# Guide de conception CX - Sans fil pour les grands réseaux publics

## Table des matières


- Introduction
  - Guide de conception CX
  - Portée et définitions
  - Grands réseaux publics
  - Références externes
  - Avertissement
- Conception du réseau
  - Considérations RF
    - Types de lieux
    - Stratégies de couverture
    - Esthétique
    - Réseaux indésirables
    - 5 GHz simple contre 5 GHz double
    - Antennes
    - Haute densité et 6 GHz
    - gestion des ressources radio
  - Configuration RF
    - Canaux
    - Débits de données
    - Puissance D'Émission
    - Équilibrage de puissance
    - RxSOP
  - Évolutivité du réseau
    - Nombre de points d'accès
    - Plate-forme WLC
    - Haute disponibilité WLC
    - Systèmes externes
    - DNS/DHCP
- Fonctionnement du réseau
  - La bonne configuration
  - SSID
    - Combien de SSID ?
    - WPA2/3 personnel
    - WPA2/3 Entreprise
    - SSID invités
    - Conclusion sur le nombre de SSID
    - Comparaison des concepts SSID hérités et SSID principal
    - Fonctionnalités SSID
  - Balise de site
  - Profil de stratégie
  - Profil de jointure AP

- Surveillance du réseau
  - Plus vous surveillez, plus vous pouvez causer vos propres problèmes
  - Problèmes spécifiques aux grands réseaux
  - Surveillance du jour 2 : Garder un oeil sur la satisfaction des utilisateurs
- Configuration pour l'évolutivité
  - Interfaces et interfaces SVI sur le 9800
  - Réponse de sonde agrégée
  - IPv6
  - mDNS
- Renforcement du réseau
  - Sécurité
  - Points d'accès indésirables
  - WiPS
  - Clients à limitation de débit
  - Restriction de l'accès client
  - Protection contre les tempêtes de trafic

Conclusion


# Introduction

Ce document décrit les directives de conception et de configuration pour les grands réseaux Wi-Fi publics.

## Guide de conception CX




Les guides de conception CX sont rédigés par des spécialistes du centre d'assistance technique (TAC) et des services professionnels (PS) de Cisco et examinés par des experts au sein de Cisco ; ces guides s'appuient sur les meilleures pratiques de Cisco ainsi que sur les connaissances et l'expérience acquises lors de nombreuses mises en oeuvre par les clients au fil des ans. Les réseaux conçus et configurés conformément aux recommandations de ce document permettent d'éviter les pièges courants et d'améliorer le fonctionnement du réseau.

## Portée et définitions

Ce document fournit des directives de conception et de configuration pour les grands réseaux sans fil publics.

Définition: Grands réseaux publics : déploiements sans fil, souvent à haute densité, qui fournissent une connectivité réseau à des milliers de périphériques clients inconnus et/ou non gérés.

Ce document suppose souvent que le réseau cible fournit des services à des événements importants et/ou temporaires. Il s'adapte également aux réseaux statiques permanents pour les lieux qui reçoivent de nombreux invités. Par exemple, un centre commercial ou un aéroport présente des similitudes avec le réseau Wi-Fi d'un stade ou d'une salle de concert, dans le sens où il n'y a aucun contrôle sur les utilisateurs finaux et qu'ils existent dans le réseau généralement pour quelques heures seulement, ou pour la journée tout au plus.

La couverture sans fil pour les grands événements ou les lieux a son propre ensemble d'exigences, qui tend à être différent des réseaux d'entreprise, de fabrication ou même de grande éducation. Les grands réseaux publics peuvent compter des milliers de personnes, concentrées dans un seul ou quelques bâtiments. Ils peuvent avoir une itinérance client très fréquente, en permanence ou pendant les pics d'activité. En outre, le réseau doit être aussi compatible que possible avec tout ce qui concerne les périphériques clients sans fil, sans contrôle sur la configuration ou la sécurité des périphériques clients.

Ce guide présente les concepts RF généraux pour la haute densité ainsi que les détails de mise en oeuvre. La plupart des concepts radio de ce guide s'appliquent à tous les réseaux haute densité, quelle que soit la plate-forme matérielle. Cependant, les détails de mise en oeuvre et les configurations sont axés sur Catalyst Wireless à l'aide du contrôleur sans fil Catalyst 9800, car il s'agit de la solution la plus répandue actuellement déployée pour les grands réseaux publics.

Ce document utilise les termes contrôleur sans fil et contrôleur de réseau local sans fil (WLC) de manière interchangeable.

## Grands réseaux publics

Les grands réseaux publics et événementiels sont uniques à bien des égards. Ce document explore et fournit des conseils sur ces domaines clés.

- Les grands réseaux publics sont intenses ; Il existe des milliers d'appareils dans un espace de radiofréquence (RF) réduit et une itinérance importante lorsque les gens se déplacent, certains événements et lieux peuvent être plus statiques avec des pics de bande passante à des moments très spécifiques. L'infrastructure doit gérer tous ces changements d'état de la manière la plus élégante possible pour les clients qui entrent et se déplacent dans la zone.
- La facilité d'intégration est une priorité. Un client associé est un client heureux. Cela signifie que vous voulez que l'association du client au réseau soit aussi rapide que possible. Un client qui n'est pas connecté au Wi-Fi recherche les points d'accès disponibles, ce qui génère de l'énergie RF indésirable, ce qui se traduit par un encombrement supplémentaire

et une perte de capacité sur les ondes.

- Le déploiement RF doit être conçu aussi soigneusement que possible. Une conception RF appropriée utilisant des antennes directionnelles est indispensable si une densité très élevée est requise, ou si le stade a de grands espaces ouverts et/ou de hauts plafonds.
- La compatibilité est un autre facteur clé. Certaines fonctionnalités sont standard dans la spécification 802.11, tandis que d'autres sont propriétaires et ne posent aucun problème aux clients. Cependant, la réalité est différente et il existe de nombreux pilotes clients mal programmés qui se comportent mal face à des balises ou des fonctionnalités/paramètres compliqués qu'ils ne comprennent pas.
- Le dépannage est difficile en raison de l'évolutivité et des contraintes de temps. Si quelque chose ne fonctionne pas avec un client spécifique, vous ne pouvez pas travailler avec cet utilisateur final pour comprendre le problème. Les utilisateurs peuvent être difficiles à trouver, mais ils peuvent également ne pas être coopératifs en raison de la nature transitoire de leur visite sur le site.
- La sécurité est un facteur important. Il y a moins de contrôle en raison de la très grande quantité de visiteurs invités et une surface d'attaque beaucoup plus grande.

## Références externes

| Nom du document | Source | Emplacement |
|---|---|---|
| Meilleures pratiques de configuration de la gamme Cisco Catalyst 9800 | Cisco | Lien |
| Dépannage du processeur du contrôleur LAN sans fil | Cisco | Lien |
| Valider le débit Wi-Fi : Guide de test et de surveillance | Cisco | Lien |
| Guide de déploiement du point d'accès Cisco Catalyst CW9166D1 | Cisco | Lien |
| Guide de déploiement du Cisco 9179F | Cisco | biellette |
| Guide de déploiement de l'antenne de stade Catalyst 9104 (C-ANT9104) | Cisco | Lien |
| Surveillance des indicateurs de performance clés (KPI) du Catalyst 9800 | Cisco | Lien |
| Dépannage du flux des problèmes de connectivité du client Catalyst | Cisco | Lien |

| Nom du document | Source | Emplacement |
|---|---|---|
| 9800 | | |
| Guide de configuration du logiciel du contrôleur sans fil Cisco Catalyst 9800 | Cisco | Lien |
| Wi-Fi 6E : Le prochain grand chapitre du livre blanc sur le Wi-Fi | Cisco | Lien |

### Avertissement

Ce document propose des recommandations basées sur certains scénarios, hypothèses et connaissances acquises lors de nombreux déploiements. Cependant, vous, le lecteur, êtes chargé de déterminer la conception du réseau, l'activité, la conformité aux réglementations, la sécurité, la confidentialité et d'autres exigences, y compris de suivre ou non les conseils ou recommandations fournis dans ce guide.

## Conception du réseau

### Considérations RF

#### Types de lieux

Ce guide se concentre sur les grands réseaux invités, généralement ouverts au public, et avec un contrôle limité sur les utilisateurs finaux et les types de périphériques clients. Ces types de réseaux peuvent être déployés sur différents sites et peuvent être temporaires ou permanents. Le cas d'utilisation principal est généralement la fourniture d'un accès Internet aux visiteurs, bien que ce soit rarement le seul cas d'utilisation.

Emplacements types :

- Stades et arénas
- Lieux de conférence
- Grands auditoriums

D'un point de vue RF, chacun de ces types d'emplacement a son propre ensemble de nuances. La plupart de ces exemples sont généralement des installations permanentes, à l'exception des

salles de conférence et de concert, car elles peuvent être permanentes ou mises en place pour un spectacle spécifique sur une base temporaire.

Autres sites :

- Bateau de croisière
- Aéroport
- Centre commercial / Centre commercial

Les aéroports et les navires de croisière sont également des exemples de déploiements qui entrent dans la catégorie des grands réseaux publics ; cependant, ces points d'accès ont des considérations supplémentaires spécifiques à chaque cas et font souvent appel à des points d'accès omnidirectionnels internes.

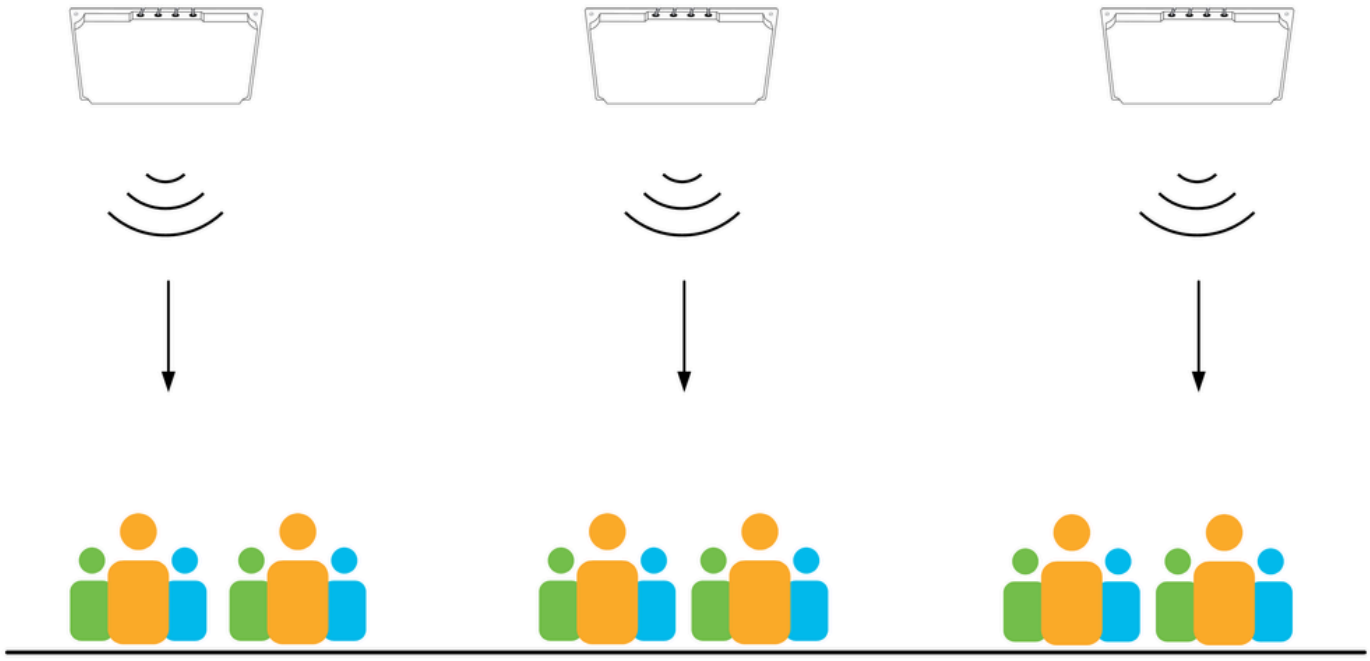
Stratégies de couverture

Les stratégies de couverture dépendent en grande partie du type de site, des antennes utilisées et des emplacements de montage disponibles.

Frais Généraux

La couverture des frais généraux est toujours privilégiée dans la mesure du possible.

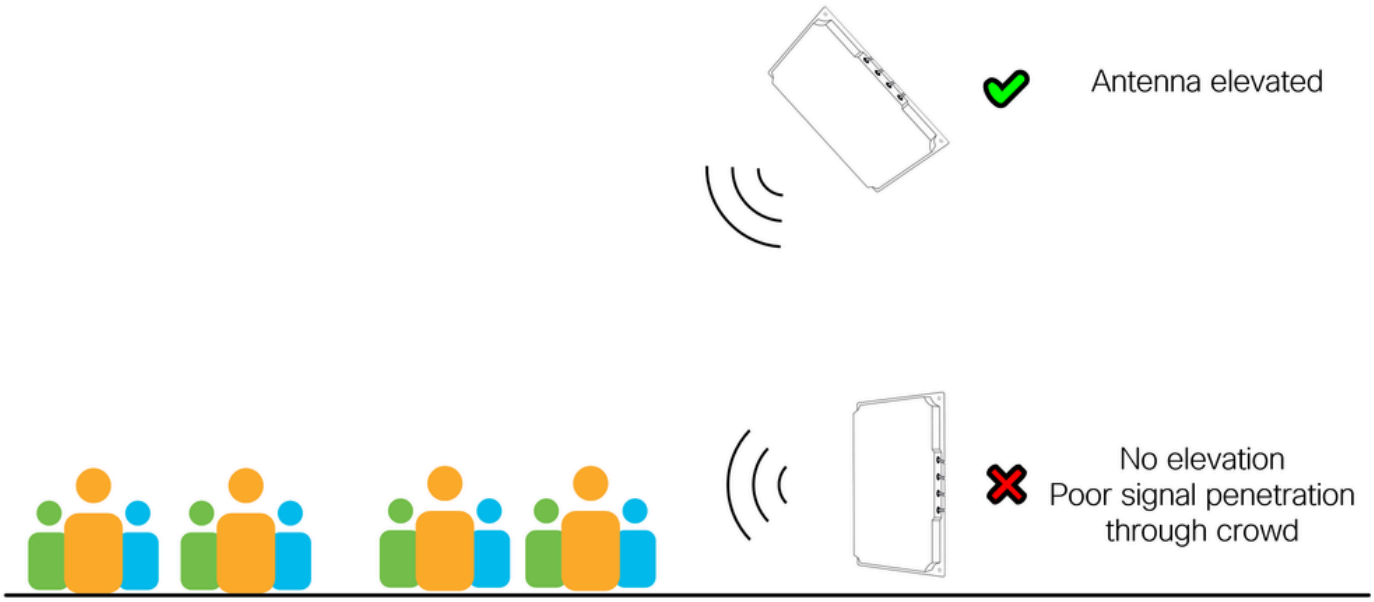
Les solutions de surcharge présentent l'avantage évident que tous les périphériques clients disposent généralement d'une ligne de vision directe vers le dessus de l'antenne, même dans les scénarios encombrés. Les solutions de surcharge utilisant des antennes directionnelles offrent une zone de couverture plus contrôlée et mieux définie, ce qui les rend moins compliquées du point de vue du réglage radio, tout en offrant un meilleur équilibrage de charge et des caractéristiques d'itinérance client. Pour plus d'informations, reportez-vous à la section Équilibrage de puissance.



AP au-dessus des clients

Côté

Les antennes directionnelles montées sur le côté sont un choix populaire et fonctionnent bien dans une variété de scénarios, en particulier lorsque le montage au plafond n'est pas possible en raison de la hauteur ou des restrictions de montage. Lors de l'utilisation d'un montage latéral, il est important de comprendre le type de zone couverte par l'antenne, par exemple s'agit-il d'une zone extérieure ouverte ou d'une zone intérieure dense ? Si la zone de couverture est une zone de forte densité avec beaucoup de personnes, alors l'antenne doit être élevée autant que possible car la propagation du signal à travers une foule humaine est toujours pauvre. Rappelez-vous que la plupart des appareils mobiles sont utilisés plus bas à la taille, pas au-dessus de la tête de l'utilisateur ! La hauteur de l'antenne est moins importante lorsque la zone de couverture est une zone de densité inférieure.




L'élévation de l'antenne est toujours meilleure

Omnidirectionnel

L'utilisation d'antennes omnidirectionnelles (internes ou externes) doit généralement être évitée dans les scénarios de très haute densité, ceci étant dû à la zone d'impact potentiellement élevée pour les interférences co-canal. Les antennes omnidirectionnelles ne doivent pas être utilisées à une hauteur supérieure à 6 m (ne s'applique pas aux unités extérieures à gain élevé).

Sous le siège

Dans certains stades ou arénas, il peut y avoir des situations où il n'y a pas d'emplacements de montage d'antenne appropriés. La dernière alternative consiste à fournir une couverture par le bas en positionnant les points d'accès sous les sièges où les utilisateurs sont assis. Ce type de solution est plus difficile à déployer correctement et est généralement plus coûteux, nécessitant un nombre bien plus important de points d'accès et de procédures d'installation spécifiques.

Le principal défi posé par le déploiement en sous-effectif est la grande différence de couverture entre un stade complet et un stade vide. Un corps humain est très efficace pour atténuer le signal radio, ce qui signifie que lorsqu'il y a une foule de personnes autour du point d'accès, la couverture qui en résulte est beaucoup plus petite que lorsque ces personnes ne sont pas là. Ce facteur d'atténuation de la foule humaine permet de déployer davantage de points d'accès, ce qui peut augmenter la capacité globale. Cependant, lorsque le stade est vide, il n'y a pas d'atténuation du corps humain et d'interférence significative, ce qui entraîne des complications lorsque le stade est partiellement plein.

Remarque : Le déploiement sous le siège est une solution valide mais peu courante, qui doit être évaluée au cas par cas. Le déploiement sous le siège n'est pas traité plus en détail dans ce document.

Esthétique

Dans certains déploiements, la question de l'esthétique entre en jeu. Il peut s'agir de zones présentant des conceptions architecturales spécifiques, une valeur historique ou des espaces où la publicité et/ou la marque dictent où l'équipement peut (ou ne peut pas) être monté. Des solutions spécifiques peuvent être nécessaires pour contourner les limites de placement. Certaines de ces solutions de contournement incluent le masquage du point d'accès/de l'antenne, le recouvrement du point d'accès/de l'antenne, le montage de l'équipement dans un boîtier ou simplement l'utilisation d'un emplacement différent. La peinture de l'antenne annule toutefois la garantie. Cisco ne vend généralement pas de boîtiers pour antennes, mais bon nombre d'entre eux sont facilement disponibles auprès de divers fournisseurs qui vendent également divers couvercles et différentes manières de faire correspondre les points d'accès à différentes esthétiques.

Toutes ces solutions de contournement ont un impact sur les performances du réseau. Les architectes sans fil commencent toujours par proposer des positions de montage optimales pour une meilleure couverture radio, et ces positions initiales offrent généralement les meilleures performances. Toute modification de ces positions entraîne souvent le déplacement des antennes loin de leur emplacement optimal.

Les emplacements où les antennes sont montées sont souvent surélevés. Il peut s'agir de plafonds, de passerelles, de structures de toit, de poutres, de trottoirs et de tout emplacement offrant une certaine élévation au-dessus de la zone de couverture prévue. Ces emplacements sont généralement partagés avec d'autres installations, telles que : matériel audio, climatisation, éclairage, caméras et différents détecteurs / capteurs. Par exemple, l'équipement audio et d'éclairage doit être installé à des emplacements très spécifiques, mais pourquoi ? Tout simplement parce que les équipements audio et d'éclairage ne fonctionnent pas correctement lorsqu'ils sont cachés dans une boîte ou derrière un mur.

Il en va de même pour les antennes sans fil. Elles fonctionnent mieux lorsqu'une ligne de visée est établie vers le périphérique client sans fil. Le fait de donner la priorité à l'esthétique peut (et c'est souvent le cas) avoir un effet négatif sur les performances sans fil, diminuant ainsi la valeur de l'investissement dans l'infrastructure.

