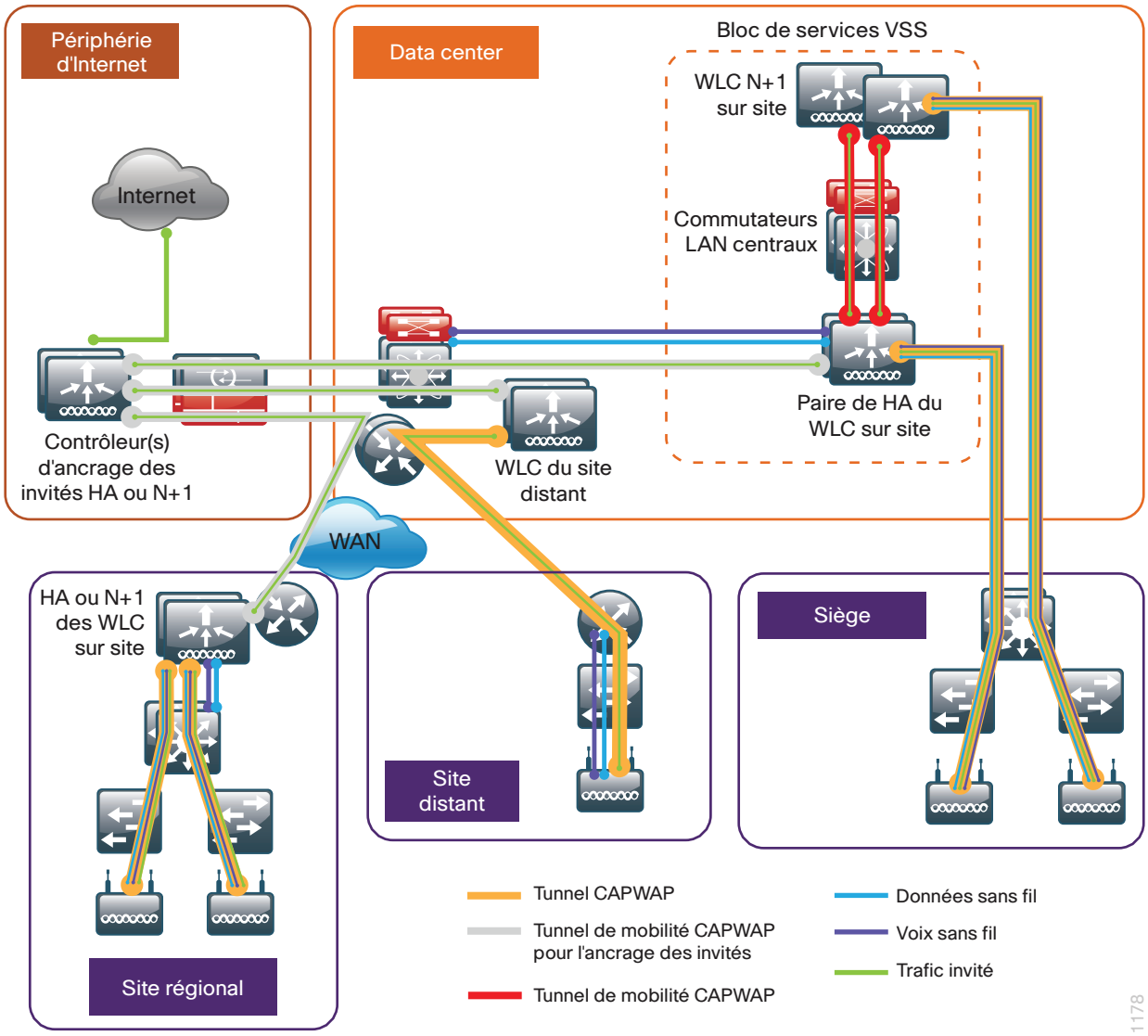
Résumé du guide de conception d'un LAN de campus sans fil

Le LAN de campus sans fil tel que défini dans ce guide de conception permet aux collaborateurs de bénéficier à tout moment d'une connectivité pour les communications vocales et l'accès aux données, et offre un accès sans fil à Internet aux invités. Où qu'ils se trouvent dans l'entreprise, sur un vaste campus et sur un site distant, les utilisateurs sans fil bénéficient de la même expérience lorsqu'ils se connectent à des services de données, voix et vidéo.

