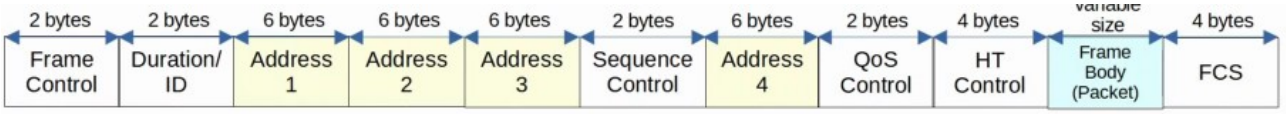
Cours 56 : Architectures Sans fil

Dans ce cours nous verrons tout d'abord le fonctionnement des messages 802.11 et le format des trames. Le Standard 802.11 pour le Wireless LANs fonctionne différemment du Standard 802.3 Wired Ethernet LANs, donc le type de messages ainsi que les trames sont aussi différentes. Nous verrons ensuite différentes Architectures de points d'accès sans fil : Autonomous AP, Lightweight AP, Cloud-based AP.
En dernier temps nous verrons le déploiement d'un Wireless LAN Controller (WLC)

Le Wireless LAN Controller est utilisé pour centraliser afin de gérer et contrôler les Point d'Accès (« AP » pour Access Point). Ils sont important dans de grands réseaux et peuvent avoir des centaines voir des milliers de point d'accès sans fil.

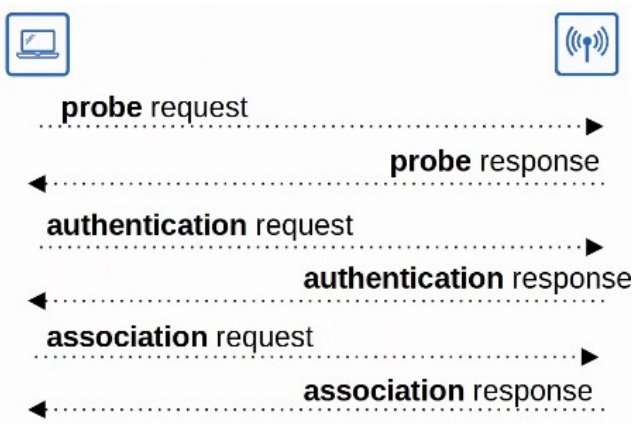
Voyons de quoi est composé une trame du Standard 802.11 :



Comme on peut le voir les trames 802.11 ont un format différent des trames Ethernet 802.3, les trames 802.11 sont plus compliqués que les trames Ethernet.
Cela peut dépendre de la version du 802.11 et du type de message mais certaines partie peuvent ne pas être présentes dans la trame.
Par exemple il y a dans la trame 4 parties différentes pour les adresses mais pas tous les messages utilisent 4 parties d'adresses différentes.
Voici en un peu plus détaillé chaque partie de la trame :
- Le Frame Control fournit des informations comme le type et sous-type de message.
- Le Duration/ID dépend du type de message, cette partie peut indiquer : le temps (en microsecondes) la chaîne dédié pour la transmission de la trame. Il peut aussi indique l'identifiant pour la connexion.
- Adresses : Jusque 4 adresses peuvent être présentes dans la trame 802.11. L'adresse présente et leur ordre dépend du type de message transmis. L'adresse peut indiquer l'adresse de destination (« DA » pour Destination Address) la réception final de la trame.
L'adresse Source (« SA » pour Source Address) l'envoyeur original de la trame.
L'adresse de réception (« RA » pour Receiver Address) le récepteur immédiat de la trame.
L'adresse de Transmission (« TA » pour Transmetter Address) l'envoyeur immédiat de la trame.
Avoir 4 adresses comme celles ci n'est pas nécessaire pour un réseau Ethernet, mais le Standard 802.11 avec les réseaux sans fil à des conditions requises spécifiques.
- Le Sequence Control est utilisé pour réassembler les fragments et éliminer les trames dupliqués.
- Le QoS Control est utilisé dans le Quality of Service pour prioriser certains trafiques.
- Le HT (High Throughput) Control est ajouté dans le 802.11n pour activer les « opération haut débit ».
802.11n est aussi connu comme le wifi Haut Débit (High Throughput)
802.11ac est aussi connu sous le nom de Wifi Thrès Haut Débit (Very HT)
- Le Frame Body est la trame ou est encapsulé le paquet transmis
- FCS (Frame Check Sequence) a la même fonction que la trame Ethernet et est utilisé pour vérifier les erreurs de la trame.