Réseaux indésirables

Les réseaux Wi-Fi non autorisés sont des réseaux sans fil qui partagent un espace RF commun mais qui ne sont pas gérés par le même opérateur. Ils peuvent être temporaires ou permanents et inclure des périphériques d'infrastructure (AP) et des périphériques personnels (tels que des téléphones mobiles partageant un point d'accès Wi-Fi). Les réseaux Wi-Fi non autorisés constituent une source d'interférences et, dans certains cas, un risque pour la sécurité. Il ne faut pas sous-estimer l'impact des périphériques non fiables sur les performances sans fil. Les transmissions Wi-Fi sont limitées à une plage relativement petite de spectre radio qui est partagée entre tous les périphériques Wi-Fi. Tout périphérique qui se comporte mal à proximité peut perturber les performances du réseau pour de nombreux utilisateurs.

Dans le cadre de grands réseaux publics, ceux-ci sont généralement conçus et réglés avec soin à l'aide d'antennes spécialisées. Une bonne conception RF ne couvre que les zones requises, en utilisant souvent des antennes directionnelles avec des caractéristiques d'émission et de réception réglées pour une efficacité maximale.

À l'autre extrémité du spectre se trouvent les périphériques grand public ou les périphériques fournis par les fournisseurs de services Internet. Ces derniers disposent d'options limitées pour le réglage fin des radiofréquences ou sont configurés pour une portée maximale et des performances perçues, souvent avec une puissance élevée, des débits de données faibles et des canaux étendus. L'introduction de tels périphériques dans un réseau d'événements de grande taille peut causer des ravages.

Que peut-on faire ?

Dans le cas des hotspots personnels, il y a très peu de choses à faire, car il serait presque impossible de surveiller des dizaines de milliers de personnes entrant dans un lieu. Dans le cas d'une infrastructure, ou de périphériques semi-permanents, il existe plusieurs options. La correction possible commence par une simple éducation, une signalisation pour la sensibilisation, des documents de politique radio signés, se terminant par une application active et une analyse du spectre. Dans tous les cas, une décision commerciale doit être prise sur la protection du spectre radioélectrique dans le lieu donné, ainsi que des mesures concrètes pour faire appliquer cette décision commerciale.

L'aspect sécurité des réseaux non autorisés entre en jeu lorsque des périphériques contrôlés par un $^{tiers}$ annoncent le même SSID que le réseau géré. Cela équivaut à une attaque de type « pot de miel » et peut être utilisé comme méthode pour voler les informations d'identification de l'utilisateur. Il est toujours recommandé de créer une règle non autorisée pour alerter de la détection des SSID d'infrastructure annoncés par des périphériques non gérés. La section relative à la sécurité traite plus en détail des systèmes non fiables.

5 GHz simple contre 5 GHz double

Dual 5GHz désigne l'utilisation des deux radios 5GHz sur les points d'accès pris en charge. Il existe une différence majeure entre une double fréquence de 5 GHz avec des antennes externes et une double fréquence de 5 GHz avec des antennes internes (par exemple, des micro/macro cellules sur des points d'accès omnidirectionnels). Dans le cas d'antennes externes, le double 5 GHz est souvent un mécanisme utile, qui offre une couverture et une capacité supplémentaires tout en réduisant le nombre total de points d'accès.

Micro/Macro/Méso

Les points d'accès internes ont les deux antennes proches l'une de l'autre (à l'intérieur du point d'accès) et sont soumis à des restrictions relatives à la puissance Tx maximale lors de l'utilisation de deux 5 GHz. La seconde radio est limitée à une faible puissance Tx (ce qui est imposé par le contrôleur sans fil) conduisant à un déséquilibre important de la puissance Tx entre les radios. Cela peut entraîner une sous-utilisation de la radio principale (plus puissante) par de nombreux clients, alors que la radio secondaire (moins puissante) est sous-utilisée. Dans ce cas, la seconde radio ajoute de l'énergie à l'environnement sans apporter d'avantages aux clients. Si ce scénario est observé, il peut être préférable de désactiver la seconde radio et d'ajouter simplement un autre AP (5 GHz) si une capacité supplémentaire est requise.

Différents modèles de points d'accès ont différentes options de configuration, la seconde radio 5 GHz peut fonctionner à des niveaux de puissance plus élevés dans les nouveaux points d'accès macro/méso comme les 9130 et 9136, et certains points d'accès Wi-Fi 6E internes comme la série 9160 peuvent même fonctionner en macro/macro. Vérifiez toujours la capacité de votre modèle AP exact. Le second emplacement 5 GHz est également limité dans son utilisation de canal, lorsqu'un emplacement fonctionne dans une bande UNII, l'autre emplacement est limité à une bande UNII différente, ce qui a un impact sur la planification du canal et par conséquent sur la puissance de transmission disponible. Tenez toujours compte de la différence de puissance Tx entre deux radios 5 GHz, ce qui est vrai dans tous les cas, y compris les points d'accès avec antennes internes.

FRA

La technologie FRA (Flexible Radio Assignment) a été introduite pour améliorer la couverture 5 GHz en commutant des radios 2,4 GHz supplémentaires en mode 5 GHz ou des radios 5 GHz potentiellement inutilisées en mode surveillance (pour les points d'accès qui la prennent en charge). Comme ce document couvre de grands réseaux publics, on suppose que les zones de couverture ainsi que la conception radio sont bien définies à l'aide d'antennes directionnelles, par conséquent une configuration déterministe est préférée à une configuration dynamique. L'utilisation de FRA n'est pas recommandée pour les grands réseaux publics.

FRA peut éventuellement être utilisé lorsque le réseau est configuré pour aider à déterminer les radios à convertir en 5 GHz, mais une fois que vous êtes satisfait du résultat, il est conseillé de geler FRA.

Réglementaire

Chaque domaine réglementaire définit les canaux disponibles et leurs niveaux de puissance maximum. Il existe également des restrictions quant aux canaux pouvant être utilisés à l'intérieur et à l'extérieur. Selon le domaine réglementaire, il peut parfois être impossible d'utiliser efficacement une solution double 5 GHz. Par exemple, dans le domaine ETSI, 30 dBm sont autorisés sur les canaux UNII-2e, mais seulement 23 dBm sur UNII1/2. Dans cet exemple, si la conception nécessite l'utilisation de 30 dBm (généralement en raison d'une plus grande distance par rapport à l'antenne), l'utilisation d'une seule radio 5 GHz peut constituer la seule solution possible.

Parfois, des canaux supplémentaires sont ajoutés dans une version ultérieure du logiciel à certains domaines réglementaires, mais il est possible que ces canaux aient également une puissance de transmission maximale différente : vérifiez que vos clients prennent en charge ces canaux et ne les utilisent que sur les points d'accès où la puissance de transmission ne posera pas de problème.
Si vous souhaitez utiliser tous les canaux disponibles, il peut être intéressant de créer des profils RF où les points d'accès nécessitant la puissance de transmission la plus élevée (tels que les points d'accès montés sur un plafond très élevé) utilisent uniquement des canaux où une puissance plus élevée est disponible et conservent des canaux de puissance plus faible pour les points d'accès qui sont plus proches du sol dans les zones plus denses.

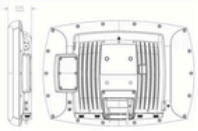
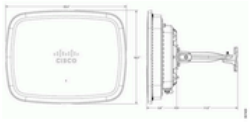
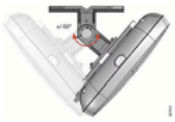
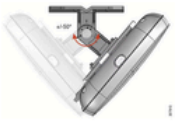
Antennes

Les grands réseaux publics peuvent utiliser n'importe quel type d'antenne et déploient généralement l'antenne la mieux adaptée à la tâche. Le mélange d'antennes dans la même zone de couverture rend le processus de conception radio plus difficile et doit être évité si possible. Cependant, les grands réseaux publics ont souvent de grandes zones de couverture avec des options de montage différentes même au sein de la même zone, ce qui rend nécessaire de mélanger les antennes dans certains cas.

Ce tableau répertorie les antennes externes les plus couramment utilisées :

| | | |
|---|---|---|
|  | C-ANT9103<br>Patch antenna (8x8)<br>6 dBi | 5GHz Beamwidth<br>70°x70°<br>~33ft (10m) |
|  | ANT2566P4W-R/S<br>Patch antenna (4x4)<br>6 dBi | 5GHz Beamwidth<br>110°x55° (120°x60°)<br>~33ft (10m) |
|  | ANT2566D4M-R/S<br>Patch antenna (4x4)<br>6 dBi | 5GHz Beamwidth<br>55°x60° (60°x60°)<br>~33ft (10m) |
|  | ANT2513P4M-N/S<br>HD "Stadium" antenna<br>13 dBi | 5GHz Beamwidth<br>31°x27° (30°x30°)<br>~66ft (20m) |

Ce tableau répertorie les antennes directionnelles intégrées les plus couramment utilisées :

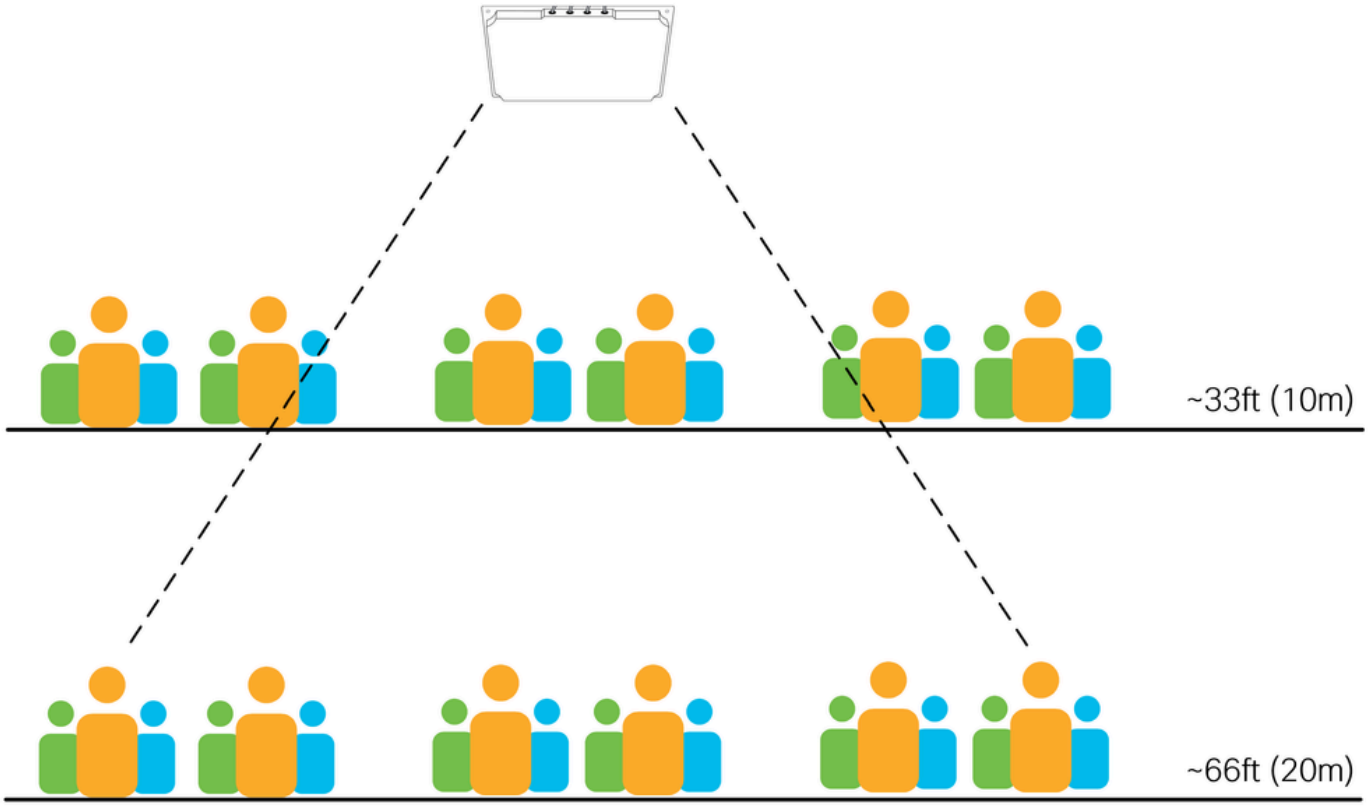
| | | | |
|---|---|---|---|
|  | CW9179F<br>Integrated directional<br>~100ft (30m)<br>*See data sheet for gain info.* | 5GHz<br>Narrow 35° x 35°<br>Wide *See data sheet* | 6GHz<br>Narrow 35° x 35°<br>Wide 70° x 35° |
|  | C-ANT9104<br>Integrated directional<br>~66ft (20m) | 5GHz<br>Narrow 25° x 25° : 10dBi<br>Wide 80° x 25° : 7dBi | |
|  | CW9166D1<br>Integrated directional<br>~33ft (10m)<br>*See data sheets for XOR info.* | 6GHz<br>60° x 60°<br>8 dBi | 5GHz<br>70° x 70°<br>6 dBi |
|  | CW9176D1<br>Integrated directional<br>~33ft (10m)<br>*See data sheets for XOR info.* | 6GHz<br>70° x 70°<br>8 dBi | 5GHz<br>70° x 70°<br>8 dBi |

Les principaux facteurs à prendre en compte lors du choix d'une antenne sont la largeur de faisceau et la distance/hauteur de l'antenne. Les tableaux présentent la largeur de faisceau des antennes couramment utilisées, les chiffres entre parenthèses indiquant des valeurs arrondies (et plus faciles à mémoriser).

Les distances suggérées dans le tableau ne sont pas des règles strictes, mais uniquement des directives basées sur l'expérience. Les ondes radio se déplacent à la vitesse de la lumière et ne s'arrêtent pas après avoir atteint une distance arbitraire. Les antennes fonctionnent toutes au-delà de la distance suggérée, mais les performances diminuent à mesure que la distance augmente. La hauteur d'installation est un facteur clé lors de la planification.

Le schéma ci-dessous montre deux hauteurs de montage possibles pour la même antenne à ~33 pieds (10 m) et ~66 pieds (20 m) dans une zone haute densité. Notez que le nombre de clients que l'antenne peut voir (et à partir desquels elle accepte les connexions) augmente avec la distance. Le maintien de cellules de petite taille devient plus difficile avec des distances plus importantes.

La règle générale est que plus la densité d'utilisateurs est élevée, plus il est important d'utiliser l'antenne correcte pour la distance donnée.




Antenne de stade

Le CW9179F est parfaitement adapté à la couverture de zones haute densité à des distances élevées. Pour plus d'informations, reportez-vous au Guide de déploiement du point d'accès sans fil Cisco 9179F.

Changements dans le temps

Les modifications de l'environnement physique au fil du temps sont courantes dans presque toutes les installations sans fil (par exemple, le déplacement des murs intérieurs ou la réorganisation des sièges des sites). Des visites régulières sur place et des inspections visuelles ont toujours été recommandées. Pour les réseaux événementiels, la complexité supplémentaire de la gestion des systèmes audio et d'éclairage et, dans de nombreux cas, d'autres systèmes de communication (tels que la 5G). Tous ces systèmes sont souvent installés à des emplacements élevés au-dessus des utilisateurs, ce qui entraîne parfois des conflits pour le même espace. Un bon emplacement pour une antenne de stade sans fil est souvent également un bon emplacement pour une antenne 5G ! En outre, à mesure que ces systèmes sont mis à niveau, ils peuvent être déplacés vers des emplacements où ils entravent le fonctionnement du système sans fil et/ou interfèrent activement avec celui-ci. Il est important de garder une trace des autres installations et de communiquer avec les équipes qui les installent, afin de s'assurer que tous les systèmes sont installés dans des endroits appropriés sans interférer les uns avec les autres (physiquement ou électromagnétiquement).

Haute densité et 6 GHz

La bande 6 GHz plus propre et moins encombrée offre une meilleure expérience sur 5 GHz tout en ayant l'avantage supplémentaire de réduire l'utilisation du temps d'antenne 5 GHz à mesure que davantage de périphériques clients adoptent 6 GHz. Les réseaux modernes doivent être conçus pour une couverture à la fois 5 GHz et 6 GHz, y compris les grands réseaux publics.
La gamme de produits Cisco inclut plusieurs périphériques 6 GHz pouvant être utilisés pour des déploiements haute densité ; le 9179F pour une portée plus longue et une couverture ciblée, ainsi que les modèles 91x6D1 pour une couverture plus large à des distances plus faibles. La combinaison de ces produits permet de nombreuses options de conception 6 GHz sur une variété d'emplacements.
La conception d'une couverture 6 GHz suit généralement la même méthodologie que celle de la couverture 5 GHz. Les directives relatives à la sélection des débits de données, des largeurs de canaux et des valeurs Rx-Sop restent les mêmes, bien qu'il faille accorder une attention particulière aux configurations de sécurité requises pour la bande 6 GHz, ainsi qu'à la planification des canaux et à l'utilisation des canaux de balayage primaire (PSC).

Dans le cadre de grands réseaux publics, ceux-ci ont souvent des zones diverses et importantes et nécessitent l'utilisation d'une combinaison d'antennes à des hauteurs différentes. Le déploiement d'un grand réseau public de bout en bout à l'aide d'une antenne 60°x60° peut s'avérer difficile en raison des limites de distance. Par conséquent, il peut également être difficile de fournir une couverture de bout en bout à 6 GHz en utilisant uniquement le CW9166D1 pour un grand réseau public.

Une approche possible consiste à utiliser la bande de couverture principale de 5 GHz, tandis que la bande de couverture principale de 6 GHz n'est utilisée que dans des zones spécifiques pour décharger les périphériques clients compatibles vers la bande de 6 GHz plus propre. Ce type d'approche utilise des antennes 5 GHz uniquement dans des zones plus étendues, tout en utilisant les antennes 6 GHz lorsque cela est possible et lorsque de la capacité supplémentaire est requise.

L'itinérance client entre les bandes 5 GHz et 6 GHz est traitée plus loin dans ce document.

Réglementaire

Comme pour la bande 5 GHz, la puissance disponible et les canaux pour la bande 6 GHz diffèrent considérablement d'un domaine réglementaire à l'autre. Il existe notamment une grande différence dans le spectre disponible entre les domaines FCC et ETSI, ainsi que des directives strictes autour de la puissance Tx disponible pour une utilisation intérieure et extérieure, basse puissance intérieure (LPI) et puissance standard (SP) respectivement. Avec la bande 6 GHz, les restrictions supplémentaires incluent les limites d'alimentation du client, l'utilisation d'antennes externes et l'inclinaison vers le bas de l'antenne, et (uniquement aux États-Unis pour le moment) la nécessité d'une coordination automatique de la fréquence (AFC) pour les déploiements SP.

Pour plus d'informations sur le Wi-Fi 6E, consultez Wi-Fi 6E : Le prochain grand chapitre du livre blanc sur le Wi-Fi.

gestion des ressources radio

La gestion des ressources radio (RRM, Radio Resource Management) est un ensemble d'algorithmes responsables du contrôle du fonctionnement radio. Ce guide fait référence à deux algorithmes RRM clés, à savoir Dynamic Channel Assignment (DCA) et Transmit Power Control (TPC). RRM est une alternative à la configuration statique des canaux et de l'alimentation.

- DCA s'exécute selon un calendrier configurable (10 minutes par défaut).
- Le PTC s'exécute automatiquement (10 minutes par défaut).

Cisco Event Driven RRM (ED-RRM) est une option DCA qui permet de prendre une décision de changement de canal en dehors du planning DCA standard, généralement en réponse à des conditions RF sévères. ED-RRM peut changer un canal immédiatement lorsque des niveaux excessifs d'interférence sont détectés. Dans des environnements bruyants et/ou instables, l'activation de ED-RRM présente un risque de modifications excessives des canaux, ce qui peut avoir un impact négatif sur les périphériques clients.

L'utilisation de RRM est encouragée et généralement préférée à la configuration statique, avec toutefois quelques mises en garde et exceptions.

- Le TPC doit être limité à une plage de valeurs appropriée utilisant le paramètre TPC min/max, selon les besoins, et toujours aligné sur la conception RF.
    - Permettre la reconnaissance des canaux TCP dans les environnements à haute densité.

