Déploiement du réseau du Château de Millemont

à l'occasion du MMM Fest 2017

Par Julien V. & Benoît S.
julien[at]vaubourg[dot]com
Le 21/10/2017

Avec la participation de :
Adrien N., olb, Lorraine Data Network, Franciliens.net,
Pierre et Cédric de SA CHATEAUX HOLDINGS,
et le regard bienveillant de bikepunk.

Merci à :
Peter B., Guillaume R. et Hugo B.

Table des matières

1 Contexte

Le Château de Millemont (78) est une propriété privée située à l'ouest de Paris [1], qui a pour but d'être dédiée aux projets et événements liés à la « transition énergétique ».

Le festival MMM Fest [2], qui a eu lieu entre le 4 et le 10 octobre 2017, est un événement de ce type : il a (1) permis à des organisations militantes de réunir leur communauté pour faire avancer leurs projets en journée et (2) permis à ces communautés de se croiser et se lier entre elles au travers d'événements musicaux en soirée.

Les sessions de travail prévues durant le festival ont nécessité la mise en place d'un réseau informatique connecté à Internet, dans le Château de Millemont.

Les contraintes étaient les suivantes :

— pas d'électricité dans le bâtiment à couvrir ;

— zone blanche Internet (pas de fibre, ADSL en bout de ligne à environ 5 Mbps, 4G médiocre ou inexistante au sol) ;

— contraintes liées aux monuments historiques classés (rien de visible dans les principales pièces, pas de faux plafonds) ;

— 1 mois seulement entre la première prise de contact de la part du staff du festival, et le festival lui-même ;

— demande explicite du propriétaire de ne pas faire d'installations temporaires, mais de concevoir directement du permanent ;

— 150 personnes attendues.

Le lieu étant propice aux façons de faire alternatives et de préférence militantes, la Fédération FFDN [3] a été invitée à venir voir ce qu'il était possible de faire sur le domaine de Millemont.

Le matériel a été financé par la société SA CHATEAUX HOLDINGS, qui gère le château. Le travail des membres FFDN a été réalisé bénévolement, avec possibilité de dormir sur place et de se faire défrayer les trajets.

Des photos de l'intérieur du Grand Château et des extérieurs sont disponibles dans l'Annexe A.

2 Conception du réseau

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

2.1 Partie LAN

2.1.1 Zones à couvrir

Le plan général du château en Figure 1 permet de situer les lieux les plus importants qui ont été utilisés durant le festival.

Le Petit Château est le bâtiment le mieux entretenu et le mieux équipé. Il a été verrouillé durant tout l'événement, à l'exception du deuxième étage qui a permis à quelques privilégié·e·s de bénéficier d'une chambre pour dormir. Le Grand Château n'est constitué que de pièces vides, et est dédié à la réception de grands événements. C'est au rez-de-chaussée et au premier étage du Grand Château qu'ont eu lieu toutes les animations et workshops en journée. Enfin, l'Orangerie, en face du Petit Château, a été utilisée pour accueillir les cuisines et la salle à manger.

1. À 45 minutes en Transilien N pour 8.20€, depuis la Gare Montparnasse et en s'arrêtant à Garancières-La Queue (prévoir ensuite 30 minutes de marche pour rejoindre le château, ou penser à prévenir en amont pour être emmené en voiture). Également facile d'accès directement en voiture, depuis la N12.
2. Millemont Makers & Music Festival - `http://mmmfest.fr`
3. `https://ffdn.org`

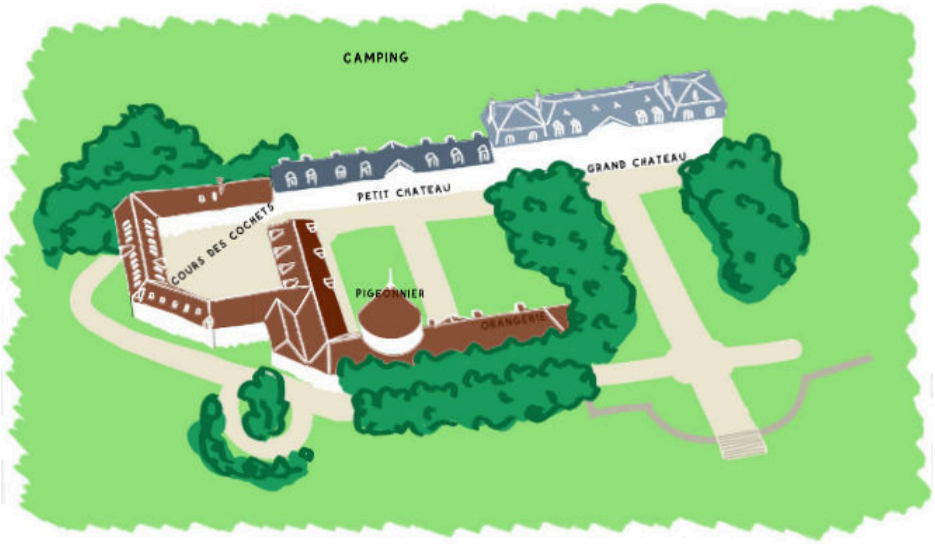


FIGURE 1 – Plan général du château (image *mmmfest.fr*)

Il s'agissait du lieu de vie le plus chaleureux, notamment parce qu'il avait la particularité d'être chauffé. Les trois principaux lieux sont illustrés en photos dans la Figure 2.

(a) Grand Château (b) Petit Château (c) Orangerie

FIGURE 2 – Principaux lieux couverts en wifi

Étant donnés les délais, nous avons restreint l'objectif de zones à couvrir en wifi aux deux étages du Grand Château, pour assurer le bon déroulement des sessions de travail. Durant le festival, nous avons ensuite étendu sa portée à la grande cour entre le Petit Château et l'Orangerie, puis à l'Orangerie elle-même.

2.1.2 Contrainte Monument Historique

Le classement Monuments Historiques dont fait l'objet le château et ses communs, ainsi que son utilisation ponctuelle pour des tournages de films [4], impose de ne pas fixer des bornes wifi (AP – Access Point) un peu partout dans les murs, avec autant de câbles qui longent les murs et plafonds. L'inconvénient d'une AP wifi, c'est que pour qu'on la capte correctement de partout, il faut idéalement qu'elle soit visible de partout.

Le rez-de-chaussée est l'espace le plus prestigieux et emblématique du château, il n'y avait pas vraiment de bonne solution pour réussir à le câbler de façon permanente de part et d'autre, sans le dénaturer. Lors de nos

4. Avez-vous vu *Coco avant Chanel* ?

tests de couverture, nous avons constaté que le plafond était particulièrement poreux : au XVIe siècle, les plafonds n'étaient pas conçus avec des armatures métalliques et étaient surtout constitués de bois et de chaux. Puisque le premier étage était moins contraignant à câbler, nous avons convenu de ne positionner des AP qu'à cet étage.

La couverture wifi du premier étage est par conséquent très condensée (une AP par pièce), avec des antennes qui sont géographiquement positionnées de façon à ce qu'elles correspondent à la fois aux principales pièces de l'étage, mais aussi aux centres des grandes pièces du rez-de-chaussée. Cette double-disposition est visible sur le plan de l'Annexe B.

2.1.3 Serveurs locaux

Nous avons prévenu rapidement le staff du festival que nous ne pouvions pas garantir la qualité de la connexion à Internet durant la semaine du festival. Nous pouvions par contre garantir le bon fonctionnement du LAN. Nous avons ainsi fait en sorte que les outils indispensables à la réussite des travaux du festival soient accessibles via le réseau local, même en cas de perte totale du réseau Internet.

Ainsi, nous avons ajouté au réseau :

1. un serveur Etherpad monté pour l'occasion (cf. Configuration 3 de l'Annexe D) ;
2. et un serveur contenant l'intégralité de la plateforme *mmmfest.fr*, fourni par Sébastien de l'Assemblée Virtuelle.

Les adresses *pad.mmmfest.fr* et *local.mmmfest.fr* ont renvoyé vers des IP locales durant toute la durée du festival. La passerelle faisait également office de DNS menteur, pour répondre elle-même à ces adresses, dans le cas où la connexion à Internet aurait été totalement perdue (cf. fin de la Configuration 1 de l'Annexe D). Les serveurs ont été coupés de leur accès à Internet dès le début du festival, pour s'assurer qu'ils n'avaient aucune dépendance accessible en ligne.

2.1.4 Matériel

Le matériel utilisé pour le LAN est principalement de marque Ubiquiti, dans sa gamme UniFi. Le contrôleur UniFi permet d'avoir une seule et même interface, pour configurer l'intégralité des équipements compatibles (switchs, routeur et AP). Un aperçu de sa page d'accueil est disponible en Figure 3.

Le matériel acheté et déployé pour le LAN est listé en Figure 4. À la fin du festival, les 300 mètres de câbles ont été quasiment intégralement utilisés. À noter que le câble n'est pas blindé, et qu'il contient un axe en plastique central, qui rend le sertissage un peu plus laborieux. À noter également que les AP wifi ne sont pas fournies avec des injecteurs PoE, il faut donc obligatoirement les raccorder en étoile à un switch (le PoE n'est pas transmis lorsqu'on chaîne les AP entre elles). Deux lots de 5 AP ont finalement suffit (sans équiper le rez-de-chaussée), le dernier sera utilisé pour les extensions futures.