Voici quelques-uns des avantages du LAN de campus sans fil :

- **Des gains de productivité grâce à un accès réseau sécurisé et indépendant du lieu** : améliorations tangibles de la productivité et communication.
- **Un réseau plus flexible :** possibilité de connecter à moindre coût les lieux difficiles à câbler par le biais du sans fil.
- **Un déploiement économique :** adoption de technologies virtualisées au sein de l'architecture sans fil globale.
- **Une gestion et une exploitation simplifiées :** possibilité de contrôler un environnement sans fil distribué à partir d'un point central.
- **Une mise en service rapide :** provisionnement automatique possible lorsqu'un point d'accès est connecté au réseau filaire associé.
- **Une conception résiliente et tolérante aux pannes :** connectivité sans fil fiable dans les environnements stratégiques, incluant une gestion complète du spectre RF.
- **Une prise en charge des utilisateurs sans fil :** modèles de conception BYOD (bring your own device).
- **L'efficacité du trafic multidiffusion :** prise en charge de nombreuses applications de communication, notamment de vidéo et « push to talk ».

Figure 1 - Présentation de la technologie sans fil



Le LAN de campus sans fil est conçu autour de deux composants principaux :

- Les contrôleurs LAN sans fil Cisco
- Les points d'accès légers Cisco

Contrôleurs LAN sans fil Cisco

Le LAN de campus sans fil est basé sur des contrôleurs LAN sans fil Cisco (WLC) qui simplifient la gestion du réseau et permettent de centraliser la configuration et le contrôle des points d'accès sans fil. Grâce à cette approche, le LAN sans fil (WLAN) peut fonctionner comme un réseau d'information intelligent et prendre en charge des services avancés. Voici certains des avantages de la conception basée sur les contrôleurs :

- **Des dépenses d'exploitation réduites :** configuration des points d'accès légers sans intervention ; une conception simple des paramètres des canaux et d'alimentation ainsi qu'une gestion en temps réel, avec identification des trous de couverture RF afin d'optimiser l'environnement RF ; une mobilité transparente sur les divers points d'accès du groupe de mobilité ; et une vue d'ensemble du réseau, permettant de prendre des décisions en matière d'évolutivité, de sécurité et d'opérations globales.
- **Un meilleur ROI :** possibilité de virtualiser les instances du contrôleur LAN sans fil, réduisant ainsi le TCO grâce à l'investissement réalisé dans la virtualisation.
- **Une évolutivité simplifiée grâce à une conception optimale :** bonne évolutivité du réseau, via la prise en charge d'une conception en mode local pour les environnements de type campus et d'une conception Cisco FlexConnect adaptée aux sites distants.
- **La commutation avec état pour la haute disponibilité :** permet d'établir une connectivité sans perturbation aux appareils clients sans fil en cas de panne d'un contrôleur LAN sans fil.

Les contrôleurs LAN sans fil Cisco sont responsables des fonctions WLAN à l'échelle du système, notamment des politiques de sécurité, de la prévention des intrusions, de la gestion RF, de la qualité de service (QoS) et de la mobilité. Ils fonctionnent conjointement avec les points d'accès légers Cisco pour la prise en charge des applications sans fil stratégiques. Des services de données et voix au suivi des emplacements, les contrôleurs LAN sans fil Cisco fournissent aux gestionnaires réseau les niveaux de contrôle, d'évolutivité, de sécurité et de fiabilité dont ils ont besoin pour concevoir des réseaux sans fil évolutifs et sécurisés.

Même si un contrôleur indépendant peut prendre en charge des points d'accès légers sur plusieurs étages et dans plusieurs bâtiments simultanément, déployez les contrôleurs par paire pour une meilleure résilience. Vous pouvez configurer la résilience des contrôleurs de différentes manières. La méthode la plus simple consiste à utiliser un modèle primaire/secondaire dans lequel tous les points d'accès du site rejoignent de préférence le contrôleur principal et ne rejoignent le contrôleur secondaire qu'en cas de défaillance.