Voyons la procédure d'association 802.11, il y a un trafique des points d'accès par pont entre la station sans fil et les autres appareils. Pour une station pour envoyer le trafique par ce point d'accès, il faut que l'appareil soit associé avec le point d'accès.

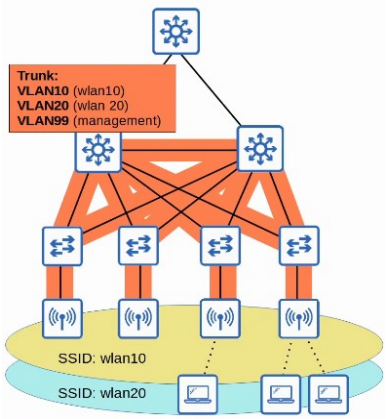
Il y a 3 états de connexion possible avec 802.11 :
- Lorsque l'appareil n'est pas authentifié ou associé avec le point d'accès
- Lorsque l'appareil est authentifié mais pas associé
- Lorsque l'appareil est authentifié et associé avec le point d'accès
La station doit être authentifié et associé avec le point d'accès pour envoyer le trafique.
La station envoie d'abord un message de sonde pour savoir quelles points d'accès et BSS sont disponibles et le point d'accès envoie une réponse sonde pour indiquer qu'il est disponible.
Il y a deux manières pour la station de scanner pour un BSS :
- Le scan actif : la station envoie des requêtes probe et écoute pour une réponse probe depuis un point d'accès.
- Le scan passif : la station écoute pour des messages de balise depuis un point d'accès.
Les messages de balises sont envoyés périodiquement par les point d'accès pour avertir le BSS.
Il y a ensuite l'authentification qui se fait avec la requête de l'appareil, par exemple la station envoie un mot de passe au point d'accès et le point d'accès authentifie l'appareil.
Si cela marche l'appareil est authentifié mais pas encore associé.
Une fois l'authentification faite il y a une requête pour l'association et une réponse.
Si cela a marché l'appareil est authentifié et associé et la station et l'appareil peuvent communiquer.



Il y a trois types de messages 802.11 :
- Trame de gestion : utilisés pour gérer le BSS, par exemple les balises, les requêtes de sonde, les réponses de sonde, l'authentification, les requêtes d'association et les réponses d'association.
- Contrôle : est utilisé pour contrôler l'accès vers le support (Par fréquence radio). Assiste avec distribution de gestion des données de trame.
Par exemple les messages : RTS (Request to Send), CTS (Clear to Send) et ACK
- Les données : sont utilisés pour envoyer des paquets de données actuel.

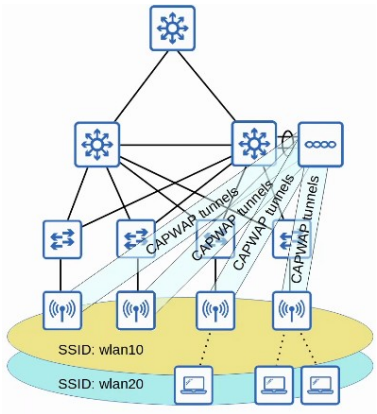
Il y a trois méthodes principales dans le déploiement de point d'accès sans fil :
1. Autonomous AP : les point d'accès autonome contiennent eux même le système ils ne s'appuient pas sur un WLC (Wireless LAN Controler), ils sont autonome et sont configurés individuellement, ils peuvent être configurés par un câble console (CLI), telnet/SSH (CLI), ou HTTP/HTTPS connexion web (GUI) une adresse IP pour la gestion distante doit être configuré. Les paramètres de radio fréquence doivent être configurés manuellement (transmettre l'énergie, la chaîne, etc.)
Les politiques de sécurité sont traité individuellement par chaque point d'accès.
Les règles QoS, etc.. sont configurés individuellement sur chaque point d'accès.
Il n'y a pas de gestion central ou de gestion des points d'accès.

