dome/brightness
  echo 0 > /sys/class/leds/ubnt\:blue\:dome/brightness
}

# AP ID of the current antenna is computed and a local IPv6 address is made based on it
# This IP is added to /etc/config/network
function set_management_addr() {
  mac_eth=$(ip link show eth0 | awk '/ether/ { print toupper($2) }')
  id=$(echo -n $mac_eth | md5sum | cut -c -4)

  uci set network.wifi.ip6addr="fe80::$id/64"
  # AVEC VLAN DE MANAGEMENT: uci set network.management.ip6addr="fe80::$id/64"

  uci commit network
}

# Add roaming stuff in /etc/config/wireless
function set_ap_roaming() {
  for i in 0 1; do
    mac_wlan=$(ip link show wlan$i | awk '/ether/ { print toupper($2) }')
    mac_wlan_nocolons=$(echo $mac_wlan | tr -d :)

    uci set wireless.@wifi-iface[$i].ieee80211r='1'
    uci set wireless.@wifi-iface[$i].mobility_domain="$ieee80211r_domain"
    uci set wireless.@wifi-iface[$i].pmk_r1_push='1'
    uci set wireless.@wifi-iface[$i].nasid="$mac_wlan_nocolons"
    uci set wireless.@wifi-iface[$i].r1_key_holder="$mac_wlan_nocolons"

    for mac_ap in $mac_aps; do
      mac_ap_nocolons=$(echo $mac_ap | tr -d :)

      uci add_list wireless.@wifi-iface[$i].r0kh="$mac_ap,$mac_ap_nocolons,$ieee80211r_pwd"
      uci add_list wireless.@wifi-iface[$i].r1kh="$mac_ap,$mac_ap,$ieee80211r_pwd"
    done
  done

  uci commit wireless
}

function is_first_boot() {
  ! test -e $firstboot_file
}

# Config files are updated only at the very first boost
if is_first_boot; then
  echo 0 > /sys/class/leds/ubnt\:white\:dome/brightness
  echo 255 > /sys/class/leds/ubnt\:blue\:dome/brightness
  sleep 1

  set_management_addr
  set_ap_roaming

  /etc/init.d/network restart

  touch $firstboot_file
  turnoff_leds
fi

# All leds are turned off when the AP is running
(sleep 3 && turnoff_leds) &

exit 0
```

Configuration 4 – Bornes wifi du LAN – Fichier /etc/rc.local pour les UAP-AC-LITE/OpenWrt.

```
#!/bin/bash
set -x

# USAGE: ./flash_uap.sh COMMAND [AP_ID]

# Fixed values
DEV_WIFI=wlp3s0
DEV_WIRE=enp0s25
PATH_FW_UNIFI=/home/ju/justiniac/openwrt/firmwares/fw-unifi-3.4.7.bin
PATH_FW_OPENWRT=/var/lib/lxc/openwrt/rootfs/root/builder/bin/targets/ar71xx/generic/lede-*-lite-squashfs-sysupgrade.bin
MAC_SWITCH=00:00:00:00:00:00
PATH_AP_MACS=/tmp/ap_macs

# When no AP ID is provided, looking for an AP on the network
# In this case, the AP should be directly wire linked to the laptop
if [ -z "$2" ]; then
  ip_ap=; while [ -z "$ip_ap" ]; do
    ip_ap=$(sudo scan6 -i ${DEV_WIRE} -L | grep -v ${MAC_SWITCH})
    sleep 1
  done

# Or use the AP ID provided as an argument
else
  ip_ap=fe80::$2
fi

# Commands for flashing
case "$1" in

  # Replace a UniFi firmware by another one (useful for downgrading)
  unifi-unifi)
    if [ ! -r "${PATH_FW_UNIFI}" ]; then
      echo "PATH_FW_UNIFI: <${PATH_FW_UNIFI}> doesn't exist or is not readable" >&2; exit 1
    fi

    sshpass -p ubnt scp -o StrictHostKeyChecking=no "${PATH_FW_UNIFI}" ubnt@[${ip_ap}%${DEV_WIRE}]:/tmp/fwupdate.bin ↩
        || exit 1
    sshpass -p ubnt ssh -o StrictHostKeyChecking=no ubnt@${ip_ap}%${DEV_WIRE} 'fwupdate.real -m /tmp/fwupdate.bin'