Les contrôleurs suivants sont inclus dans le LAN de campus sans fil :

- Contrôleur LAN sans fil de la gamme Cisco 2500
- Contrôleur LAN sans fil de la gamme Cisco 5500
- Modules Cisco WiSM2 (Wireless Services Module 2)
- Contrôleur LAN sans fil de la gamme Cisco 5760
- Contrôleur LAN sans fil virtuel Cisco
- Contrôleur cloud de la gamme Cisco Flex 7500

La flexibilité associée aux licences logicielles vous permet d'ajouter des points d'accès supplémentaires à mesure que les impératifs commerciaux évoluent. Par conséquent, vous pouvez choisir le contrôleur qui répondra à vos besoins à long terme, mais acheter des licences de point d'accès incrémentielles uniquement lorsque vous en avez besoin.

Points d'accès légers Cisco

Au sein des architectures réseau sans fil unifié Cisco, les points d'accès sont *légers*. En d'autres termes, ils ne peuvent pas fonctionner indépendamment d'un contrôleur LAN sans fil. Lorsque le point d'accès communique avec le contrôleur LAN sans fil, il télécharge sa configuration et synchronise son image de logiciel ou de micrologiciel.

Les points d'accès légers Cisco fonctionnent avec un contrôleur LAN sans fil Cisco pour connecter des appareils sans fil au LAN. Ils prennent en charge des fonctions simultanées de transfert de données et de contrôle d'environnement radio. Le LAN de campus sans fil repose sur les points d'accès sans fil Cisco de deuxième génération, qui offrent une couverture du réseau sans fil avec un débit jusqu'à 9 fois supérieur à celui des réseaux 802.11a/b/g. Les points d'accès suivants sont inclus dans le LAN de campus sans fil :

- Points d'accès de la gamme Cisco Aironet 1600
- Points d'accès de la gamme Cisco Aironet 2600
- Points d'accès de la gamme Cisco Aironet 3600
- Points d'accès de la gamme Cisco Aironet 3700

C'est la prise en charge de deux technologies clés qui différencie les points d'accès du LAN de campus sans fil tel que défini dans le guide de conception :

- **La technologie Cisco CleanAir :** fournit aux responsables IT une visibilité sur leur spectre radio et leur permet de gérer les interférences RF et d'empêcher les temps d'arrêt inattendus. Cisco CleanAir permet de protéger les performances des réseaux 802.11n. Cette technologie utilisant des données de puce électronique crée un réseau sans fil doté de capacités d'auto-réparation et d'auto-optimisation qui limitent l'impact des interférences sans fil. Pour plus d'informations sur Cisco CleanAir, voir la section Technologie CleanAir sans fil de campus.
- **Le 802.11ac :** la spécification IEEE 802.11ac Wave 1 améliore considérablement les performances du réseau sans fil. Pour plus d'informations sur la spécification 802.11ac, voir les sections Performances de la bande passante 802.11ac et Planification des canaux 802.11ac.

Tableau 1 - Prise en charge des points d'accès pour la technologie Cisco CleanAir et la spécification IEEE 802.11ac

Point d'accès de la gamme Cisco Aironet	Prise en charge de Cisco CleanAir	Prise en charge 802.11ac
1600	Non[1]	Non
2600	Oui	Non
3600	Oui	Oui[2]
3700	Oui	Oui

[1]Les points d'accès de la gamme Cisco Aironet 1600 peuvent prendre en charge la technologie CleanAir Express, qui n'est pas incluse dans le LAN de campus sans fil défini dans le guide de conception.

[2]Les points d'accès de la gamme Cisco Aironet 3600 peuvent prendre en charge le 802.11ac si le module radio adaptatif 802.11ac Wave 1 est installé.