- Le cycle DCA doit être modifié par rapport au paramètre par défaut de 10 minutes.
    - N'utilisez pas ED-RRM dans des environnements occupés, bruyants et à haute densité.
    - Désactiver Éviter le chargement de Cisco AP.
    - Les options d'évitement de points d'accès indésirables comme Éviter l'interférence de points d'accès étrangers peuvent entraîner un environnement instable s'il y a beaucoup de points d'accès indésirables. Il est toujours préférable de supprimer le pirate plutôt que d'essayer d'y répondre.
- Les décisions RRM peuvent être influencées par les points d'accès/antennes qui ne s'entendent pas correctement, comme dans le cas d'antennes directionnelles qui pointent à l'opposé les unes des autres.
- Certaines antennes (C9104 par exemple) ne prennent pas en charge RRM et nécessitent toujours une configuration statique.
- RRM ne résout pas les problèmes de conception RF.

Dans tous les cas, RRM doit être déployé avec une compréhension du résultat attendu, et réglé pour fonctionner dans les limites qui sont appropriées pour l'environnement RF donné. Les

sections suivantes de ce document explorent ces points plus en détail.

## Configuration RF

### Canaux

En général, plus il y a de canaux, mieux c'est. Dans les déploiements à haute densité, il peut y avoir des points d'accès et des radios plus déployés que les canaux disponibles, ce qui implique un taux de réutilisation des canaux important et, avec cela, des niveaux plus élevés d'interférence entre canaux. Tous les canaux disponibles doivent être utilisés et il est généralement déconseillé de limiter la liste des canaux disponibles.

Il peut arriver qu'un système sans fil spécifique (et distinct) doive coexister dans le même espace physique et que des canaux dédiés lui soient attribués, tout en supprimant le ou les canaux attribués de la liste DCA du système principal. Ces types d'exclusions de canaux doivent être évalués très attentivement et utilisés uniquement lorsque cela est nécessaire. Par exemple, une liaison point à point fonctionnant dans une zone ouverte adjacente au réseau principal ou une zone de presse à l'intérieur d'un stade. Si plus d'un ou deux canaux sont exclus de la liste des ACD, cela peut être un motif de réévaluation de la solution proposée. Dans certains cas, comme dans les stades à très haute densité, l'exclusion même d'un seul canal peut parfois ne pas être une option envisageable.

L'attribution dynamique de canal (DCA) peut être utilisée avec la RRM basée sur WLC ou la RRM améliorée par AI.

L'intervalle DCA par défaut est de 10 minutes, ce qui peut entraîner des changements fréquents de canal dans les environnements RF instables. Le compteur DCA par défaut doit être augmenté par rapport aux 10 minutes par défaut dans tous les cas, l'intervalle DCA spécifique doit être aligné sur les exigences de fonctionnement pour le réseau en question. Voici un exemple de configuration : DCA interval 4 hours, anchor time 8. Ceci limite les changements de canal à une fois toutes les 4 heures, à partir de 8h.

Comme les interférences sont inévitables, s'y adapter à chaque cycle de DCA n'apporte pas nécessairement de valeur, car la plupart de ces interférences sont temporaires. Une bonne technique consiste à utiliser le DCA automatique pendant les premières heures et à geler l'algorithme et le plan de canaux lorsque vous avez quelque chose de stable qui vous satisfait.

Lorsque le WLC est redémarré, DCA fonctionne en mode agressif pendant 100 minutes pour trouver un plan de canal approprié. Il est conseillé de redémarrer le processus manuellement lorsque des modifications importantes sont apportées à la conception RF (par exemple, l'ajout ou la suppression de nombreux points d'accès ou la modification de la largeur de canal). Pour

démarrer ce processus manuellement, utilisez cette commande.

```
ap dot11 [24ghz | 5ghz | 6ghz] rrm dca restart
```

---



Remarque : Les changements de canal peuvent perturber les périphériques clients.

---

2,4 GHz

La bande 2,4 GHz a souvent été critiquée. Il n'a que trois canaux sans chevauchement et de nombreuses autres technologies que le Wi-Fi l'utilisent, ce qui crée des interférences indésirables. Certaines organisations insistent pour fournir des services, alors quelle est une conclusion raisonnable ? Il est un fait que la bande 2,4 GHz ne fournit pas une expérience satisfaisante pour les utilisateurs finaux. Pire encore, en essayant de fournir un service sur 2,4 GHz, vous affectez d'autres technologies 2,4 GHz telles que Bluetooth. Dans les grandes salles ou les grands événements, de nombreuses personnes s'attendent toujours à ce que leur casque sans fil fonctionne lorsqu'elles passent un appel ou que leurs appareils portables intelligents continuent à fonctionner comme d'habitude. Si votre Wi-Fi dense fonctionne à 2,4 GHz, vous impactez les périphériques qui n'utilisent même pas votre Wi-Fi 2,4 GHz.

Une chose est sûre, si vous devez réellement fournir un service Wi-Fi 2,4 GHz, il est préférable de le faire sur un SSID distinct (dédiez-le aux périphériques IoT ou appelez-le « hérité »). Cela signifie que les périphériques double bande ne se connectent pas à 2,4 GHz involontairement et que seuls les périphériques monobande 2,4 GHz s'y connectent.

Cisco ne conseille ni ne prend en charge l'utilisation de canaux 40 MHz dans la bande 2,4 GHz.

5 GHz

Déploiement type pour les réseaux sans fil haute densité. Utilisez tous les canaux disponibles lorsque cela est possible.

Le nombre de canaux varie en fonction du domaine réglementaire. Tenir compte de l'impact du radar à l'endroit précis, utiliser les canaux DSF (y compris les canaux TDWR) dans la mesure du possible.

La largeur de canal de 20 MHz est fortement recommandée pour tous les déploiements haute densité.

40MHz peut être utilisé sur la même base que 2.4GHz, c'est seulement quand (et où) absolument nécessaire.

Évaluer les besoins et les avantages réels des canaux 40 MHz dans un environnement spécifique. Les canaux 40 MHz nécessitent un rapport signal/bruit (SNR) plus élevé pour obtenir une amélioration possible du débit. Si un SNR plus élevé n'est pas possible, les canaux 40 MHz ne remplissent pas de fonction utile. Les réseaux haute densité privilégient le débit moyen pour tous les utilisateurs par rapport au débit potentiellement plus élevé pour un seul utilisateur. Il est préférable de placer plus de points d'accès sur des canaux de 20 MHz que d'avoir des points d'accès utilisant 40 MHz, car le canal secondaire est utilisé uniquement pour les trames de données et donc utilisé beaucoup moins efficacement que d'avoir deux cellules radio différentes, chacune fonctionnant sur 20 MHz (en termes de capacité totale, pas en termes de débit client unique).

Le détail le plus important est de conserver la même largeur de canal à l'intérieur d'une zone donnée. En effet, si vous configurez une largeur de canal différente, les clients ont tendance à s'en tenir aux AP ayant la plus grande largeur de canal même s'il y a un autre AP plus proche à une plus forte intensité de signal.

6 GHz

La bande 6 GHz n'est pas encore disponible dans tous les pays. En outre, certains périphériques sont équipés d'une carte Wi-Fi compatible 6 GHz, mais nécessitent une mise à jour du BIOS pour être activés dans le pays concerné. La façon la plus populaire dont les clients découvrent les radios 6GHz en ce moment est via l'annonce RNR (Reduced Neighbor Report), qui annonce l'existence de réseaux 6GHz aux clients utilisant l'une des autres radios AP. Cela signifie que 6 GHz ne doit pas fonctionner seul sans une autre radio sur le même point d'accès.

Lors de la configuration d'un SSID bibande (5 GHz et 6 GHz), l'annonce 5 GHz inclura un RNR pour le SSID 6 GHz, permettant au client de trouver rapidement le SSID 6 GHz sans avoir à scanner la bande.

Une autre approche consiste à configurer un SSID factice (et/ou masqué) sur 2,4 GHz, l'intention ici est d'annoncer le RNR 6 GHz à l'aide de la radio 2,4 GHz, sans offrir un SSID 2,4 GHz. Cette approche est utile dans les situations où la capacité 6 GHz doit être ajoutée sans ajouter de radios 5 GHz à l'environnement.

La bande passante de 6 GHz permet d'utiliser des canaux plus larges, mais cela dépend fortement du nombre de canaux disponibles dans le domaine réglementaire. Avec 24 canaux 6 GHz disponibles en Europe, il n'est pas déraisonnable de considérer les canaux 40 MHz pour fournir un meilleur débit maximum par rapport aux 20 MHz que vous utilisez probablement dans 5 GHz. Aux États-Unis, avec près du double du nombre de canaux, l'utilisation de 40 MHz est une

évidence et même aller pour 80 MHz n'est pas déraisonnable. Une bande passante plus large ne doit pas être utilisée dans les événements ou les lieux à forte densité.

L'inconvénient avec des largeurs de canaux de 6 GHz plus importantes est qu'il n'est pas toujours possible d'utiliser la même largeur de canal dans 5 GHz, et cela aura un impact sur le comportement d'itinérance sur certains périphériques clients. Le détail le plus important est de conserver la même largeur de canal à l'intérieur d'une zone donnée. En effet, si vous configurez une largeur de canal différente, les clients ont tendance à s'en tenir aux points d'accès avec la plus grande largeur de canal même s'il y a un autre point d'accès plus proche à une plus forte intensité de signal, cela s'applique également à l'itinérance entre les bandes 5GHz et 6GHz.

Débits de données

Le débit de données qu'un client négocie avec un point d'accès est en grande partie fonction du rapport signal sur bruit (SNR) de cette connexion, et l'inverse est également vrai, des débits de données plus élevés nécessitent un SNR plus élevé. En fait, c'est principalement le SNR qui détermine la vitesse de liaison maximale possible, mais pourquoi est-ce important lors de la configuration des débits de données ? C'est parce que certains débits de données ont une signification particulière.

Les débits de données OFDM (802.11a) classiques peuvent être configurés dans l'un des trois paramètres suivants : Désactivé, pris en charge ou obligatoire. Les débits OFDM sont les suivants (en Mbits/s) : 6, 9, 12, 18, 24, 36, 48, 54, et le client et le point d'accès doivent tous deux prendre en charge un débit avant de pouvoir l'utiliser.

Pris en charge : le point d'accès utilise le débit

Obligatoire : le point d'accès utilise le débit et envoie le trafic de gestion en utilisant ce débit

Désactivé : le point d'accès n'utilise pas le débit, ce qui force le client à utiliser un autre débit

---



Remarque : Les taux obligatoires sont également appelés taux de base

---

La signification du débit obligatoire est que toutes les trames de gestion sont envoyées à l’aide de ce débit, ainsi que les trames de diffusion et de multidiffusion. Si plusieurs débits obligatoires sont configurés, les trames de gestion utilisent le débit obligatoire configuré le plus faible et les débits de diffusion et de multidiffusion utilisent l’un des débits obligatoires (ce point peut être configuré dans le profil RF).

Les trames de gestion incluent des balises qui doivent être entendues par le client pour pouvoir s’associer au point d’accès. L’augmentation du débit obligatoire augmente également le débit minimal requis pour cette transmission, rappelez-vous que des débits de données plus élevés nécessitent un débit minimal plus élevé, ce qui signifie généralement que le client doit être plus proche du point d’accès pour pouvoir décoder la balise et s’associer. Par conséquent, en manipulant le débit de données obligatoire, nous manipulons également la plage d'association effective du point d'accès, forçant les clients à se rapprocher du point d'accès ou vers une décision d'itinérance potentielle. Les clients proches du point d’accès utilisent des débits de données plus élevés et des débits de données plus élevés utilisent moins de temps d’antenne. L’effet recherché est une cellule plus efficace. Il est important de rappeler que l'augmentation du débit de données n'affecte que le débit de transmission de certaines trames, elle n'affecte pas la propagation RF de l'antenne ou la plage d'interférence. De bonnes pratiques de conception RF sont toujours nécessaires pour minimiser les interférences et le bruit dans les mêmes canaux.

À l'inverse, le fait de laisser des débits inférieurs obligatoires signifie généralement que les clients peuvent s'associer à distance, ce qui est utile dans les scénarios de faible densité de points d'accès, mais risque d'entraîner des dommages liés à l'itinérance dans les scénarios de densité supérieure. Quiconque a essayé de localiser un point d'accès non autorisé qui diffuse à 6 Mbits/s sait que vous pouvez détecter le point d'accès très loin de son emplacement physique !

En ce qui concerne la diffusion et la multidiffusion, dans certains cas, un second débit obligatoire (supérieur) est configuré pour augmenter le débit de transmission du trafic de multidiffusion. Cela réussit rarement, car la multidiffusion n’est jamais reconnue et ne fait jamais l’objet d’une retransmission en cas de perte de trames. Comme une certaine perte est inhérente à tous les systèmes sans fil, il est inévitable que certaines trames de multidiffusion soient perdues, quel que soit le débit configuré. Les techniques de conversion de multidiffusion en monodiffusion qui transmettent la multidiffusion sous la forme d'un flux de monodiffusion offrent une meilleure approche de la transmission multidiffusion fiable, ce qui présente l'avantage de débits de données plus élevés et d'une transmission fiable (avec accusé de réception).

Il est préférable d'utiliser un seul taux obligatoire, de désactiver tous les taux inférieurs au taux obligatoire et de laisser tous les taux supérieurs au taux obligatoire comme pris en charge. Le débit spécifique à utiliser dépend du cas d'utilisation, comme déjà mentionné, les débits inférieurs sont utiles dans les scénarios de densité inférieure et en extérieur où les distances entre les points d'accès sont plus grandes. Pour les réseaux à haute densité et d'événements, les débits faibles doivent être désactivés.

Si vous ne savez pas par où commencer ; utilisez un débit obligatoire de 12 Mbits/s pour les déploiements à faible densité et de 24 Mbits/s pour les déploiements à haute densité. De nombreux événements à grande échelle, stades et même déploiements de bureaux d'entreprise haute densité ont prouvé leur fiabilité avec un débit obligatoire de 24 Mbits/s. Des tests appropriés sont recommandés pour des cas d'utilisation spécifiques où des débits inférieurs à 12 Mbits/s ou supérieurs à 24 Mbits/s sont nécessaires.

Remarque : Il est préférable de laisser tous les débits 802.11n/ac/ax/be activés (tous les débits dans la section High Throughput de l'interface graphique du WLC), il est rarement nécessaire de désactiver l'un de ces débits.

Puissance D'Émission

Les recommandations de puissance de transmission varient en fonction du type de déploiement. Nous distinguons ici les déploiements en intérieur utilisant des antennes omnidirectionnelles de ceux utilisant des antennes directionnelles. Les deux types d'antennes peuvent exister dans un grand réseau public, bien que celles-ci couvrent généralement différents types de zones.

Pour les déploiements omnidirectionnels, il est courant d'utiliser le contrôle de puissance de transmission (TPC) automatique avec un seuil minimum configuré de manière statique, et dans certains cas également un seuil maximum configuré de manière statique.

Remarque : Les seuils TPC se rapportent à la puissance de transmission radio et excluent le gain d'antenne. Assurez-vous toujours que le gain d'antenne est configuré correctement pour le modèle d'antenne utilisé, ceci est fait automatiquement dans le cas d'antennes internes et d'antennes auto-identifiantes.

Exemple 1

TPC min. : 5 dBm, TPC max. : Maximum (30 dBm)

L'algorithme TPC déterminerait ainsi automatiquement la puissance de transmission, sans jamais descendre en dessous du seuil minimum configuré de 5 dBm.

Exemple 2

TPC min. : 2 dBm, TPC max. : 11 dBm

L'algorithme TPC détermine ainsi automatiquement la puissance de transmission, mais en restant toujours entre 2 dBm et 11 dBm.

Une bonne approche consiste à créer plusieurs profils RF avec différents seuils, par exemple faible puissance (2-5dBm), moyenne puissance (5-11dbM) et haute puissance (11-17dBM), puis à

attribuer des points d'accès omnidirectionnels à chaque profil RF en fonction des besoins. Les valeurs de chaque profil RF peuvent être ajustées en fonction du cas d'utilisation prévu et de la zone de couverture. Cela permet aux algorithmes RRM de fonctionner de manière dynamique tout en restant dans des limites prédéfinies.

L'approche pour les antennes directionnelles est très similaire, la seule différence étant le niveau de précision requis. Le positionnement de l'antenne directionnelle doit être conçu et vérifié lors d'une étude RF préalable au déploiement, et les valeurs de configuration radio spécifiques sont généralement le résultat de ce processus.

Par exemple, si une antenne patch montée au plafond est nécessaire pour couvrir une certaine zone à partir d'une hauteur de ~26ft (8m), l'étude RF doit déterminer la puissance Tx minimale requise pour atteindre cette couverture prévue (ce qui détermine la valeur TPC minimale pour le profil RF). De même, à partir de la même étude RF, nous pourrions comprendre le chevauchement possible nécessaire entre cette antenne et la suivante, ou même le point auquel nous voulons que la couverture se termine - cela fournirait la valeur TPC maximale pour le profil RF.

Les profils RF des antennes directionnelles sont généralement configurés avec les mêmes valeurs TPC minimale et maximale ou avec une plage étroite de valeurs possibles (généralement <= 3dBm).

Les profils RF sont préférés pour assurer la cohérence de la configuration, la configuration statique de points d'accès individuels n'est pas recommandée. Il est recommandé de nommer les profils RF en fonction de la zone de couverture, du type d'antenne et du cas d'utilisation, par exemple RF-Auditorium-Patch-Ceiling.

La puissance fiscale correcte est obtenue lorsque la valeur SNR requise est atteinte par le client le plus faible dans la zone de couverture prévue, et pas plus. 30dBm est une excellente valeur cible SNR client dans des conditions réelles (c'est-à-dire dans un lieu plein de gens).

CHD

La détection des trous de couverture (CDP) est un algorithme distinct permettant d'identifier et de corriger les trous de couverture. Le CHD est configuré globalement ainsi que par WLAN. Un effet possible du CHD est l'augmentation de la puissance Tx pour compenser les trous de couverture (zones avec des clients constamment détectés avec un signal faible), cet effet est au niveau radio et affecte tous les WLAN, même lorsqu'il est déclenché par un seul WLAN configuré pour le CHD.

Les grands réseaux publics sont généralement configurés à des niveaux de puissance spécifiques à l'aide de profils RF, certains peuvent se trouver dans des zones ouvertes avec des clients qui se déplacent vers et hors des zones, il n'est pas nécessaire d'utiliser un algorithme pour ajuster

dynamiquement la puissance AP Tx en réponse à ces événements client.

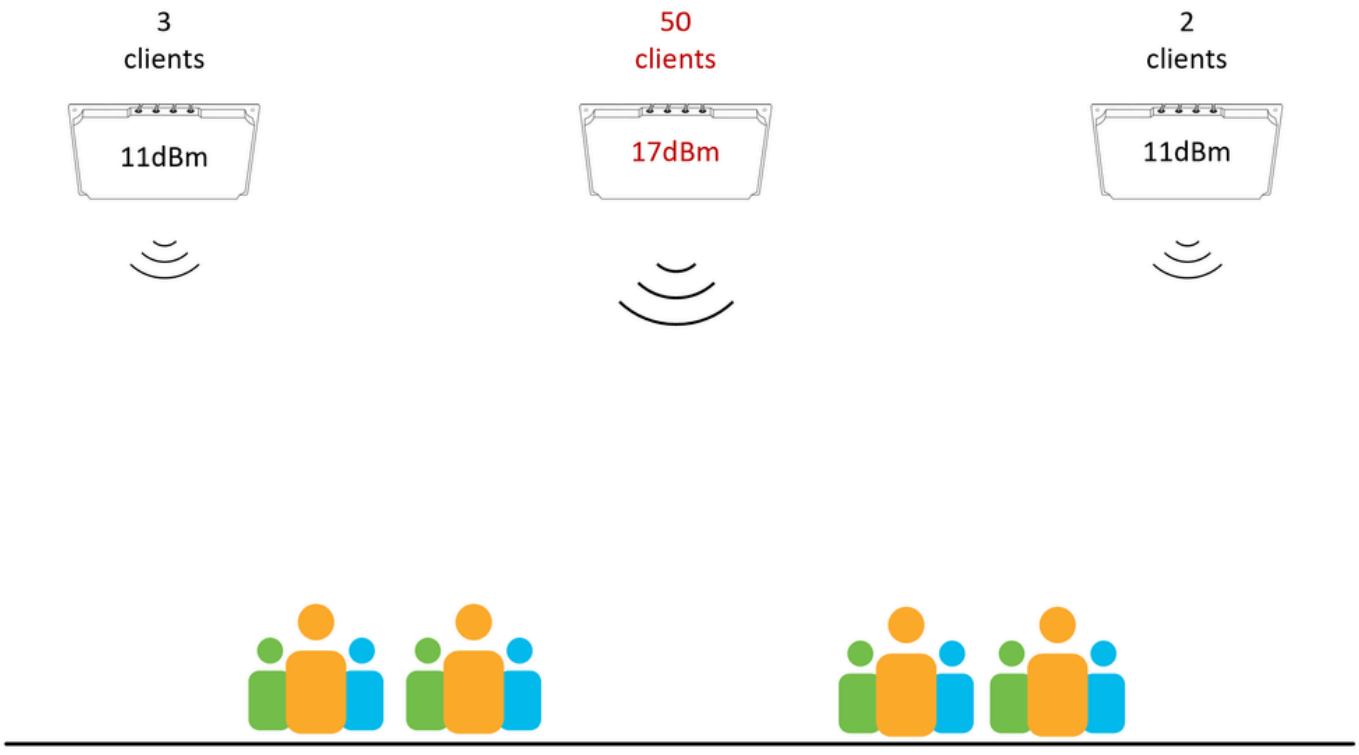
La fonction CHD doit être désactivée globalement pour les grands réseaux publics.

