WIFI

I. Introduction

Un réseau sans fil est un réseau dans lequel au moins deux terminaux sont capables de communiquer entre eux grâce à des signaux radioélectriques. Les réseaux sans fil ne sont pas tout récents, mais avec le développement de l'informatique et des systèmes d'information, la technologie est venue au besoin primaire de l'homme : la mobilité et la facilité.
Ces réseaux dits « sans-fil » sont de plusieurs sortes : WIFI (Wireless Fidelity), BLUETOOTH, BLR (Boucle Locale Radio), UMTS (Universal Mobile Telecommunications System) etc..

Les technologies dites « sans fil », la norme 802.11 en particulier, facilitent et réduisent le coût de connexion pour les réseaux de grande taille.
Avec peu de matériel et un peu d'organisation, de grandes quantités d'informations peuvent maintenant circuler sur plusieurs centaines de mètres, sans avoir recours à une compagnie de téléphone ou de câblage.

Ces technologies peuvent être classées en quatre parties :
- Les réseaux personnels sans fil : Wireless Personal Area Network (WPAN)
- Les réseaux locaux sans fil : Wireless Local Area Network (WLAN)
- Les réseaux métropolitains sans fil : Wireless Metropolitan Area Network (WMAN)
- Les larges réseaux sans fil : Wireless Wide Area Network (WWAN)

La norme WiFi (Wireless Fidelity) est le nom commercial donné à la norme IEEE.

La Wi-Fi Alliance, anciennement Wireless Ethernet Compatibility Alliance (WECA), est un consortium qui possède la marque Wi-Fi. Il est situé à Austin au Texas. WECA a été renommée Wi-Fi Alliance en 2003.

Grâce aux normes Wi-Fi, il est possible de créer des réseaux locaux sans fil à haut débit. En pratique, le Wi-Fi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA), des objets communicants ou même des périphériques à une liaison haut débit : de 11 Mbit/s théoriques ou 6 Mbit/s réels en 802.11b, à 54 Mbit/s théoriques ou environ 25 Mbit/s réels en 802.11a ou 802.11g, 600 Mbit/s théoriques pour le 802.11n et 1,3 Gbit/s théoriques pour le 802.11ac normalisé depuis décembre 2013.

Il est évident que le débit pratique varie en fonction de l'environnement.
Le WiFi utilise la gamme de fréquence de 2.4 GHz, la même que celle des fours à micro-ondes ; leur principe est le suivant : l'onde émise à très forte puissance est absorbée par les molécules d'eau contenues dans les aliments. Cette absorption « agite » les molécules d'eau et génère la chaleur permettant de réchauffer ou cuire les aliments.
De la même façon, suivant le même principe, tout obstacle situé sur une liaison WiFi 2.4GHz contenant de l'eau ou suffisamment dense (béton armé, foule importante, ...) atténuera plus ou moins cette liaison.

II. Les fréquences WIFI

Un modem/routeur peut utiliser deux fréquences pour transmettre des signaux wifi : la 2,4 GHz et la 5 GHz.

La fréquence 2,4 GHz compte 13 canaux, dont le 1, le 6 et le 11 sont les seuls à ne pas se chevaucher. Il y a donc peu de place sur la 2,4 GHz et les modems/routeurs peuvent rapidement interférer.

La fréquence 5 GHz ne connaît pas ce problème : aucun de ces 23 canaux ne se chevauche.

Pour en savoir plus : https://fr.wikipedia.org/wiki/Liste_des_canaux_Wi-Fi#Utilisation_des_fr%C3%A9quences

5 GHz et 2,4 GHz correspondent donc à deux fréquences WiFi différentes, principalement caractérisées par deux éléments :

- la **distance de transmission** du signal WiFi : il s'agit de la distance que les données peuvent parcourir entre deux appareils (votre box internet et votre ordinateur par exemple).
- la **vitesse de transmission** du réseau : elle est liée à la **bande-passante**, soit la quantité maximale de données qui peuvent être échangées par un réseau internet, sur une période définie à l'avance (généralement une seconde). Par exemple, plus la vitesse de transmission est élevée, plus vos fichiers se téléchargeront rapidement.

Voilà donc ce qui différencie ces deux signaux WiFi : ils ne possèdent pas les mêmes paramètres en termes de vitesse et de distance de transmission.