    # reboot
    false; while [ ! $? -eq 0 ]; do
      sshpass -p ubnt ssh -o StrictHostKeyChecking=no ubnt@${ip_ap}%${DEV_WIRE}\\
        'mac=$(ifconfig eth0 | awk "/HWaddr/ { print \$5; }"); echo -n "$mac "; echo -n $mac | md5sum | cut -c -4' >> ↩
            "${PATH_AP_MACS}"
    done
    ;;

  # Replace a UniFi firmware by an OpenWrt one
  unifi-openwrt)
    if [ ! -r "${PATH_FW_OPENWRT}" ]; then
      echo "PATH_FW_OPENWRT: <${PATH_FW_OPENWRT}> doesn't exist or is not readable" >&2; exit 1
    fi

    sshpass -p ubnt scp -o StrictHostKeyChecking=no "${PATH_FW_OPENWRT}" ↩
        ubnt@[${ip_ap}%${DEV_WIRE}]:/tmp/fwupdate.bin || exit 1
    sshpass -p ubnt ssh -o StrictHostKeyChecking=no ubnt@${ip_ap}%${DEV_WIRE} 'mtd write /tmp/fwupdate.bin kernel0'
    sshpass -p ubnt ssh -o StrictHostKeyChecking=no ubnt@${ip_ap}%${DEV_WIRE} 'mtd -r write /tmp/fwupdate.bin kernel1'
    ;;

  # Replace an OpenWrt firmware by another one (useful for default config updates)
  openwrt-openwrt)
    if [ ! -r "${PATH_FW_OPENWRT}" ]; then
      echo "PATH_FW_OPENWRT: <${PATH_FW_OPENWRT}> doesn't exist or is not readable" >&2; exit 1
    fi

    scp -o StrictHostKeyChecking=no "${PATH_FW_OPENWRT}" root@[${ip_ap}%${DEV_WIRE}]:/tmp/fwupdate.bin || exit 1
    ssh -o StrictHostKeyChecking=no root@${ip_ap}%${DEV_WIRE} 'sysupgrade -n /tmp/fwupdate.bin'
    ;;

  # Just test if an AP is alive
  ping)
    ping6 ${ip_ap}%${DEV_WIRE}
  ;;

  # Lazy way to SSH an AP from its ID (from wired connection)
  sshwired)
    ssh root@${ip_ap}%${DEV_WIRE}

  # Lazy way to SSH an AP from its ID (from wifi connection)
  sshwifi)
    ssh root@${ip_ap}%${DEV_WIFI}
esac

exit 0
```

CONFIGURATION 5 – Bornes wifi du LAN – Script pour flasher les UAP-AC-LITE, de UniFi à UniFi (downgrade), de UniFi à OpenWrt (migration), ou de OpenWrt à OpenWrt (mise à jour).

```
config interface 'loopback'
      option ifname 'lo'
      option proto 'static'
      option ipaddr '127.0.0.1'
      option netmask '255.0.0.0'

config interface 'lan'
      option type 'bridge'
      option ifname 'eth0'
      option proto 'static'
      option netmask '255.255.255.0'
      option ipaddr '192.168.XXX.1'
      option ip6addr '2a03:XXXX:XXXX:XX01::1/64'

config interface 'wan'
      option ifname 'eth1'
      option proto 'static'
      option ipaddr '89.XXX.XXX.XXX'
      option netmask '255.255.255.255'
      option dns '91.224.148.10 91.224.149.254 2a03:7220:8080:0a00::1'
      option ip6addr '2a03:XXXX:XXXX:XX00::1/56'
      option ip6gw 'fe80::XXXX'