Le gros manque de notre devis a été l'onduleur. Le réseau électrique du domaine étant instable (18A pour tout le domaine), tout ce matériel coûteux mériterait d'être protégé des coupures et surtensions.

2.1.5 Extensions du réseau wifi

L'extension du réseau wifi à la grande cour entre le Petit Château et l'Orangerie a été réalisée en utilisant le matériel restant dans le stock acheté. Deux AP ont été fixées aux fenêtre du Petit Château, avec des câbles volants provenant du premier étage du Grand Château. Un switch temporaire a été posé près de la fenêtre du Grand Château, à la fois pour ajouter des ports disponibles, et pour dépasser les 100 mètres maximum des câbles ethernet cuivrés. Des photos d'illustration sont disponibles dans la Figure 20 de l'Annexe C.

La couverture wifi a ensuite été étendue à l'Orangerie. Ne disposant plus d'assez de câble pour atteindre le lieu, un pont wifi a été utilisé pour relier l'Orangerie à l'une des AP accrochées à l'extérieur du Petit Château. Une antenne NanoStation LocoM5 (prêtée par Lorraine Data Network) a été posée sur la fenêtre de l'Orangerie en mode

FIGURE 3 – Aperçu de l'interface du contrôleur UniFi

Nb	Produit	Description	Prix TTC x1
1	Network Tools Kit (4 Tools)	LSA Punch Down Tool, Modular Crimp Tool 8P8C, Stripping Tool, Cable Tester RJ11 & RJ12 & RJ45 https://www.eurodk.com/en/products/ethernet-tools/network-tools-kit-4-tools	18€
1	ToughCable Connectors	Specifically designed for use wtih Ubiquiti ToughCable, 100 pack https://www.eurodk.com/en/products/connectors/toughcable-connectors	44.50€
3	UniFi AC Pro 5-pack	Indoor/Outdoor 2.4GHz 450Mbps & 5GHz 1300Mbps, 2xGLAN, 802.11ac https://www.eurodk.com/en/products/unifi/unifi-ac-pro-5-pack	564.20€
3	UniFi Switch 8 150W	8 Gigabit Ports & 2 SFP Cages, Max. Power Consumption 150W https://www.eurodk.com/en/products/8-ports/unifi-switch-8-150w	177€
1	UniFi Cable CAT6 CMR (300m)	Category 6, Up to 10G Ethernet, 23 AWG Solid Copper Conductor Pairs https://www.eurodk.com/en/products/lan-cables-c/unifi-cable-cat6-cmr	142.60€
1	UniFi Security Gateway	Enterprise Gateway Router with Gigabit Ethernet and Integrated with UniFi Controller https://www.eurodk.com/en/products/ubnt-routers/unifi-security-gateway	101.10€
1	UniFi Cloud Key	Hybrid Cloud UniFi Device Management https://www.eurodk.com/en/products/ubnt-routers/unifi-cloud-key	71.80€
1	Livraison	Eurodk Standard (environ 2 semaines)	44€
1	PowerEdge 840	Serveur pour le service Etherpad local, prêté par Benoît	0€
1	Switch Cisco Catalyst	Prêté par Benoît pour relier la passerelle VPN	0€
1	Serveur X	Serveur pour la plateforme MMM Fest locale, prêté par Sébastien de l'Assemblée Virtuelle	0€

TABLEAU 4 – Achats pour la partie LAN : total de 2645.60€ TTC

Station, en direction de l'AP extérieure. À l'intérieur de l'Orangerie, une AP classique aurait pu être utilisée : mais en l'absence d'injecteurs PoE pour l'alimenter, le wifi de l'Orangerie a été diffusé avec une seconde NanoStation LocoM5 (les injecteurs PoE des NanoStation ne peuvent pas être utilisés pour les AP AC-PRO qui sont en 48V). Des photos de l'installation sont disponibles dans la Figure 20d de l'Annexe C. La configuration permettant à une NanoStation de diffuser un wifi sur lequel des ordinateurs et smartphones sont capables de se connecter (uniquement en 5Ghz avec les M5), est disponible dans la Figure 21.

Les antennes AC-PRO sont prévues pour être outdoor, ce qui n'était pas le cas du câble ethernet utilisé (principal risque de dégradation lié à l'exposition aux UV). Étant donnée la durée du festival, ce détail n'a cependant pas

posé de problème. Toutes les extensions (antennes extérieures et NanoStation) ont été retirées et décâblées à l'issue du festival. Elles seront éventuellement reproduites plus tard, en prenant soin de dissimuler proprement les câbles et d'installer correctement le matériel.

2.2 Partie WAN

2.2.1 Études préliminaires

Plusieurs solutions ont été envisagées, pour relier le château à une connexion Internet, suffisamment puissante pour accueillir 150 personnes :

— Nous n'avons trouvé aucun bâtiment à vue qui serait équipé d'une bonne connexion à Internet : la solution du pont wifi directionnel a donc été abandonnée.

— Les devis effectués par SFR et Bouygues Télécom ont tous les deux conclus à une inégibilité du château à la 4G. Le service client de Orange n'a pas été capable de fournir des données fiables en terme d'éligibilité, et Free ne propose aucune offre de type « Box 4G » ou « Événementiel 4G ».

— Le satellite aurait été possible, avec un abonnement de 200€/mois et des recharges data de 200 Go à 400€ l'unité (22 Mbps en down et 8 Mbps en up en théorie, avec une latence de plusieurs secondes). C'est la solution qui avait été retenue pour la POC21 [5], et nous avions la possibilité de réutiliser leur matériel, moyennant l'embauche d'un·e antenniste. Mais de l'aveu des organisateurs, cette solution n'était pas la bonne : elle a coûté plusieurs milliers d'euros à l'organisation, tout en étant une source de tension durant tout l'événement. Les connexions par satellites sont onéreuses, lentes et aléatoires.

— Toute autre solution (ouverture et agrégation de lignes ADSL, raccordement à une DSP THD, etc) ne semblait pas envisageable à mettre en place en quelques semaines.

La seule solution qui semblait réalisable était de parier sur la qualité maximum qu'on pouvait obtenir de la 4G Orange et Free, et d'utiliser des abonnements destinés à des usages personnels. L'inconvénient de cette solution étant qu'elle est contractuellement interdite, et que les opérateurs peuvent à tout moment décider de faire chuter le débit, s'ils réalisent qu'il y a trop de connexions simultanées, ou que la consommation de data est trop élevée (forfait illimité ou non).

2.2.2 Réalisation

Le château est situé sur un point haut de le région, et est à vue de plusieurs antennes téléphoniques.

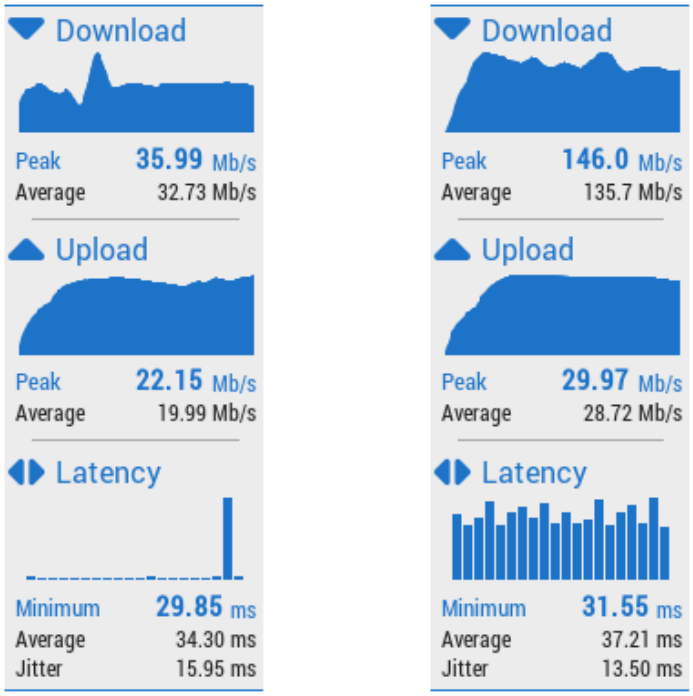
Éligibilité et débits Après étude des antennes alentour grâce aux données issues de l'ANFR et l'ARCEP [6], nous constatons que Orange possède une antenne 4G en activité à proximité. Free en possède également une, mais le site n'est pas capable de confirmer son activation. Les tests de la 4G de Orange depuis le toit du château, avec un smartphone personnel, ont indiqué que le débit était plutôt bon (plusieurs dizaines de Mbps). Par contre, il nous a été impossible de trouver quelqu'un avec un téléphone 4G avec un abonnement Free. Seule l'employé·e de ménage a été capable de nous confirmer qu'ille utilisait auparavant un forfait Free et qu'il lui semblait bien avoir de la 4G au château.

Matériel Des modems 4G et des antennes 4G extérieures directionnelles ont été commandées, pour obtenir les meilleurs débits possibles. La documentation du Camp Climat Espère 2016 [7] a permis de nous conforter dans notre direction, et de nous orienter vers les bons modems 4G.