Équilibrage de puissance

La plupart des périphériques clients préfèrent un signal reçu plus élevé lorsqu'ils choisissent le point d'accès auquel s'associer. Les situations où un point d'accès est configuré avec une puissance Tx considérablement plus élevée par rapport aux autres points d'accès environnants doivent être évitées. Les points d'accès fonctionnant à une puissance Tx plus élevée attirent plus de clients, ce qui entraîne une répartition inégale des clients entre les points d'accès (par exemple, un point d'accès/radio unique est surchargé de clients alors que les points d'accès environnants sont sous-utilisés). Cette situation est courante dans les déploiements avec un chevauchement de couverture important à partir de plusieurs antennes, et dans les cas où un point d'accès a plusieurs antennes reliées.

Les antennes de stade telles que le C9104 nécessitent une attention particulière lors de la sélection de la puissance Tx, car les faisceaux d'antenne se chevauchent par conception. Pour plus d'informations, consultez les guides de déploiement d'antenne appropriés.

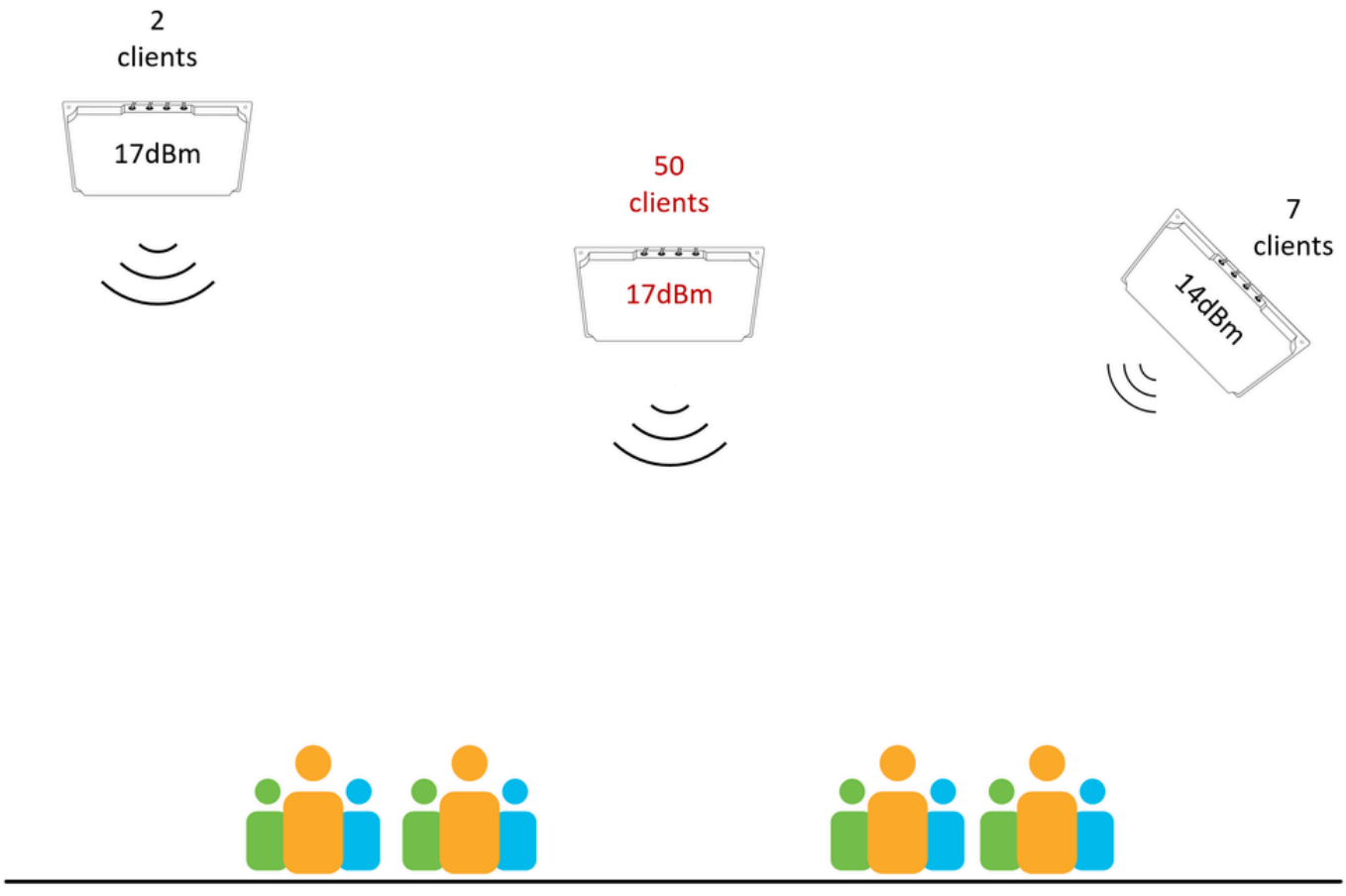
Dans le schéma ci-dessous, l'antenne centrale est configurée avec une puissance Tx supérieure à celle des antennes environnantes. Cette configuration risque d'entraîner une « collage » des clients à l'antenne centrale.



Un point d'accès avec une puissance supérieure à celle de ses voisins attire tous les clients autour

Le schéma suivant illustre une situation plus compliquée : toutes les antennes ne sont pas à la même hauteur et toutes les antennes n'utilisent pas la même inclinaison/orientation. L'obtention d'une puissance équilibrée est plus compliquée que la simple configuration de toutes les radios avec la même puissance Tx. Dans des scénarios comme celui-ci, une étude de site post-déploiement peut être requise, ce qui fournit une vue de la couverture du point de vue du périphérique client (sur le terrain). Les données de l'enquête peuvent ensuite être utilisées pour équilibrer la configuration afin d'obtenir la meilleure couverture et la meilleure distribution des clients.

La conception d'emplacements de point d'accès uniformes qui évitent des situations compliquées comme celle-ci est la meilleure façon d'éviter des scénarios de réglage RF difficiles (bien que parfois il n'y ait pas d'autre choix !).

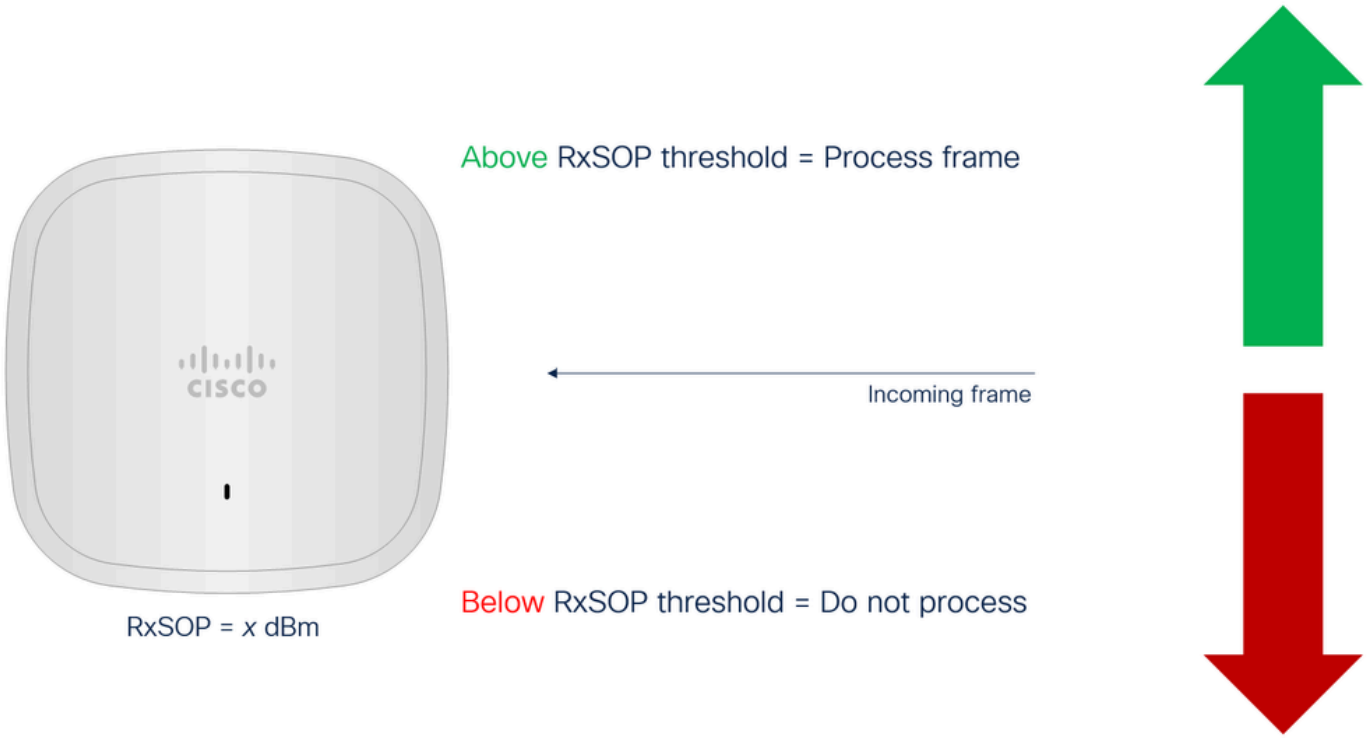



Un point d'accès attire tous les clients, même si la puissance Tx est similaire, mais la hauteur et les angles jouent un rôle

RxSOP

Contrairement aux mécanismes tels que la puissance Tx ou les débits de données qui affectent les caractéristiques de la cellule de transmission, RxSOP (Receiver Start of Packet detection) vise

à influencer la taille de la cellule de réception. Essentiellement, RxSOP peut être considéré comme un seuil de bruit, en ce qu'il définit le niveau de signal reçu en dessous duquel le point d'accès ne tente pas de décoder les transmissions. Toutes les transmissions arrivant avec un niveau de signal inférieur au seuil RxSOP configuré ne sont pas traitées par le point d'accès et sont effectivement traitées comme du bruit.



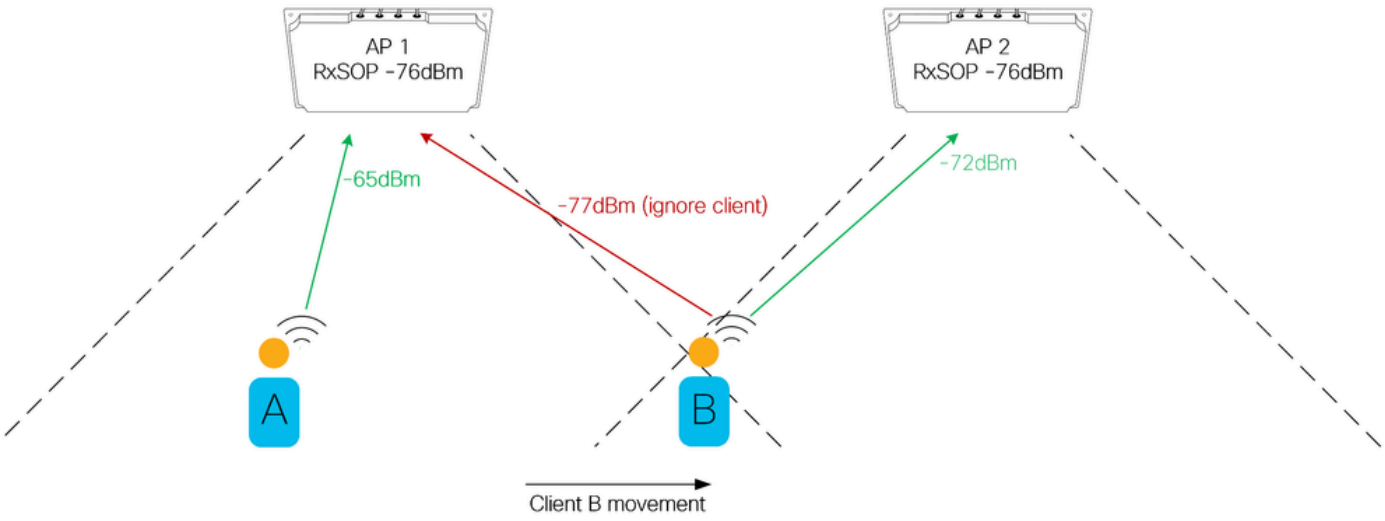

Explication du concept RxSOP

La signification de RxSOP

RxSOP a plusieurs utilisations. Il peut être utilisé pour améliorer la capacité des points d'accès à transmettre dans des environnements bruyants, pour contrôler la distribution des clients entre les antennes, ainsi que pour optimiser les clients plus faibles et rémanents.

Dans le cas d'environnements bruyants, rappelez-vous qu'avant de transmettre une trame 802.11, la station émettrice (le point d'accès dans ce cas) doit d'abord évaluer la disponibilité du support, une partie de ce processus consiste à écouter d'abord les transmissions qui ont déjà lieu. Dans les environnements Wi-Fi denses, il est courant que de nombreux points d'accès coexistent dans un espace relativement limité, souvent en utilisant les mêmes canaux. Dans de tels environnements occupés, le point d'accès peut signaler l'utilisation du canal à partir des points d'accès environnants (y compris les réflexions) et retarder sa propre transmission. En définissant le seuil RxSOP approprié, le point d'accès peut ignorer les transmissions plus faibles (réduction de l'utilisation perçue du canal), ce qui conduit à des opportunités de transmission plus fréquentes et à des performances améliorées. Les environnements dans lesquels les points d'accès signalent une utilisation significative du canal (par exemple > 10 %) sans aucune charge client (par exemple un site vide) sont de bons candidats pour le réglage RxSOP.

Pour l'optimisation client à l'aide de RxSOP, considérez ce schéma.




Itinérance du client affectée par rxsop

Dans cet exemple, il y a deux points d'accès/antennes avec des zones de couverture bien définies. Le client B se déplace de la zone de couverture du point d'accès AP1 vers la zone de couverture du point d'accès AP2. Il existe un point de croisement au niveau duquel le point d'accès AP2 entend mieux le client que le point d'accès AP1, mais le client n'a pas encore atteint le point d'accès AP2. C'est un bon exemple de la façon dont la définition du seuil RxSOP peut imposer la limite de la zone de couverture. S'assurer que les clients sont toujours connectés au point d'accès le plus proche améliore les performances en éliminant les connexions client distantes et/ou faibles desservies à des débits de données inférieurs. La configuration des seuils RxSOP de cette manière nécessite une compréhension approfondie de l'endroit où la zone de couverture attendue de chaque point d'accès commence et se termine.

Les dangers de RxSOP.

Si vous définissez le seuil RxSOP de manière trop agressive, vous obtenez des trous de couverture, car le point d'accès ne décode pas les transmissions valides à partir des périphériques clients valides. Cela peut avoir des conséquences néfastes pour le client, car le point d'accès ne répond pas ; après tout, si la transmission du client n'a pas été entendue, il n'y a aucune raison de répondre. Le réglage des seuils RxSOP doit être effectué avec soin, en veillant toujours à ce que les valeurs configurées n'excluent pas les clients valides dans la zone de couverture. Notez que certains clients ne peuvent pas répondre correctement à être ignorés de cette façon, trop agressif RxSOP paramètres ne donnent pas au client une chance d'itinérance naturelle, forçant effectivement le client à trouver un autre AP. Un client qui peut décoder une balise à partir d'un point d'accès suppose qu'il est capable de transmettre à ce point d'accès. Par conséquent, l'intention du réglage RxSOP est de faire correspondre la taille de la cellule de réception à la plage de balises du point d'accès. Gardez à l'esprit qu'un périphérique client (valide) n'a pas toujours une ligne de vue directe vers le point d'accès, le signal est souvent atténué par les utilisateurs qui sont face à l'antenne ou qui transportent leurs périphériques dans des sacs ou des poches.

Configuration de RxSOP

RxSOP est configuré par profil RF.

Pour chaque bande, il existe des seuils prédéfinis (Faible/Moyen/Élevé) à des valeurs de dBm prédéfinies. Ces préréglages sont différents pour chaque bande (par exemple "Low" a une valeur différente en dBm entre 2,4 GHz et 5 GHz). Il est recommandé ici d'utiliser toujours des valeurs personnalisées, même si la valeur prévue est l'un des préréglages disponibles, ce qui rend la configuration plus lisible. Le paramètre « Auto » désactive efficacement RxSOP, dans le sens où le point d'accès tente de décoder tout paquet qu'il peut comme d'habitude.

| Setting | Value |
|---|---|
| Auto | Not configured |
| Low | -80dBm |
| Medium | -78dBm |
| High | -76dBm |
| Custom | -60dBm to -85dBm |

Tableau des paramètres RxSop

Remarque : Les modifications RxSOP ne nécessitent pas de réinitialisation radio et peuvent être effectuées à la volée.

## Évolutivité du réseau

En général, utiliser un périphérique au maximum de ses capacités documentées est une mauvaise idée. Les fiches signalent la vérité, mais les chiffres mentionnés peuvent être dans des conditions d'activité spécifiques. Les contrôleurs sans fil sont testés et certifiés pour prendre en charge un certain nombre de clients et de points d'accès, et un certain débit, mais cela ne suppose pas que les clients sont en itinérance chaque seconde, que vous pouvez avoir configuré des listes de contrôle d'accès uniques extrêmement longues pour chaque client ou activé toutes les fonctionnalités de surveillance disponibles. Il est donc important d'examiner tous les aspects attentivement afin de s'assurer que le réseau évolue pendant les heures de pointe et de conserver une marge de sécurité pour la croissance future.

Nombre de points d'accès

L'une des premières tâches à effectuer pour déployer un réseau consiste à établir un budget et à commander la quantité d'équipement appropriée. Le facteur variable le plus important est le nombre et le type de points d'accès et d'antennes. Les solutions sans fil doivent toujours être basées sur une conception de radiofréquence, cependant (et malheureusement), il s'agit très souvent de la deuxième étape du cycle de vie du projet. Dans le cas de déploiements d'entreprise en intérieur simples, il existe de nombreuses techniques d'estimation qui peuvent, à un niveau de certitude raisonnable, prédire combien de points d'accès peuvent être nécessaires avant même qu'un architecte sans fil ne se penche sur les plans d'étage. Les modèles prédictifs peuvent également être très utiles dans ce cas.

Pour les installations plus complexes, telles que les réseaux industriels, extérieurs ou publics de grande taille, ou partout où des antennes externes sont nécessaires, les techniques d'estimation simples sont souvent inadéquates. Un certain niveau d'expérience est requis avec des installations similaires précédentes pour estimer adéquatement le type et la quantité d'équipement nécessaire. Une visite sur site par un architecte sans fil est le strict minimum pour comprendre la disposition d'un site ou d'une installation complexe.

Cette section fournit des directives sur la façon de déterminer le nombre minimum de points d'accès et d'antennes pour le déploiement donné. Les quantités finales et les emplacements de montage spécifiques seront toujours déterminés par le biais d'une analyse des besoins et d'un processus de conception radio.