Là où un WiFi 2,4 GHz offre une solution optimale pour couvrir de longues distances avec une vitesse de transmission quelque peu ralentie, le WiFi 5 GHz fournit des débits de données extrêmement rapides sur une distance plus courte.

Pour information, des discussions au niveau des régulateurs sont en cours pour « ouvrir » une nouvelle bande de fréquence sans licence pouvant être utilisée pour les futurs usages du WiFi : la bande des 6 GHz.

III. Les normes WIFI

La norme IEEE 802.11 est en réalité la norme initiale publiée en 1997 qui offrait des débits de 1 ou 2 Mbit/s (Wi-Fi est un nom commercial, et c'est par abus de langage que l'on parle de « normes » Wi-Fi).

Depuis 1999, de nombreuses normes ont vu le jour et ont toutes apportées avec elles d'importantes évolutions technologiques autour du WiFi. On compte aujourd'hui 20 normes WiFi jusqu'à l'apparition cette année de la nouvelle norme WiFi 6.

Le consortium Wi-Fi Alliance dans le cadre d'une simplification de la nomenclature à décider de nommer la nouvelle norme « wifi 6 » au lieu de « 802.11ax ».

Le but étant d'utiliser des termes qui permettra de s'assurer plus facilement qu'un appareil est bien équipé de la dernière norme en date.

Les anciennes normes 802.11n, 802.11ac etc.. sont également renommées.

Liste non exhaustive des normes :

Evolution des normes WiFi

Norme WiFi	Année de création	Description
WiFi 802.11a (WiFi 1)	1999	Débit théorique : 54 Mbit/s Portée maximale : 10m
WiFi 802.11b (WiFi 2)	2000	Débit théorique : 11 Mbit/s Portée maximale : 140m
WiFi 802.11g (WiFi 3)	2003	Débit théorique : 54 Mbit/s Portée maximale : 140m
WiFi 802.11n (WiFi 4)	2006	Débit théorique : 450 Mbit/s Portée maximale : 250m
WiFi 802.11ac (WiFi 5)	2014	Débit théorique : 1,3 Gbit/s Portée maximale : 35m
WiFi 802.11ax (WiFi 6)	2019	Débit théorique : 10 Gbit/s Portée maximale : 35m

IV. La réglementation française

L'ARCEP est chargé de réguler les télécommunications et dans ce cadre, publie régulièrement des études et des réglementations en lien avec la technologie Wifi.

La réglementation radioélectrique prévoit une puissance maximale (puissance isotrope rayonnée équivalente, ou PIRE) de 100 mW pour les équipements WiFi fonctionnant à 2,45 GHz.
Pour les équipements WiFi utilisés dans les bandes de fréquences autour de 5 GHz, la réglementation radioélectrique prévoit une PIRE maximale de 200 mW dans la bande 5 150-5 350 MHz, uniquement pour une utilisation intérieure, et de 1 W dans la bande 5 470-5 725 MHz, pour une utilisation intérieure comme extérieure.

Compte tenu de l'aspect non permanent de l'émission radioélectrique en WiFi, la puissance moyenne rayonnée est toujours inférieure à ce niveau maximal autorisé.

La valeur du champ électromagnétique décroît rapidement lorsque la distance à l'antenne augmente, ce qui entraîne, au vu des faibles puissances en jeu, qu'au-delà de quelques mètres, la contribution d'un équipement WIFI utilisé dans les conditions nominales prescrites par le constructeur devient très faible en termes d'exposition.

V. Structure

Les normes 802.11 s'attachent à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- la couche physique proposant quatre types de codage de l'information ;
- la couche liaison de données, constituée de deux sous-couches :
    - le contrôle de la liaison logique (Logical Link Control, ou LLC) ;
    - le contrôle d'accès au support (Media Access Control, ou MAC).

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique.

<table>
<tr><td rowspan="2">Couche liaison de données</td><td>802.2 (LLC)</td></tr>
<tr><td>802.11 (MAC)</td></tr>
<tr><td>Couche physique (PHY)</td><td><table><tr><td>DSSS</td><td>FHSS</td><td>OFDM</td><td>Infrarouge</td></tr></table></td></tr>
</table>

Il est possible d'utiliser n'importe quel protocole de transport basé sur IP sur un réseau 802.11 au même titre que sur un réseau Ethernet.