Voici un exemple d’un point d’accès autonome :

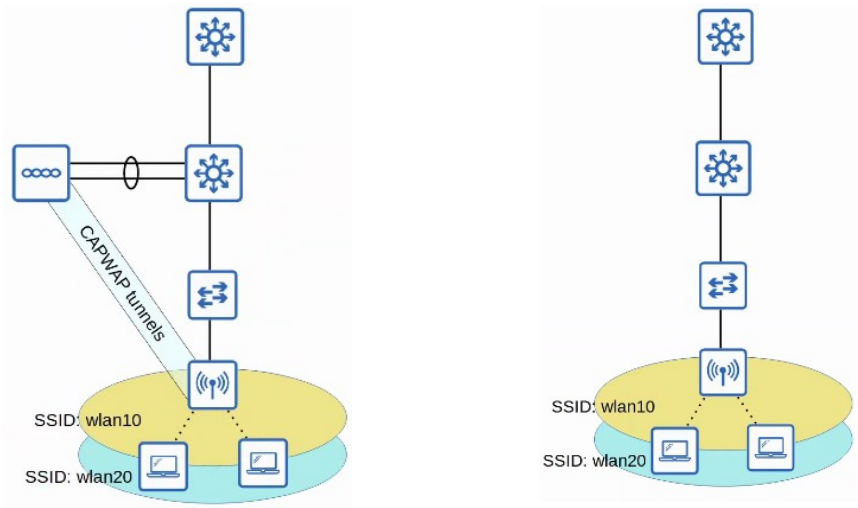


Les points d’accès autonome se connectent au réseau câblé avec un lien Trunk.
Le trafique de donnée depuis les clients sans fil ont un chemin direct vers le réseau câblé ou vers d’autres clients sans fil associés avec le même point d’accès.
Chaque VLAN doit d’étirer sur tout le réseau. Cela est considéré comme mauvaise pratique car il y aura en conséquence un large domaine de broadcast, mais aussi le spanning Tree va désactiver les liens. Ajouter et supprimer des VLAN est un travail très laborieux.
Les points d’accès autonome peuvent donc être utilisés dans de petits réseaux mais ils ne sont pas viables dans un milieu avec de grands réseaux. Les grands réseaux peuvent être constitués de plusieurs milliers de points d’accès et configurer chacun de ces points d’accès n’est pas réaliste.
Les points d’accès autonome peuvent fonctionner dans les modes vue auparavant qui sont : Repeater, Outdoor Bridge, Workgroup Bridge.

2. Lightweight AP : Les fonctions d’un point d’accès peuvent être divisés en le point d’accès et le Wireless LAN Controller (WLC). Le Lightweight AP gère en temps réel des opérations comme transmettre/recevoir le trafique par radiofréquence et le trafique de cryptage/décryptage, envoyer des balises et sondes, etc. d’autres fonctions sont possible avec WLC par exemple la gestion des radiofréquence, la gestion de sécurité/QoS, l’authentification client, association client/itinérant, etc. Cela est appelé l’architecture split-MAC puisque les fonctions sont divisés entre l’AP lightweight et le WLC. Le WLC est aussi utilisé pour configurer de manière centralisé les points d’accès lightweight. Le WLC peut être localisé dans le même sous réseau/VLAN que le point d’accès lightweight qu’il gère, ou bien sur des sous réseau/VLAN différents.
Le WLC et les points d’accès lightweight s’authentifient chacun en utilisant des certificats digitaux installés sur chaque appareils (certificat X.509 standard). Cela assure que seulement les points d’accès autorisés peuvent joindre le réseau.
Voici un exemple d’un point d’accès lightweight :

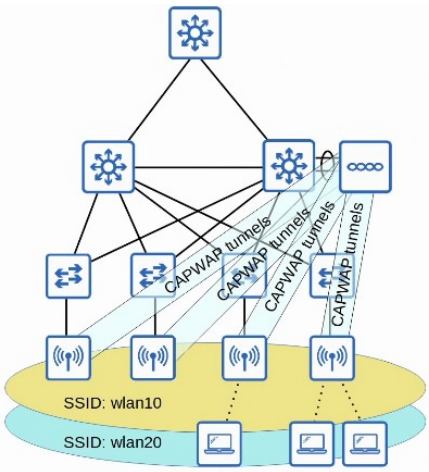


Le WLC et les points d’accès lightweight utilise un protocole appelé CAPWAP (Control And Provisioning Of Wireless Access Points) pour communiquer.
Basé sur un ancien protocole appelé LWAPP (Lightweight Access Point Protocol).
Deux tunnels sont crées entre chaque point d’accès et le WLC :
Un Control Tunnel (UDP port 5246). Ce tunnel est utilisé pour configurer le point d’accès, et contrôler/gérer les opérations. Tout le trafique dans ce tunnel est crypté par défaut.
Un Tunnel de données (UDP port 5247). Tout le trafique depuis le client sans fil est envoyé sur ce tunnel vers le WLC. Il ne va pas directement vers le réseau câblé.
Le trafique dans ce tunnel n’est pas crypté par défaut, mais il est possible de le crypter avec DTLS (Datagram Transport Layer Security).
Puisque tout le trafique depuis des clients sans fil est en tunnel vers le WLC avec CAPWAP, les points d’accès se connecte au port d’accès du switch, non pas des ports Trunk.
Voyons comment démontrer cela avec des diagrammes :
Ci dessous à gauche est présent une architecture avec des points d’accès Lightweight, à droite est présent des points d’accès autonomes :



