

Généralisation des équipements individuels mobiles (EIM)



REFERENTIEL TECHNIQUE POUR LA MISE EN ŒUVRE DE L'INFRASTRUCTURE WI-FI

Version 2.1
Juin 2022

SOMMAIRE

1. Introduction	3
1.1. Contexte et ambitions du référentiel	3
1.2. Usages envisagés des EIM	3
1.3. Postulats de base relatifs au déploiement des EIM	4
2. Description de l'infrastructure Wifi cible des sites	5
2.1. Les différents éléments de l'infrastructure	5
2.2. Lien internet	6
2.3. Locaux techniques	8
2.4. Câblage VDI	10
2.5. Switch	11
2.6. Bornes	14
2.7. Contrôleur	18
2.8. Sécurité	18
3. Synthèse des prérequis	21
4. Annexes	23
4.1. Annexe 1 : Débit internet requis pour les usages courants	23
4.2. Annexe 2 : Cadre réglementaire	24
4.3. Annexe 3 : Destinataires du document	24
4.4. Annexe 4 : Lien Internet – Différences entre les supports	25
4.5. Glossaire	26

1. Introduction

1.1. CONTEXTE ET AMBITIONS DU REFERENTIEL

En accord avec le Cadre de Référence pour l'Accès aux Ressources pédagogiques via un équipement Mobile (CARMO), Le Département des Yvelines offre la possibilité d'équiper les élèves d'un outil numérique individuel (EIM).

L'utilisation de ces EIM au sein d'un site nécessite un accès Internet. L'option de connexion par un réseau mobile (4G/5G) n'est pas retenue.

Vis-à-vis du contexte précédemment énoncé, les objectifs de ce référentiel sont les suivants :

- Etablir les prérequis d'infrastructure Wifi à respecter afin de garantir la bonne utilisation des EIM dans les sites,
- Etablir les prérequis de sécurité assurant la protection des mineurs et de leurs données,
- Proposer des choix techniques en adéquation avec le contexte de chaque site,
- Respecter la réglementation en vigueur, et notamment la loi Abeille.

Suivant les directives du CARMO, SYN offre la possibilité aux établissements d'équiper les élèves d'un équipement individuel mobile (EIM) permettant d'accéder à des ressources pédagogiques numériques.

Ce référentiel décrit l'infrastructure Wifi à mettre en place les sites afin de garantir la bonne utilisation des EIM en matière d'usages et de sécurité.

1.2. USAGES ENVISAGES DES EIM

Dans le cadre de ce référentiel, l'infrastructure préconisée est adaptée aux usages des EIM uniquement. Les usages personnels ne sont pas prévus.

Les EIM seront donnés à l'ensemble des élèves et leurs enseignants afin qu'ils puissent accéder à des contenus pédagogiques et des outils de bureautiques (traitement de texte, tableur...).

Les contenus et applications concernés sont essentiellement disponibles sur Internet. Certains usages bureautiques (Word, Excel, autres...) sont également permis en étant hors-ligne.

L'enseignant pourra utiliser son EIM avec les élèves. Des logiciels lui permettront de contrôler les EIM des élèves et de projeter des contenus sur les écrans numériques de la classe.

Les EIM ne sont pas destinés au visionnage de contenu vidéo en streaming sur l'ensemble des appareils en parallèle.

Ces éléments d'usages sont pris en compte dans ce référentiel, notamment en matière de dimensionnement du débit Internet requis.

1.3. POSTULATS DE BASE RELATIFS AU DEPLOIEMENT DES EIM

1.3.1. Dimensionnement et périmètre du réseau Wifi pour les EIM

Ce référentiel s'applique en amont d'un projet de déploiement d'EIM. Son objectif principal est de donner les clés pour déployer une infrastructure Wifi qui permettra aux EIM de se connecter à Internet.

Les hypothèses de dimensionnement prises en compte par ce document sont les suivantes :

- Une classe compte 30 EIM,
- Toutes les salles de classes sont susceptibles d'utiliser les EIM et doivent être couvertes par le réseau Wifi,
- La couverture Wifi concerne l'ensemble du périmètre intérieur du site (pas de couverture en extérieur),
- 70% des classes d'un même site doivent pouvoir utiliser leurs EIM en parallèle sans baisse de qualité du service,

1.3.2. Principes de déploiement des EIM

Lorsque les EIM sont livrés au site dans lequel l'infrastructure préconisée a été déployée, ils sont prêts à l'emploi :

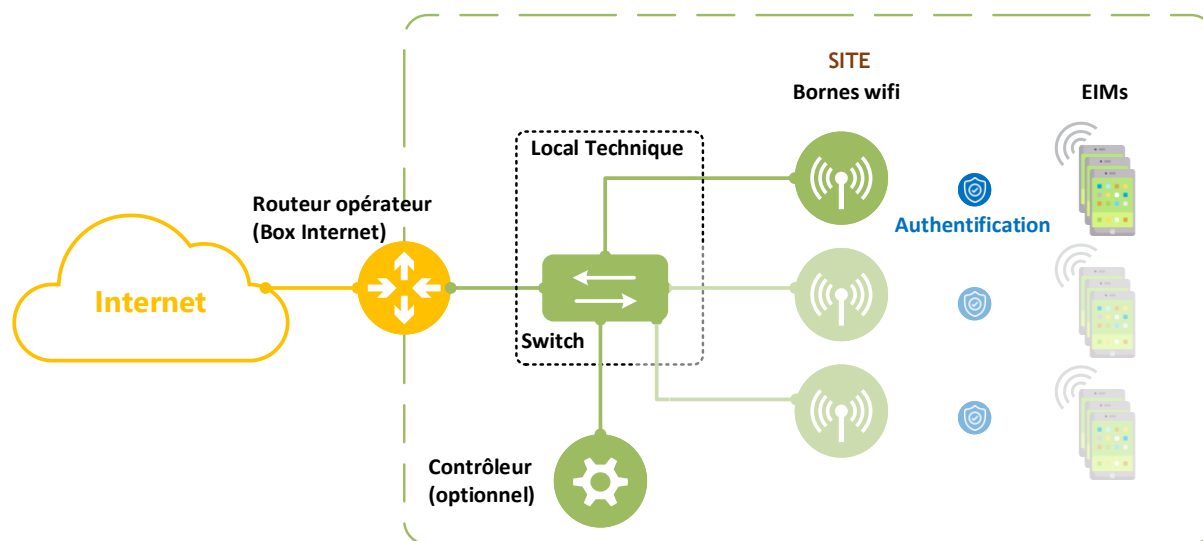
- Les paramètres Wifi sont déjà installés,
- La connexion se fait automatiquement, sans intervention de l'utilisateur,
- Une solution de proxy (filtrage) est installée et empêche les élèves d'accéder à du contenu non pédagogique.

Un serveur de cache est livré et installé dans le site en parallèle des EIM. Grâce à celui-ci, tous les EIM n'ont pas besoin d'utiliser Internet pour les téléchargements (mise à jour, installation d'applications). Ce serveur a pour but d'alléger les flux internet.