config switch
      option name 'switch0'
      option reset '1'
      option enable_vlan '1'

config switch_vlan
      option device 'switch0'
      option vlan '1'
      option ports '1 2 3 4 0'

config interface 'wan6'
      option proto 'static'
      option ifname 'eth1'
      option ip6addr 'fe80::YYYY/64'

config route
      option interface 'wan'
      option onlink '1'
      option target '0.0.0.0/0'
      option gateway '91.XXX.XXX.XXX'
```

CONFIGURATION 6 – Fichier /etc/config/network pour le routeur du château.

```
#!/bin/sh

# Enable router mode
echo 1 > /proc/sys/net/ipv4/ip_forward
echo 1 > /proc/sys/net/ipv6/conf/all/forwarding

# autoconf=0 - Do not accept auto-generated (NDP) IPv6 address
# accept_ra=0 - Do not accept information broadcasted by other IPv6 routers
for i in /proc/sys/net/ipv6/conf/*; do for j in autoconf accept\_ra; do echo 0 > $i/$j; done;done

# eth1 - LAN interface on which the directional antenna is plugged (eth0=VDSL2)
ip link set eth1 up

# Set a local IP to this interface, and add a route to the (new) routing table 25 (could be another number) for the whole network
ip addr add 172.XXX.XXX.1/24 dev eth1
ip route add 172.XXX.XXX.0/24 dev eth1 table 25

# Creation of the VPN tunnel with a virtual interface named tuncar
openvpn --mktun --dev-type tun --dev tuncar
ip link set tuncar up
openvpn --dev tuncar --dev-type tun --cipher none --auth none --lport 0 --remote 91.XXX.XXX.1 65139 --proto udp ↩
    --daemon --keepalive 10 60 --log-append /root/vpn-XXX.log

# Set a local IPv4 to the VPN client interface, for the communication with the VPN server (.1) through the tunnel
ip addr add 10.XXX.XXX.2/24 dev tuncar

# The VPN tunnel is used for the new default route, to redirect the forwarded Internet traffic there
ip route add default dev tuncar table 25
ip -6 route add default dev tuncar table 25

# Every IP packet with 172.XXX.XXX.1 or 10.XXX.XXX.2 as FROM address (ie. packets generated by the shuttle itself, eg. when the destination address is in the same network) will be routed using the routes set in the routing table number 25
ip rule add from 172.XXX.XXX.1 table 25
ip rule add from 10.XXX.XXX.2 table 25

# Every IP packet coming through the directional antenna or the VPN tunnel will also be routed using the table 25
ip rule add from all iif tuncar table 25
ip -6 rule add from all iif tuncar table 25
ip rule add from all iif eth1 table 25
ip -6 rule add from all iif eth1 table 25

# Set an IPv6 link address, used as a default route by the users' routers
ip -6 addr add fe80::YYYY/64 dev eth1

# Set two public IPv4 addresses owned by TTNN to the shuttle
# These addresses are used as default routes by the users' routers
# There are not unique on the Internet and they are set on every TTNN shuttle: public addresses are used only to avoid to use a private IPv4 network that the users would like to use
# One of these two addresses should be removed in the future
ip addr add 89.YYY.YYY.YYY/32 dev eth1
ip addr add 91.XXX.XXX.XXX/32 dev eth1

# Specific routes for the users
# 2 lines to add for each user connected behind the directional antenna
# Set the routes for the IPv4 address and the IPv6 range allocated to the user, as a TTNN member
# fe80::XXXX is the IPv6 link address set on the user's router

ip route add 89.XXX.XXX.XXX dev eth1 table 25
ip -6 route add 2a03:XXXX:XXXX:XXXX::/56 via fe80::XXXX dev eth1 table 25

exit 0
```

CONFIGURATION 7 – Fichier /etc/rc.local du Shuttle (passerelle VPN), utilisé par TTNN.