La nomenclature initiale doit être basée sur deux facteurs : type d'antennes et quantité d'antennes.

Type d'antennes

Il n'y a pas de raccourci ici. Le type d'antenne est déterminé par la zone à couvrir et par les options de montage disponibles dans cette zone. Il n'est pas possible de déterminer cela sans une compréhension de l'espace physique, ce qui signifie qu'une visite de site est requise par une personne ayant une compréhension des antennes et de leurs modèles de couverture.

Nombre d'antennes

La quantité d’équipement nécessaire peut être déduite d’une compréhension du nombre attendu de connexions client.

Périphériques par personne

Le nombre d'utilisateurs humains peut être déterminé par la capacité d'accueil d'un site, ou le nombre de billets vendus, ou le nombre attendu de visiteurs sur la base de statistiques historiques. Chaque utilisateur humain peut transporter plusieurs périphériques et il est courant de

supposer que chaque utilisateur possède plus d'un périphérique, bien que la capacité d'un utilisateur humain à utiliser activement plusieurs périphériques en même temps soit discutable. Le nombre de visiteurs qui se connectent activement au réseau dépend également du type d'événement et/ou de déploiement.

Exemple 1 : Il est normal qu'un stade de 80 000 places ne dispose pas de 80 000 appareils connectés. Ce pourcentage est généralement beaucoup plus faible. Des taux d'utilisateurs connectés de 20 % ne sont pas rares lors d'événements sportifs, ce qui signifie que pour l'exemple du stade de 80 000 places, le nombre attendu d'appareils connectés peut être de 16 000 (80 000 x 20 % = 16 000). Ce nombre dépend également du mécanisme d'intégration utilisé. Si l'utilisateur doit effectuer une action (par exemple, cliquer sur un portail Web), les chiffres sont inférieurs à ceux qui s'appliquent lorsque l'intégration de l'appareil est automatique. L'intégration automatique peut être aussi simple qu'une clé prépartagée dont on s'est souvenu lors d'un événement précédent, ou quelque chose de plus avancé comme l'utilisation d'OpenRoaming qui intègre des périphériques sans interaction de l'utilisateur. Les réseaux OpenRoaming peuvent entraîner des taux de connexion des utilisateurs bien supérieurs à 50 %, ce qui peut avoir un impact significatif sur la planification de la capacité.

Exemple 2 : Il est raisonnable de s'attendre à ce qu'une conférence technologique ait un taux de connexion utilisateur élevé. Les participants à la conférence passent plus de temps à se connecter au réseau et s'attendent à pouvoir accéder à leur messagerie électronique et effectuer des tâches quotidiennes tout au long de la journée. Il est également plus probable que ce type d'utilisateur connecte plusieurs périphériques au réseau, même s'il n'utilise qu'un seul périphérique à la fois. Pour les conférences technologiques, l'hypothèse est que 100 % des visiteurs se connectent au réseau, ce nombre peut être inférieur en fonction du type de conférence.

Dans les deux exemples, la clé est de comprendre le nombre attendu de périphériques connectés et il n'existe pas de solution unique pour chaque grand réseau public. Dans les deux cas, une antenne est connectée à une radio et ce sont les périphériques clients (et non les utilisateurs humains) qui se connectent à cette radio. Par conséquent, les périphériques clients par radio sont une mesure utilisable.

Périphériques par radio

Les points d'accès Cisco ont un nombre maximal de clients de 200 périphériques connectés par radio pour les points d'accès Wi-Fi 6 et de 400 périphériques par radio pour les points d'accès Wi-Fi 6E. Cependant, il n'est pas recommandé de concevoir un nombre maximal de clients. À des fins de planification, il est recommandé de maintenir le nombre de clients par radio bien en dessous de 50 % de la capacité maximale du point d'accès. En outre, le nombre de radios dépend du type de point d'accès et d'antenne utilisé. La section relative à la fréquence simple ou double 5 GHz l'étudie plus en détail.

À ce stade, il est conseillé de diviser le réseau en zones distinctes, avec le nombre de périphériques prévu par zone. Rappelez-vous que cette section vise à estimer un nombre

minimum de points d'accès et d'antennes.

Prenons un exemple de trois zones de couverture distinctes, le nombre de clients prévu est fourni pour chaque zone et une valeur (saine) de 75 clients par radio est utilisée pour estimer le nombre de radios nécessaires.

| Area | Expected Devices | Devices / Radio | Radios |
|---|---|---|---|
| Area 1 | 1000 | 75 | 14 |
| Area 2 | 2000 | 75 | 27 |
| Area 3 | 2500 | 75 | 34 |
| Total | | | 75 |

Nombre prévu de radios/clients par zone

Ces chiffres initiaux doivent maintenant être combinés avec la compréhension des types de points d'accès et d'antennes qui sont déployés dans chaque zone, et si une ou deux fréquences de 5 GHz sont utilisées. Les calculs 6 GHz suivent la même logique que les calculs 5 GHz. 2,4 GHz n'est pas pris en compte dans cet exemple.

Supposons que chacune des trois zones utilise une combinaison d'antenne de raccordement 2566P et d'antenne de stade 9104, avec une combinaison de 5 GHz simple et double - ce scénario est utilisé à des fins d'illustration.

| Area | Total Radios | 2566P (Dual 5GHz) | 2566P (Single 5GHz) | 9104 (Dual 5GHz) |
|---|---|---|---|---|
| Area 1 | 14 | 0 | 6 | 4 |
| Area 2 | 27 | 6 | 3 | 6 |
| Area 3 | 34 | 7 | 0 | 10 |
| Total Antennas | | 26 | 9 | 20 |
| Total APs | | 13 | 9 | 0 (integrated) |

Antennes par zone

Chaque zone répertorie le type d'antennes et de points d'accès requis. Notez que dans le cas d'un double 5 GHz, le rapport est de deux antennes pour un point d'accès.

Cette section présente une approche permettant d'estimer le nombre initial d'antennes et de points d'accès nécessaires à un déploiement. L'estimation nécessite une compréhension des zones physiques, des options de montage possibles dans chaque zone, du type d'antennes à utiliser dans chaque zone et du nombre de périphériques clients attendus.

Chaque déploiement est différent et un équipement supplémentaire est souvent nécessaire pour couvrir des domaines spécifiques ou difficiles. Ce type d'estimation ne tient compte que de la capacité du client (et non de la couverture) et sert à décrire l'ampleur de l'investissement nécessaire. L'emplacement final des points d'accès/antennes et le nombre total d'équipements sont toujours soumis à une compréhension approfondie du cas d'utilisation et à une vérification sur site par un professionnel sans fil expérimenté.

Débit attendu

Chaque canal sans fil peut offrir une quantité de capacité disponible qui est généralement traduite en débit. Cette capacité est partagée entre tous les périphériques connectés à la radio, ce qui signifie que les performances de chaque utilisateur diminuent à mesure que de nouvelles connexions utilisateur sont ajoutées à la radio. Cette baisse des performances n'est pas linéaire et dépend également du nombre exact de clients connectés.

Les capacités du client varient selon les périphériques en fonction du chipset client et du nombre de flux spatiaux pris en charge par le client. Les débits de données client maximaux pour chaque nombre de flux spatiaux pris en charge sont répertoriés dans le tableau ci-dessous. Notez que la plupart des périphériques clients prennent en charge un maximum de 2 flux spatiaux.

| Client Capability | 20MHz channel Wi-Fi 5 (802.11ac) | 20MHz channel Wi-Fi 6 (802.11ax) |
|---|---|---|
| 1 Spatial Stream(s) | 86.7Mbps | 121.9Mbps |
| 2 Spatial Stream(s) | 173.3Mbps | 243.8Mbps |
| 3 Spatial Stream(s) | 288.9Mbps | 365.6Mbps |
| 4 Spatial Stream(s) | 346.7Mbps | 487.5Mbps |

Débit réel maximal attendu pour chaque type de client

Les débits indiqués sont des débits MCS (Modulation and Coding Scheme) maximaux théoriques dérivés de la norme 802.11 et supposent un rapport signal sur bruit (SNR) > 30dBm. L'objectif principal de la conception de réseaux sans fil performants est d'atteindre ce niveau de SNR pour tous les clients, où qu'ils se trouvent, ce qui est rarement le cas. Les réseaux sans fil sont dynamiques par nature et utilisent des fréquences sans licence. Diverses interférences non contrôlées ont un impact sur le SNR du client, en plus des capacités du client.

Même dans les cas où le niveau requis de SNR est atteint, les débits indiqués précédemment ne tiennent pas compte de la surcharge de protocole. Par conséquent, ils ne correspondent pas directement au débit réel (mesuré par divers outils de test de vitesse). Le monde réel dans son ensemble est toujours inférieur au taux MCS.

Pour tous les réseaux sans fil (y compris les grands réseaux publics), le débit client dépend toujours des éléments suivants :

- Capacités du client.
- Rapport signal/bruit du client à ce moment précis.
- Nombre d'autres clients connectés à ce moment précis.
- Capacités des autres clients à ce moment précis.
- Activité d'autres clients à ce moment précis.
- Interférence à ce moment précis.

En raison de la variabilité de ces facteurs, il n'est pas possible de garantir un minimum par client pour l'ensemble des réseaux sans fil, quel que soit le fournisseur d'équipement.

Pour plus d'informations, consultez la page Valider le débit Wi-Fi : Guide de test et de surveillance.

Plate-forme WLC

Choisir votre plate-forme WLC peut sembler facile. La première chose à laquelle vous pouvez penser est de regarder le nombre estimé de points d'accès et le nombre de clients que vous souhaitez gérer. La fiche technique de chaque plate-forme WLC contient tous les objets maximum pris en charge sur la plate-forme : ACL, nombre de clients, balises de site, etc. Il s'agit de nombres maximaux littéraux et souvent, il y a une application difficile. Vous ne pouvez pas joindre 6001 AP à un 9800-80 qui ne prend en charge que 6000 AP, par exemple. Mais est-il sage de viser le maximum partout ?

Les contrôleurs sans fil Cisco sont testés pour atteindre ces maximums, mais ils ne peuvent pas nécessairement atteindre tous les maximums documentés dans toutes les conditions en même temps. Prenons l'exemple du débit : un 9800-80 peut atteindre jusqu'à 80 Gbit/s de transfert de données client, mais dans le cas où chaque paquet client est la taille maximale et optimale de 1 500 octets. Avec une combinaison de tailles de paquets, le débit maximal effectif est plus faible. Si vous activez le cryptage DTLS, le débit est encore réduit, de même pour la visibilité des applications. Il est optimiste de s'attendre à plus de 40 Gbit/s sur un 9800-80 dans des conditions réalistes sur un grand réseau doté de nombreuses fonctionnalités. Étant donné que cela varie considérablement en fonction des fonctionnalités utilisées et du type d’activité du réseau, la seule façon d’avoir une idée réelle de la capacité est de mesurer l’utilisation du chemin de données à l’aide de cette commande. Concentrez-vous sur la mesure de charge, qui est un pourcentage du

débit maximal que le contrôleur peut transmettre.

```
WLC#show platform hardware chassis active qfp datapath utilization summary

  CPP 0:                      5 secs        1 min        5 min       60 min

Input:     Total (pps)            9            5            5            8

                  (bps)        17776         7632         9024        10568

Output:    Total (pps)            5            3            3            6

                  (bps)        11136        11640        11440        41448

Processing: Load (pct)            0            0            0            0


WLC#
```

De la même manière, le 9800-80 peut parfaitement gérer 6000 points d'accès avec une activité régulière. Cependant, 6 000 points d'accès dans un lieu public tel qu'un stade ou un aéroport ne comptent pas comme activité régulière. Compte tenu de la quantité d'itinérance client et de sondage ambiant, de grands réseaux publics à une échelle maximale peuvent entraîner une utilisation accrue du CPU sur un seul WLC. Si vous ajoutez la surveillance et les déroutements SNMP à envoyer chaque fois que des clients se déplacent, la charge peut rapidement devenir trop importante. L'une des principales caractéristiques d'un grand lieu public ou d'un grand événement est qu'il y a beaucoup plus d'événements d'intégration de clients lorsque les gens se déplacent et s'associent/se dissocient constamment, ce qui entraîne une pression supplémentaire sur le processeur et le plan de contrôle.

De nombreux déploiements ont montré qu'une seule paire de contrôleurs sans fil 9800-80 peut gérer un grand déploiement dans un stade avec plus de 1 000 points d'accès. Il est également courant de distribuer les points d'accès sur deux paires de contrôleurs ou plus pour des événements critiques où le temps de disponibilité et la disponibilité sont des préoccupations principales. Lorsque de grands réseaux sont distribués sur plusieurs WLC, l'itinérance entre contrôleurs devient encore plus complexe. L'itinérance client doit être prise en compte avec soin dans des espaces confinés tels qu'un stade.

Voir aussi la section Balise de site dans ce document.

Haute disponibilité WLC

Il est conseillé d'utiliser une paire de commutateurs avec état haute disponibilité (HA SSO), ce qui assure la redondance matérielle mais protège également contre les défaillances logicielles. Avec

HA SSO, une panne logicielle sur un périphérique est transparente pour les utilisateurs finaux, car le WLC secondaire prend le relais de manière transparente. Un autre avantage d'une paire d'unités SSO haute disponibilité réside dans les mises à niveau transparentes offertes par la fonctionnalité In-Service Software Upgrade (ISSU).

Si le réseau est assez grand, il est également conseillé d'utiliser un contrôleur supplémentaire (N+1). Il peut servir plusieurs objectifs que l'OSP HA ne peut pas atteindre. Vous pouvez tester une nouvelle version logicielle sur ce WLC avant de mettre à niveau la paire de production (et migrer seulement quelques AP de test vers elle pour tester une section spécifique du réseau). Certaines conditions rares peuvent affecter les deux WLC dans une paire HA (quand le problème est répliqué sur la veille) et ici le N+1 permet d'avoir un WLC sûr dans un scénario actif-actif où vous pourriez progressivement migrer des AP vers et depuis. Il peut également vous servir de contrôleur de mise en service pour configurer de nouveaux points d'accès.

Les 9800-CL sont très évolutifs et puissants. Il est à noter qu'ils ont une capacité de transfert de données beaucoup plus faible (de 2 Gbit/s à 4 Gbit/s pour l'image SR-IOV) ce qui tend à les limiter aux scénarios de commutation locale FlexConnect (et peut-être un petit nombre de points d'accès dans la commutation centrale). Ils peuvent toutefois être utiles en tant que périphériques N+1 lorsque vous avez besoin de contrôleurs supplémentaires pendant une fenêtre de maintenance ou lors du dépannage d'un problème.

Systèmes externes

Bien que ce document se concentre principalement sur le composant sans fil des grands réseaux événementiels, de nombreux systèmes de prise en charge doivent également être pris en compte au cours de la phase d'évolutivité et de conception. Certains de ces éléments sont traités ici.

Réseau principal

Les grands réseaux sans fil sont généralement déployés en mode de commutation centrale et avec de grands sous-réseaux. Cela implique qu'un très grand nombre d'adresses MAC et d'entrées ARP client sont transmises à l'infrastructure câblée adjacente. Il est essentiel que les systèmes adjacents dédiés aux différentes fonctions L2 et L3 possèdent les ressources adéquates pour gérer cette charge. Dans le cas des commutateurs de couche 2, une configuration courante est le réglage du modèle SDM (Switch Device Manager), qui est responsable de l'allocation des ressources système, l'équilibrage entre les fonctionnalités de couche 2 et de couche 3 dépendant de la fonction du périphérique dans le réseau. Il est important de s'assurer que les périphériques de couche 2 principaux peuvent prendre en charge le nombre d'entrées d'adresses MAC attendu.

NAT de passerelle

L'utilisation la plus courante des réseaux publics consiste à fournir un accès Internet aux visiteurs.

Quelque part le long du chemin de données, il doit y avoir un périphérique responsable de la traduction NAT/PAT. Les passerelles Internet doivent disposer des ressources matérielles et de la configuration de pool d'adresses IP nécessaires pour gérer la charge. N'oubliez pas qu'un seul périphérique client sans fil peut être responsable de nombreuses traductions NAT/PAT.

DNS/DHCP

Ces deux systèmes sont essentiels pour garantir une bonne expérience client. Les services DNS et DHCP nécessitent non seulement l'évolutivité appropriée pour gérer la charge, mais également une prise en compte de l'emplacement au sein du réseau. Des systèmes rapides et réactifs, placés au même endroit que le WLC, garantissent la meilleure expérience et évitent de longs délais d'intégration du client.

Portail AAA/Web

Personne n'aime une page Web lente, le choix d'un système approprié et bien adapté pour l'authentification Web externe est important pour une bonne expérience d'intégration du client. De même pour AAA, les serveurs d'authentification RADIUS doivent être capables de faire face aux demandes du système sans fil. Gardez à l'esprit que dans certains cas, la charge peut atteindre un pic pendant des moments clés, par exemple la mi-temps au cours d'un match de football, ce qui peut générer une charge d'authentification élevée en un temps réduit. Il est essentiel de faire évoluer le système pour qu'il soit correctement chargé simultanément. Une attention particulière doit être apportée lors de l'utilisation de fonctionnalités telles que la comptabilité AAA. Évitez à tout prix la comptabilité basée sur le temps et si vous utilisez la comptabilité, essayez de désactiver la comptabilité provisoire. Un autre élément important à prendre en compte est l'utilisation d'équilibreurs de charge, où des mécanismes de ping de session doivent être utilisés pour garantir des flux d'authentification complets. Veillez à conserver le délai d'attente RADIUS à 5 secondes ou plus.

Si vous utilisez un SSID 802.1X avec un grand nombre de clients (par exemple avec OpenRoaming), assurez-vous d'activer 802.11r Fast Transition (FT), sinon les clients peuvent provoquer une tempête d'authentification chaque fois qu'ils se déplacent.

DNS/DHCP

Quelques recommandations pour DHCP :

- Assurez-vous que le pool DHCP est au moins trois fois supérieur au nombre de clients attendus. Les adresses IP restent attribuées pendant un certain temps, même après la déconnexion du client. Ainsi, en fonction du temps de séjour des invités, cela peut consommer davantage d'adresses IP. Essayez de faire correspondre la durée du bail à la durée prévue de la visite de l'utilisateur sur le site. Il est inutile d'attribuer une adresse IP

pour une semaine si la durée d'une visite type est de deux heures, ce qui permet d'annuler les baux périmés.
- L'utilisation d'un seul grand sous-réseau pour les clients est recommandée, le WLC a une fonctionnalité ARP de proxy et ne transmet pas les diffusions par défaut (autre que DHCP). L'utilisation d'un sous-réseau client de grande taille (par exemple /16) pour vos clients ne pose pas de problème. Un seul grand VLAN est plus simple qu'un groupe de VLAN comportant de nombreux VLAN. La configuration de nombreux sous-réseaux plus petits (par exemple /24) et de groupes de VLAN n'a pas d'incidence sur le domaine de diffusion et entraîne uniquement une configuration plus compliquée, ce qui entraîne des problèmes tels que des VLAN sales et la nécessité de garder une trace des divers pools DHCP qui ne peuvent pas être utilisés de manière uniforme. Cette recommandation s'applique aux points d'accès en mode local et au trafic commuté de manière centrale. Dans le cas de FlexConnect avec commutation locale, il n'est pas pris en charge de placer plus de 100 (ou 300 après 17.9) AP dans le même sous-réseau car ils souffrent d'un grand nombre de transmissions de diffusion. Flexconnect nécessite que les AP desservent le même VLAN afin de prendre en charge l'itinérance transparente et par conséquent, il est déconseillé de prendre en charge de grands sous-réseaux dans ce scénario.
- Maintenez DHCP en mode de pontage sur le contrôleur sans fil avec la fonctionnalité de relais DHCP gérée par la passerelle de couche 3 du sous-réseau. Cela permet une efficacité et une simplicité maximales. L'idée est de ne pas impliquer du tout le contrôleur sans fil dans le processus DHCP.
- Utilisez DHCP Required sur n'importe quel WLAN public, quelle que soit la méthode d'authentification. Bien que cela puisse déclencher un faible pourcentage d'échecs d'associations de clients, cela peut empêcher des problèmes de sécurité importants, soit par des clients essayant de s'attribuer des adresses IP statiques, soit par des clients se comportant mal et essayant de réutiliser une adresse IP précédente sans autorisation.