2. Description de l'infrastructure Wifi cible des sites

2.1. LES DIFFERENTS ELEMENTS DE L'INFRASTRUCTURE

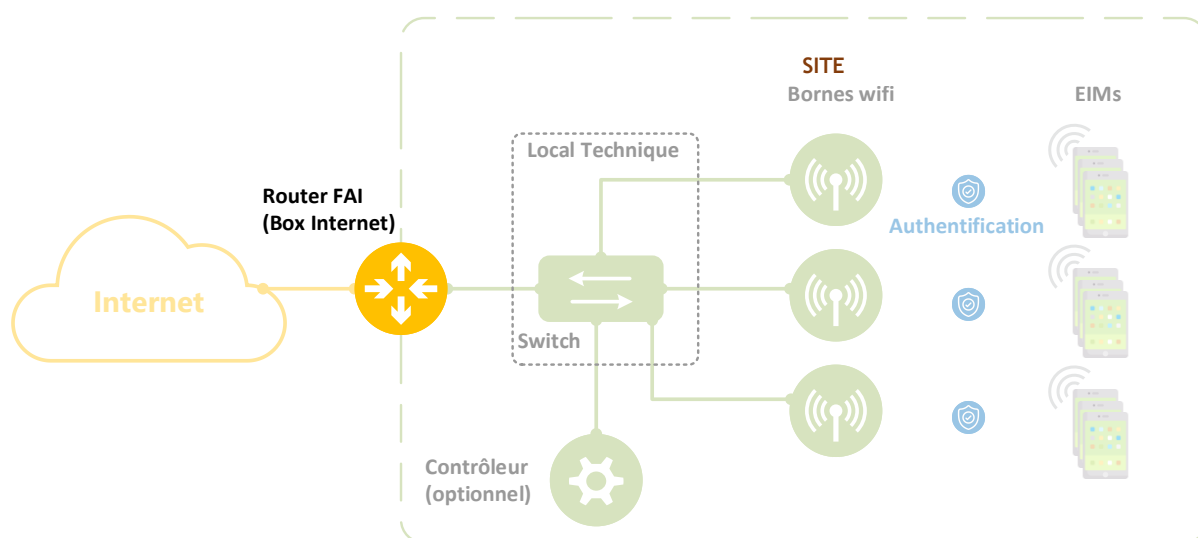
Sans considération sur la taille du site, son nombre d'élèves, l'infrastructure Wifi à mettre en place suit le schéma explicatif et contient les éléments décrits ci-dessous :



- **Le lien internet** : Il apporte la connectivité du site avec l'extérieur. Les applications utilisées par les élèves étant hébergées sur Internet, il est obligatoire que le site soit équipé d'un tel lien pour que les élèves puissent accéder à leurs ressources pédagogiques via les EIM. Il se termine dans un routeur généralement fourni par le FAI et sa caractéristique essentielle dans le contexte de ce référentiel est son débit.
- **Le local technique** : Local dédié à l'installation des équipements informatiques (switchs, serveurs, routeurs). Il est, idéalement, climatisé et son accès est restreint au personnel qualifié. Il est le point de terminaison du câblage VDI menant aux différents espaces du site (classes, bureaux, CDI, etc...).
- **Le câblage VDI (courant faible)** : Ensemble des liaisons filaires reliant les prises (RJ45) des différentes salles du site, au local technique. Il sert à relier les bornes Wifi aux switches, en Ethernet.
- **Commutateur (=Switch)** : Equipement réseau installé, de préférence, dans un local technique. Il dispose de plusieurs ports Ethernet (de 4 à 48 ports suivant les modèles). Grâce au câblage VDI et à travers le routeur du FAI, Il fait la liaison entre les bornes Wifi et Internet.
- **La/les bornes Wifi** : Equipements réseau servant d'interface entre le réseau filaire et le réseau Wifi. Elles sont placées stratégiquement dans le site de manière à propager un signal radio sur une zone de couverture ciblée. Elle(s) apporte(nt) la connectivité locale aux EIM.

- **Le contrôleur** : Equipement central assurant l'administration, la cohésion et l'orchestration des bornes entre elles, dans un contexte d'infrastructure composée de plusieurs bornes.
- **La sécurité** : Elle regroupe plusieurs concepts, notamment l'authentification des utilisateurs et le proxy (filtrage des flux Internet). L'objectif est notamment de se protéger contre les actes malveillants visant à récupérer des données personnelles en limitant l'accès au réseau aux utilisateurs et appareils connus uniquement.

2.2. LIEN INTERNET



Le lien internet apporte la connectivité du site avec l'extérieur. Les applications utilisées par les élèves étant hébergées sur Internet, il est obligatoire que le site soit équipé d'un tel lien pour que les élèves puissent accéder à leurs ressources pédagogiques via les EIM. Il se connecte dans un routeur généralement fourni par le FAI et sa caractéristique essentielle dans le contexte de ce référentiel est son débit.

2.2.1. Type de lien

La majorité des flux générés par les EIM en utilisation transitent à travers le lien internet. Ce lien partagé par tous les EIM, constitue le goulot d'étranglement de l'infrastructure. Son débit doit donc être dimensionné en adéquation avec les usages prévus des EIM.

Certaines applications ne sont pas consommatrices en bande passante, en dehors du téléchargement de l'application en lui-même (120s, 10 Frame Fill Plus, Apprendre à Lire - Syllabique, Bee-bot, Blue-bot, etc...).

D'autres sont consommatrices en bande passante descendante comme les bibliothèques numériques par exemple, dans le cas où tous les EIM téléchargent un livre en parallèle.

Les applications pour lesquelles le travail de l'élève doit être sauvegardé sur un serveur (photos, images, tableurs, fichiers texte...), sont aussi consommatrices en bande passante montante.

Exemples simples :

Chaque EIM doit télécharger un fichier de 5Mo, un livre par exemple.

1 Mégaoctet (ou 1Mo) est égal à 8 Mégabit (ou 8Mb). Cela représente au total 1200Mb à télécharger (30 EIM * 5*8 = 1200)

Si le lien internet a un débit descendant de 100Mbps (typiquement un lien FTTH), Il faudra alors 12 secondes au total pour que le livre soit téléchargé sur tous les EIM.

Si le lien internet a un débit descendant de 10Mbps (typiquement un lien ADSL), il faudra alors 120 secondes au total pour que le livre soit téléchargé sur tous les EIM.

Dans le cas d'une sauvegarde de fichier sur un serveur, la bande passante consommée est dans le sens montant. Pour les offres ADSL, le débit montant est entre 0 et 1.5Mbps. En imaginant, la sauvegarde d'un fichier de 5Mo sur le serveur par chaque EIM avec un débit de 1Mbps, il faudrait 20 minutes pour que l'ensemble des fichiers soit transféré.

#1	Le lien internet du site est préconisé sur support Fibre (FTTH, FTTE, FTT0, Cf. Annexe 4 pour détail des supports) dès lors que le site y est éligible.
----	---

Certaines applications peuvent être gourmandes en bande passante montante et descendante comme les applications de création de contenus vidéo (Adobe Spark Vidéo par exemple) ou les systèmes de visioconférences. L'usage de ces dernières est compliqué voire impossible via un lien ADSL/VDSL.

L'annexe 1 donne des valeurs indicatives et conseillées de débit dans le cas d'usages courants des EIM en fonction du nombre de classes (estimation moyenne de la bande passante de 0.5Mbps par EIM).