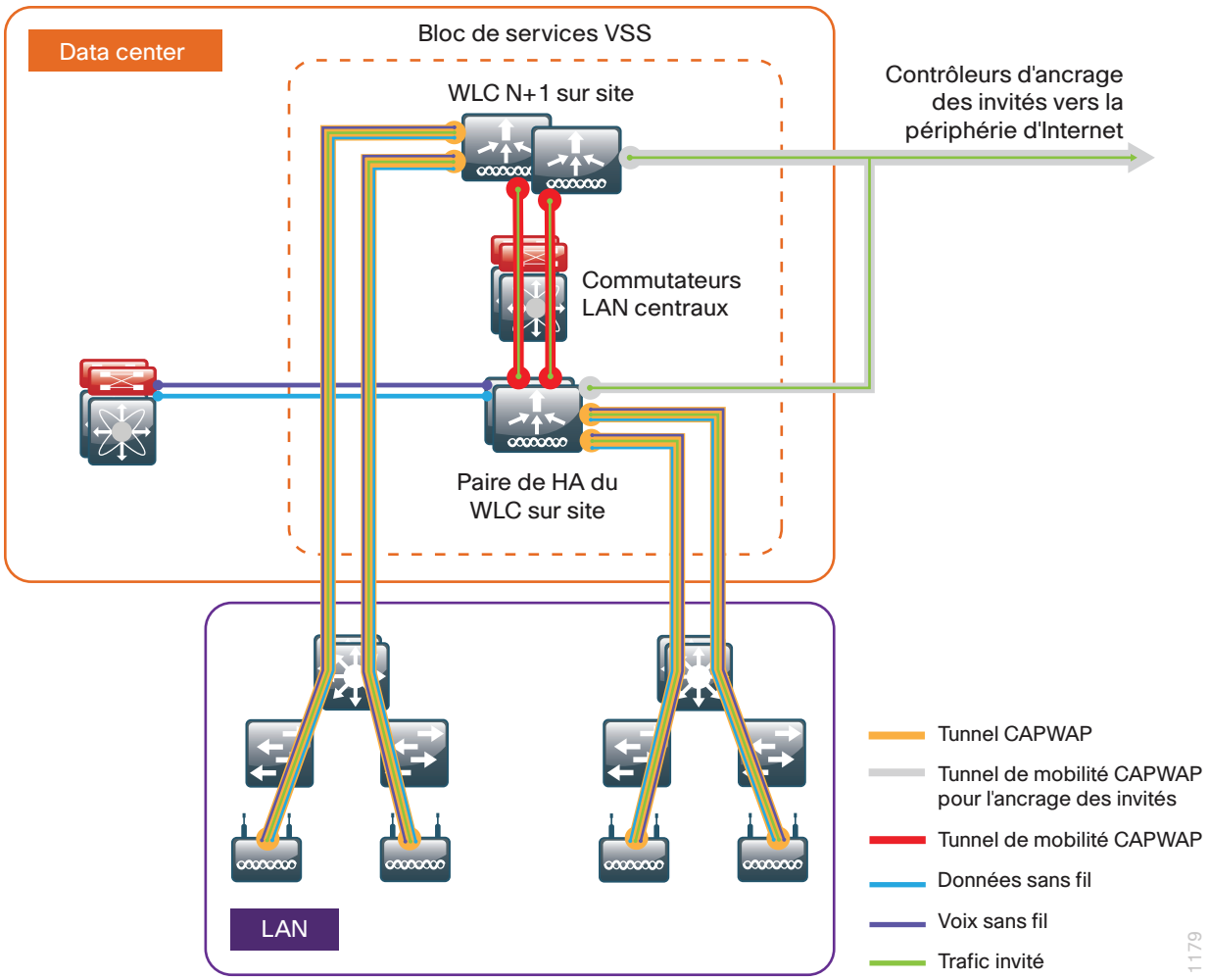
Modèles de conception sans fil

Les réseaux sans fil unifiés Cisco prennent en charge deux modèles pour les environnements de type campus : le mode local et Cisco FlexConnect.

Modèle de conception en mode local

Dans ce type de modèle, le contrôleur LAN sans fil et les points d'accès partagent les mêmes locaux. Le contrôleur LAN sans fil peut être connecté à un bloc de services de data center ou à une couche de distribution LAN. Le trafic sans fil entre les clients LAN sans fil et le LAN est transmis via le protocole CAPWAP (Control and Provisioning of Wireless Access Points) entre le contrôleur et le point d'accès sans fil.

Figure 2 - Modèle de conception en mode local



Une architecture en mode local utilise le contrôleur comme point unique de gestion des fonctions de sécurité et des politiques réseau sans fil de couche 2. Elle permet également l'application cohérente et coordonnée des services au niveau du trafic filaire et sans fil.