# Fonctionnement du réseau

## La bonne configuration

Il est tentant d'activer de nombreuses options pour bénéficier de toutes les dernières fonctionnalités du Wi-Fi moderne. Cependant, certaines fonctionnalités fonctionnent parfaitement dans les environnements de petite taille, mais ont un impact considérable dans les environnements de grande taille et denses. De même, certaines fonctionnalités peuvent poser des problèmes de compatibilité. Même si les équipements Cisco respectent toutes les normes et offrent une compatibilité avec une grande variété de clients testés, le monde est rempli de périphériques clients uniques qui ont parfois des versions logicielles de pilotes avec des bogues ou une incompatibilité avec certaines fonctionnalités.

Selon le niveau de contrôle que vous exercez sur les clients, vous devez être prudent. Par exemple, si vous déployez le Wi-Fi pour le grand rassemblement annuel de votre entreprise, vous savez que la plupart des clients sont des périphériques de l'entreprise et vous pouvez planifier

l'ensemble de fonctionnalités pour l'activer en conséquence. D'un autre côté, si vous utilisez un réseau Wi-Fi dans un aéroport, votre niveau de satisfaction des clients est directement lié à leur capacité à se connecter à votre réseau, et vous n'avez aucun contrôle sur les appareils clients que les gens peuvent utiliser.

## SSID

### Combien de SSID ?

La recommandation a toujours été d'utiliser le moins de SSID possible. Ceci est exacerbé dans les réseaux à haute densité car la possibilité d'avoir plusieurs AP sur le même canal est presque garantie. En général, de nombreux déploiements utilisent trop de SSID, reconnaissent qu'ils en ont trop, mais déclarent qu'ils ne peuvent pas en utiliser moins. Vous devez effectuer une étude commerciale et technique pour chaque SSID afin de comprendre les similitudes entre les SSID et les options de regroupement de plusieurs SSID en un seul.

Passons en revue quelques types de sécurité/SSID et leur utilisation.

### WPA2/3 personnel

Un SSID de clé pré-partagée est extrêmement populaire en raison de sa simplicité. Vous pouvez soit imprimer la clé quelque part sur des badges ou sur du papier ou des panneaux, soit la communiquer d'une manière ou d'une autre aux visiteurs. Parfois, un SSID de clé pré-partagée est préférable même pour un SSID invité (à condition que la clé soit bien connue de tous les participants). Il peut aider à empêcher l'épuisement du pool DHCP en raison de la nature délibérée de la connexion. Les périphériques qui passent par ne se connectent pas automatiquement au réseau et ne peuvent donc pas utiliser une adresse IP du pool DHCP.

La clé WPA2 PSK ne garantit pas la confidentialité, car le trafic peut facilement être décrypté, car tout le monde utilise la même clé. Au contraire, WPA3 SAE assure la confidentialité et même si tout le monde possède la clé principale, il n'est pas possible de dériver la clé de chiffrement utilisée par d'autres clients.

WPA3 SAE est le meilleur choix pour la sécurité et de nombreux smartphones, ordinateurs portables et systèmes d'exploitation le prennent en charge. Certains périphériques IoT ou dispositifs portables intelligents peuvent encore avoir une prise en charge limitée et les clients plus anciens en général sont susceptibles de rencontrer des problèmes s'ils ne reçoivent pas les pilotes ou les mises à jour de microprogramme récents.

Il peut être tentant d'envisager un mode de transition WPA2 PSK-WPA3 SAE SSID pour simplifier

les choses, mais cela a été montré sur le terrain pour causer des problèmes de compatibilité. Les clients mal programmés n'attendent pas deux types de méthodes de clé partagée sur le même SSID. Si vous souhaitez proposer les options WPA2 et WPA3, il est conseillé de configurer des SSID distincts.

Le Wi-Fi 7 nécessite la configuration de deux nouveaux AKM (SAE-EXT et SAE-EXT-FT) sur le SSID WPA3 ainsi que le cryptage GCMP256, ce qui renforce la nécessité de faire un choix (si vous souhaitez conserver la compatibilité WPA2, il est potentiellement préférable d'oublier la fonctionnalité Wi-Fi 7). Les modèles AP et les clients ne prennent pas tous en charge GCMP256 pour le moment.

WPA2/3 Entreprise

WPA3 Enterprise (utilisant le cryptage AES 128 bits) est techniquement la même méthode de sécurité (au moins telle qu'annoncée dans les balises SSID) que WPA2 Enterprise, ce qui permet une compatibilité maximale.

Pour la norme 802.1X, un SSID de mode de transition est conseillé car aucun problème de compatibilité n'est détecté avec les périphériques récents (des problèmes ont été signalés avec Android 8 ou les anciennes versions d'Apple IOS). IOS XE 17.12 et versions ultérieures permettent d'avoir un seul SSID Transition Enterprise où seul WPA3 est utilisé et annoncé sur 6 GHz tandis que WPA2 est proposé en option sur la bande 5 GHz. Nous vous conseillons d'activer WPA3 sur les SSID d'entreprise dès que possible.

Les SSID d'entreprise WPA peuvent être utilisés pour les utilisateurs clés pour lesquels il existe une base de données de fournisseur d'identité qui permet de renvoyer des paramètres AAA (tels que des VLAN ou des ACL) en fonction de l'identité de l'utilisateur. Ces types de SSID peuvent inclure l'eduroam ou l'OpenRoaming qui combinent les avantages des SSID invités (en permettant aux visiteurs de se connecter facilement sans entrer d'informations d'identification) avec la sécurité d'un SSID d'entreprise. Ils réduisent considérablement la complexité de l'intégration généralement associée à la norme 802.1X, car les clients n'ont rien à faire pour se connecter au SSID eduroam ou OpenRoaming, à condition d'avoir un profil sur leur téléphone (qui peut être facilement fourni via une application événementielle)

La prise en charge du Wi-Fi 7 peut nécessiter (avec les clients les plus stricts) que le point d'accès offre également le cryptage GCMP256 qui nécessite IOS-XE 17.18.3 et les versions ultérieures du logiciel.

SSID invités

Un SSID invité est souvent synonyme d'authentification ouverte. Vous pouvez ajouter un portail

Web (ou non) derrière (selon la convivialité souhaitée ou les exigences locales) sous ses différentes formes : l'authentification web externe, locale ou centrale, mais le concept reste le même. Lors de l'utilisation d'un portail invité, l'évolutivité peut rapidement devenir un problème dans les grands environnements. Consultez la section Configuration pour l'évolutivité pour plus d'informations sur ce sujet.

Les opérations 6 GHz nécessitent que votre SSID invité utilise l'option Enhanced Open plutôt que l'option Open. Cela permet à tout le monde de se connecter, mais fournit la confidentialité (une meilleure confidentialité que WPA2-PSK même !) et le cryptage, le tout sans fournir aucune clé ou informations d'identification lors de la connexion sur le SSID. Les principaux fournisseurs de smartphones et systèmes d'exploitation prennent désormais en charge Enhanced Open, mais cette prise en charge n'est pas encore très répandue dans la base de clients sans fil. Le mode de transition Enhanced Open est interdit avec les opérations Wi-Fi 7 et 6 GHz. Par conséquent, la bonne approche consiste probablement à exécuter le SSID ouvert amélioré sur la bande 6 GHz uniquement et à conserver le SSID entièrement ouvert sur la bande 5 GHz pour des raisons de compatibilité. Vous devez attribuer un nom différent aux SSID, car ils utilisent des méthodes de sécurité différentes. Ceci ajoute un SSID dans la liste de balayage du client, mais n'ajoute pas de SSID supplémentaire par la radio, car ils sont présents sur différentes bandes.

Dans les grands événements et les lieux, il est souvent conseillé de configurer un PSK sur le SSID invité plutôt que de le laisser purement ouvert (le mode Enhanced Open Transition serait préférable, mais cela crée deux SSID et la compatibilité client doit encore être largement prouvée). Bien que cela rende l'intégration un peu plus compliquée (vous devez imprimer le PSK sur les badges ou les billets des gens ou l'annoncer d'une manière ou d'une autre), cela évite aux clients occasionnels de se connecter au réseau automatiquement sans que l'utilisateur final n'ait l'intention d'utiliser le réseau. De plus en plus de fournisseurs de systèmes d'exploitation mobiles ne donnent plus la priorité aux réseaux ouverts et affichent un avertissement de sécurité. Dans d'autres situations, vous pouvez vouloir un nombre maximal de passants à se connecter et donc ouvert est le meilleur choix.

Conclusion sur le nombre de SSID

Il ne peut pas y avoir de réponse satisfaisante à la question du nombre de SSID que vous devez respecter. L'effet dépend du débit de données minimum configuré, du nombre de SSID et du nombre de points d'accès diffusant sur le même canal. Lors d'un événement important organisé par Cisco, l'infrastructure sans fil utilisait 5 SSID : le PSK WPA2 principal, un SSID SAE WPA 3 pour la sécurité et la couverture 6 GHz, un SSID Eduroam d'entreprise pour la facilité d'accès pour les participants aux cours, un SSID OpenRoaming pour accueillir en toute sécurité toute personne ayant configuré le Wi-Fi à partir de l'application d'événement et un SSID 802.1X distinct pour l'accès au réseau du personnel et de l'administrateur.  C'était déjà presque trop, mais l'effet est resté raisonnable grâce au grand nombre de canaux disponibles, et aux antennes directionnelles utilisées pour réduire au maximum le chevauchement des canaux.

## Comparaison des concepts SSID hérités et SSID principal

Pendant un certain temps, il a été conseillé de limiter le service 2,4 GHz à un SSID distinct « hérité » annoncé uniquement dans 2,4 GHz. Cela devient de moins en moins populaire car les gens cessent de fournir un service 2,4 GHz. Cependant, l'idée peut et doit persister, mais avec d'autres concepts. Vous voulez déployer WPA3 SAE, mais le mode de transition vous pose des problèmes de compatibilité avec vos clients ? Disposez d'un SSID « hérité » WPA2 et d'un SSID SAE WPA3 principal. En nommant le SSID le moins performant « hérité », il n'attire pas les clients et vous êtes en mesure de voir facilement combien de clients font encore face à des problèmes de compatibilité avec votre SSID principal et ont besoin de cet hérité.

Mais pourquoi s'arrêter là ? Vous avez entendu des rumeurs selon lesquelles 802.11v a causé des problèmes avec certains clients plus anciens ou que certains pilotes clients n'aiment pas voir Device Analytics activé sur le SSID ? Activez toutes ces fonctionnalités pratiques sur votre SSID principal avancé et laissez-les sur votre SSID hérité/compatibilité. Cela vous permet de tester le déploiement de nouvelles fonctionnalités sur votre SSID principal tout en fournissant un SSID de compatibilité maximale pour les clients vers lesquels revenir. Ce système ne fonctionne que de cette façon. Si vous nommez votre SSID basé sur la compatibilité comme principal et que vous nommez votre SSID avancé avec quelque chose comme « <name>-WPA3 », vous remarquerez que les personnes s'en tiennent à l'ancien SSID auquel elles étaient habituées, et que l'adoption reste faible pendant de nombreuses années sur votre « nouveau » SSID. Le déploiement de nouveaux paramètres ou de nouvelles fonctionnalités entraîne des résultats peu concluants en raison du nombre moins élevé de clients qui s'y connectent.

## Fonctionnalités SSID

- Il est préférable de maintenir les extensions Aironet désactivées. Elles sont particulièrement utiles pour les études de site et les opérations WGB, mais elles peuvent parfois poser des problèmes avec certains clients existants. Aironet IE annonce également le nom d'hôte AP qui n'est pas souhaité dans les déploiements soucieux de la sécurité.
- CCKM est un protocole déconseillé (en faveur de FT) et doit être désactivé.
- À l'heure actuelle, il est préférable d'utiliser le cryptage AES-128, même dans WPA3 en raison de la faible prise en charge par le client de cryptage plus élevé (sauf si vous pouvez vous permettre un SSID spécifique plus sécurisé et plus restrictif)
- La détection des trous de couverture est mieux désactivée (pour tous les SSID). Les grands déploiements utilisent généralement des antennes directionnelles, ce qui nécessite une étude approfondie du site. Les niveaux de puissance de chaque antenne seraient le résultat du processus de conception RF et généralement configurés à des niveaux spécifiques.
- La fonction FT adaptative doit être désactivée, car certains clients peuvent rencontrer des problèmes lorsque la fonction FT n'est pas entièrement annoncée, mais présente dans certains attributs. Désactivez entièrement FT (pour une compatibilité maximale) ou optez pour FT+802.1X, que la plupart des clients (sauf s'ils sont anciens ou plus orientés IoT) prennent en charge. Lors de la configuration de FT+802.1X, même les clients non-FT sont

autorisés à joindre le SSID. Le seul problème possible est avec certains clients qui ne toléreraient pas de voir deux options de sécurité sur le même SSID.
- Désactivez 802.11ac MU-MIMO. Il ajoute de la complexité et présente un très faible avantage en 802.11ac.
- Désactivez le temps de réveil cible BSS. Il est peu adopté du côté du client actuellement.
- Désactivez l'équilibrage de charge agressif et la sélection de bande. Band Select n'est pas nécessaire si vous n'annoncez pas le SSID dans 2,4 GHz (ou s'il est sur un SSID dédié) et l'équilibrage de charge agressif retarde l'association du client en rejetant le client plusieurs fois avant de l'accepter finalement s'il insiste pour se connecter à un AP chargé. Vous avez quand même chargé des points d'accès dans un environnement occupé et cela est négatif pour l'expérience client.
- Désactivez FastLane+.
- Désactiver l'administration universelle, cette fonctionnalité était pour 3700 AP et seulement dans le domaine -UX. Le laisser allumé laisse ouvert un vecteur d'attaque inutile.
- Maintenez la mise en cache des clés opportunistes activée. Il sert de mécanisme d’itinérance rapide pour les clients ne prenant pas en charge FT.
- Laissez WMM autorisé. La désactivation de votre réseau reviendrait à l'ère 802.11g et son utilisation n'apporterait aucun avantage sur la plate-forme 9800.
- Activez la protection de source IP.
- Désactivez le profilage RADIUS. Dans un environnement très occupé, ceci peut envoyer des messages de comptabilité RADIUS excessifs (chaque fois que les clients font DHCP ou envoient des paquets HTTP) et a un très réel potentiel de surcharge de votre serveur RADIUS.
- Évitez d'utiliser des SSID masqués. Cela n'a aucun but de sécurité, le nom SSID peut toujours être découvert facilement avec des applications simples ou en prenant une capture de renifleur. Le masquage du SSID ralentit l'itinérance de tous les clients, car ils ne bénéficient plus de l'analyse de balise passive et doivent compter sur l'analyse active pour obtenir les informations d'AP voisines.
- Essayez de ne pas utiliser plus de quatre WLAN par radio, car cela a un impact significatif sur l'utilisation des radiofréquences. Il ne s'agit pas d'une limite stricte, l'utilisation de cinq WLAN peut fonctionner, mais soyez très conscient du temps d'antenne perdu en utilisant de plus en plus de WLAN.
- Les normes 802.11v et 802.11k sont de plus en plus prises en charge par les types de clients les plus répandus. Ils ne posent généralement pas de problème en ce qui concerne la connexion du client. Les avantages qu'ils apportent dépendent beaucoup de la façon dont les clients utilisent ces protocoles et peuvent parfois (dans le cas de la norme 802.11k) entraîner une utilisation légèrement plus élevée du CPU. Vous pouvez les garder hors de votre IoT ou SSID hérité, mais ils doivent être activés si possible sur votre SSID de production.

## Balise de site

Les balises de site sont un élément de configuration qui permet de regrouper les points d'accès qui partagent les mêmes paramètres FlexConnect ainsi que les paramètres de profil de jointure AP (tels que les informations d'identification, les détails SSH et le code de pays). Pourquoi les

balises de site sont-elles importantes ? Les balises de site définissent également la manière dont les points d'accès sont gérés par le processus WNCD dans le Catalyst 9800. Voici quelques exemples à titre d'illustration :

- Si vous configurez quatre balises de site sur un 9800-80 qui a huit processus WNCD, chaque balise de site est assignée à un processus WNCD différent (en exécutant chacun sur un coeur de CPU distinct) et quatre processus WNCD ne font rien. Cela signifie que vous n'utilisez pas tous les CPU de votre 9800-80 et il ne serait pas recommandé de le charger avec le maximum de 6000 AP pris en charge.

| Site tag 1 | Site tag 2 | Site tag 3 | Site tag 4 | - | - | - | - |
|---|---|---|---|---|---|---|---|
| WNCD 1 | WNCD 2 | WNCD 3 | WNCD 4 | WNCD 5 | WNCD 6 | WNCD 7 | WNCD 8 |
| CPU | CPU | CPU | CPU | CPU | CPU | CPU | CPU |

Premier exemple d'équilibrage des balises de site

- Si vous configurez 10 balises de site sur un 9800-80 qui a huit processus WNCD, deux processus WNCD prennent en charge deux balises de site chacune, tandis que les six autres gèrent une balise de site chacune.

| Site tag 1<br>Site tag 9 | Site tag 2<br>Site tag 10 | Site tag 3 | Site tag 4 | Site tag 5 | Site tag 6 | Site tag 7 | Site tag 8 |
|---|---|---|---|---|---|---|---|
| WNCD 1 | WNCD 2 | WNCD 3 | WNCD 4 | WNCD 5 | WNCD 6 | WNCD 7 | WNCD 8 |
| CPU | CPU | CPU | CPU | CPU | CPU | CPU | CPU |

Deuxième exemple d'équilibrage des balises de site

Pour les déploiements géographiquement étendus comportant de nombreux sites et de nombreuses balises de site, il est recommandé de multiplier le nombre de balises de site par le nombre de processus WNCD sur la plate-forme que vous utilisez.

Cependant, pour les réseaux événementiels qui sont généralement situés sous un même toit ou dans plusieurs bâtiments d'un même site, il est recommandé de faire correspondre le nombre d'étiquettes de site au nombre exact de WNCD sur la plate-forme donnée. L'objectif final est que chaque processus WNCD (et donc chaque coeur de processeur alloué aux tâches sans fil) gère un nombre d'événements d'itinérance client à peu près similaire, de sorte que la charge soit équilibrée sur tous les coeurs de processeur.

| Platform type | Number of WNCD processes |
|---|---|
| 9800-CL small OVA | 1 |
| 9800-CL medium OVA | 3 |
| 9800-CL large OVA | 7 |
| 9800-L | 1 |
| 9800-40/CW9800-M | 5 |
| 9800-80/CW9800-H | 8 |

Nombre de processus WNCD pour chaque type de plateforme

Au coeur, ce qui compte vraiment est de regrouper les AP qui sont dans le même voisinage physique dans la même balise de site, de sorte que les événements d'itinérance fréquents du client entre ces AP restent dans le même processus CPU. Cela signifie que même si vous avez un seul grand lieu, il est recommandé de diviser le lieu en plusieurs balises de site (autant que vous avez des processus WNCD qui gèrent le lieu) et de regrouper les points d'accès aussi logiquement que possible en ces groupes pour former des groupes de voisinage RF logiques qui sont également répartis uniformément entre les balises de site.

À partir de IOS XE 17.12, un algorithme d'équilibrage de charge peut être activé de sorte que le WLC regroupe les AP en fonction de leur proximité RF. Cela vous enlève la charge des mains et crée une répartition équilibrée des points d'accès à travers le processus WNCD. Cela peut être utile si vous ne pouvez pas facilement dessiner des groupes de points d'accès voisins à placer dans la quantité correcte de balises de site. Une spécificité de cet algorithme est qu'il attribue des AP au processus WNCD indépendamment de leur attribution de balise de site, ce qui signifie qu'il ne change pas l'attribution de balise de site de l'AP. Vous pouvez ensuite attribuer des balises de site purement basiques sur une logique de configuration et laisser l'algorithme équilibrer les AP entre les CPU de la manière la plus optimale.

La fonction d'équilibrage de charge automatique AP basée sur RF est documentée dans le Guide de configuration du logiciel du contrôleur sans fil de la gamme Cisco Catalyst 9800, Cisco IOS XE Dublin 17.12.x.