VI. Les avantages et inconvénients

Voici les principaux avantages et inconvénients à déployer un réseau sans fil WiFi :

Avantages :

- *Mobilité :* les utilisateurs sont généralement satisfaits des libertés offertes par un réseau sans fil et de fait sont plus enclins à utiliser le matériel informatique.
- *Facilité et souplesse :* un réseau sans fil peut être utilisé dans des endroits temporaires, couvrir des zones difficiles d'accès aux câbles, et relier des bâtiments distants.
- *Coût :* si leur installation est parfois un peu plus coûteuse qu'un réseau filaire, les réseaux sans fil ont des coûts de maintenance très réduits ; sur le moyen terme, l'investissement est facilement rentabilisé.
- *Évolutivité :* les réseaux sans fil peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins.

Inconvénients :

- *Qualité et continuité du signal :* ces notions ne sont pas garanties du fait des problèmes pouvant venir des interférences, du matériel et de l'environnement.
- *Sécurité :* la sécurité des réseaux sans fil n'est pas encore tout à fait fiable du fait que cette technologie est novatrice.

VII. Modèles de déploiement

Les appareils d'un réseau sans fil sont configurés de sorte à communiquer soit indirectement par le biais d'une plateforme centrale (ou point d'accès), soit directement entre eux.

Dans le premier cas, on parle de « mode infrastructure ». Le second type de communication est le mode « ad hoc » (ou protocole P2P, *peer-to-peer*).

Bien que vous puissiez sélectionner l'un ou l'autre de ces deux modes pour votre réseau sans fil, les appareils communiquant directement entre eux doivent utiliser le même mode. En d'autres termes, si vous travaillez au sein d'une entreprise disposant déjà d'un réseau sans fil, la question ne se pose pas.

Les différences principales entre ces deux modes sont les suivantes :

Le mode infrastructure : c'est un mode de fonctionnement qui permet de connecter les ordinateurs équipés d'une carte réseau WiFi entre eux via un ou plusieurs points d'accès

qui agissent comme des concentrateurs. Il est essentiellement utilisé en entreprise. La mise en place d'un tel réseau oblige de poser à intervalle régulier des points d'accès dans la zone qui doit être couverte par le réseau.

Le mode « Ad-Hoc » : c'est un mode de fonctionnement qui permet de connecter directement les ordinateurs équipés d'une carte réseau WiFi, sans utiliser un matériel tiers tel qu'un point d'accès. Ce mode est idéal pour interconnecter rapidement des machines entre elles sans matériel supplémentaire.

VIII. Différents modes de déploiement d'un point d'accès

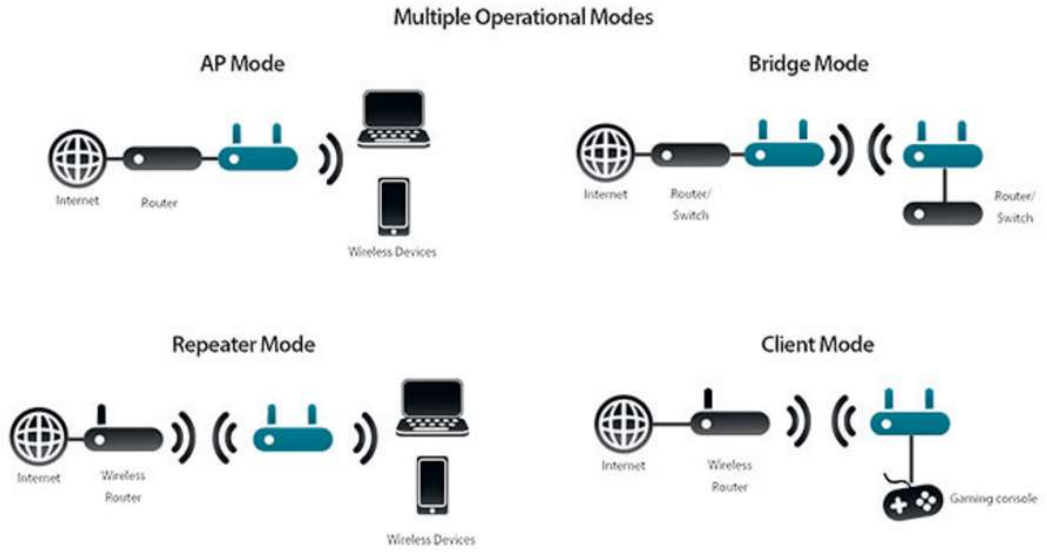
D'autres modes d'accès existent :

Le mode « pont » : Un point d'accès en mode « Pont » sert à connecter un ou plusieurs points d'accès entre eux pour étendre un réseau filaire, par exemple entre deux bâtiments. La connexion se fait au niveau 2 de la couche du modèle OSI.