5. http://www.poc21.cc / https://lafonderie-idf.fr/infographie-poc21/
6. En particulier : https://www.monreseaumobile.fr
7. https://docs.google.com/document/d/1XUwNMmq9NnPVhJ5x7KZ8JZi5LcN9hcUui0lcItw3yzc/

Forfaits 4G Orange ne propose aucun forfait 4G illimité. Nous nous sommes rabattus sur le Jet 100Go à 45€ (en promo), malgré l'engagement sur 12 mois. Afin d'améliorer le débit moyen, d'avoir un lien redondant, et d'anticiper une éventuelle sanction de Orange durant le festival, un forfait 4G « illimité » Free à 15.99€ est également commandé. Cette commande s'est faite en croisant les doigts pour que Free soit finalement effectivement un bon candidat. La carte SIM Free est arrivée avec 4 jours d'avance, tandis que celle de Orange n'était toujours pas arrivée au début du festival. Le forfait Orange a finalement été remplacé en urgence par un forfait Orange Parnasse Mobile (sorte de service client Orange pour millionnaires[8]) qui propose de la 4G « illimitée » à 120€, sans engagement.

Tests en conditions réelles Le matériel et les cartes SIM n'ont été disponibles que quelques jours avant le festival. Les tests de débit (jusqu'à 140 Mbps pour Free, cf. Figure 5) ont confirmé que nous avions fait les bons choix. Les antennes ont été fixées sur des mâts aux cheminées (cf. Figure 6), en pointant vers le Nord pour Free et vers le Sud pour Orange.



(a) Orange (b) Free

FIGURE 5 – Tests de débit de la 4G de Orange et Free, depuis les toits du château, avec des antennes directionnelles (tests effectués avec `http://www.ariase.com/fr/vitesse/`)

La connexion WAN du réseau déployé consiste donc à faire du load balancing sur deux connexions 4G, de deux opérateurs différents, situés sur des antennes physiques différentes. Pour plus de sécurité, des tunnels VPN ont également été montés sur ces connexions.

8. À titre d'exemple, alors que nous n'avons jamais réussi à avoir un·e commercial·e Orange au téléphone en utilisant les services client classiques, le commercial Parnasse est venu de Paris avec sa voiture pour nous déposer la carte SIM en mains propres, le lendemain de la commande. Lorsque nous avons eu un problème à l'activation, nous nous sommes retrouvés à avoir jusqu'à deux correspondant·e·s à la fois, sur deux téléphones différents. Voici la politique sociale de Orange.

(a) Antenne 4G

(b) Antenne 4G côté Sud (vers Orange)

(c) Antenne 4G côté Nord (vers Free)

(d) Modems 4G temporairement dans le grenier, sous le seau (câbles co-axiaux noirs vers le toit, et câbles ethernet blancs vers l'étage inférieur)

(e) Passage d'étage des liens 4G

FIGURE 6 – Installations 4G liées au WAN

2.2.3 Tunnels VPN

Les deux connexions 4G ont été équipées de tunnels VPN chiffrés, fournis par Lorraine Data Network [9] (LDN), membre de la Fédération FFDN [10]. Les VPN des FAI membres de FFDN permettent d'accéder à un Internet « propre et nettoyé » [11], en les surchargeant par des accès non-filtrés, non-bridés, respectueux de la vie privée et de la Neutralité du Net.

L'utilisation de tunnels VPN sur les liens 4G a également permis de réduire le risque de subir une réduction du débit, dû à notre usage non-contractuel des forfaits (l'opérateur ne voit plus qu'une seule et unique session active, vers un seul serveur).

Le bilan des achats et abonnements pour la partie WAN est disponible dans la Figure 7.

2.2.4 Load balancing et VPN

Dans un premier temps, la Security Gateway a été directement utilisée pour faire le load balancing entre deux interfaces correspondant à des tunnels VPN (un tunnel correspondant à un port WAN). La Configuration 1 de l'Annexe D correspond aux commandes utilisées dans l'interface CLI de la Security Gateway, pour y parvenir.

Ces fonctionnalités ne sont pas disponibles via le contrôleur, et ce dernier écrase les configurations dont il n'est pas responsable. Pour lui faire appliquer les modifications persos lorsqu'il écrase toute la configuration de la gateway, il est nécessaire d'ajouter un fichier JSON dans son arborescence. Une fois les modifications faites en

9. https://ldn-fai.net
10. https://ffdn.org
11. Définition d'après https://cfacile.labriqueinter.net. Ceci est un placement de produit malicieux.

Nb	Produit	Description	Prix TTC x1
2	Huawei E5186s-22a	Routeur 4G+ LTE-A blanc Gigabit WiFi AC https://www.amazon.fr/dp/B018TO4I9W/ref=pe_3044141_185740131_TE_item	160€
2	Poynting XPOL-A002	Antenne 4G outdoor directionnelle https://www.amazon.fr/dp/B00PUVLPA8/ref=pe_3044141_185740131_TE_item	163.40€
1	Livraison	Amazon Express en 1 jour ouvré	10.00€
1	Abonnement 4G Orange Parnasse	Illimité, sans engagement, réservé aux membres Parnasse	120€/mois
1	Abonnement 4G Free	Illimité, sans engagement, et lié à la Freebox du château	15.99€/mois (+ 10€ à la commande)
1	Consommation VPN	Merci à LDN qui a accepté de faire un tarif spécial événement, sans contrainte d'abonnement	30€
1	HP DC 7800	Serveur pour la passerelle VPN, prêté par Benoît	0€

TABLEAU 7 – Achats et abonnements pour la partie WAN : total de 666.80€ TTC (+ 135.99€ TTC par mois)

CLI sur la gateway, il suffit d'exporter sa configuration [12], puis d'ouvrir ce fichier pour y faire le tri à la main. Il faut faire en sorte de ne conserver que les parties personnalisées. Ce fichier est à placer en SSH dans le répertoire */srv/unifi/data/sites/default/* du contrôleur [13].

Dès la veille du festival, nous avons réalisé que les performances de la Security Gateway n'étaient pas suffisantes pour supporter le chiffrement des VPN, et qu'elle écrasait ainsi drastiquement le débit en le limitant à une dizaine de Mbps (le chiffrement et le routage des paquets OpenVPN sont gérés en userland et non en offload). C'est à cette occasion qu'une machine dédiée à été déployée, pour faire office de passerelle VPN. La Configuration 2 de l'Annexe D est celle qui a été utilisée sur cette machine (Debian stable). Via le switch, cette machine a permis de fournir deux liens WAN directement tunnelisés, sur lesquels la Security Gateway a pu se contenter de faire le load balancing.

2.2.5 Modems 4G

Les modems-routeurs Huawei E5186s sont simplissimes à configurer. Ils semblent fonctionner quel que soit l'opérateur de la carte micro-SIM, et récupèrent automatiquement la configuration des APN. L'interface web propose directement de visualiser la réception du réseau téléphonique et le mode de connexion data utilisé. Puisque ce type de matériel propose également nativement une rediffusion de son réseau en wifi, il est possible de consulter la jauge de réception de la 4G depuis un smartphone, tout en réglant les antennes (reliées en co-axial) à l'extérieur.

Dans le cadre de cette installation, les seuls réglages personnalisés sur les Huawei ont été la limitation à la 4G, la désactivation du DHCP et la suppression du réseau wifi.

2.3 Topologie finale

2.3.1 Conception

La topologie générale du réseau déployé est visible à la Figure 8. Le type de matériel correspondant aux pictogrammes, ainsi que leur situation physique dans le château, sont consultables dans l'Annexe B.

Le découpage en VLAN utilisé est le suivant :

- v_1 Management
- v_2 Servers
- v_3 Private (SSID *ChateauMillemont*, WPA2)
- v_4 Guest (SSID *MMM-Fest*, Unsecured)

12. Commande `mca-ctrl -t dump-cfg > config.gateway.json`
13. https://help.ubnt.com/hc/en-us/articles/215458888-UniFi-How-to-further-customize-USG-configuration-with-config-