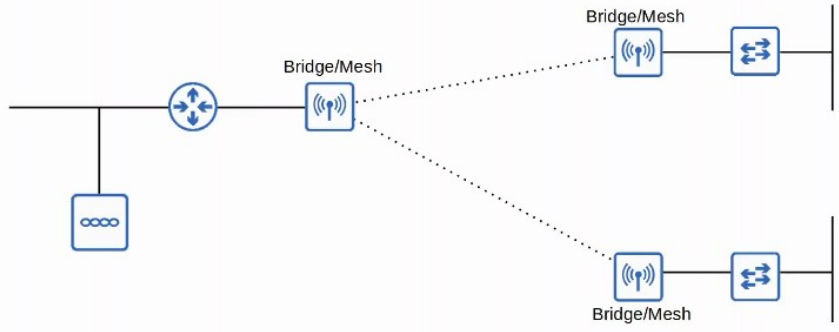
Lorsque l’on utilise un réseau autonome, un lien trunk est utilisé pour se connecter. Il doit y avoir un VLAN pour chaque SSID que le point d’accès propose.
Avec un point d’accès lightweight le client n’a pas besoin de se connecter avec un lien Trunk, un lien d’accès est suffisant. Un lien Trunk est cependant nécessaire pour connecter le WLC vers le réseau câblé.

Il y a des avantages à utiliser des architectures split MAC :



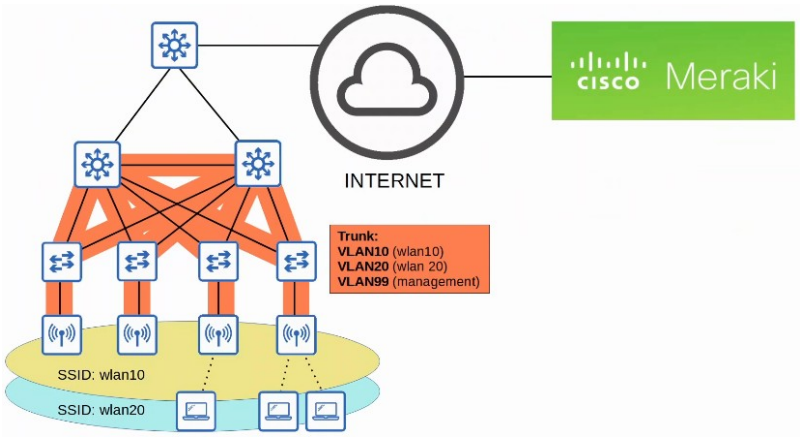
- Scalability ou évolutivité : avec WLC (ou il est bien plus simple de construire et supporter un réseau avec plusieurs milliers de points d'accès.
- Dynamic Channel Assignment : Le WLC peut automatiquement sélectionner quelle chaîne chaque point d'accès devra utiliser.
- Transmettre l'optimisation de puissance : le WLC peut automatiquement placer la puissance approprié pour chaque point d'accès.
- Re-génération de la couverture sans fil : Lorsque le point d'accès arrête de fonctionne, le WLC peut augmenter la transmission de puissance des points d'accès pour empêcher les espaces non couvert.
- Gestion de Securité/QoS : La gestion central de la sécurité et la politique QoS s'assure de la consistance à travers le réseau.