Le mode « Répéteur » : Un point d'accès en mode « Répéteur » permet de répéter un signal Wi-Fi plus loin. Chaque « saut » supplémentaire augmente cependant le temps de latence de la connexion. Un répéteur a également une tendance à diminuer le débit de la connexion. En effet, son antenne doit recevoir un signal et le retransmettre par la même interface ce qui en théorie divise le débit par deux.

Le mode « WDS », le mode « Client » etc…

Exemple :



IX. La sécurité, protocole WEP, WPA, WPA2, WPA3

- WEP

Lors de l'arrivée des premiers réseaux WiFi, il a rapidement été primordial d'en sécuriser l'accès. Pour cela, le protocole de sécurité WEP a été créé en septembre 1999 permettant ainsi de crypter la connexion par l'intermédiaire d'un mot de passe, aussi appelé "clé WEP".

Cependant, ce protocole a rapidement montré ses limites, laissant un niveau encore trop élevé de vulnérabilité sur les réseaux wifi. Il fut progressivement remplacé par le WPA.

Pour résumer, les différentes vulnérabilités du WEP sont :

- Contre la confidentialité du fait de la réutilisation de la suite chiffrée, de la faiblesse du RC4 et d'une possible fausse authentification.
- Contre l'intégrité du fait de la capacité à modifier les paquets et d'en injecter des faux.

Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données. Pour autant, il sera indispensable de mettre en oeuvre une protection WEP 128 bits afin d'assurer un niveau de confidentialité minimum quant aux données de l'entreprise.

- **WPA**

Le WPA, développé par l'IEEE, est un autre protocole de sécurisation des réseaux sans fil offrant une meilleure sécurité que le WEP car il est destiné à en combler les faiblesses.

À la période où la norme de sécurité sans fil 802.11i était en développement, WPA a été utilisé en tant qu'amélioration de la sécurité temporaire pour WEP. Une année avant que WEP soit officiellement abandonné, WPA a formellement été adopté.

WPA a été une amélioration importante pour WEP, mais comment les composants principaux étaient créés de manière à ce qu'ils puissent être déployés à travers des actualisations de firmware sur des dispositifs disposant de WEP, ils dépendent encore d'éléments exploités.

Le WPA permet un meilleur cryptage de données qu'avec le WEP car il utilise des clés TKIP (Temporal Key Integrity Protocol) - dites dynamiques - et permet l'authentification des utilisateurs grâce au 802.1x - protocole mis au point par l'IEEE - et à l'EAP (Extensible Authentification Protocol).

Le TKIP rajoute par rapport aux clés WEP :

- Vecteur d'initialisation de 48 bits au lieu de 24 bits pour le WEP. Le crackage de la clé WEP provient en effet du fait que le pirate peut déterminer la clé WEP à partir du vecteur d'initialisation de 24 bits. Donc, il sera bien plus difficile à déterminer la clé avec un vecteur d'initialisation de 48 bits.
- Génération et distribution des clés : le WPA génère et distribue les clés de cryptage de façon périodique à chaque client. En fait, chaque trame utilise une nouvelle clé, évitant ainsi d'utiliser une même clé WEP pendant des semaines voire des mois.
- Code d'intégrité du message : ce code, appelé MIC (Message Integrity Code), permet de vérifier l'intégrité de la trame. Le WEP utilise une valeur de vérification d'intégrité ICV (Integrity Check Value) de 4 octets, tandis que le WPA rajoute un MIC de 8 octets.