2.2.2. DHCP et nombre d'adresses IP disponibles

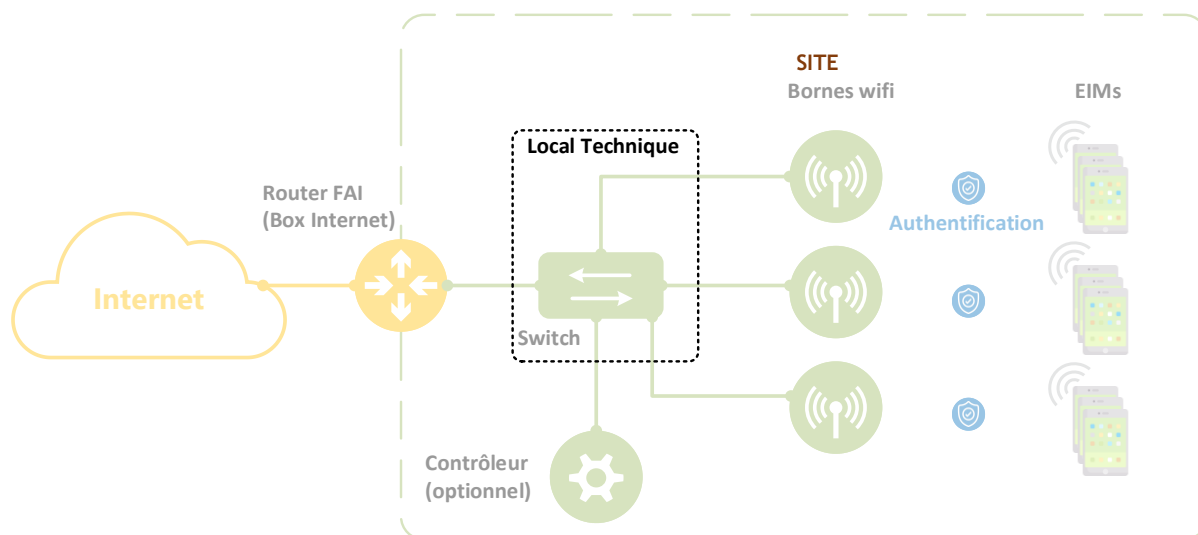
Le service DHCP des box internet non-professionnelles fournies par les opérateurs traditionnels n'est pas prévu pour connecter plusieurs centaines d'appareils. La plage d'adresses IP privée fournie sur le réseau local par le service DHCP du routeur opérateur ne contient que 252 adresses IP (donc 252 appareils connectés au réseau dans le même temps).

Si les adresses IP locales, privées, sont fournies par le service DHCP d'un serveur local (AmonEcole par exemple), il peut être nécessaire d'adapter sa configuration.

#2	Le service DHCP (équipement opérateur ou serveur local) doit fournir une plage IP privée comprenant plus d'adresses IP que d'appareils utilisant le réseau. Les appareils à prendre en compte sont les EIM mais aussi les équipements réseaux et les autres appareils éventuellement connectés sur le réseau filaire tels que les imprimantes)
----	--

A partir de plus de 7 classes, les offres internet « standards » des opérateurs risquent de ne pas satisfaire cette condition. Il est alors nécessaire d'effectuer une requête pour obtenir l'élargissement de la plage DHCP. Par exemple, passer d'un réseau en /24 à un réseau en /23 permet de doubler le nombre d'adresses IP disponible.

2.3. LOCAUX TECHNIQUES



Les locaux techniques sont des locaux physiques dédiés à l'installation des équipements informatiques (switchs, serveurs, routeurs). Ils sont, idéalement, climatisés et leur accès est restreint au personnel qualifié. Ils sont les points de terminaisons des liaisons Ethernet (câblage courant faible) menant aux différents espaces d'un site (classes, bureaux, CDI, etc...).



Les équipements informatiques et les panneaux de brassages (point de terminaisons du câblage) sont installés dans des baies (= racks) standards prévues à cet effet. Ci-dessous les

images de l'intérieur d'un local technique ainsi que la face arrière d'une baie équipée de panneau de distribution.

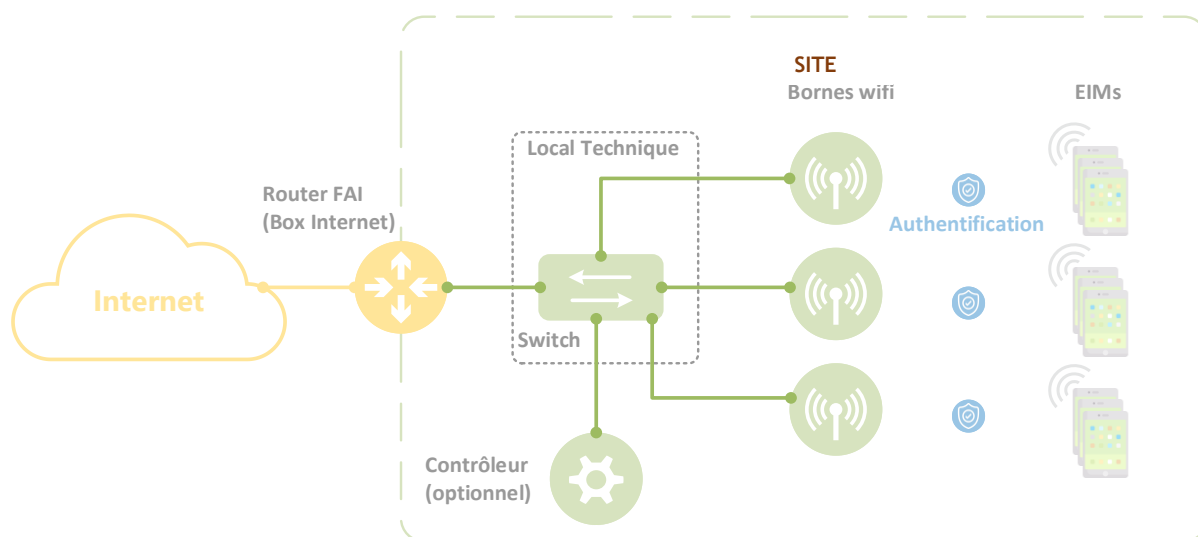


Dans le contexte du site, les besoins informatiques ne justifient pas toujours l'existence d'un local dédié. Les locaux techniques peuvent alors être remplacés par des baies fermées de plus petites tailles. Elles sont moins encombrantes, ne nécessitent pas d'être placées dans un espace dédié et peuvent accueillir un nombre limité mais suffisant d'élément d'infrastructure réseau d'un site. Ci-dessous un exemple de baie décrite précédemment :



- | | |
|----|--|
| #3 | L'accès physique aux équipements réseau (switchs et router opérateurs) doit être restreint au personnel du local. Ils sont installés, idéalement dans un local technique, sinon dans une baie fermée à clef. S'il est impossible d'installer une baie fermée à clef, les équipements doivent à minima être dans une pièce dont l'accès est restreint au personnel du site. |
|----|--|

2.4. CABLAGE VDI



Concernant le courant faible, le câblage est constitué de l'ensemble des liaisons Ethernet reliant les différentes salles du site au local technique ou à la baie dédiée. Il sert à relier les bornes Wifi au switch.

Grace au PoE (normes IEEE 802.3), les bornes Wifi peuvent être alimentées directement par le switch à travers le câblage courant faible. Cela permet d'éviter les travaux liés à l'installation du courant fort qui sont parfois problématiques dû à l'emplacement des bornes.

L'alimentation des bornes à travers le câblage courant faible génère en revanche une forte dissipation de chaleur. Pour cette raison, des câbles spécifiques doivent être utilisés

- | | |
|----|--|
| #4 | Le câblage courant faible reliant les bornes aux équipements réseaux actifs (switch) doit être à minima de catégorie 6A. Seuls les câbles de types U/FTP, F/FTP et S/FTP sont préconisés (U/UTP et F/UTP sont proscrits).
Dans le cadre d'une infrastructure de câblage existante, les câbles de catégorie 5e FTP sont tolérés. |
|----|--|