L'utilisation CPU des processus WNCD doit être surveillée lors d'événements importants. Si un ou plusieurs processus WNCD présentent une utilisation élevée, il se peut que le WNCD traite trop de points d'accès ou de clients, ou que les points d'accès ou les clients qu'il gère soient plus occupés que la moyenne (si tous sont constamment en itinérance, par exemple dans un aéroport).

## Profil de stratégie

- Activez le protocole ARP et le proxy DAD (Duplicate Address Detection), ce qui permet au WLC de répondre au nom des clients sans fil lorsqu'un périphérique tente d'apprendre l'adresse MAC d'un périphérique sans fil. Cela permet également d'économiser les batteries

des clients sans fil.
- N'activez pas les fonctionnalités WGB sauf si nécessaire.
- Activer DHCP requis pour éviter les clients avec des adresses IP statiques.
- Maintenez le délai d'inactivité court (300 secondes). Certains administrateurs prennent du temps pour éviter que les clients ne soient à nouveau authentifiés, mais un délai d'inactivité trop long entraîne des entrées client fantômes (affectant la création de rapports) lorsque le nombre de clients est retardé par rapport au temps réel. Il est préférable de maintenir le délai d'inactivité inférieur au délai de rotation de la clé de groupe pour éviter les inondations comptables lorsque les clients sont supprimés. L'intervalle de rotation des clés de groupe peut être configuré dans l'interface utilisateur Web sous Configuration > Security > Advanced EAP comme « EAP-Broadcast Key Interval »
- Expiration de la session de 86400 secondes pour éviter les déconnexions et les réauthentifications inutiles.

## Profil de jointure AP

- Assurez-vous que l'ajustement TCP MSS est activé.
- Activez Trust DSCP en amont. De nombreux clients sans fil n'utilisent pas l'étiquetage 802.11e WMM UP. Malheureusement, l'approbation du champ DSCP est un moyen sûr de fournir la priorité appropriée aux applications vocales.
- Activez Syslog pour vos points d'accès. La configuration d'une adresse IP de serveur Syslog permet aux points d'accès de monodiffuser leurs journaux de console. Il est non seulement utile de dépanner les AP, mais il est également meilleur pour le réseau que le paramètre par défaut qui fait que les AP diffusent leur Syslog dans le VLAN local. La journalisation AP peut générer une charge de messages importante, même dans les cas où AP Syslog n'est pas surveillé, il est toujours bon de limiter le nombre d'événements en définissant la gravité de message appropriée, et/ou en configurant une adresse IP Syslog factice (par exemple 0.0.0.0) pour empêcher les messages d'être diffusés.
- Maximisez les tentatives CAPWAP et le délai d'attente. Les problèmes sont détectés moins rapidement, mais le réseau résiste mieux aux abandons de paquets transitoires mineurs.
- Activez SSH et configurez les informations d'identification. Désactivez la console AP.
- Activez le contrôle AP si nécessaire, mais pas le contrôle radio.
- Activez la détection des systèmes non fiables et configurez un seuil RSSI de -70 dBm.

## Surveillance du réseau

Une fois que le réseau est opérationnel, vous devez le surveiller de près pour détecter les problèmes. Dans un environnement de bureau standard, les utilisateurs connaissent le réseau et peuvent soit s'entraider en cas de problème, soit ouvrir un ticket d'assistance interne. Dans un lieu plus grand avec de nombreux visiteurs viennent vous voulez vous concentrer sur les plus grands problèmes plutôt que sur des individus spécifiques qui peuvent juste avoir une mauvaise configuration, donc vous devez avoir la bonne stratégie de surveillance.

Il est possible de surveiller le réseau à partir de l'interface de ligne de commande ou de l'interface graphique du Catalyst 9800, mais ce n'est pas le meilleur outil pour effectuer une surveillance quotidienne. C'est le plus direct lorsque vous avez déjà des soupçons et/ou des données sur le problème et que vous voulez exécuter des commandes spécifiques en temps réel. Les principales options de surveillance sont Cisco Catalyst Center ou éventuellement un tableau de bord télémétrique personnalisé. Il est possible d'utiliser des outils de surveillance tiers, mais lorsque ceux-ci utilisent SNMP comme protocole, les données sont loin d'être en temps réel et les outils de surveillance tiers habituels ne sont pas assez granulaires avec toutes les spécificités des fournisseurs sans fil. Si vous choisissez le protocole SNMP, assurez-vous d'utiliser SNMPv3 car SNMPv2 a une sécurité obsolète.

Cisco Catalyst Center est la meilleure option car elle vous permet de gérer votre réseau en plus de le surveiller. Outre la surveillance, il permet également de dépanner en direct et de résoudre de nombreuses situations.

Un tableau de bord de télémétrie personnalisé peut être utile si vous souhaitez afficher des mesures et des widgets très spécifiques sur un écran de façon permanente pour un centre d'exploitation du réseau ou un centre d'exploitation du réseau. S'il existe des zones très spécifiques de votre réseau que vous souhaitez surveiller, vous pouvez créer des widgets dédiés pour afficher les métriques du réseau dans ces zones de la manière de votre choix.

Pour les réseaux d'événements, il est conseillé de surveiller les statistiques RF à l'échelle du système, en particulier l'utilisation des canaux et le nombre de clients par point d'accès. Cela peut se faire à partir de l'interface de ligne de commande, mais ne fournit qu'un instantané à un moment donné. L'utilisation du canal est en général dynamique et mieux adaptée à la surveillance dans le temps. Pour ce type de surveillance, un tableau de bord personnalisé est généralement une bonne approche. D'autres mesures plus utiles lorsqu'elles sont surveillées au fil du temps peuvent inclure l'utilisation du WNCD, le nombre de clients et leur état, et des mesures spécifiques au site. La surveillance de l'utilisation et/ou de la charge d'une zone ou d'un emplacement spécifique, par exemple la salle X dans le cas d'un centre de conférence, ou la zone d'occupation des sièges Y dans le cas d'un lieu d'événement, est un exemple de mesures spécifiques.

Pour la surveillance personnalisée, les méthodes de télémétrie en continu NETCONF RPC (pull) et NETCONF (push) sont valides, bien que l'utilisation de la télémétrie en continu personnalisée en association avec Catalyst Center nécessite une certaine diligence, car il existe une limite au nombre d'abonnements télémétriques qui peuvent être configurés sur le WLC et Catalyst Center préremplit (et utilise) bon nombre d'entre eux.

Lors de l'utilisation de NETCONF RPC, certains tests sont nécessaires pour s'assurer que le WLC n'est pas surchargé avec des requêtes NETCONF. Il est particulièrement important de garder à l'esprit les taux d'actualisation pour certains points de données et le temps nécessaire pour que les données soient renvoyées. Par exemple, l'utilisation du canal AP est actualisée (d'AP à WLC) toutes les 60 secondes, et la collecte de métriques RF pour 1000 AP (à partir de WLC) peut

prendre plusieurs secondes. Dans cet exemple, interroger le WLC toutes les 5 secondes ne serait pas utile, une meilleure approche serait de collecter des métriques RF à l'échelle du système toutes les 3 minutes.

NETCONF est toujours préférable à SNMP.

Enfin, la surveillance des composants du réseau principal ne peut pas être négligée, notamment l'utilisation du pool DHCP, le nombre d'entrées NAT sur les routeurs principaux, etc. Comme la défaillance de l'un de ces éléments peut facilement être la cause d'une panne sans fil.

Plus vous surveillez, plus vous pouvez causer vos propres problèmes

Il existe quelques scénarios classiques où une surveillance excessive crée des problèmes :

- Les capteurs sans fil agissant en tant que clients peuvent être utiles pour mesurer le débit et la connectivité à des emplacements spécifiques du réseau, mais n'oubliez pas que la définition d'une fréquence élevée de tests signifie que le capteur passera beaucoup de temps à effectuer des transferts de données volumineux et donc à occuper le canal et le réseau, même s'il n'en était pas autrement. C'est l'exemple parfait de « plus vous surveillez, moins vos indicateurs semblent bons ».
- Comme nous l'avons déjà mentionné, SNMP est un protocole hérité qui a un impact important sur le processeur. L'exécution d'un grand sondage SNMP peut facilement saturer le processeur de votre réseau sans fil de requêtes dès que vous surveillez fréquemment tous vos clients ou points d'accès sans fil lorsque vous en avez un grand nombre. Tenez toujours compte de la quantité d'objets que vous interrogez avant de définir un intervalle d'interrogation agressif. Le démon SNMP se trouve à l'intérieur du processus IOSd dans IOS-XE, de sorte que lorsqu'il est sur un CPU élevé, il peut avoir un impact sur le reste des fonctionnalités IOS.
- Même si la télémétrie est plus efficace que le protocole SNMP, les grands réseaux sans fil peuvent avoir un très grand nombre de clients, de points d'accès, mais aussi d'interféreurs et de périphériques indésirables. Si votre configuration de télémétrie est définie de manière trop agressive et que le WLC doit constamment signaler tout changement de signal d'un périphérique non autorisé, cela peut également saturer facilement n'importe quel dispositif de contrôleur. Assurez-vous de garder un oeil sur votre processus « pubd » qui est en charge de la télémétrie et assurez-vous qu'il n'est pas sur l'utilisation élevée du CPU. Si c'est le cas, reconsidérez vos seuils et assurez-vous de suivre les meilleures pratiques du 9800.

Problèmes spécifiques aux grands réseaux

Si vous avez un SSID utilisant l'authentification Web, un problème peut être celui des clients qui se connectent à ce SSID et obtiennent une adresse IP mais ne s'authentifient jamais parce que l'utilisateur final n'essaie pas activement de se connecter (le périphérique connecté

automatiquement). Le contrôleur doit intercepter chaque paquet HTTP envoyé par les clients qui sont dans l'état appelé authentification Web en attente et cela utilise des ressources WLC. Une fois que votre réseau est en cours d'exécution, surveillez régulièrement le nombre de clients en attente d'authentification Web à un moment donné afin de comparer leur état à celui des numéros de référence. Même chose pour les clients dans l'état IP Learn. Vous avez toujours des clients dans cet état lorsqu'ils exécutent leur processus DHCP, mais le fait de connaître le bon numéro de fonctionnement de votre réseau permet de définir une ligne de base et d'identifier les moments où ce numéro peut être trop élevé et indiquer un problème plus important.

Pour les grands sites, il n'est pas rare de voir ~10 % des clients dans l'état Web Auth Pending.

Surveillance du jour 2 : Garder un oeil sur la satisfaction des utilisateurs

Une fois que le réseau est opérationnel, il existe deux types de plaintes types d'utilisateurs finaux : ils ne peuvent pas se connecter ou ont du mal à se connecter (déconnexions), ou le Wi-Fi fonctionne plus lentement que prévu. Ce dernier est très difficile à identifier car il dépend d'abord des attentes de la vitesse ainsi que de la densité en temps réel d'une zone donnée. Citons quelques ressources qui peuvent vous être utiles pour la surveillance quotidienne d'un grand réseau de salles publiques.

Valider le débit Wi-Fi : Guide de test et de surveillance. Ce document cisco.com explique comment surveiller un réseau pour détecter les problèmes de débit. Elle consiste à déterminer le débit auquel les clients peuvent raisonnablement s'attendre sur votre réseau lorsque les choses sont calmes et à estimer la diminution de ces estimations à mesure que le nombre de clients et la charge augmentent. Il s'agit d'une étape clé pour déterminer si une plainte de l'utilisateur final concernant le débit est légitime d'un point de vue technique ou non, et si vous devez reconcevoir cette zone pour la charge à laquelle elle est potentiellement confrontée.

Lorsque des clients signalent des problèmes de connectivité, après que cela a été isolé et clarifié avec Catalyst Center, jetez un oeil à Dépanner le flux des problèmes de connectivité du client Catalyst 9800.

Enfin, en tant que bonne pratique générale, gardez un oeil sur les mesures clés globales du WLC avec l'aide de surveiller les indicateurs de performance clés (KPI) Catalyst 9800 (Key Performance Indicators).

## Configuration pour l'évolutivité

Interfaces et interfaces SVI sur le 9800

Évitez de créer des interfaces SVI pour les VLAN clients sur le WLC. Les administrateurs habitués aux anciens WLC AireOS ont tendance à avoir le réflexe de créer une interface de couche 3 pour chaque VLAN client, mais cela est rarement nécessaire. Les interfaces augmentent le vecteur d'attaque du plan de contrôle et peuvent nécessiter davantage de listes de contrôle d'accès avec des entrées plus complexes. Le WLC est accessible, par défaut, sur n'importe laquelle de ses interfaces, plus de travail est nécessaire pour protéger un WLC avec plus d'interfaces. Il complique également le routage, il est donc préférable de l'éviter.

Depuis IOS XE 17.9, les interfaces SVI ne sont plus nécessaires pour la surveillance mDNS ou les scénarios de relais DHCP. Il y a donc très peu de raisons de configurer une interface SVI dans un VLAN client.

Réponse de sonde agrégée

Pour les grands réseaux publics, il est conseillé de modifier l'intervalle de sonde agrégée par défaut envoyé par les points d'accès. Par défaut, les AP mettent à jour le WLC toutes les 500 ms sur les sondes envoyées par les clients. Ces informations sont utilisées par les fonctions d'équilibrage de charge, de sélection de bande, d'emplacement et 802.11k. S'il y a beaucoup de clients et de points d'accès, il est conseillé de modifier l'intervalle de mise à jour pour éviter les problèmes de performances du plan de contrôle dans le WLC. Le paramètre recommandé est de 50 réponses de sonde agrégées toutes les 64 secondes. Assurez-vous également que vos points d'accès ne signalent pas les sondes à partir des adresses MAC administrées localement car il n'y a pas de suivi ponctuel de ceux qui considèrent qu'un seul client pourrait utiliser de nombreux MAC administrés localement lors de l'analyse pour éviter le suivi à dessein.

```
wireless probe limit 50 64000

no wireless probe locally-administered-mac
```

IPv6

De nombreux administrateurs réseau refusent toujours IPv6. Il n'existe que deux options acceptables avec IPv6 : soit vous le prenez en charge et devez déployer une configuration adéquate partout, soit vous ne le faites pas et vous devez le bloquer. Il n'est pas acceptable de ne pas se soucier d'IPV6 et de le laisser activé à certains endroits sans configuration appropriée. Cela laisserait le monde de l'IP dans lequel votre sécurité réseau serait aveugle.

Si vous activez IPv6, il est obligatoire de configurer une adresse IPv6 virtuelle dans la plage 2001:DB8::/32 (c'est une étape souvent oubliée).

Il est important de noter que, bien qu'IPv6 repose beaucoup sur la multidiffusion pour ses opérations de base, il peut toujours fonctionner si vous désactivez le transfert de multidiffusion sur le WLC. Le transfert multidiffusion fait référence au transfert de données multidiffusion client et non à la découverte de voisins, aux sollicitations de routeur et aux autres protocoles requis pour faire fonctionner IPv6.

Si votre connexion Internet ou votre fournisseur d'accès Internet fournit des adresses IPv6, vous pouvez décider d'autoriser l'IPv6 pour vos clients. C'est une décision différente de l'activation d'IPv6 dans votre infrastructure. Vos points d'accès peuvent continuer à fonctionner en IPv4 uniquement, mais continuent à transporter le trafic de données client IPv6 à l'intérieur de leurs paquets CAPWAP. L'activation d'IPv6 sur votre infrastructure nécessite également que vous réfléchissiez à la protection de l'accès client à vos points d'accès, WLC et sous-réseau de gestion.

Vérifiez la fréquence d'annonce de routeur de vos passerelles client. Le WLC offre une politique de limitation d'annonce de routeur qui limite le nombre d'annonces de routeur transmises aux clients, car celles-ci peuvent parfois être bavardes.

mDNS

En général, il est préférable de maintenir mDNS complètement désactivé dans un déploiement de grande envergure.

Le pontage mDNS fait référence au concept d'autorisation d'envoi des paquets mDNS sous la forme d'une multidiffusion de couche 2 (par conséquent vers l'ensemble du sous-réseau client). mDNS est devenu populaire dans les environnements domestiques et de petits bureaux où il est très pratique de découvrir des services dans votre sous-réseau. Cependant, dans un grand réseau, cela signifie envoyer le paquet à tous les clients du sous-réseau, ce qui est problématique du point de vue du trafic dans un grand réseau public. D'un autre côté, le pontage ne cause aucune surcharge au CPU du point d'accès ou du WLC car il est considéré comme un trafic de données normal. Le proxy mDNS ou la passerelle mDNS fait référence au concept d'utilisation du WLC comme répertoire pour tous les services du réseau. Cela permet d'offrir des services mDNS au-delà des limites de la couche 2 de manière efficace et de réduire également le trafic global. Avec la passerelle mDNS, une imprimante, par exemple, envoie son annonce de service périodique via mDNS avec une multidiffusion de couche 2 de même sous-réseau, mais le WLC ne la transfère pas à tous les autres clients sans fil. Au lieu de cela, il prend note du service offert et l'enregistre dans son répertoire de services. Chaque fois qu'un client demande des services d'un type donné disponibles, le WLC répond au nom de l'imprimante avec l'annonce. Cela évite à tous les autres clients sans fil d'entendre parler de demandes et d'offres de services inutiles et d'obtenir une réponse uniquement lorsqu'ils demandent quels services existent. Bien qu'il améliore considérablement l'efficacité du trafic, il provoque une surcharge sur le WLC (ou l'AP, si vous comptez sur AP mDNS dans les scénarios FlexConnect) en raison de la surveillance du trafic mDNS. Si vous utilisez une passerelle mDNS, il est essentiel de garder un oeil sur l'utilisation du processeur.

Le pontage entraîne une tempête de multidiffusion dans votre grand sous-réseau et la surveillance (avec la fonctionnalité de passerelle mDNS) entraîne une utilisation importante du processeur. Désactivez-le globalement ainsi que sur chaque WLAN.

Certains administrateurs activent mDNS parce que certains services en ont besoin à des endroits spécifiques, mais il est important de comprendre la quantité de trafic indésirable que cela ajoute. Les appareils Apple font souvent de la publicité et recherchent constamment des services, ce qui provoque un bruit de fond de requêtes mDNS même lorsque personne n'utilise un service particulier. Si vous devez autoriser mDNS en raison d'une certaine exigence commerciale, activez-le globalement, puis activez-le uniquement sur le WLAN où il est requis et essayez de limiter l'étendue où mDNS est autorisé.

## Renforcement du réseau

### Sécurité

Dans les grands réseaux publics, de nombreuses choses peuvent se produire sans que l’administrateur ne le sache. Les gens demandent des branchements de câble dans des endroits aléatoires, ou branchent un commutateur de qualité domestique dans un endroit pour avoir plus de ports de commutation pour leurs manigances, ... Ils essaient généralement ces choses sans demander d'abord la permission. Cela signifie que, même en l'absence d'un mauvais acteur, la sécurité peut déjà être compromise par des clients et/ou des employés qui le souhaitent. Il devient alors très facile pour un mauvais acteur de se promener et de trouver un câble à brancher et de voir quel accès réseau il obtient à partir de là. La configuration de l'authentification 802.1X sur tous les ports de commutation est presque indispensable pour maintenir une sécurité correcte dans un grand réseau. Catalyst Center peut vous aider à automatiser ce déploiement et des exceptions peuvent être faites pour des périphériques spécifiques qui ne prennent pas en charge l'authentification 802.1X, mais essayez de vous fier le moins possible à l'authentification basée sur MAC, car ce n'est (sincèrement) pas de la vraie sécurité.

### Points d'accès indésirables

Votre stratégie de lutte contre les escrocs dépend de quelques facteurs. De nombreux administrateurs optent instinctivement pour des règles très strictes, mais les principales questions sont les suivantes :

- Lorsque vous recevez des centaines (voire des milliers) d'alertes de voyous, disposez-vous des ressources humaines nécessaires pour les analyser toutes et prendre des mesures pour les résoudre toutes ?
- Votre objectif est-il d'éliminer physiquement les parasites afin de conserver un spectre RF propre ? Si c'est le cas, vous avez besoin de beaucoup de gens pour mener cette opération.

Ou peut-être que votre objectif est de ne garder qu'un oeil sur le facteur de sécurité et de simplement vous assurer que les voleurs ne représentent aucun danger ? Cela a un coût du travail humain beaucoup plus gérable.