```
!Current Configuration:
!
!System Description "EdgeSwitch 16-Port 150W, 1.7.3.5050176,
!Linux 3.6.5-f4a26ed5, 0.0.0.0000000"
!System Software Version "1.7.3.5050176"
!System Up Time "99 days 22 hrs 56 mins 20 secs"
!Additional Packages QOS,IPv6 Management,Routing
!Current SNTP Synchronized Time: SNTP Last Attempt Status Is Not Successful
!
network protocol none
network parms 10.1.0.1 255.255.255.0 0.0.0.0
vlan database
vlan 20
vlan name 20 "wan"
exit
no ip http server
ip ssh server enable
ip ssh protocol 2
no ip telnet server enable
configure
username "ubnt" password <HASH>
line console
exit
line telnet
exit
line ssh
exit
!
interface 0/1
vlan participation exclude 20
exit
interface 0/2
vlan participation exclude 20
exit
interface 0/3
lude 20
exit
interface 0/4
vlan participation exclude 20
exit
interface 0/5
vlan participation exclude 20
exit
!SUITE
interface 0/6
vlan participation exclude 20
exit
interface 0/7
vlan participation exclude 20
exit
interface 0/8
vlan participation exclude 20
exit
interface 0/9
vlan participation exclude 20
exit
interface 0/10
vlan participation exclude 20
exit
interface 0/11
vlan participation exclude 20
exit
interface 0/12
vlan participation exclude 20
exit
interface 0/13
vlan participation exclude 20
poe opmode passive24v
exit
interface 0/14
vlan participation exclude 20
exit
interface 0/15
vlan pvid 20
vlan acceptframe admituntaggedonly
vlan participation include 20
poe opmode passive24v
exit
interface 0/16
vlan pvid 20
vlan acceptframe admituntaggedonly
vlan participation include 20
exit
exit
```

CONFIGURATION 8 – Running-config du EdgeSwitch (sans VLAN de management).

```
(UBNT EdgeSwitch) >enable
(UBNT EdgeSwitch) #vlan database
(UBNT EdgeSwitch) (Vlan)#vlan 20
(UBNT EdgeSwitch) (Vlan)#vlan name 20 wan
(UBNT EdgeSwitch) (Vlan)#exit
(UBNT EdgeSwitch) #config
(UBNT EdgeSwitch) (Config)#interface 0/1-0/14
(UBNT EdgeSwitch) (Interface 0/1-0/14)#vlan participation exclude 20
(UBNT EdgeSwitch) (Interface 0/1-0/14)#exit
(UBNT EdgeSwitch) (Config)#interface 0/15,0/16
(UBNT EdgeSwitch) (Interface 0/15,0/16)#vlan pvid 20
(UBNT EdgeSwitch) (Interface 0/15,0/16)#vlan acceptframe admituntaggedonly
(UBNT EdgeSwitch) (Interface 0/15,0/16)#vlan participation include 20
(UBNT EdgeSwitch) (Interface 0/15,0/16)#exit
(UBNT EdgeSwitch) (Config)#interface 0/13,0/15
(UBNT EdgeSwitch) (Interface 0/13,0/15)#poe opmode passive24v
(UBNT EdgeSwitch) (Interface 0/13,0/15)#exit
(UBNT EdgeSwitch) (Config)#write memory
```

CONFIGURATION 9 – Commandes en CLI pour obtenir la running-config de la Configuration 8.