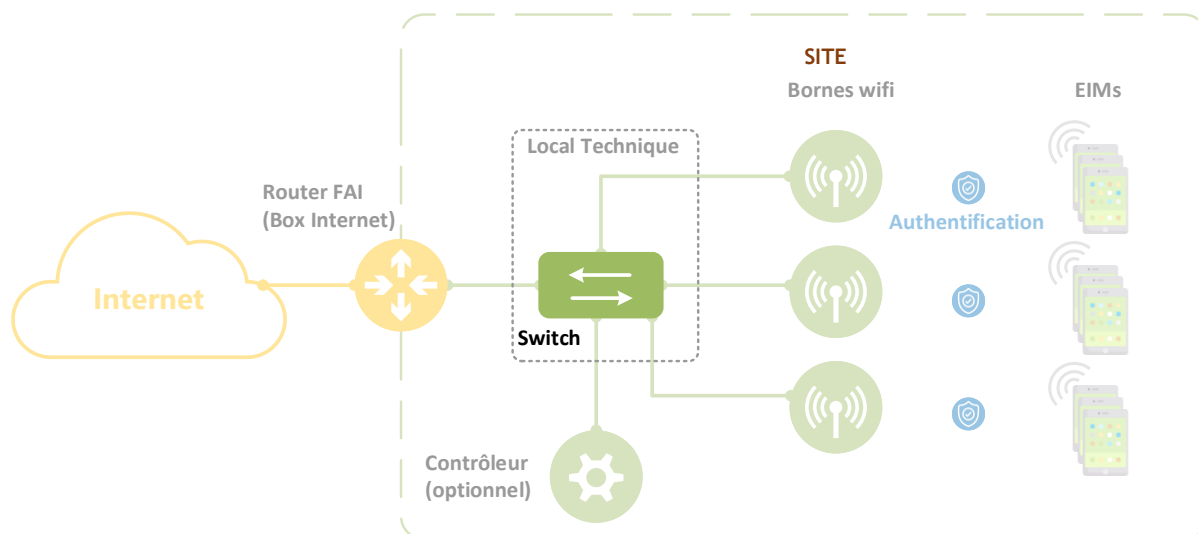
Afin de garantir le bon fonctionnement et la pérennité de l'installation, les câbles doivent être installés dans le respect des bonnes pratiques et des règles de l'art.

- | | |
|----|--|
| #5 | Le câblage courant faible reliant les bornes aux équipements réseaux actifs (switch) doit respecter les bonnes pratiques : |
|----|--|

- Longueur maximale du câble = 90m,
- Les câbles doivent être posés et non tirés,
- Les câbles doivent être identifiés (numéro de la prise) aux deux extrémités à l'aide d'un feutre à encre indélébile, ou par des rubans pré imprimés,
- Les rayons de courbure doivent être supérieurs à 10 fois le diamètre du câble,
- Les câbles ne doivent jamais être pliés,
- Aucun « love de câble » ne doit être laissé à l'intérieur d'une goulotte ou d'un boîtier,
- ...

Pour simplifier l'exploitation et la maintenance de l'infrastructure Wifi du site, il est également recommandé d'utiliser des cordons de brassage d'une couleur différente pour les bornes Wifi. Il s'agit ici du cordon entre le switch et le panneau de brassage. Cela facilite les interventions en cas de problèmes, le repérage du câble étant en évidence.

2.5. SWITCH



Le switch est un équipement réseau qui dispose de plusieurs port Ethernet (de 4 à 48 ports suivant les modèles). Il est d'une part reliée au router opérateur et d'autre part aux bornes Wifi. Sans ce maillon de la chaîne, les clients Wifi (EIM) ne peuvent pas joindre la sortie vers Internet.



Il y a, à minima, un câble reliant chaque borne à un switch. Il est donc nécessaire d'avoir des ports disponibles sur les switches pour y connecter les bornes.

- | | |
|----|--|
| #6 | <p>Il doit y avoir à minima autant de ports disponibles sur les switches que de bornes à installer plus 5 ports par switch.</p> <p>Ces 5 ports disponibles après le déploiement forment une marge d'évolutivité et permettent d'anticiper les futurs besoins.</p> <p>Les switches doivent avoir la capacité de faire de l'autonégociation sur ces ports.</p> |
|----|--|

Les équipements réseaux les plus anciens sont équipés de ports « Fast Ethernet » limités à un débit de 100Mbps (Mégabit par seconde). L'utilisation de ces derniers risque d'être limitante en termes de débit. Le goulot d'étranglement ne serait plus au niveau du lien internet, mais au niveau des liens locaux internes au site.

- | | |
|----|---|
| #7 | <p>Les ports sur lesquels sont connectés les bornes doivent supporter à minima un débit de 1Gbps. L'autonégociation doit être activée afin que le lien connectant la borne soit correctement négocié en Full duplex et speed = 1Gbps.</p> |
|----|---|

Comme indiqué dans le chapitre précédent, les switches peuvent alimenter électriquement les bornes. Cette capacité n'est pas incluse dans tous les modèles d'équipements réseaux.

- | | |
|---|---|
| #8 (valable uniquement si bornes alimentées via courant faible) | <p>Les switches doivent implémenter à minima la norme 802.3at (Norme PoE+) et pouvoir alimenter toutes les bornes de l'infrastructure du site dans le même temps.</p> |
|---|---|

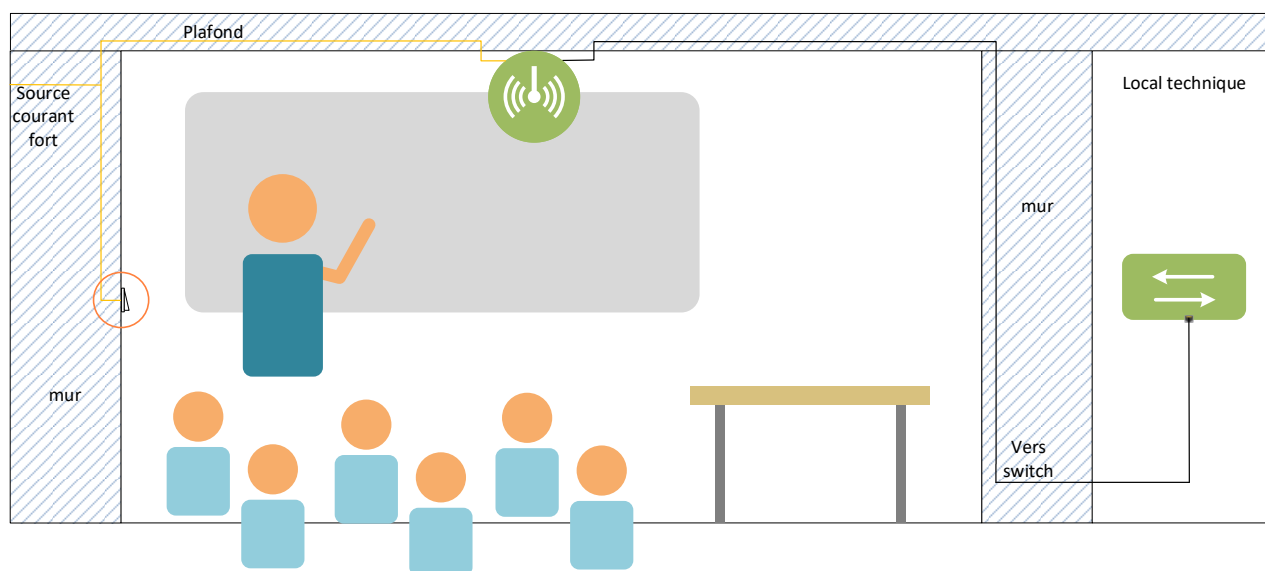
Bien que l'option d'alimentation par courant faible soit fortement recommandée, il n'est pas interdit d'alimenter les bornes par courant fort si cela aide à suivre les directives imposées par la loi ABEILLE.

2.5.1. Respect de la loi ABEILLE

Selon la loi ABEILLE, pour les classes dans lesquelles le site a installé du WiFi, il doit être coupé lorsqu'il n'est pas utilisé pour les activités pédagogiques.