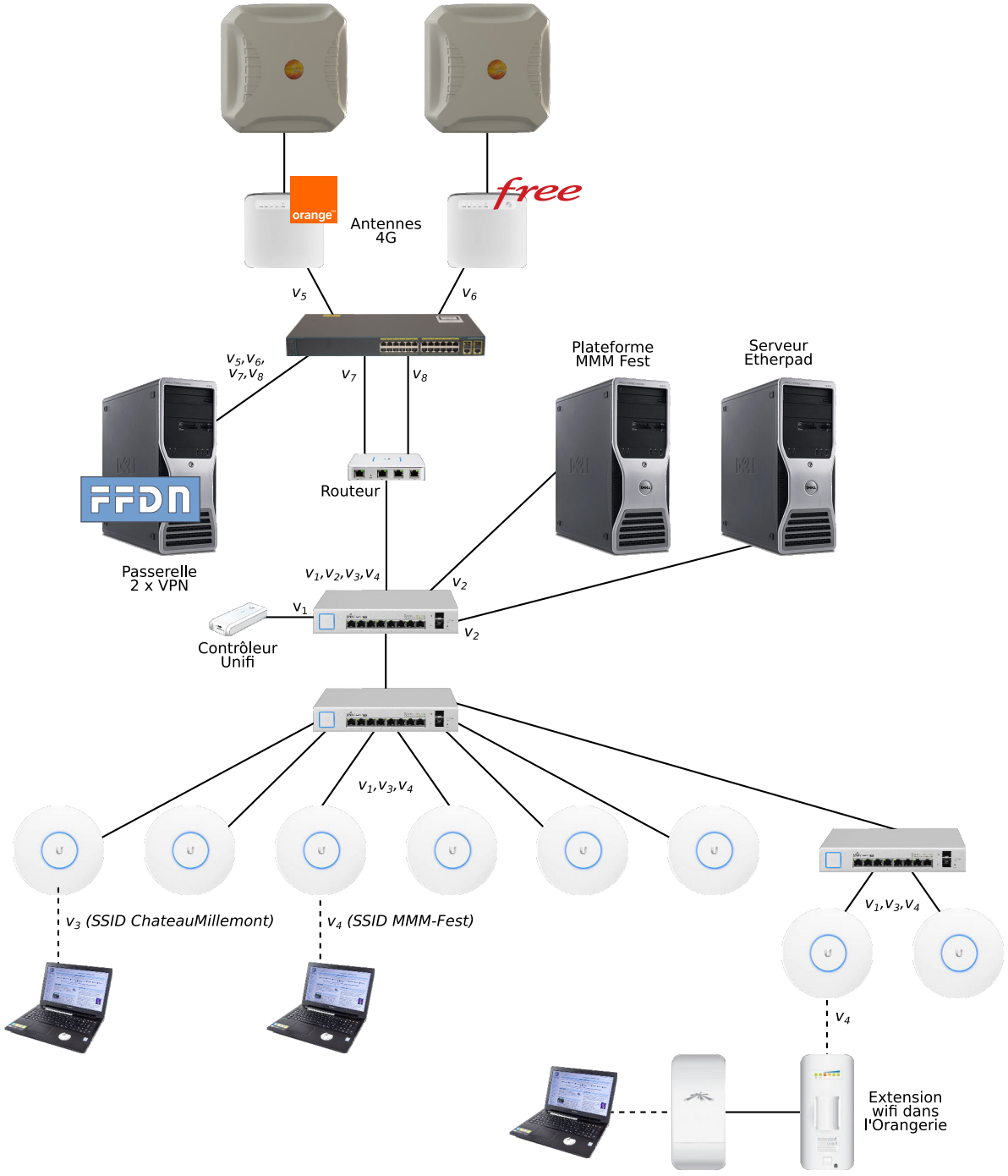


FIGURE 8 – Topologie du réseau installé (numéros de VLAN anonymisés en v_x)

Les VLAN v_{5-8} sont utilisés uniquement pour séparer la connexion+VPN de Orange de la connexion+VPN de Free. Par défaut, le pare-feu de la Security Gateway route tout le trafic entre les VLAN, à partir du moment où le réseau duquel le client a récupéré son IP, ne correspond pas à un réseau de type Guest. Il est donc nécessaire de configurer le pare-feu pour autoriser explicitement le réseau associé au SSID MMM-Fest à communiquer avec le réseau associé aux serveurs locaux.

2.3.2 Chronologie

Déroulement chronologique des principaux points d'étape :

04/09/2017 Guillaume R., co-organisateur du MMM Fest, contacte Julien V. et lui parle de la problématique de Millemont. Envoi d'un mail dans la journée à la liste des membres de FFDN, pour trouver des ami·e·s.

07/09/2017 Première visite du château de Millemont pour Adrien N. et Julien, sur un après-midi.

11/09/2017 Retour au château de Julien, qui y reste 3 jours.

12/09/2017 Première visite du château pour Benoît S.

13/09/2017 Tous les plans du château (éparpillés entre le rapport historique du château, les plans de tournage de *Coco avant Chanel* et les documents personnels du propriétaire) ont été retrouvés, numérisés et actualisés.

18/09/2017 Envoi du devis final pour toutes les installations LAN (grâce à l'aide de olb), après avoir passé du temps sur place à estimer le nombre d'AP nécessaires et leur emplacement, ainsi que repérer les points de passage possibles des câbles (entre les pièces et entre les étages), estimer leur longueur et réaliser les premiers plans réseau.

23/09/2017 Retour au château de Julien, qui y reste jusqu'à la fin du festival. Benoît dépose des serveurs de prêt et vient aider à envisager l'installation du LAN.

24/09/2017 Envoi du devis final pour toutes les installations et abonnements liés au WAN. L'étude de la bonne solution pour la connexion à Internet avait activement démarré dès la première visite du château : demandes de devis chez tous les opérateurs 4G (services clients particuliers et entreprises), échanges avec Orange Parnasse, échanges avec plusieurs personnes de POC21 sur la solution du satellite, recherche en ligne et tests sur place pour estimer la fiabilité de la 4G selon les opérateurs, recherche de bâtiments à vue avec une bonne connexion pour une solution à base de pont wifi, etc.

25/09/2017 Amazon a décidé de verrouiller le compte de Julien (ouvert pour l'occasion à contre-cœur) et d'annuler la commande. Nouvelle commande depuis le compte de Adrien en livraison express.

27/09/2017 Souscription en urgence à un forfait Orange Parnasse Mobile pour remplacer le forfait Orange initialement souscrit et pour lequel la carte SIM n'arrivera jamais à temps (temps de validation de la commande incroyablement long).

28/09/2017 Le matériel WAN et la SIM Free arrivent au château.

29/09/2017 Le matériel LAN et la SIM Orange Parnasse Mobile arrivent au château. Les câbles électriques ont été déployés dans le Grand Château par les employés. Création en urgence de deux comptes VPN chez LDN, pour remplacer ceux initialement prévus qui ne seront pas disponibles.

30/09/2017 Nous apprenons entre temps que l'installation du LAN doit être conçue de façon durable (murs percés et câbles fixés), et qu'il faudrait éviter de poser des AP au rez-de-chaussée. Dernière journée de travail entre Benoît et Julien pour déterminer la disposition exacte des câbles et des équipements, en fonction des nouvelles contraintes. La nouvelle disposition nécessite de trouver des rallonges co-axiales : après un achat raté en magasin (mauvais connecteurs) de Julien et une recherche en ligne vaine de Adrien, nous décidons de laisser temporairement les modems 4G dans le grenier, le temps du festival.

01/10/2017 L'environnement logiciel de Ubiquiti/UniFi est pris en main, et la configuration pour le load balancing sur deux tunnels VPN d'un même opérateur, directement depuis la Security Gateway, est prête (une bonne partie de la nuit est passée juste sur ce dernier point).

02/10/2017 Achat des mâts pour poser les antennes 4G, et fixation et réglage des antennes sur le toit, avec un employé. Installation des équipements et câblage du bâtiment. Deux employés nous aident pour tirer les câbles et prennent en charge la perforation des murs (passages de câbles et pose des AP). Julien et Benoît sertissent les câbles, aménagent et installent les locaux techniques, et procèdent aux premiers tests.

03/10/2017 Second jour d'installation et de tests avec les employés. Installation et configuration en parallèle du serveur Etherpad. La Security Gateway avec les VPN écrase beaucoup trop le débit des liens WAN :

installation et configuration en urgence d'un serveur de spare pour créer une passerelle VPN, et ajout d'un nouveau switch de prêt pour le brassage. Le serveur de la plateforme MMM Fest arrive en soirée et est relié au réseau, après quelques modifications dans sa configuration.

04/10/2017 Premier jour de festival ! Premiers retour très encourageants des participant·e·s.

05/10/2017 Extension du réseau wifi, en ajoutant un switch temporaire et deux AP sur la façade du Petit Château, pour couvrir l'extérieur.

08/10/2017 Extension du réseau wifi, en ajoutant une paire de NanoStation LocoM5, pour couvrir l'intérieur de l'Orangerie.

10/10/2017 Démontage des extensions temporaires en soirée, et retrait des matériels de prêt, spécifiques au festival.

21/10/2017 Première version de ce compte-rendu d'expérience.

3 Durant le festival

Les retours pris sur le terrain ont été globalement très bon durant tout le festival.

Quelques accidents ponctuels ont eu lieu :

— Une baisse de débit subite a eu lieu le premier jour. En montant sur le toit, nous y avons trouvé un couvreur en train de prendre sa pause en fumant une cigarette juste devant l'antenne 4G qui pointait vers Orange.

— Avec notre accord, un·e bénévole a souhaité travailler sur le portage OpenWRT d'une AP wifi de spare. Il s'est branché sur le switch du premier étage, en libérant un port sur lequel était relié l'AP d'une salle à proximité. Il avait bien vérifié avant que la salle n'était pas actuellement occupée, mais n'a pas réalisé que les AP du premier étage couvrent également le rez-de-chaussée.