Mode d'authentification :

- Le mode entreprise : il nécessite un serveur central qui répertorie les utilisateurs - par exemple un serveur RADIUS. Il faut pour cela un ordinateur exprès, ce qui coûte cher.
- Le mode personnel : il permet une méthode simplifiée d'authentification des utilisateurs sans utiliser un serveur central. Ce mode s'appelle également PSK (Pre-Shared Key). Il s'agit alors de saisir un mot de passe alphanumérique (« passphrase »).

Quelques problèmes subsistent tout de même à ce protocole et notamment l'attaque de type « déni de service ».

En effet, si quelqu'un envoie au moins deux paquets chaque seconde utilisant une clé de cryptage incorrecte, alors le point d'accès sans fil « tuera » toutes les connexions utilisateurs pendant une minute. C'est un mécanisme de défense pour éviter les accès non-autorisés à un réseau protégé, mais cela peut bloquer tout un réseau sans fil.

- **WPA2**

La norme de sécurité sans fil 802.11i basée sur le protocole a été introduit en 2004. L'amélioration plus importante de WPA2 sur WPA était l'usage d'Advanced Encryption Standard (AES). AES est approuvé par le gouvernement des États-Unis pour le codage des informations classées top secrètes, il doit donc être suffisamment bon pour protéger des réseaux particuliers.

Le WPA-2, tout comme son prédécesseur - le WPA - assure le cryptage ainsi que l'intégrité des données mais offre de nouvelles fonctionnalités de sécurité telles que le « Key Caching » et la « Pré-Authentification ».

Le Key Caching :

Il permet à un utilisateur de conserver la clé PMK (Pairwise Master Key) - variante de PSK (Pre-Shared Key) du protocole WPA - lorsqu'une identification s'est terminée avec succès afin de pouvoir la réutiliser lors de ses prochaines transactions avec le même point d'accès. Cela signifie qu'un utilisateur mobile n'a besoin de s'identifier qu'une seule fois avec un point d'accès spécifique. En effet, celui-ci n'a plus qu'à conserver la clé PMK - ce qui est géré par le PMKID (Pairwise Master Key IDentifier) qui n'est autre qu'un hachage de la clé PMK, l'adresse MAC du point d'accès et du client mobile, et une chaîne de caractère. Ainsi, le PMKID identifie de façon unique la clé PMK.

La Pré-Authentification :

Cette fonction permet à un utilisateur mobile de s'identifier avec un autre point d'accès sur lequel il risque de se connecter dans le futur. Ce processus est réalisé en redirigeant les trames d'authentification générées par le client envoyé au point d'accès actuel vers son futur point d'accès par l'intermédiaire du réseau filaire. Cependant, le fait qu'une station puisse se connecter à plusieurs points d'accès en même temps accroît de manière significative le temps de charge.
Pour résumer, le WPA-2 offre par rapport au WPA :

- Une sécurité et une mobilité plus efficaces grâce à l'authentification du client indépendamment du lieu où il se trouve.
- Une intégrité et une confidentialité fortes garanties par un mécanisme de distribution dynamique de clés.
- Une flexibilité grâce à une ré-authentification rapide et sécurisée.

- **WPA3**

Wi-Fi Alliance a annoncé le protocole de sécurité WPA3 en 2018, qui fournit une méthode beaucoup plus sûre et fiable pour remplacer WPA2 et les anciens protocoles de sécurité. Les lacunes fondamentales de WPA2, comme une négociation à quatre voies imparfaite et l'utilisation d'une PSK (clé pré-partagée), exposent les connexions Wi-Fi à un risque. WPA3 apporte d'autres améliorations de sécurité qui rendent plus difficile l'accès aux réseaux en devinant les mots de passe.
Voici les considérations d'implémentation recommandées:

La protection fiable par mot de passe :
WPA3-Enterprise a allongé le cryptage à 192 bits (cryptage 128 bits en mode WPA3-Personal) pour améliorer la force du mot de passe. Il protège contre les mots de passe faibles qui peuvent être craqués relativement facilement par devinettes.

La protection des périphériques réseaux :
WPA3 remplace la clé pré-partagée WPA2 (PSK) par l'authentification simultanée d'égaux (SAE) pour éviter les attaques de réinstallation de clés comme le KRACK notoire. Il gardera vos périphériques réseau en sécurité lors de la connexion à un point d'accès sans fil. SAE est également une défense efficace contre les attaques par dictionnaire hors ligne.