Pour respecter cette condition, les enseignants doivent avoir à leur disposition un outil simple permettant de couper le Wifi en fin d'activité. Plusieurs options sont possibles :

- **Alimenter la borne via courant fort, relié à un interrupteur** : Option satisfaisante mais qui peut induire des travaux de câblages courant forts, en supplément des travaux courant faible. L'emplacement de l'interrupteur dans la salle doit être stratégique pour éviter que quelqu'un ne « joue » avec. Les équipements Wifi ne sont pas prévus pour être allumés/éteints à répétition rapide. Le schéma explicatif suivant illustre cette option :



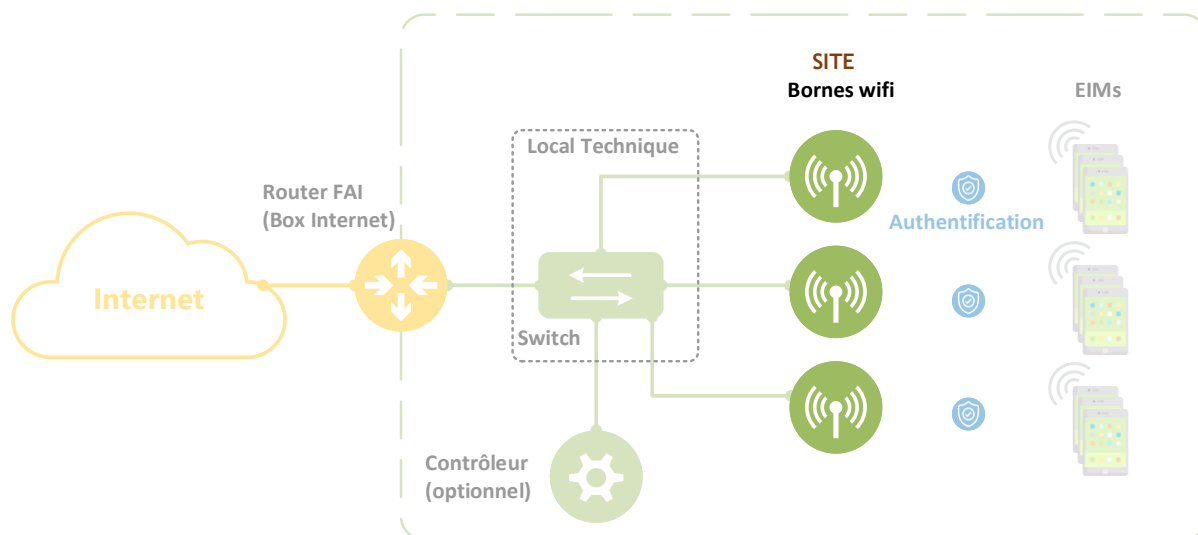
- **Alimenter la borne via courant faible par l'intermédiaire d'un port Ethernet commandable** : Il existe sur le marché des solutions permettant de couper l'alimentation PoE d'une liaison courant faible via un interrupteur relié au câble. Elle consiste en général à installer un boîtier en rupture entre la borne et le switch. Ce boîtier est commandable, à distance ou non. Ces solutions mettent en œuvre un équipement supplémentaire sur la chaîne de liaison (boîtier en coupure), induisant des contraintes d'exploitation et de maintenance supplémentaires pouvant être difficiles à satisfaire. (Quelques exemple de solutions de ce type : PoE-Sea de PoE-Tic, WOD de Xenium)



#9

La loi ABEILLE doit être respectée : les enseignants doivent avoir à leur disposition un outil simple permettant de couper le Wifi.

2.6. BORNES



Les bornes Wifi sont les équipements réseau servant d'interface entre le média filaire et le média Wifi. Elles sont placées stratégiquement à travers le site de manière à propager un signal radio sur une zone de couverture voulue. Elles apportent la connectivité locale aux EIM.

2.6.1. Zone de couverture

La zone de couverture du réseau Wifi doit s'étendre sur tout le périmètre intérieur du site. Plusieurs éléments bâtementaires peuvent absorber les ondes radio et doivent être pris en compte afin de déterminer l'emplacement des bornes :

- Murs et portes - Plus les murs sont épais, plus ils sont susceptibles d'absorber les ondes. Certaines matières sont plus « perméables » aux ondes que les autres (le béton n'absorbe pas de la même manière que le bois).
- L'eau (sanitaires et tuyauterie)
- Les structures métalliques

L'environnement des sites doit être considéré comme environnement de haute densité. Cette hypothèse est cruciale pour l'étude de couverture. Pour rappel, 70% des classes d'un même site doivent pouvoir utiliser leurs EIM en parallèle sans baisse de qualité du service.

L'objectif n'est pas uniquement de fournir du signal Wifi en tout point des salles de classes mais bien de fournir un signal qualitatif à l'ensemble des 30 EIM de chaque classe dans le même temps ainsi que dans le reste des espaces du site. Les interférences doivent être minimisées afin de garantir le meilleur rapport signal sur bruit aux EIM.

- | | |
|-----|---|
| #10 | Il est obligatoire de faire une étude de couverture en amont d'un déploiement. Le résultat de l'étude de couverture doit donner l'emplacement des bornes garantissant la bonne couverture des salles de classe et du site ainsi que les hypothèses de paramétrage radio utilisés pour faire l'étude.

Ces hypothèses doivent prendre en compte un environnement de haute densité. |
|-----|---|

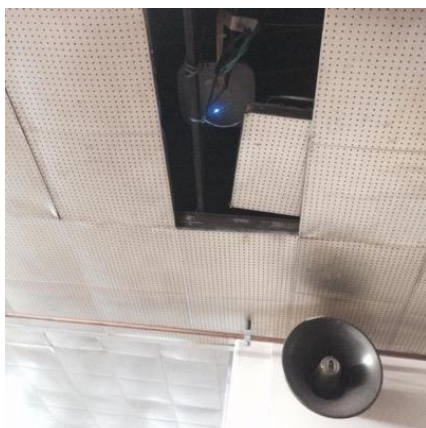
L'étude de couverture peut être faite sur plan. Elle permettra de déterminer l'emplacement idéal théorique des bornes. Elle peut aussi être faite directement dans le site ce qui permet une meilleure appréhension de l'environnement ainsi que le repérage des éventuels chemins de câbles existants. Elle peut aussi être utile à identifier la nature et l'envergure des travaux de câblages à prévoir (perçement, rebouchages, habillages...).

2.6.2. Pose des bornes

Comme le câblage, la pose des bornes doit suivre l'état de l'art et les bonnes pratiques. Ces règles garantissent le bon fonctionnement et la pérennité de l'installation. Par exemple, fixer les bornes au mur ou au plafond évite aux utilisateurs de les manipuler et limite le risque de casse du matériel.

- | | |
|-----|--|
| #11 | Les bornes doivent être hors de portées des élèves et fixées. Elles ne doivent pas pouvoir être déplacées. |
|-----|--|

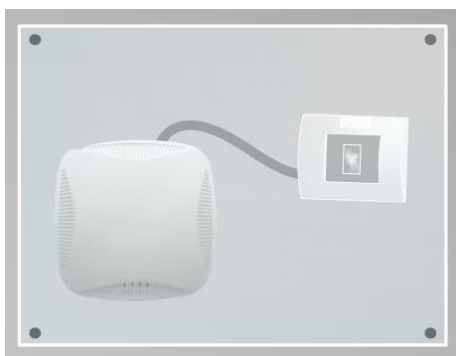
Pour les raisons citées dans le paragraphe précédent « 2.6.1 Zone de couverture », les bornes ne doivent pas être placées à proximité d'obstacles (particulièrement, les structures métalliques). Ci-dessous quelques exemples à ne pas reproduire :



- | | |
|-----|--|
| #12 | La pose des bornes doit respecter les consignes suivantes : <ul style="list-style-type: none"> La borne n'est pas cachée derrière un obstacle (faux-plafond, cage métallique...). Deux bornes doivent être espacées de 3 mètres minimum. |
|-----|--|

- Si la borne doit être posée à une hauteur supérieure à 4 mètres, le type de borne doit être adapté.
- Le rayonnement de la borne doit être pris en compte pour savoir si elle doit être posée à l'horizontale ou à la verticale (les bornes traditionnelles sont omnidirectionnelles et doivent être posées à l'horizontale, typiquement au plafond)
- Si des antennes externes sont utilisées, elles doivent toutes être du même type.
- Les bornes doivent être, autant que possible, visibles (à l'œil) des EIM. Elles doivent être posées dans les classes plutôt que les couloirs.