— Des participant·e·s ont dormi dans le Grand Château durant le festival. L'une de ces personnes ne souhaitait pas subir les ondes wifi durant la nuit, alors qu'il n'y avait plus d'activité le château. Elle a suivi le câble ethernet d'upstream qui reliait le local technique principal au switch du premier étage, et l'a débranché sur ce dernier. Cette initiative a eu pour conséquence de couper l'accès à Internet de toutes les AP (y compris celles à l'extérieur et à l'Orangerie)... sans pour autant couper l'émission des ondes. Nous lui avons indiqué être favorables à trouver un compromis pour les prochaines nuits, en tentant de baliser des zones « sans » wifi, mais elle n'est pas revenu vers nous ensuite.

— Sur le réseau MMM-Fest, un portail captif était actif : il ne demandait aucune authentification (simplement de cliquer sur un bouton « Connect »), mais faisait office d'accueil sur le réseau, en expliquant qu'il fallait éviter les usages consommateurs, comme le streaming vidéo, pour réduire la consommation data des forfaits 4G. Les portails captifs fonctionnent particulièrement bien sur les smartphones, qui les détectent et redirigent automatiquement dessus. Dans les autres cas, il est impératif, la première fois, d'ouvrir son navigateur sur un site en HTTP, pour que la redirection vers le portail captif fonctionne (la Security Gatewat propose de faire des redirections HTTPS, mais elles impliquent de demander de prendre l'habitude de lever une exception de sécurité). Quelques personnes sont venues nous voir en nous indiquant que l'accès à Internet ne fonctionnait pas pour eux : leur navigateur s'ouvrait systématiquement sur une page en HTTPS, notamment pour les recherches Google. Le portail captif a fini par être tout simplement désactivé.

— Nous avons régulièrement surveillé l'activité sur le réseau, pour détecter les usages très consommateurs. Nous avons eu deux cas de périphérique qui consommaient à eux seuls le total de toutes les autres connexions (plusieurs Go). Grâce aux noms des périphériques et aux AP sur lesquelles ils étaient branchés, nous avons pu aller à leur rencontre, et leur demander de vérifier s'ils n'avaient pas un streaming vidéo non indispensable qui tournerait. Dans le premier cas, la personne avait effectivement un onglet YouTube pour écouter de la musique (même dans ce cas, YouTube fait passer un flux vidéo). Elle pouvait s'en passer sans aucun problème, elle n'avait simplement pas réalisé que ça consommait autant. Dans le second cas, le pic de trafic correspondait à un transfert de fichiers ponctuel, dans le cadre d'un workshop. Nous précisons que le réseau n'analyse aucune

des activités des personnes connectées, et se contente d'afficher des compteurs de consommation en octets associés à des adresses MAC.

— Un câble ethernet qui traversait un couloir a difficilement résisté au passage des participant·e·s. Le ducttape dessus était en parfait état, mais les brins de cuivre étaient à nu sur une partie du câble ethernet.

— La Security Gateway a été décommissionnée (et donc réinitialisée) par erreur depuis le contrôleur UniFi, lors du démontage des extensions réseau temporaires. Une fois la Security Gateway réinstallée et de nouveau adoptée par le contrôleur, tous les autres équipements UniFi du réseau se sont retrouvés mystérieusement orphelins et impossible à adopter. Ils ont dû tous être réinitialisés pour être de nouveau adoptés par le contrôleur. Nous supposons que ce problème est lié à l'attribution des IP de management par DHCP : utiliser des IP fixes pour les équipements réseau pourrait être une solution plus stable à l'avenir.

Deux problèmes durables ont également eu lieu :

1. Les connexions 4G sont capricieuses (météo, encombrement des antennes, maintenance, etc). Les chutes de débit ponctuelles ont été courantes, ce qui a suffit à donner l'impression à quelques personnes d'avoir des coupures.
2. Le serveur utilisé pour la passerelle VPN (Celeron 1.80 Ghz) n'a pas suffit pour encaisser les opérations de chiffrement liées au trafic passant dans les tunnels VPN. De courts – mais relativement fréquents – pics de CPU à 100% ont été constatés, et plusieurs personnes se sont plaintes d'un réseau dégradé, lorsqu'on activait les VPN. Ces derniers n'auront donc été finalement activés que peu de temps durant le festival.

La consommation totale durant la semaine aura été d'environ 30 Go. La moyenne de consommation par périphérique connecté au réseau, aura été de moins de 300 Mo (cf. statistiques de la Figure 9).

Minimum	8.5 KB
1er quartile	28.0 MB
Médiane	85.5 MB
Moyenne	277.0 MB
3e quartile	302.2 MB
Maximum	2.9 GB

(a) Download

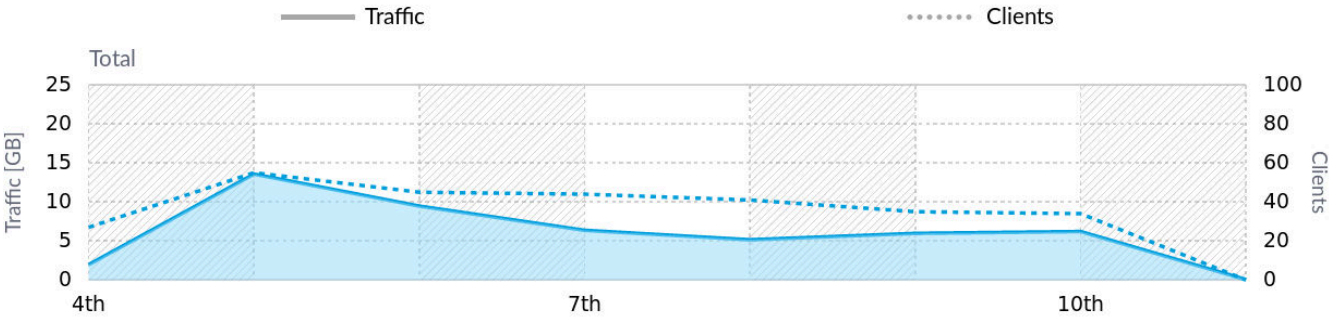
Minimum	5.1 KB
1er quartile	4.8 MB
Médiane	19.2 MB
Moyenne	86.9 MB
3e quartile	70.2 MB
Maximum	1.5 GB

(b) Upload

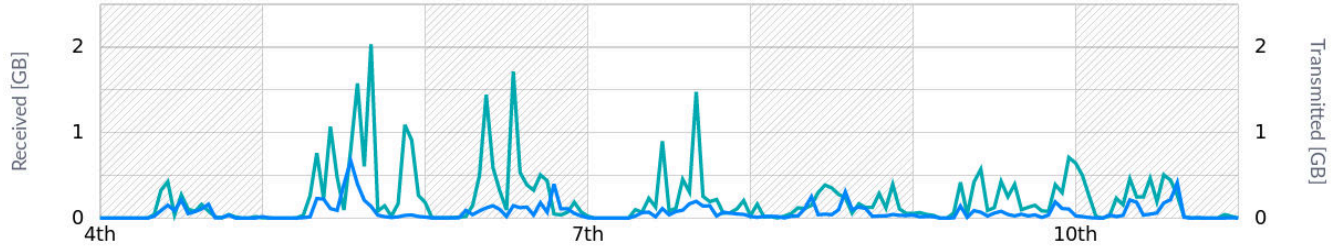
Tableau 9 – Consommation de données par client, sur 132 clients, avec un total sur la durée du festival de environ 30 GB en download

La consommation totale aura été bien en deçà de ce qui était planifié, et nous a donné l'assurance de ne pas être bridé par les opérateurs. Cependant, si chaque participant·e avait librement utilisé des plateformes vidéos sans se restreindre, la consommation serait facilement montée en flèche, jusqu'à en devenir éventuellement critique (on estime à 100-150 Go par forfait le seuil critique pour lever des alertes). Il semble compliqué de trouver le bon compromis dans le discours à tenir. La Figure 10 indique l'évolution de la consommation, durant la semaine du festival.

Enfin, puisque les adresses MAC des périphériques connectés correspondent à des constructeurs particuliers, la Figure 11 permet de constater que Apple aura été le grand vainqueur de la semaine.



(a) Trafic réseau du point de vue des AP



(b) Trafic réseau du point de vue du routeur (Tx en bleu, Rx en vert)

FIGURE 10 – Statistiques trafic

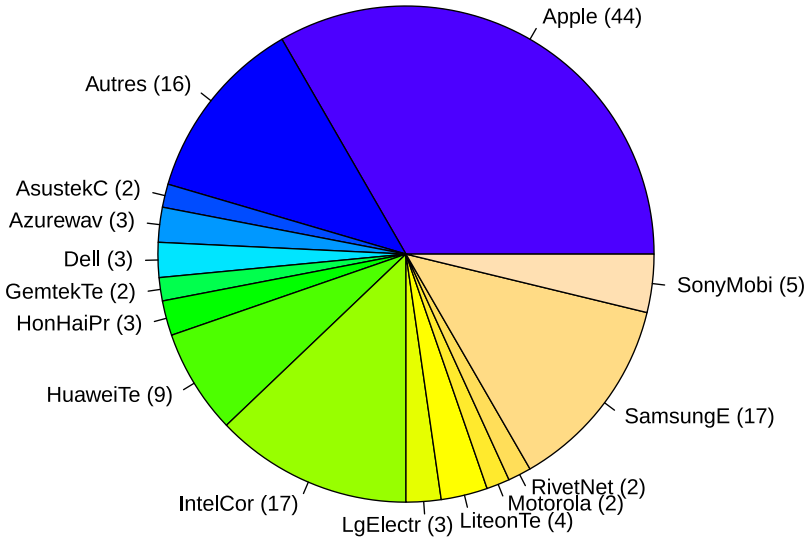


FIGURE 11 – Type de matériel utilisé par les clients

4 Perspectives

4.1 À court terme

À court terme, le réseau actuel aurait besoin d'être légèrement amélioré :

— Il faudrait ajouter un onduleur. Le propriétaire y est favorable, il faut juste faire une proposition et l'installer.