Les points d'accès lightweight peuvent être configurés pour fonctionner sur des modes variés :
- Local : c'est le mode par défaut ou le point d'accès offre un BSS (plusieurs BSS) au client pour s'associer avec lui.
- FlexConnect : Comme un point d'accès lightweight dans un mode local, il offre un ou plusieurs BSS aux clients pour s'associer avec. Seulement FlexConnect permet au point d'accès de changer localement entre le réseau câblé et sans fil si le tunnel WLC ne fonctionne plus.
- Sniffer : Le point d'accès n'offre pas un BSS au client. Il est dédié pour capturer les trames 802.11 et les envoyer vers l'appareil qui lance un logiciel comme Wireshark.
- Monitor : Le point d'accès n'offre pas un BSS aux clients. Il est dédié à recevoir une trame 802.11 pour détecter les appareil rogues. Si un client est trouvé et est un appareil rogue, un point d'accès peut dé-authentifier les messages pour dé-associer l'appareil rogue depuis le point d'accès.
- Rogue Detector : Le point d'accès n'utilise pas sa radio. Il écouté le trafique sur le réseau câblé uniquement, mais il reçoit une liste d'appareil suspectés être des clients rogue et les adresse MAC des points d'accès par le WLC. En écoutant les messages ARP sur un réseau câblé et faisant le rapport avec les informations qu'il reçoit du WLC, il peut détecter les appareils rogue.
- SE-Connect (Spectrum Expert Connect) : Le point d'accès n'offre pas un BSS aux clients.il est dédié au spectre d'analyses radiofréquences sur toutes les chaînes. Il peut envoyer des informations au logiciel comme Cisco Spectrum Expert sur un PC pour collecter et analyser les données.
- Bridge/Mesh : Tout comme les point d'accès autonome Outdoor Bridge Mode, les points d'accès lightweight peuvent être un pont dédié entre des sites, même sur une longue distance. Un maillage peut être fait entre les points d'accès. Voici un exemple :

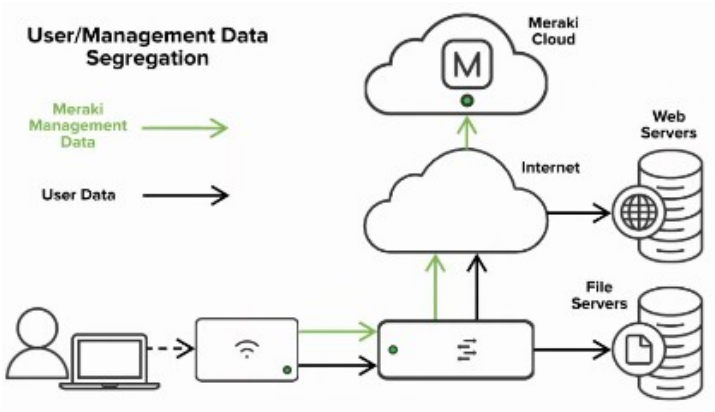


- Flex plus Bridge : ajoute la fonctionnalité FlexConnect au mode Bridge/Mesh. Ce qui permet aux points d'accès sans fil de partager localement le trafique même si la connectivité vers le WLC est perdu.

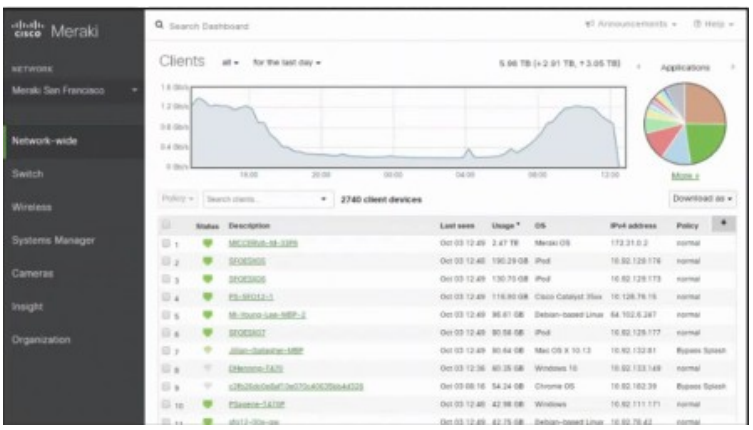
3. Cloud based : Les architecture basé sur le Cloud est un milieu entre les points d'accès autonome et les architecture split-MAC. Cela implique des points d'accès autonome qui sont géré de manière centralisé dans le Cloud.
Cisco Meraki est une solution Wifi populaire basé sur le Cloud.
Le dashboard Meraki peut être utilisé pour configurer des points d'accès, gérer le réseau, générer des rapports de performance, etc...
Meraki indique à chacun de ses points d'accès quelle chaîne utiliser, quelle énergie transmettre, etc.
Le trafique de donnée n'est pas envoyé vers le Cloud. Il est envoyé directement vers le réseau câblé comme lorsque des points d'accès autonome sont utilisés.
Seulement se que l'on appelle gestion/contrôle du trafique est envoyé vers le Cloud.
Voici un exemple :