Si les bornes nécessitent une protection (dans un gymnase par exemple), elle doit être en plexiglass (pas de métal) et s'étendre sur la prise RJ45 et le cordon :



2.6.3. Spécifications techniques du matériel

Afin de satisfaire les problématiques liées au contexte de haute densité représenté par le nombre d'EIM en utilisation simultanée, les bornes doivent avoir des spécifications techniques particulières.

#13	<p>Les bornes Wifi doivent avoir à minima les spécifications techniques suivantes :</p> <ul style="list-style-type: none"> ▪ Radio : 5GHz 2x2 SU-MIMO (2 Spatial streams) configurable ▪ Normes IEEE implémentées : 802.11 (a, b, g, n, ac) dans le cas de matériel préexistant, et 802.11 (a, b, g, n, ac, ax) pour le matériel neuf. ▪ Modulations supportées : QPSK, 16-QAM, 64-QAM, 256-QAM ▪ Puissance d'émission configurable, et adaptatif (ARM) ▪ Fréquences (canaux) configurables, et adaptatives (ARM) ▪ Protocoles d'optimisation : MRC, STBC, TxBF, LDPC, CDD/CSD ▪ Antennes omnidirectionnelles ▪ Port Ethernet (uplink) supportant 802.3af/at (PoE, PoE+) ▪ Fonction contrôleur intégrée
-----	--

2.6.4. Paramètres radio

Afin de satisfaire les problématiques liées au contexte de haute densité représenté par le nombre de EIM en utilisation en parallèle, des paramétrages Radio-Fréquences (RF) sont requis. Ils minimisent les interférences. Ils évitent à un EIM d'être priorisé et garantissent l'égalité du service Wifi entre les EIM.

#14	<p>Les paramètres RF suivants doivent être appliqués :</p> <ul style="list-style-type: none"> ▪ Désactivation de la bande de fréquence 2.4Ghz (pour le SSID dédié) ▪ Désactivation des bas débits (de 1Mbps à 11Mbps inclus) ▪ Activation des algorithmes automatiques de gestion des canaux, fréquences et puissance - ARM, RRM, FRA, DFS, etc... ▪ Régler le seuil de puissance d'émission des bornes à 50% max. ▪ Limitation de la largeur des canaux à 20Mhz.
-----	--

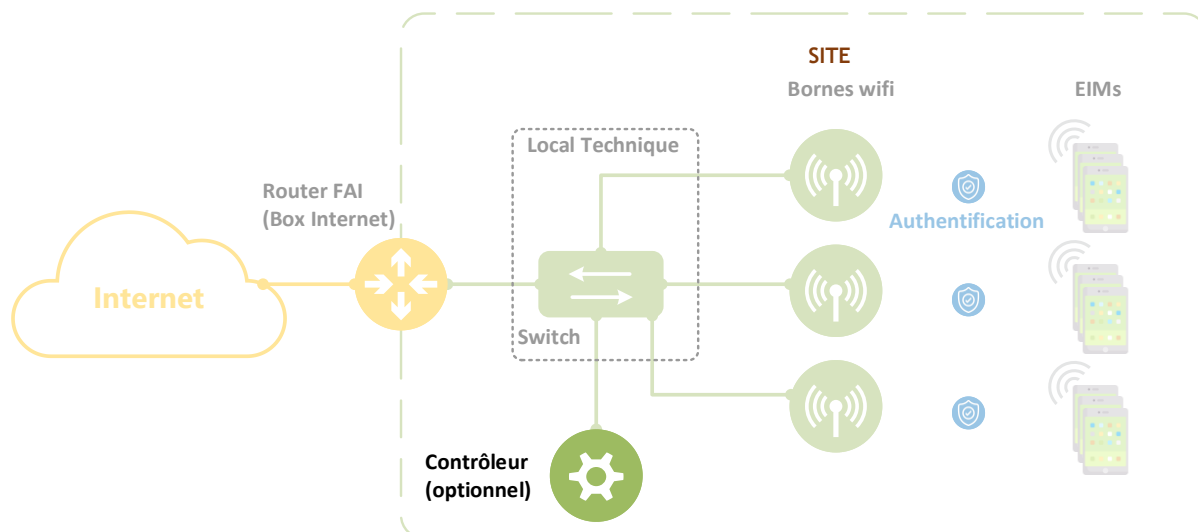
Il est recommandé de partager ces paramètres cibles aux prestataires ou aux entités responsables de faire l'étude de couverture et l'installation de l'infrastructure.

2.6.5. Paramètres réseau

#15	<p>Un SSID dédié aux EIM doit être émis. Le nom du SSID est imposé et transmis par SYN.</p>
-----	---

La configuration réseau des EIM est effectuée en amont et elle inclut le nom du SSID. Les EIM ne peuvent donc pas se connecter automatiquement à un réseau Wifi dont le SSID est différent.

2.7. CONTROLEUR



Le contrôleur est l'équipement central qui assure l'administration, la cohésion et l'orchestration des bornes entre-elles, dans un contexte d'infrastructure composée de plusieurs bornes.

C'est via l'interface Web du contrôleur que les configurations sont faites (paramétrages RF et de sécurité). L'accès à cette interface doit lui-même être sécurisé :

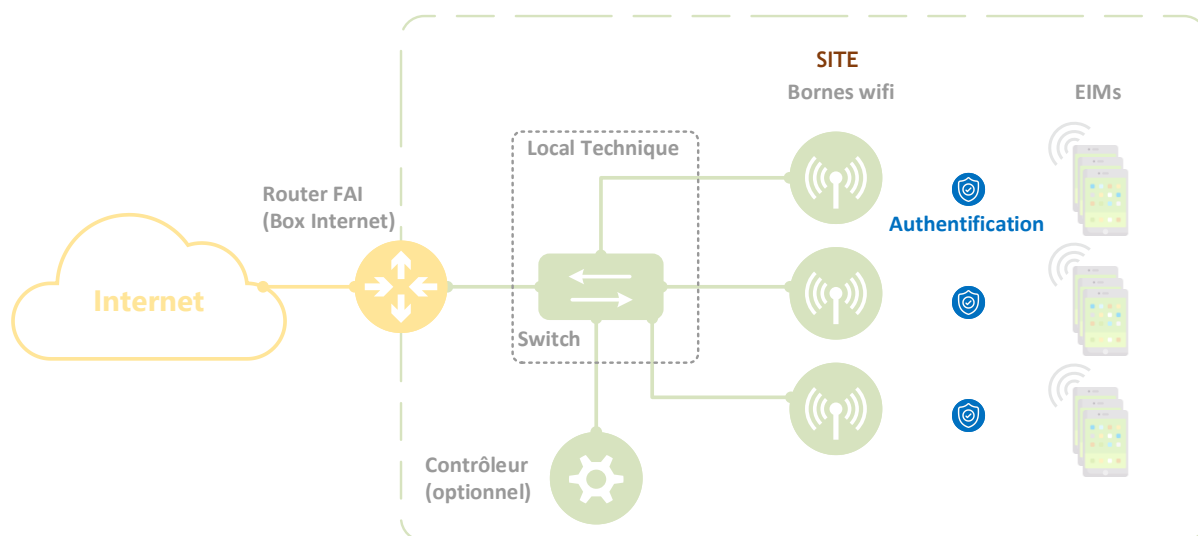
#16	L'interface Web d'administration du contrôleur doit se faire via le protocole sécurisé HTTPS (HTTP est proscrit).
-----	---

Dans les infrastructures de grande envergure (à partir de 100 bornes), le contrôleur est un équipement physique dédié (ou une machine virtuelle dédiée). Les usages prévus dans les sites ne justifient pas le déploiement d'une centaine de borne. Pour cette raison les fonctions gérées par le contrôleur peuvent être déportées directement sur les bornes elle-même. L'infrastructure est alors sans contrôleur.