— Les modems 4G ne devraient pas rester dans le grenier. Ils auraient plutôt leur place dans le local technique

principal, qui est plus simple à sécuriser. Pour cela, il faut acheter des rallonges de câbles co-axiaux pour les antennes (deux par antenne), d'environ 15 mètres chacune. Attention toutefois, ce n'est pas le même co-axial que celui utilisé pour les équipements TV (type F), et il est plus souvent vendu comme câble pour antenne wifi. Il faut également bien vérifier la compatibilité des connecteurs (l'écrou et la vis sont parfois inversés) :

- Connecteur des antennes :
  - type RP-SMA ;
  - mâle (petite pointe au milieu) ;
  - avec un pas de vis intérieur (comme un écrou) ;
  - `https://lut.im/grCNW6skO0/OB3BM2Rmjk7ayU4r.JPG`
- Connecteur des modems :
  - type RP-SMA ;
  - femelle (petit trou au milieu) ;
  - avec un pas de vis extérieur (comme une vis) ;
  - `https://lut.im/9L3Nw39bpK/abpyAoqIsQMSmaeV.JPG`

- La passerelle VPN a été retirée, puisque la machine appartenait à Benoît. Il faudrait en racheter une plus puissante, et souscrire à deux abonnements VPN associatifs. Le propriétaire est d'accord pour le faire, et semble vouloir encourager ce type d'association.
- Le contrôleur UniFi est actuellement connecté au « cloud » de `https://unifi.ubnt.com`. Cette possibilité offerte par Ubiquiti, permet d'avoir accès au contrôleur du réseau local depuis Internet et donc de superviser et administrer le réseau à distance (elle a notamment permis de détecter la coupure de nuit du réseau, lorsque toutes les AP ont été désactivées). Puisque les simili-accès à Internet en 4G ne permettent pas d'autoriser des connexions entrantes, cette option est très pratique. Cependant, elle nécessite d'ouvrir des accès sur un réseau privé à une entreprise tierce, et n'est donc pas idéale. Une fois que la passerelle VPN sera robuste, les tunnels VPN pourront être directement utilisés pour remplacer le service en ligne de Ubiquiti.

4.2 À moyen terme

Les évolutions à moyen terme du réseau actuel pourraient être les suivantes :

- Le contrôleur UniFi est propriétaire. Il pourrait être remplacé [14], et les matériels pourraient également peut-être évoluer vers du OpenWRT.
- Remplacer le contrôleur permettrait d'arrêter de faire du vieil Internet, et ajouter l'IPv6, qui serait très simple à déployer et cohérent avec les valeurs défendues par la Fédération.
- Remplacer le contrôleur permettrait également d'éliminer les fonctionnalités de DPI qu'il propose. Elles sont naturellement désactivées depuis le début de la mise en production du réseau, mais la prochaine personne en charge de ce réseau n'aura qu'un seul bouton à cliquer pour les activer.
- Le réseau wifi pourrait être facilement étendu au Petit Château et aux dépendances. Une dizaine d'AP sont actuellement stockées sans être utilisées, et un switch est également déjà disponible en stock.

4.3 À long terme

À long terme, la 4G pourrait être remplacée par une solution plus stable et plus performante. Le propriétaire du château semble motivé pour trouver une solution, et éventuellement en faire profiter une association de la Fédération.

14. Peut-être en demandant à SCANI (`https://www.scani.fr`) quelle est leur solution à ce sujet ?

Deux solutions mériteraient d'être creusées :

1. Le département des Yvelines a construit un réseau de fibre dont la dorsale passe à proximité du domaine du château (cf. Figure 12). Cette fibre est exploitée par COVAGE [15], dans le cadre d'une délégation de service public (DSP). Il suffirait de dérouler quelques kilomètres de fibre au travers de la forêt, pour relier le château à cette dorsale. La forêt appartenant au domaine, il n'y aurait pas d'autorisation à demander pour le passage des fourreaux, et le propriétaire peut mettre à disposition du matériel pour faire une tranchée, ainsi que des employés pour gérer ce projet. Il resterait encore à connaître les modalités pour se raccorder à la dorsale. La première étape serait de demander le catalogue tarifaire lié à cette DSP. Si un FAI de la Fédération s'en charge, celui-ci pourrait alors avoir la possibilité d'obtenir un accès à la porte de collecte, pour opérer pour le château, mais aussi éventuellement pour n'importe qui d'autre qui aurait accès à cette DSP dans les villes alentour.

2. Le domaine possède deux tours Chappe [16], anciennement utilisées pour les télécommunications. L'une de ces tours, à proximité de la dorsale, pourrait être reliée en fibre, en étant suffisamment aménagée pour pouvoir abriter du matériel informatique en son sein. Un relais wifi pourrait ensuite ramener la connexion jusqu'au château (le château serait à vue, en se contentant de réduire quelques arbres, en accord avec le garde forestier). Le matériel de la tour Chappe pourrait être alimenté à l'aide de batteries et de panneaux solaires.

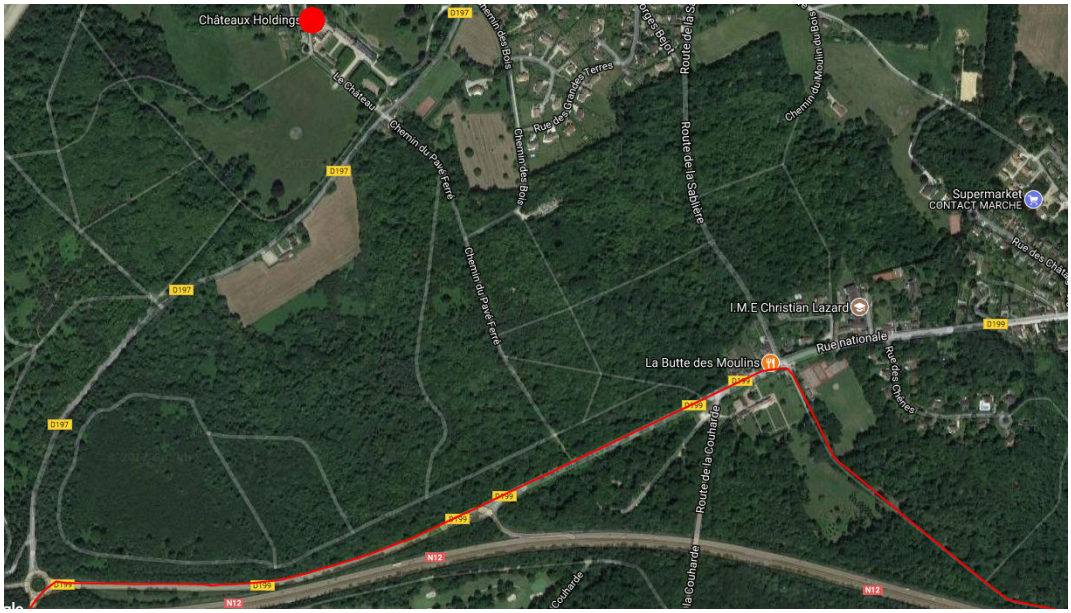


FIGURE 12 – Dorsale de fibre Covage (YVELINES THD – ligne rouge) à proximité du domaine du Château de Millemont, situé au niveau du rond rouge (`http://yvelines-thd.com/le-reseau`)

Une fois le château raccordé – d'une façon ou d'une autre – par la fibre, il sera possible d'exploiter la situation en point haut du château, pour délivrer des accès à Internet par ponts wifi aux villages alentours (actuellement en zone blanche pour certains d'entre eux). De nouveau, ce serait l'occasion pour un FAI de la Fédération d'agrandir son réseau et son champ de compétences. Cette opportunité permettrait également au château de renforcer son image de hub d'expérimentations de la région.

15. `http://yvelines-thd.com`
16. `https://fr.wikipedia.org/wiki/T%C3%A9l%C3%A9graphe_Chappe`

5 Conclusion

Le Château de Millemont est désormais équipé d'un réseau informatique parfaitement fonctionnel, avec du matériel de qualité. La connexion Internet dépasse les 100Mbps, et est redondée avec deux opérateurs différents, situés sur deux antennes physiques différentes, à plusieurs kilomètres de distance.

Les opportunités pour les associations de la Fédération FFDN sont désormais nombreuses dans ce lieu, en particulier après cette expérience concluante : il ne reste plus qu'à les saisir.