Sur le site de Cisco Meraki est donné ce schéma :

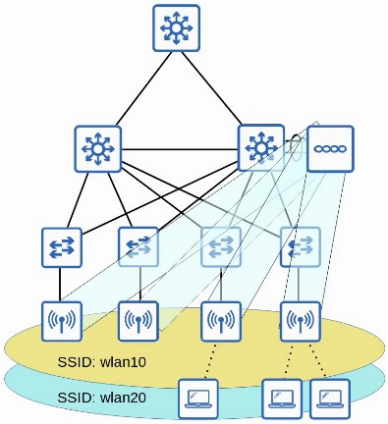


Le dashboard Meraki ressemble à cela :



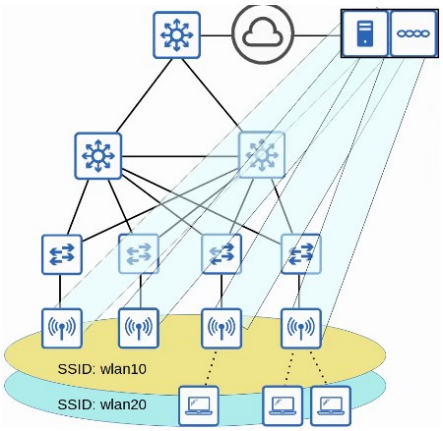
Voyons à présent le déploiement WLC.
Dans une architecture split-MAC, il y a 4 principaux modèles de déploiement :
- Unified : Le WLC est un matériel dans une localisation central du réseau.
- Cloud-Based : Le WLC est une VM lancé dans un serveur, de manière normal dans un cloud privée dans un data center. Ce n'est pas le même que l'architecture Cloud Based comme discuté auparavant.
- Embedded : Le WLC est intégré dans le Switch
- Mobility Express : Le WLC est intégré dans le point d'accès.

Voici un exemple d'un WLC unifié :



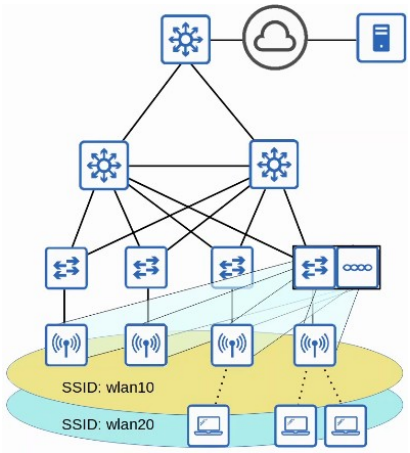
Le WLC est un matériel déployé dans une localisation centralisé du réseau.
Un WLC unifié peut supporter jusqu'à 6000 points d'accès.
S'il y en a plus de 6000, des WLC supplémentaires peuvent être ajoutés au réseau.

Voici un exemple de WLC Cloud Based :



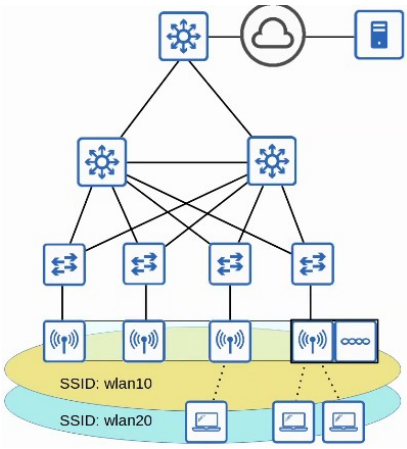
Le WLC est une VM lancé sur un serveur, de manière normal dans un cloud privée dans un data center. Un WLC cloud-based peut supporter jusqu'à 3000 points d'accès.
Si plus de 3000 points d'accès sont nécessaire, plus de VM WLC peuvent être déployés.

Voici un exemple de Embedded WLC :



Le WLC est embedded dans le Switch.
Un WLC Embedded peut supporter jusqu'à 200 points d'accès.
Si plus de 200 points d'accès sont nécessaire, plus de Switchs avec un WLC embedded peuvent être ajoutés.

Voici un exemple de Cisco Mobility Express WLC :



Le WLC est embedded dans le point d'accès.
Un Mobility Express WLC peut supporter jusqu'à 100 points d'accès.
Si plus de 100 points d'accès sont nécessaires plus de points d'accès embedded Mobility Express WLC peuvent être ajoutés.