#17	Il n'y a pas d'exigences concernant le choix d'architecture du contrôleur (dédié, cloud ou fonctions déportées dans les bornes). En revanche, il est obligatoire qu'une ressource technique humaine ait accès au contrôleur pour assurer l'exploitation de l'infrastructure. Cette ressource doit être identifiée et joignable, en cas de besoin.
-----	--

2.8. SECURITE

2.8.1. Authentification



La connexion au réseau Wifi est soumise à un protocole d'authentification. Ce protocole certifie que l'appareil souhaitant se connecter au réseau est un appareil connu et donc légitime.

Un protocole d'authentification trop faible laisse la possibilité aux hackers de se connecter au réseau Wifi et d'y récupérer le trafic généré par les autres appareils. Ce trafic pouvant notamment inclure des données personnelles d'élèves, le protocole doit être fort.

#18	<p>L'authentification liée au SSID dédié aux EIM doit suivre les règles suivantes :</p> <ul style="list-style-type: none"> ▪ WPA est proscrit et doit être désactivé. ▪ L'algorithme de chiffrement TKIP est proscrit et doit être désactivé ▪ L'algorithme de chiffrement recommandé est CCMP (ou plus sécurisé). ▪ WPA3 - Personnel doit être privilégié. ▪ WPA2 - Personnel est toléré dans les infrastructures préexistantes ne supportant pas WPA3. ▪ WPS doit être désactivé.
-----	---

L'utilisation de WPA3 (ou WPA2) Personnel implique l'utilisation d'un mot de passe de connexion unique partagé par tous les EIM.

#19	<p>Le mot de passe ne doit être divulgué à personne excepté l'intégrateur de la solution. Il est imposé et transmis par SYN.</p>
-----	--

En cas de changement de mot de passe, la configuration peut être faite à distance sur les EIM mais nécessite également une action manuelle de reconfiguration sur le contrôleur (ou les bornes, selon l'architecture). Les EIM ne pourront pas se connecter au réseau Wifi entre le moment où ils auront été reconfigurés et le moment où le contrôleur est reconfiguré.

2.8.2. Proxy

La configuration du proxy est effectuée via le MDM, en amont de la livraison des EIM dans le site. L'accès internet des EIM est donc soumis à des règles, notamment du filtrage d'URL, grâce à une brique proxy mise à disposition par SYN.

Cet élément d'infrastructure de sécurité n'a pas besoin d'être déployé en local par les sites.

Pour rappel, la mise en place de ce filtrage est obligatoire comme stipulé par la circulaire n° 2004-035 du 18/02/2004 sur la protection du milieu scolaire dont voici un extrait : *

« Les déploiements d'accès généralisés à l'internet dans les sites ne peuvent s'effectuer qu'en prenant en compte les besoins des enseignants et des équipes éducatives de disposer d'outils leur permettant de sélectionner ou de contrôler l'information mise à disposition des élèves ».

La configuration est faite de telle sorte que l'ensemble du trafic internet généré par les EIM passe par un serveur central l'autorisant ou non. Il n'est pas possible pour les élèves d'accéder à ces éléments de configuration. L'accès Internet est donc soumis aux règles dès la réception de l'EIM par l'élève.

2.8.3. Firewall

Les flux entrants doivent être bloqués. La configuration par défaut des pare-feux inclus dans les box opérateurs suivent cette directive lorsqu'elle existe. Il n'est pas nécessaire d'y apporter de modifications dans le cadre du déploiement de l'infrastructure Wifi en elle-même.

Certaines offres n'incluent pas le service pare-feu par défaut, il est alors nécessaire de souscrire à l'option supplémentaire sauf si le site dispose déjà d'un pare-feu local.

3. Synthèse des prérequis

Le tableau suivant constitue un récapitulatif des prérequis à respecter dans le cadre du déploiement d'une infrastructure Wifi en amont d'un déploiement d'EIM.

Les prérequis ont été résumés afin de faciliter la lecture du tableau. Pour pouvoir les comprendre et les appliquer, il est nécessaire de se référer aux paragraphes explicatifs indiqués dans la colonne « Paragraphe ».

Une grille de conformité est fournie en document annexe. Elle doit être complétée et communiquée à SYN pour validation.

Réf	Prérequis	Paragraphe	Document de référence
#1	Le lien internet du site est préconisé sur support Fibre (FTTH, FTTE, FTTO) dès lors que le site y est éligible.	2.2.1	Contrat Internet
#2	Le service DHCP doit fournir une plage IP privée comprenant plus d'adresses IP que d'appareils utilisant le réseau.	2.2.2	
#3	L'accès physique aux équipements réseaux (switchs et router opérateurs) doit être restreint au personnel du site.	2.3	Photos des baies
#4	Le câblage courant faible reliant les bornes aux équipements réseaux actifs (switch) doit être à minima de catégorie 6A. Seuls les câbles de types U/FTP, F/FTP et S/FTP sont préconisés (U/UTP et F/UTP sont proscrits).	2.4	Cahier de recette
#5	Le câblage courant faible reliant les bornes aux équipements réseaux actifs (switch) doit respecter les bonnes pratiques.		
#6	Il doit y avoir à minima autant de ports disponibles sur les switchs que de bornes à installer plus 5 ports par switch.	2.5	Données techniques
#7	Les ports sur lesquels sont connectées les bornes doivent supporter à minima un débit de 1Gbps. L'autonégociation doit être activée afin que le lien connectant la borne soit correctement négocié en Full duplex et speed = 1Gbps (ou plus).		
#8*	Les switchs doivent implémenter à minima la norme 802.3at (Norme PoE+) et pouvoir alimenter toutes les bornes de l'infrastructure du site dans le même temps.		
#9	La loi ABEILLE doit être respectée : les enseignants doivent avoir à leur disposition un outil simple permettant de couper le Wifi.	2.5.1	Données techniques
#10	Il est obligatoire de faire une étude de couverture en amont d'un déploiement. Le résultat de l'étude de couverture doit donner l'emplacement des bornes garantissant la bonne couverture des salles de classe en prenant en compte l'environnement de haute densité.	2.6.1	Résultats de l'étude

#11	Les bornes doivent être hors de portées des élèves et fixées. Elles ne doivent pas pouvoir être déplacées.	2.6.2	Photos des bornes posées
#12	La pose des bornes doit respecter les bonnes pratiques.		
#13	Les bornes Wifi doivent avoir à minima les spécifications techniques fournies (Cf. paragraphe).	2.6.3	Données techniques
#14	Les paramètres RF fournis (Cf. paragraphe) doivent être appliqués.	2.6.4	
#15	Un SSID dédié aux EIM doit être émis. Le nom du SSID est imposé et transmis par SYN	2.6.5	
#16	L'interface Web d'administration du contrôleur doit se faire via le protocole sécurisé HTTPS (HTTP est proscrit).	2.7	
#17	Il est obligatoire qu'une ressource technique humaine ait accès au contrôleur pour assurer l'exploitation de l'infrastructure.		
#18	L'authentification liée au SSID dédié aux EIM doit suivre les règles fournies (Cf. paragraphe).	2.8.1	
#19	Le mot de passe ne doit être divulgué à personne excepté l'intégrateur de la solution. Il est imposé et transmis par SYN.		