A Illustrations générales

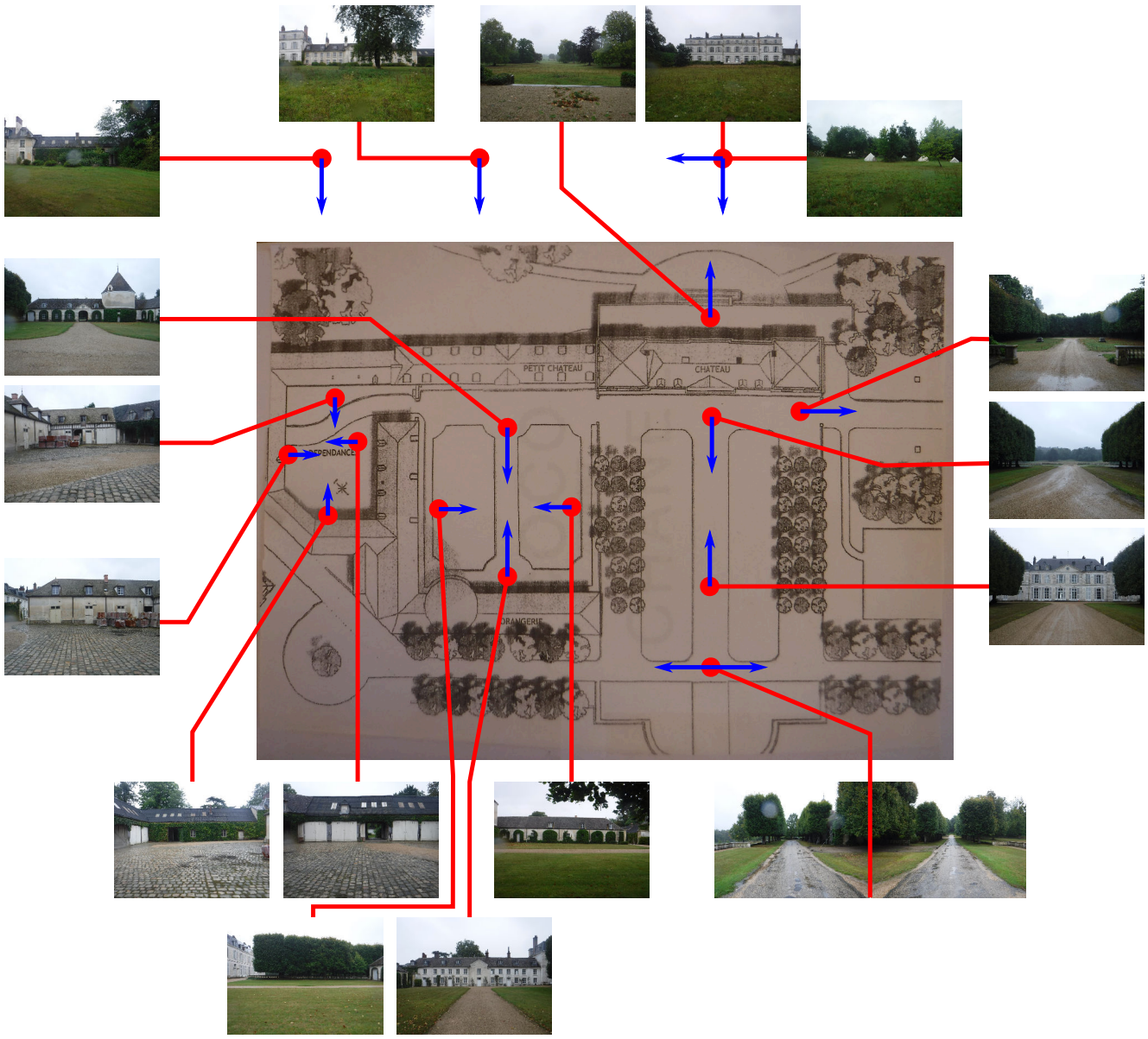


FIGURE 13 – Vues extérieures du site des deux châteaux et leurs dépendances

(a) Boudoir (b) Salle de billard (c) Grand salon (vers l'Ouest)

(d) Escalier principal (e) Salon des voyageurs (f) Bibliothèque (vers l'Ouest)

(g) Bibliothèque (vers l'Est) (h) Grand salon (vers le Sud) (i) Depuis la salle du tronc

FIGURE 14 – Aperçu de quelques pièces du rez-de-chaussée du Grand Château

(a) Chambre de Gabrielle (b) Grand chambre blanche (c) Couloir principal

(d) Escalier principal (e) Salle de bain de Gabrielle (f) Chambre rouge

(g) Escalier principal (h) Chambre bleue (i) Escalier de service (j) Entrée de chambre

FIGURE 15 – Aperçu de quelques pièces du premier étage du Grand Château

B Plan de placement des équipements

FIGURE 16 – Situation géographique des équipements (les plans ont malheureusement été floutés pour être intégrés à ce document, de façon à ne pas les rendre publics, à la demande du propriétaire)

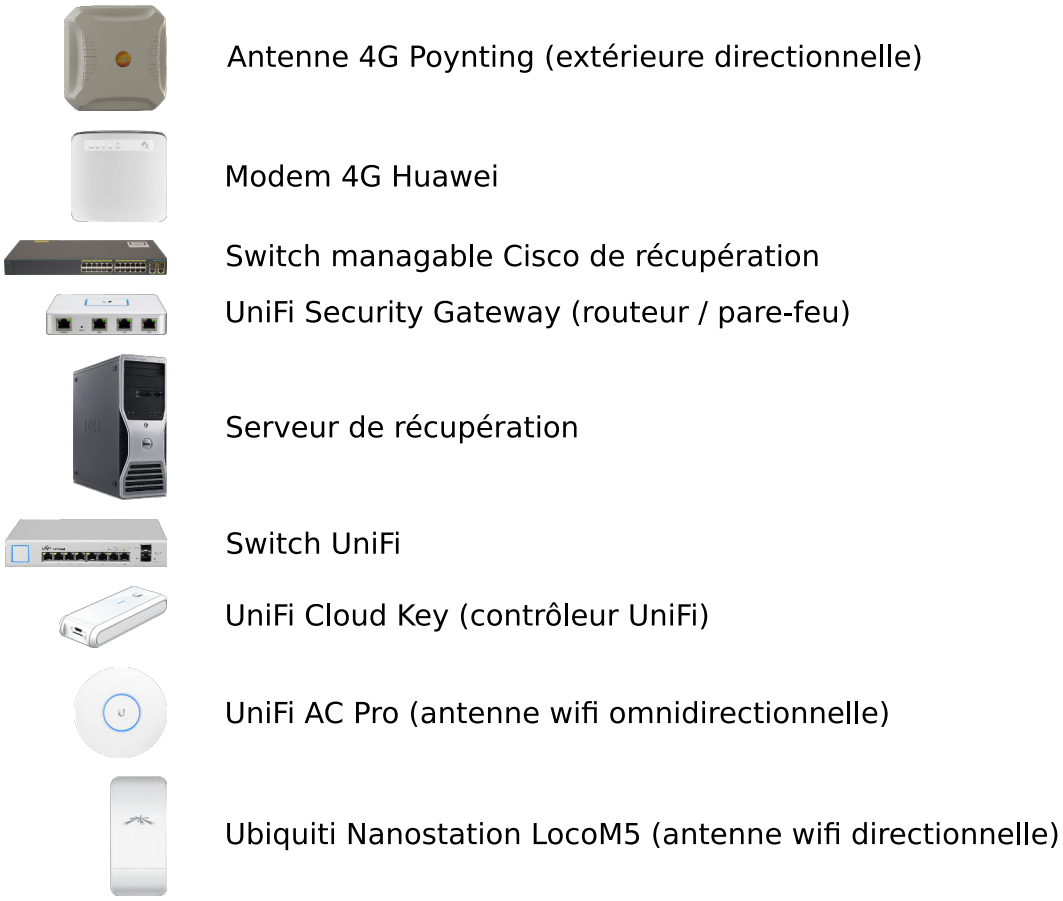


FIGURE 17 – Pictogrammes correspondant aux équipements utilisés

C Photos des installations LAN

(a) Switch du premier étage

(b) Câblage intérieur (câbles électriques noirs au sol le temps du festival)

(c) Vue d'ensemble du local technique principal, en entresol à l'Est du Grand Château