La Connexion plus sûre dans l'espace public :
Même si les attaquants obtiennent des clés de chiffrement du trafic, il est difficile de calculer l'utilisation du trafic et les données transmises avec WPA3-Personal. SAE offre l'avantage de la confidentialité du transfert et beaucoup plus de sécurité des données sur un réseau ouvert. WPA3 fournit également des cadres de gestion protégés (PMF) pour éviter l'écoute clandestine et la falsification de la zone publique.

X. Les antennes WIFI

Il existe deux principaux modèles d'antennes :

- Les antennes omnidirectionnelles qui ont un gain variant entre 1 et 15 dBi et qui offrent un rayonnement sur 360°. Elles s'installent généralement sur le point d'accès relié au réseau voire sur les cartes PCI.
- Les antennes directionnelles ont un gain allant de 5 à 24 dBi avec un rayonnement directif. Elles permettent d'établir des liaisons point à point mais également de couvrir une zone limitée dans le cas d'une antenne à angle d'ouverture important. Elles sont de plusieurs types comme par exemple les antennes paraboles ou encore les antennes panneaux.

Les antennes Wi-Fi sont généralement dotées de connecteurs SMA, RP-SMA (reverse polarity SMA), ou N selon le constructeur. Cependant, les antennes à gain (exprimé en dBi ou en dBd) employées à l'émission (réception libre) doivent respecter la réglementation PIRE (puissance isotrope rayonnée équivalente).

Les connectiques :

- Type N
  - La connectique d'antenne standard

- Type TNC-RP
  - Utilisée par les constructeurs Cisco et Linksys

- Type SMA
  - Répandue sur les cartes PCI et le matériel Dlink

- Type MMCX
  - Dédiées aux sorties mini-PCMCIA

XI. Types d'infrastructures WIFI

Les dernières notions importantes à considérer pour le déploiement d'infrastructure WiFi sont les différents types d'infrastructures qui, dans le cas d'environnements classiques en entreprise, se répartissent en trois catégories :

Le **mode autonome** est le mode historique des bornes WiFi. Chaque borne était alors indépendante, avait pour charge toutes les fonctions radios et réseaux, et n'interagissait pas avec les autres bornes de l'infrastructure. Il était alors nécessaire de se connecter à chacune d'entre elles pour effectuer les configurations et les mises à jour. Ce mode n'est plus d'actualité pour la plupart des constructeurs et ne pourrait être envisagé que pour des cas de limitation de budget conséquent et de projets petits à l'échelle de quelques bornes tout au plus.

L'**architecture contrôlée** est arrivée rapidement et est encore très présente aujourd'hui. Le principe initial est de déporter l'intelligence de toutes les bornes dans un seul et unique boitier à installer sur le réseau afin de les laisser se charger de la partie radio uniquement. Ce mode permet le déploiement de très nombreuses bornes, potentiellement sur plusieurs sites, dépendant d'un système de contrôleurs (au moins 2 pour la redondance).

Dans ce type d'architecture, les flux radio des bornes à destination du réseau sont remontés centralement aux contrôleurs au travers du réseau filaire par des tunnels dit « CAPWAP », avant d'être commutés centralement par les équipements contrôleurs. Ainsi, ces architectures ont un défaut : en cas de panne des contrôleurs, l'ensemble des services WiFi ne fonctionnent plus. C'est pourquoi de nombreuses solutions actuelles proposent un mode de fonctionnement différent qui est de laisser l'intelligence réseau à la main des bornes pour effectuer la commutation localement (local switching). Ce type d'architecture reste toujours prisé pour sa fonction de centralisation des flux malgré ses défauts.

Finalement, l'**architecture managée** est arrivée il y a une dizaine d'années. Celle-ci a pour objectif de conserver les fonctions de management et de supervision centralisées apportées par le contrôleur, mais en relocalisant l'intelligence au niveau des bornes WiFi en leur fournissant la capacité à s'organiser entre elles d'elles-mêmes. La brique « manager » devient alors purement logicielle, peut s'installer sur son réseau ou être disponible dans le Cloud, et ne constitue pas un point névralgique (ou SPOF : Single Point Of Failure) de notre solution.

Si le manager tombe en panne, le reste de l'infrastructure continue à fonctionner sans problème, seules les fonctions d'administration et de supervision seront temporairement perdues.