4. Annexes

4.1. ANNEXE 1 : DEBIT INTERNET REQUIS POUR LES USAGES COURANTS

Nombre de classes équipées en EIM	Débit minimum (montant et descendant)
1	15 Mbps
2	30 Mbps
3	45 Mbps
4	45 Mbps
5	60 Mbps
6	75 Mbps
7	75 Mbps
8	90 Mbps
9	105 Mbps
10	105 Mbps
11	120 Mbps
12	135 Mbps
13	135 Mbps
14	150 Mbps
15	165 Mbps

4.2. ANNEXE 2 : CADRE REGLEMENTAIRE

Plusieurs cadres de références, et référentiels thématiques ont été rédigés par la Direction du Numérique pour l'éducation et sont librement à disposition sur le site internet de eduscol. Ils sont à prendre en compte pour tout type de projets liés au numériques dans les établissements scolaires :

- CARMO (<https://eduscol.education.fr/1087/cadre-de-reference-carmo-version-30>)
- CARINE (<https://eduscol.education.fr/1078/referentiel-s2i2e-carine>)
- Référentiels Wifi (<https://eduscol.education.fr/1083/referentiel-wi-fi>)

Les consignes de sécurité utilisée dans ces référentiels sont tirées des recommandations de l'ANSSI. Les référentiels de l'ANSSI impliqués sont décrits dans le chapitre 4.4 du CARMO « Référentiels ANSSI ».

Le Cadre de Référence des services d'Infrastructures Numériques d'Établissements scolaires et des écoles (CARINE) dresse la liste des référentiels existants ainsi que leurs interactions dans son chapitre 1.3 « Positionnement dans le corpus référentiel ».

Le présent référentiel constitue une version appliquée des référentiels existants, au contexte de la mise en place (ou l'évolution) d'une infrastructure Wifi dans les sites assurant la qualité de l'accès au réseau des EIM.

Les documents pris en compte sont notamment : le CARMO, le CARINE ainsi que les 3 référentiels thématiques « Référentiel sur l'usage du Wi-Fi en établissement et en écoles » (Cadre technique, Radiofréquence et Santé, Usages et cadre juridique). Ces 3 référentiels considèrent la loi **ABEILLE** stipulant notamment que les bornes Wifi doivent être coupées lorsque qu'elles n'ont pas besoin d'être utilisées dans le cadre pédagogique.

En conséquence, il est impossible de respecter les cadres de références, et la loi ABEILLE, en vigueur sans suivre les prérequis exigés dans ce document.










4.3. ANNEXE 3 : DESTINATAIRES DU DOCUMENT

Ce référentiel vise à faciliter le dialogue entre les différentes parties prenantes dans le cadre de la mise en œuvre de projet d'infrastructures Wifi dans les sites, en amont des projets d'équipements mobiles.

Les principaux destinataires sont notamment les suivants :

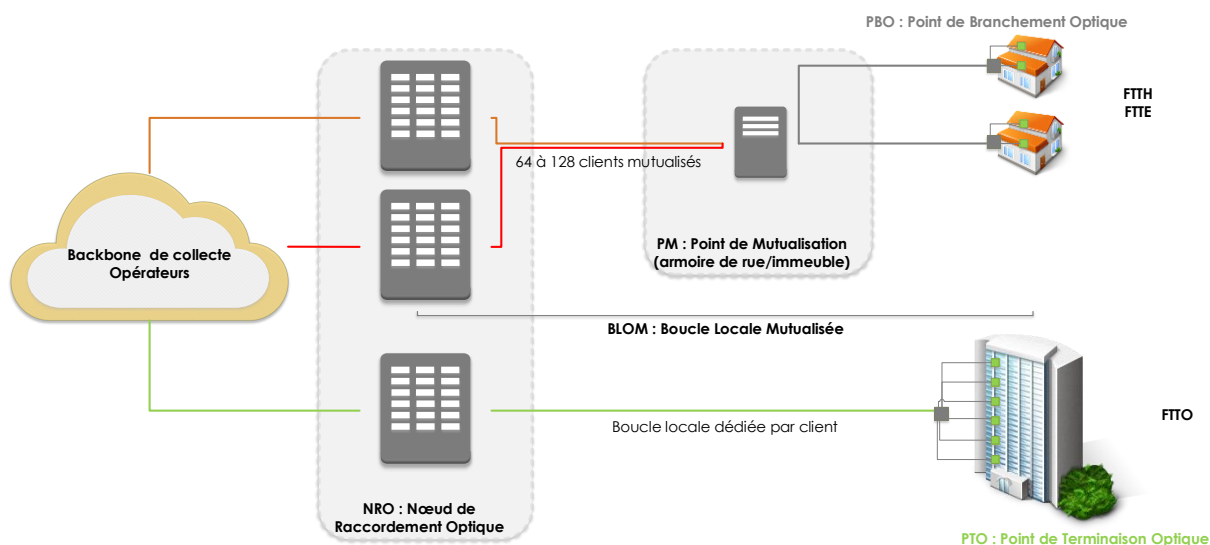
- Les chefs d'établissement et directeurs de sites : ils définissent et mettent en œuvre les projets pédagogiques,
- Les enseignants,
- L'académie de Versailles,
- Les personnes ressources du site (en particulier « administrateurs »),
- Fournisseurs de solutions d'infrastructures (Fourniture de matériel, installation, configuration, maintenance et exploitation),
- Prestataires des maîtrises d'ouvrage académiques et territoriales

4.4. ANNEXE 4 : LIEN INTERNET – DIFFERENCES ENTRE LES SUPPORTS

	 Cuivre			 Fibre		
	ADSL	SDSL	VDSL	FTTH	FTTE	FTTO
Débit Garanti et symétrique					 	
Débit descendant	Jusqu'à 20Mbps	Jusqu'à 20Mbps	Jusqu'à 90Mbps	Jusqu'à 1Gbps et plus		
Débit montant	Jusqu'à 1Mbps	Jusqu'à 20Mbps	Jusqu'à 30Mbps	Jusqu'à 1Gbps et plus		

VDSL intéressant si proche du NRA (<1,5km)
Réseau cuivre de moins en moins maintenu et fin annoncée à partir de 2019

FTTH : pas de GTR
FTTE : FTTH avec GTR et débits minimum
FTTO : lien fibre dédié avec débits garantis et GTR
Mais aussi :
FTTLA : terminaison coaxiale, en France principalement SFR (ex-Numericable)



4.5. GLOSSAIRE

ARM

Adaptive Radio Management17

BPSK

Binary Phase Shift Keying17

CARMO

Cadre de Référence pour l'Accès aux
Ressources pédagogiques via un
équipement Mobile 3

CCMP

Counter Mode CBC-MAC20

CDD/CSD

Cyclic Delay/Shift Diversity17

DFS

Dynamic Frequency Selection18

DHCP

Dynamic Host Configuration Protocol . 7

EIM

Équipement Individuel Mobile 4

F/UTP

Foiled with Unshielded Twisted Pair..11

FAI

Fournisseur d'Accès Internet 5

FRA

Flexible Radio Assignment18

FTTE

Fiber To The Enterprise 7

FTTH

Fiber To The Home..... 7

FTTO

Fiber To The Office..... 7

HTTP

Hypertext Transfer Protocol.....19

HTTPS

Hypertext Transfer Protocol Secure ..19

LDPC

Low-Density Parity-Check17

MDM

Mobile Device Management.....21

MRC

Maximal Ratio Combining.....17

PoE

Power Over Ethernet11

QAM

Quadrature Amplitude Modulation17

QPSK

Quadrature Phase Shift Keying17

RRM

Radio Ressource Management18

S/FTP

Shielded Foiled Twisted Pair11

SSID

Service Set Identifier18

STBC

Space-Time Block Coding.....17

SU-MIMO

Single User Multiple Input Multiple
Output.....17

SYN

Seine et Yvelines Numériques..... 3

TKIP

Temporal Key Integrity Protocol.....20

TxBF

Transmit Beamforming with explicit
Feedback17

U/FTP

Unshielded Foiled Twisted Pair.....11

U/UTP

Unshielded twisted pair11

URL

Uniform Resource Locator21

VDI

Voix, Données, Images 5

WPA

WiFi Protected Access.....20

WPS

Wifi Protected Setup.....20