(d) Local technique principal : armoire des serveurs

(e) Local technique principal : armoire du cœur de réseau

FIGURE 18 – Locaux techniques

(a) Chambre rouge (b) Petite chambre blanche (c) Salle de bain de Gabrielle

(d) Chambre bleue (e) Grande chambre blanche (f) Chambre de Gabrielle

FIGURE 19 – Les AP wifi du Grand Château

(a) AP wifi extérieures

(b) Câblage temporaire par l'extérieur

(c) Switch temporaire vers l'extérieur, dans la boîte en plastique

(d) Relais wifi dans l'Orangerie

FIGURE 20 – Installations temporaires le temps du festival

D Configurations

```
# Before applying these commands, you have to check this option through the web interface of the controler:
# Settings > Configure VOIP port as WAN2 on UniFi Security Gateway 3P

configure

set protocols static table 2 route 0.0.0.0/0 next-hop <IP_WAN2_REMOTE_GW>
ip rule add from <IP_WAN2_LOCAL_IP> table 2

set interfaces openvpn vtun0 config-file /config/openvpn/vpn1/client.conf
set interfaces openvpn vtun1 config-file /config/openvpn/vpn2/client.conf

commit

set service nat rule 5004 destination address 0.0.0.0/0
set service nat rule 5004 outbound-interface vtun0
set service nat rule 5004 type masquerade

set service nat rule 5005 destination address 0.0.0.0/0
set service nat rule 5005 outbound-interface vtun1
set service nat rule 5005 type masquerade

set protocols static table 10 interface-route 0.0.0.0/0 next-hop-interface vtun0
set protocols static table 20 interface-route 0.0.0.0/0 next-hop-interface vtun1

set load-balance group wan_failover interface vtun0
set load-balance group wan_failover interface vtun0 route table 10
set load-balance group wan_failover interface vtun0 route-test initial-delay 20
set load-balance group wan_failover interface vtun0 route-test interval 10
set load-balance group wan_failover interface vtun0 weight 50

set load-balance group wan_failover interface vtun1
set load-balance group wan_failover interface vtun1 route table 20
set load-balance group wan_failover interface vtun1 route-test initial-delay 20
set load-balance group wan_failover interface vtun1 route-test interval 10
set load-balance group wan_failover interface vtun1 weight 50

delete load-balance group wan_failover interface eth0
delete load-balance group wan_failover interface eth2

# DNS menteur
set system static-host-mapping host-name local.mmmfest.fr inet 10.2.0.10
set system static-host-mapping host-name pad.mmmfest.fr inet 10.2.0.40
set system static-host-mapping host-name pad1.mmmfest.fr inet 10.2.0.41
set system static-host-mapping host-name pad2.mmmfest.fr inet 10.2.0.42
set system static-host-mapping host-name pad3.mmmfest.fr inet 10.2.0.43

commit
save
```

Configuration 1 – Load balancing entre deux VPN sur deux WAN, directement depuis la Security Gateway (+ DNS menteur pour les serveurs locaux)

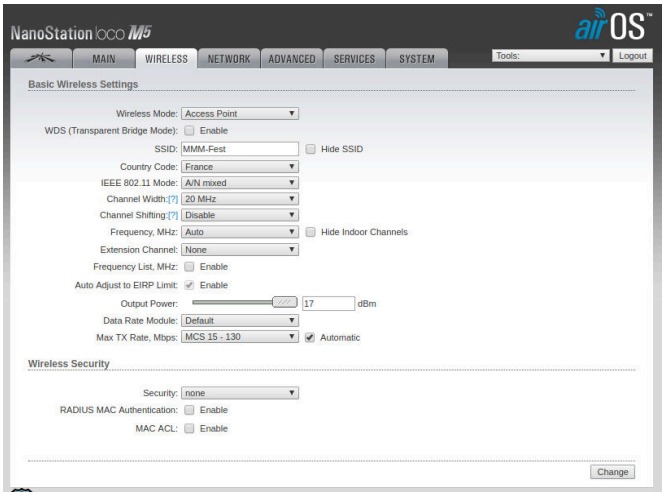
```
#!/bin/bash

set -xe

# echo 'nameserver 80.67.188.188' > /etc/resolv.conf
# echo 'nameserver 80.67.169.12' >> /etc/resolv.conf
# chattr +i /etc/resolv.conf

ip link add link enp0s25 name enp0s25.<VLAN_v5> type vlan id <VLAN_v5>
ip link add link enp0s25 name enp0s25.<VLAN_v6> type vlan id <VLAN_v6>
ip link add link enp0s25 name enp0s25.<VLAN_v7> type vlan id <VLAN_v7>
ip link add link enp0s25 name enp0s25.<VLAN_v8> type vlan id <VLAN_v8>

ip netns add vpn1
ip netns add vpn2

ip netns exec vpn1 sysctl -w net.ipv4.ip_forward=1
ip netns exec vpn2 sysctl -w net.ipv4.ip_forward=1

ip link set enp0s25.<VLAN_v5> netns vpn1
ip link set enp0s25.<VLAN_v6> netns vpn2
ip link set enp0s25.<VLAN_v7> netns vpn1
ip link set enp0s25.<VLAN_v8> netns vpn2

ip netns exec vpn1 ip link set enp0s25.<VLAN_v5> up
ip netns exec vpn2 ip link set enp0s25.<VLAN_v6> up
ip netns exec vpn1 ip link set enp0s25.<VLAN_v7> up
ip netns exec vpn2 ip link set enp0s25.<VLAN_v8> up

ip netns exec vpn1 ip addr add 192.168.5.42/24 dev enp0s25.<VLAN_v5>
ip netns exec vpn1 ip route add default via 192.168.5.1
ip netns exec vpn2 ip addr add 192.168.6.42/24 dev enp0s25.<VLAN_v6>
ip netns exec vpn2 ip route add default via 192.168.6.1

ip netns exec vpn1 ip addr add 192.168.7.1/24 dev enp0s25.<VLAN_v7>
ip netns exec vpn2 ip addr add 192.168.8.1/24 dev enp0s25.<VLAN_v8>

ip netns exec vpn1 openvpn --config /root/openvpn/vpn1/client.conf &
ip netns exec vpn2 openvpn --config /root/openvpn/vpn2/client.conf &

sleep 5m

ip netns exec vpn1 iptables -t nat -A POSTROUTING -o tun0 -j MASQUERADE
ip netns exec vpn2 iptables -t nat -A POSTROUTING -o tun0 -j MASQUERADE

exit 0
```

Configuration 2 – Configuration de la passerelle VPN : création de deux VLAN correspondant aux deux WAN, mais directement avec tunnels VPN (le load balancing reste ainsi géré par la Security Gateway)

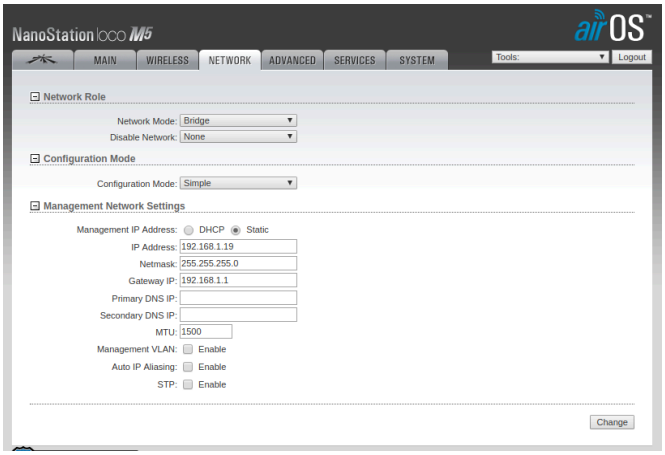
```
#!/bin/bash

set -xe

# echo 'nameserver 80.67.188.188' > /etc/resolv.conf
# echo 'nameserver 80.67.169.12' >> /etc/resolv.conf
# chattr +i /etc/resolv.conf

ip addr add 10.2.0.41/24 dev enp5s0
ip addr add 10.2.0.42/24 dev enp5s0

su etherpad -c '/opt/etherpad-lite/bin/run.sh -s /opt/etherpad-lite/settings_pad1.json' &
su etherpad -c '/opt/etherpad-lite/bin/run.sh -s /opt/etherpad-lite/settings_pad2.json' &

iptables -t nat -A PREROUTING -i enp5s0 -p tcp -d 10.2.0.41 --dport 80 -j DNAT --to-destination 10.2.0.41:9001
iptables -t nat -A PREROUTING -i enp5s0 -p tcp -d 10.2.0.42 --dport 80 -j DNAT --to-destination 10.2.0.42:9001

systemctl start nginx

exit 0
```

Configuration 3 – Configuration du serveur Etherpad : lancement de deux instances

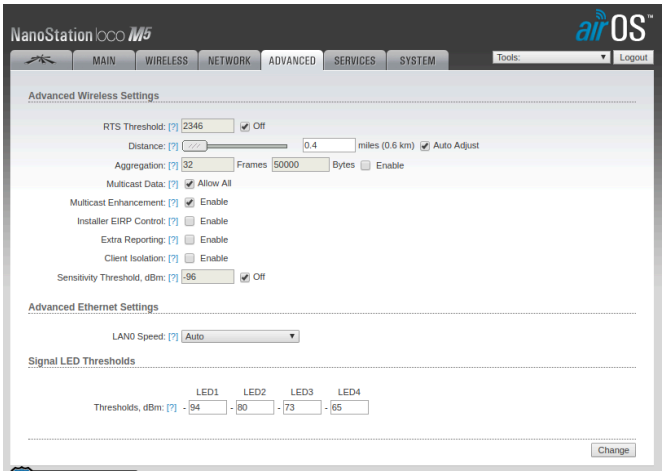
(a) Penser à désactiver airMax



(b) Mode Access Point pour diffuser un réseau wifi (uniquement en 5Ghz pour les M5)



(c) Mode Bridge : c'est le DHCP derrière l'AP à laquelle elle sera connectée, qui délivrera les adresses sur ce wifi



(d) Quelques paramètres à désactiver, pour que les ordinateurs et smartphones se connectent sans problème

FIGURE 21 – Configuration d'une Nanostation LocoM5 à utiliser en AP pour ordinateurs et smartphones