- L'activation de la détection des systèmes non fiables peut avoir un impact sur votre temps d'antenne et le confinement des systèmes non fiables a généralement un impact encore plus important. Avez-vous analysé cet impact et l'avez-vous pris en compte ?

En ce qui concerne l'impact de la détection des systèmes non fiables, les modèles 9120 et 9130 disposent d'une puce CleanAir dédiée qui se charge de l'analyse hors canal (et donc de la détection des systèmes non fiables), ce qui rend l'impact presque nul sur la radio du service client. Les points d'accès de la gamme 9160 avec leur puce CleanAir Pro ont une capacité de balayage sans impact similaire, mais d'autres points d'accès qui n'ont pas la puce CleanAir doivent prendre leur radio de service client hors canal pour rechercher les indésirables ou pour faire le confinement. Le modèle de point d'accès que vous utilisez joue donc un rôle dans la décision d'utiliser des points d'accès en mode surveillance dédiés pour la détection et le confinement des systèmes non fiables ou non.

---

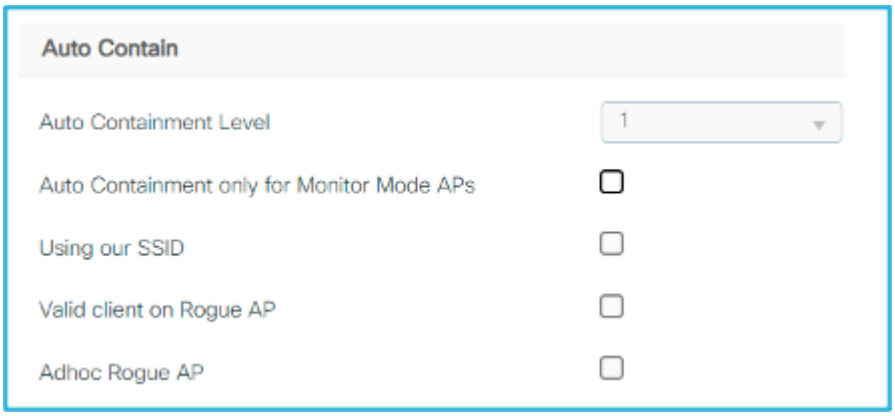


Remarque : Les téléphones mobiles partageant un point d'accès Wi-Fi fonctionnent en mode « infrastructure », tout comme les points d'accès traditionnels, le mode « ad hoc » fait référence à une connexion directe entre les appareils mobiles et est moins courant.

---

La limitation des systèmes non fiables est souvent interdite par les réglementations. Il est donc essentiel de vérifier auprès de votre autorité locale avant de l'activer. Le fait de contenir un client indésirable ne signifie pas qu'il doit être arrêté à distance, mais qu'il doit envoyer un spam aux clients qui tentent de se connecter au point d'accès indésirable à l'aide de trames de désauthentification afin qu'ils ne se connectent pas. Cela ne peut fonctionner que sur le SSID de sécurité hérité (cela ne fonctionne pas dans WPA3 ou lorsque le PMF est activé dans WPA2) parce que vos points d'accès ne sont pas en mesure de signer correctement les trames de désauthentification. Le confinement a un impact négatif sur les performances RF sur le canal cible, car vos points d'accès remplissent le temps d'antenne avec des trames de désauthentification. Par conséquent, elle doit uniquement être considérée comme une mesure de sécurité visant à empêcher vos propres clients légitimes de s'associer par erreur à un point d'accès non autorisé. Pour toutes les raisons mentionnées, il est recommandé de ne pas effectuer de confinement car cela ne résout pas complètement le problème indésirable et provoque plus de problèmes RF. Si vous devez utiliser le confinement, il est logique de l'activer uniquement pour les pirates qui usurpent l'un de vos SSID gérés, car il s'agit d'une attaque manifeste.

Vous pouvez configurer la contenance automatique avec l'option « Utilisation de nos SSID » :




Contenir automatiquement les paramètres

Vous pouvez également configurer des règles indésirables pour les classer comme points d'accès indésirables malveillants en fonction de vos propres critères. N'oubliez pas d'entrer le nom de vos SSID voisins et approuvés en tant qu'éléments indésirables pour les supprimer de votre liste d'alarmes.

Activez l'authentification AP ou PMF pour protéger vos AP contre l'emprunt d'identité.

Un pirate filaire est un point d'accès pirate connecté à votre réseau filaire, ce qui constitue une menace de sécurité accrue. La détection des pirates filaires est plus compliquée, car l'adresse MAC Ethernet d'un pirate informatique diffère généralement de son adresse MAC radio. Cisco Catalyst Center dispose d'algorithmes qui tentent toujours de détecter si un client indésirable est câblé et recherche les adresses MAC client indésirables qui sont à la fois entendues en direct et visibles sur l'infrastructure câblée. La meilleure solution pour empêcher les pirates filaires est de sécuriser tous vos ports de commutation avec l'authentification 802.1X.

Si vous devez agir physiquement sur un point d'accès non autorisé, l'utilisation de Cisco Spaces est essentielle pour avoir une localisation précise du non autorisé. Vous avez probablement encore besoin de rechercher autour une fois sur le site que les gens ont tendance à cacher des points d'accès indésirables parfois, mais la réduction de la zone de recherche à quelques mètres rend une entreprise très faisable. Sans espaces, le voyous est montré sur la carte à côté de l'AP le plus fort qui détecte ce qui rend une zone de recherche assez grande. Il existe de nombreux outils et périphériques sans fil qui vous indiquent le signal du point d'accès non autorisé en temps réel pour vous aider à le localiser physiquement.

Pas exactement lié aux parasites, mais puisque CleanAir vient d'être couvert, il est important de noter que l'activation de CleanAir n'a pas d'impact négatif notable sur les performances, sauf sur la détection de la balise BLE, car cela a un impact sur les performances 2,4 GHz. Vous pouvez configurer votre réseau sans fil pour ignorer les interférences Bluetooth car elles sont omniprésentes dans le monde actuel et vous ne pouvez pas empêcher vos clients d'activer leur Bluetooth.

Il existe une autre catégorie de programmes indésirables qui n'apparaît pas dans votre liste de détection des programmes indésirables. Certains clients peuvent utiliser le Wi-Fi directement entre eux et n'utilisent donc aucun point d'accès. Cela ne représente pas vraiment un problème de sécurité, mais utilise le temps d'antenne RF.
Un exemple est Apple AirDrop où deux appareils se détectent par Bluetooth et peuvent ensuite s'entendre sur l'utilisation d'un canal Wi-Fi pour le transfert de fichiers. Les utilisateurs veulent transférer ce fichier de toute façon, il est donc conseillé de le leur permettre aussi vite que possible afin que l'interférence cesse dès que possible. Cependant, sachez que la détection de gouttes d'air peut parfois faire basculer un tunnel VPN si l'application VPN ne gère pas correctement le changement d'état de l'interface AWDL et pour les utilisateurs finaux, il semble que c'est votre infrastructure Wi-Fi qui est de mauvaise qualité alors qu'en réalité c'est la combinaison de leur application VPN avec le protocole de gouttes d'air qui provoque le basculement. Si la désactivation du Bluetooth sur le client résout le problème, il ne s'agit pas d'un problème côté Wi-Fi.
Un autre exemple bien connu est Apple SideCar où vous pouvez utiliser votre iPad pour étendre votre écran d'ordinateur à un autre moniteur. Cela peut entraîner une utilisation RF importante car la transmission en continu est continue et peut utiliser une largeur de canal importante.

WiPS

WiPS couvre des vecteurs d'attaque plus avancés que la simple détection de la présence d'un périphérique non autorisé. En plus de ces attaques, il fournit également parfois un PCAP de l'événement pour l'analyse de la criminalistique.

Bien qu'il s'agisse d'une fonctionnalité de sécurité très utile pour l'entreprise, un réseau public doit faire face à l'éternelle question : que faire contre cela ?

Avec la difficulté de gérer de nombreux clients que vous ne contrôlez pas, il est possible de diviser les alarmes en deux catégories. Les alarmes que vous pouvez décider d'ignorer à partir de Cisco Catalyst Center si vous en voyez trop sont :

- 10001: DoS : Alarme De Flottement D'Authentification
- 10002: DoS : Alarme de demande d'association
- 10003: DoS : Alarme d'inondation de sonde de diffusion
- 10004: DoS : Alarme De Dissociation Des Inondations
- 10005: DoS : Alarme De Désassociation De Diffusion
- 10006: DoS : Alarme contre les inondations de désauthentification
- 10007: DOS : Alarme de désauthentification de diffusion
- 10008:  DOS : Alarme d'attaque de déconnexion EAPOL
- 10009: alarme d'inondation CTS
- 10010: Alarme de demande d'association RTS
- 10011: Déluge de désauthentification par paire
- 10021: Session Airdrop (celle-ci se produit généralement beaucoup dans n'importe quel

réseau et décrit simplement une activité d'égal à égal régulière entre les périphériques Apple)
- 10022: Demande d'association incorrecte
- 10023: Échec de l'authentification Inondation par signature
- 10024: OUI MAC non valide par signature
- 10025: Authentification incorrecte

Ces alarmes peuvent être causées par un client qui se comporte mal. Il n'est pas possible d'empêcher automatiquement une attaque par déni de service puisque, essentiellement, vous ne pouvez pas empêcher un client défaillant de maintenir le temps d'antenne occupé. Même si l'infrastructure ignore le client, elle serait toujours en mesure d'utiliser le support et le temps d'antenne pour transmettre, ce qui aurait un impact sur les performances des clients qui l'entourent.

Les autres alarmes sont si spécifiques qu'elles dépeignent très probablement une attaque malveillante réelle et peuvent difficilement se produire en raison de mauvais pilotes client. Il est préférable de continuer à surveiller ces alarmes :

- 10012: Balise floue
- 10013: Demande de sonde floue
- 10014: Réponse de sonde floue
- 10015: Inondation du sondage PS par signature
- 10016: EAPOL Start V1 Flood par signature
- 10017: Inondation de la demande de réassociation par destination
- 10018: Inondation de balise par signature
- 10019: Inondation de réponse de sonde par destination
- 10020: Blocage de l'accusé de réception par signature
- 10026/10027 : Attaque RTS et CTS Virtual Carrier Sense

L'infrastructure sans fil peut parfois prendre des mesures d'atténuation, telles que le blocage de la liste du périphérique en cause, mais la seule véritable action pour se débarrasser d'une telle attaque est d'y aller physiquement et de retirer le périphérique en cause.

Il est conseillé d'activer toutes les formes d'exclusion des clients pour économiser le temps d'antenne perdu en interagissant avec les clients défaillants.

Clients à limitation de débit

Il est tentant pour la direction et les administrateurs d'envisager des utilisateurs de limitation de débit afin d'empêcher un utilisateur de monopoliser la bande passante à un emplacement spécifique. Cependant, il a été prouvé sur le terrain à de nombreuses reprises qu'il est plus efficace, du point de vue du temps d'antenne global, de ne pas limiter le débit. Plus vite les

utilisateurs accèdent au réseau et effectuent leurs activités, et plus vite ils sont également hors du réseau. Les vitesses de transfert à limitation de débit n'empêchent pas un utilisateur d'effectuer des transferts de fichiers volumineux, elles les ralentissent simplement et abandonnent des paquets dans le processus, ce qui signifie que le temps d'antenne total gaspillé est encore plus généralement que sans aucune limitation. La limitation du débit sur le réseau sans fil est effectuée en abandonnant des paquets après que le point d'accès a transféré une certaine quantité de paquets dans une certaine fenêtre temporelle en provenance d'un client, si vous ne faites pas cela par application, vous risquez d'abandonner le trafic important du client. Mais si vous faites cela par application, cela peut avoir un effet différent de ce que vous voulez car certaines applications utilisent plusieurs connexions et cela peut compliquer le calcul du débit pour cette application. Les experts de Cisco CX conseillent d'abandonner complètement certaines applications que vous ne souhaitez pas plutôt que d'utiliser la limitation de débit. Cette question est également traitée dans la documentation Cisco Wireless Meraki Cloud : https://documentation.meraki.com/Wireless/Operate_and_Maintain/How_Tos/Firewall_and_Traffic_Shapin

ainsi que dans la documentation Cisco Wireless Catalyst https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215441-configure-qos-rate-limiting-on-catalyst.html

Restriction de l'accès client

Il est conseillé d'activer le blocage peer-to-peer sur tous vos WLAN (sauf si vous avez des exigences strictes en matière de communication client-à-client, mais cela doit être soigneusement étudié et peut-être limité). Cette fonctionnalité empêche les clients du même WLAN de se contacter. Ce n'est pas une solution parfaite car les clients sur différents WLAN peuvent toujours se contacter et les clients appartenant à différents WLC dans le groupe de mobilité peuvent également contourner cette restriction. Mais il constitue une première couche de sécurité et d'optimisation simple et efficace. Un autre avantage de cette fonctionnalité de blocage peer-to-peer est qu'elle empêche également le protocole ARP client à client, ce qui empêche les applications de détecter d'autres périphériques sur le réseau local. Sans blocage peer-to-peer, l'installation d'une application simple sur le client peut afficher tous les autres clients connectés au sous-réseau avec éventuellement leur adresse IP et leurs noms d'hôte.

En outre, il est recommandé d'appliquer une liste de contrôle d'accès IPv4 et IPv6 (si vous utilisez IPv6 sur votre réseau) sur vos réseaux locaux sans fil pour empêcher la communication client à client. L'application d'une liste de contrôle d'accès qui bloque la communication client-client au niveau du WLAN fonctionne, que vous ayez ou non des interfaces SVI client.

L'autre étape obligatoire consiste à empêcher l'accès du client sans fil à toute forme de gestion de votre contrôleur sans fil.

Exemple :

```
ip access-list extended ACL_DENY_CLIENT_VLANS
 10 deny ip any 10.131.0.0 0.0.255.255
 20 deny ip 10.131.0.0 0.0.255.255 any
 30 deny ip any 10.132.0.0 0.0.255.255
 40 deny ip 10.132.0.0 0.0.255.255 any
 50 deny ip any 10.133.0.0 0.0.255.255
 60 deny ip 10.133.0.0 0.0.255.255 any
 70 deny ip any 10.134.0.0 0.0.255.255
 80 deny ip 10.134.0.0 0.0.255.255 any
 90 deny ip any 10.135.0.0 0.0.255.255
 100 deny ip 10.135.0.0 0.0.255.255 any
 110 deny ip any 10.136.0.0 0.0.255.255
 120 deny ip 10.136.0.0 0.0.255.255 any
 130 deny ip any 10.137.0.0 0.0.255.255
 140 deny ip 10.137.0.0 0.0.255.255 any
 150 permit ip any any
```

Cette liste de contrôle d'accès peut être appliquée à l'interface de gestion SVI :

```
interface Vlan130
 ip access-group ACL_DENY_CLIENT_VLANS in
```

Ceci est fait sur un WLC avec les VLAN client 131 à 137 créés dans la base de données VLAN de couche 2 mais sans aucune SVI correspondante, et une seule SVI existe pour le VLAN 130 qui est la façon dont le WLC est géré. Cette ACL empêche tous les clients sans fil d'envoyer tout trafic aux plans de gestion et de contrôle WLC complètement. N'oubliez pas que la gestion SSH ou de l'interface utilisateur Web n'est pas la seule chose que vous devez autoriser, car une connexion CAPWAP vers tous les points d'accès doit également être autorisée. C'est pourquoi cette ACL a une autorisation par défaut, mais bloque les plages de clients sans fil, plutôt que de compter sur une action par défaut deny all qui nécessiterait de spécifier toutes les plages de sous-réseaux AP et les plages de gestion autorisées.

De même, vous pouvez créer une autre liste de contrôle d'accès qui spécifie tous les sous-réseaux de gestion possibles :

```
ip access-list standard ACL_MGMT
 10 permit 10.128.0.0 0.0.255.255
 20 permit 10.127.0.0 0.0.255.255
 30 permit 10.100.0.0 0.0.255.255
 40 permit 10.121.0.0 0.0.255.255
 50 permit 10.141.0.0 0.0.255.255
```

Vous pouvez ensuite appliquer cette liste de contrôle d'accès pour l'accès CLI :

```
line vty 0 50
 access-class ACL_MGMT in
 exec-timeout 180 0
 ipv6 access-class ACL_IPV6_MGMT in
 logging synchronous
 length 0
 transport preferred none
 transport input ssh
 transport output ssh
```

La même liste de contrôle d’accès peut également être appliquée pour l’accès administrateur Web.

Protection contre les tempêtes de trafic

Les multidiffusions et les diffusions sont plus utilisées par certaines applications que d'autres. Lorsque vous envisagez un réseau uniquement filaire, la seule précaution à prendre consiste souvent à se protéger contre les tempêtes de diffusion. Cependant, une multidiffusion est aussi douloureuse qu'une diffusion lorsqu'elle est envoyée en direct et il est important de comprendre pourquoi. Tout d'abord, imaginez un paquet envoyé (par diffusion ou multidiffusion) à tous vos clients sans fil, qui s'ajoute rapidement à de nombreuses destinations. Chaque point d’accès doit alors transmettre cette trame par voie hertzienne de la manière la plus fiable possible (bien qu’elle ne soit pas garantie comme fiable) et cela est obtenu en utilisant un débit de données obligatoire (il est configurable quel est le débit obligatoire utilisé). En termes simples, cela signifie que la trame est envoyée à l’aide d’un débit de données OFDM (802.11a/g), ce qui n’est évidemment

pas très pratique.

Dans un grand réseau public, il est déconseillé de se fier à la multidiffusion pour préserver le temps d'antenne. Cependant, dans un réseau d'entreprise de grande taille, vous pouvez avoir besoin de maintenir la multidiffusion activée pour une application spécifique, bien que vous deviez la contrôler autant que possible pour limiter son impact. Il est conseillé de documenter les détails de l'application, l'adresse IP de multidiffusion, et de veiller à bloquer les autres formes de multidiffusion. Comme expliqué précédemment, l'activation du transfert multidiffusion n'est pas une condition requise pour activer IPv6. Il est préférable de désactiver complètement le transfert de diffusion. Les diffusions sont parfois utilisées par les applications pour détecter d'autres périphériques sur le même sous-réseau, ce qui constitue clairement un problème de sécurité dans un grand réseau.

Si vous activez le transfert multidiffusion global, assurez-vous d'utiliser le paramètre CAPWAP de point d'accès multidiffusion-multidiffusion. Lorsque cette option est activée, lorsque le WLC reçoit un paquet de multidiffusion de l'infrastructure filaire, il l'envoie à tous les AP intéressés avec un seul paquet de multidiffusion, ce qui permet d'économiser beaucoup de duplication de paquets. Assurez-vous de définir une adresse IP de multidiffusion CAPWAP différente pour chacun de vos WLC, sinon les AP reçoivent le trafic de multidiffusion d'autres WLC, ce qui n'est pas souhaité.

Si vos points d'accès se trouvent dans d'autres sous-réseaux de votre interface de gestion sans fil du WLC (qui est probablement dans un grand réseau), vous devez activer le routage de multidiffusion sur votre infrastructure filaire. Vous pouvez vérifier que tous vos AP reçoivent correctement le trafic de multidiffusion avec la commande :

```
show ap multicast mom
```

Il est également conseillé d'activer la multidiffusion IGMP (pour la multidiffusion IPv4) et MLD (pour IPv6) dans tous les cas si vous devez compter sur la multidiffusion. Ils permettent uniquement aux clients sans fil intéressés (et donc uniquement aux points d'accès qui ont des clients intéressés) de recevoir le trafic de multidiffusion. Le WLC transmet l'enregistrement par proxy au trafic de multidiffusion et s'occupe de maintenir l'enregistrement actif, déchargeant ainsi les clients.

## Conclusion

Les grands réseaux publics sont complexes, chacun est unique et présente des exigences et des résultats spécifiques.

Le respect des instructions de ce document constitue un excellent point de départ et vous aide à

réussir votre déploiement tout en évitant les problèmes les plus courants. Cependant, les lignes directrices ne sont que des lignes directrices et peuvent exiger d'être interprétées ou ajustées dans le contexte du lieu spécifique.

Cisco CX dispose d'équipes de professionnels sans fil dédiés aux grands déploiements sans fil, avec une expérience dans de nombreux grands événements, y compris des événements sportifs et des conférences. Contactez l'équipe chargée de votre compte pour obtenir de l'aide.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.