```
!Current Configuration:
!
!System Description "EdgeSwitch 16-Port 150W, 1.7.3.5050176,
! Linux 3.6.5-f4a26ed5, 0.0.0.0000000"
!System Software Version "1.7.3.5050176"
!System Up Time "2 days 4 hrs 10 mins 3 secs"
!Additional Packages QOS,IPv6 Management,Routing
!Current SNTP Synchronized Time: SNTP Last Attempt Status Is Not Successful
!
network protocol none
network parms <IPV4_SWITCH> 255.255.255.0 0.0.0.0
vlan database
vlan 10,20
vlan name 10 "wifi"
vlan name 20 "wan"
exit
no ip http server
ip ssh server enable
ip ssh protocol 2
no ip telnet server enable
configure
username "ubnt" password <HASH> level 15 encrypted
line console
exit
line telnet
exit
line ssh
exit
!
interface 0/1
vlan pvid 10
vlan acceptframe admituntaggedonly
vlan participation exclude 1,20
vlan participation include 10
exit
interface 0/2
vlan acceptframe vlanonly
vlan participation exclude 20
vlan participation include 10
vlan tagging 1,10
exit
interface 0/3
vlan acceptframe vlanonly
vlan participation exclude 20
vlan participation include 10
vlan tagging 1,10
exit
interface 0/4
vlan acceptframe vlanonly
vlan participation exclude 20
vlan participation include 10
vlan tagging 1,10
exit
interface 0/5
vlan acceptframe vlanonly
vlan participation exclude 20
vlan participation include 10
vlan tagging 1,10
exit
interface 0/6
vlan acceptframe vlanonly
vlan participation exclude 20
vlan participation include 10
vlan tagging 1,10
exit
!SUITE
interface 0/7
vlan acceptframe vlanonly
vlan participation exclude 20
vlan participation include 10
vlan tagging 1,10
exit
interface 0/8
vlan acceptframe vlanonly
vlan participation exclude 20
vlan participation include 10
vlan tagging 1,10
exit
interface 0/9
vlan acceptframe vlanonly
vlan participation exclude 20
vlan participation include 10
vlan tagging 1,10
exit
interface 0/10
vlan acceptframe vlanonly
vlan participation exclude 20
vlan participation include 10
vlan tagging 1,10
exit
interface 0/11
vlan acceptframe vlanonly
vlan participation exclude 20
vlan participation include 10
vlan tagging 1,10
exit
interface 0/12
vlan acceptframe vlanonly
vlan participation exclude 20
vlan participation include 10
vlan tagging 1,10
poe opmode passive24v
exit
interface 0/13
vlan pvid 20
vlan acceptframe admituntaggedonly
vlan participation exclude 1,10
vlan participation include 20
poe opmode passive24v
exit
interface 0/14
vlan pvid 20
vlan acceptframe admituntaggedonly
vlan participation exclude 1,10
vlan participation include 20
exit
interface 0/15
vlan pvid 10
vlan acceptframe admituntaggedonly
vlan participation exclude 1,20
vlan participation include 10
exit
interface 0/16
vlan acceptframe admituntaggedonly
vlan participation exclude 10,20
exit
exit
```

Configuration 10 – Running-config du EdgeSwitch (avec VLAN de management).

```
(UBNT EdgeSwitch) >enable
(UBNT EdgeSwitch) #vlan database
(UBNT EdgeSwitch) (Vlan)#vlan 10
(UBNT EdgeSwitch) (Vlan)#vlan name 10 wifi
(UBNT EdgeSwitch) (Vlan)#vlan 20
(UBNT EdgeSwitch) (Vlan)#vlan name 20 wan
(UBNT EdgeSwitch) (Vlan)#exit
(UBNT EdgeSwitch) #config
(UBNT EdgeSwitch) (Config)#interface 0/1,0/15
(UBNT EdgeSwitch) (Interface 0/1,0/15)#vlan pvid 10
(UBNT EdgeSwitch) (Interface 0/1,0/15)#vlan acceptframe admituntaggedonly
(UBNT EdgeSwitch) (Interface 0/1,0/15)#vlan participation exclude 1
(UBNT EdgeSwitch) (Interface 0/1,0/15)#vlan participation include 10
(UBNT EdgeSwitch) (Interface 0/1,0/15)#vlan participation exclude 20
(UBNT EdgeSwitch) (Interface 0/1,0/15)#exit
(UBNT EdgeSwitch) (Config)#interface 0/2-0/12
(UBNT EdgeSwitch) (Interface 0/2-0/12)#vlan tagging 1,10
(UBNT EdgeSwitch) (Interface 0/2-0/12)#vlan acceptframe vlanonly
(UBNT EdgeSwitch) (Interface 0/2-0/12)#vlan participation include 1
(UBNT EdgeSwitch) (Interface 0/2-0/12)#vlan participation include 10
(UBNT EdgeSwitch) (Interface 0/2-0/12)#vlan participation exclude 20
(UBNT EdgeSwitch) (Interface 0/2-0/12)#exit
(UBNT EdgeSwitch) (Config)#interface 0/12,0/13
(UBNT EdgeSwitch) (Interface 0/12,0/13)#poe opmode passive24v
(UBNT EdgeSwitch) (Interface 0/12,0/13)#exit
(UBNT EdgeSwitch) (Config)#interface 0/13-0/14
(UBNT EdgeSwitch) (Interface 0/13,0/114)#vlan pvid 20
(UBNT EdgeSwitch) (Interface 0/13,0/114)#vlan acceptframe admituntaggedonly
(UBNT EdgeSwitch) (Interface 0/13,0/114)#vlan participation exclude 1
(UBNT EdgeSwitch) (Interface 0/13,0/114)#vlan participation exclude 10
(UBNT EdgeSwitch) (Interface 0/13,0/114)#vlan participation include 20
(UBNT EdgeSwitch) (Interface 0/13,0/114)#exit
(UBNT EdgeSwitch) (Config)#interface 0/16
(UBNT EdgeSwitch) (Interface 0/16)#vlan pvid 1
(UBNT EdgeSwitch) (Interface 0/16)#vlan acceptframe admituntaggedonly
(UBNT EdgeSwitch) (Interface 0/16)#vlan participation include 1
(UBNT EdgeSwitch) (Interface 0/16)#vlan participation exclude 10
(UBNT EdgeSwitch) (Interface 0/16)#vlan participation exclude 20
(UBNT EdgeSwitch) (Interface 0/16)#exit
(UBNT EdgeSwitch) (Config)#write memory
```

CONFIGURATION 11 – Commandes en CLI pour obtenir la running-config de la Configuration 10.

# D Ressources complémentaires

*... du même auteur.*

— Documentation similaire pour un autre réseau de château :
`https://julien.vaubourg.com/files/cr_millemont.pdf`

— Fonctionnement d'Internet 1/2 (coûts et papiers) :
`https://julien.vaubourg.com/files/internet-is-coming-1.mp4`

— Fonctionnement d'Internet 2/2 (technique avec BGP) :
`https://julien.vaubourg.com/files/internet-is-coming-2.mp4`

— Pourquoi IPv6 ne doit surtout pas être ignoré :
`https://julien.vaubourg.com/files/intranet-ipv4-ou-internet-ipv6.webm`

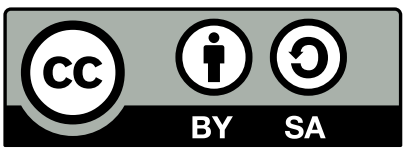
— Comprendre IPv6 en détails :
`https://julien.vaubourg.com/files/lothaire-yarding_ipv6.pdf`
`https://julien.vaubourg.com/files/adressage-ipv6-ipv4.webm`

— Pourquoi la vie privée est importante :
`https://julien.vaubourg.com/files/conf-rien-a-cacher-high.webm`
`https://julien.vaubourg.com/files/conf-rien-a-cacher-high_questions.webm`
`https://julien.vaubourg.com/files/sex-alcool-vieprivee.webm`
`https://julien.vaubourg.com/files/fr3_videosurveillance.webm`

— À propos de l'auteur :
`https://julien.vaubourg.com/files/fr3_portrait.webm`

— Autres :
`https://julien.vaubourg.com`

# Liste des Figures et Tableaux


BY
SA