Outre les avantages traditionnels que représente l'approche de réseau sans fil unifié Cisco, le modèle de conception en mode local répond aux exigences clients suivantes :

- **La mobilité transparente** : permet une itinérance rapide sur le campus, afin que les utilisateurs restent connectés à leur session même en cas de déplacement entre divers étages ou bâtiments adjacents dépendant de sous-réseaux différents.
- **La prise en charge multimédia :** augmente la robustesse de la voix grâce au contrôle d'admission des appels (CAC, Call Admission Control) et à la multidiffusion avec la technologie Cisco VideoStream.
- **La gestion centralisée des politiques :** permet une inspection intelligente via l'utilisation de pare-feu, ainsi que l'inspection des applications, le contrôle d'accès au réseau, la mise en application des politiques et la classification correcte du trafic.

Si l'**une** des affirmations suivantes s'applique à un site, vous devriez y déployer un contrôleur localement :

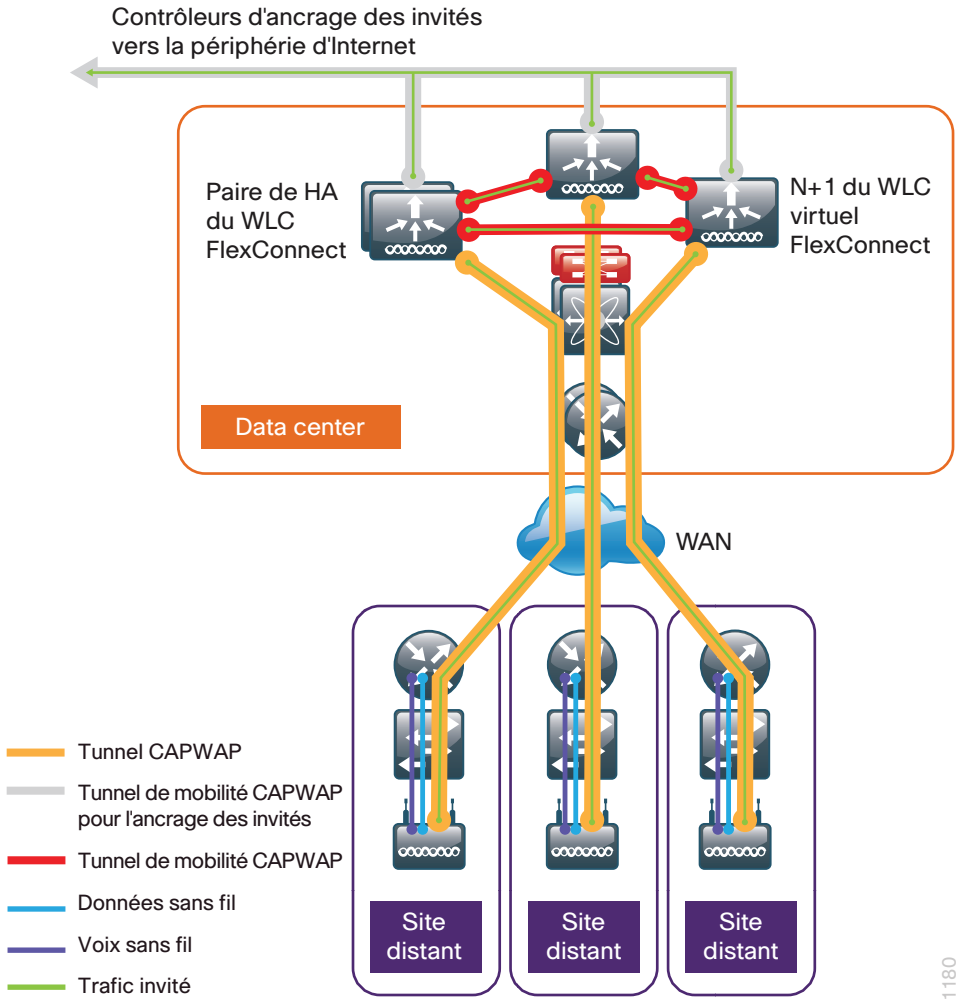
- Le site possède un data center.
- Le site possède une couche de distribution LAN.
- Le site possède plus de 50 points d'accès.
- Le site présente une latence WAN supérieure à 100 ms (aller-retour vers un contrôleur partagé spécifique).

Pour un déploiement utilisant ces caractéristiques, utilisez un contrôleur LAN sans fil des gammes Cisco 2500, 5500, WiSM2 ou 5700. En termes de résilience, le réseau du guide de conception d'un LAN de campus sans fil utilise au moins deux contrôleurs LAN sans fil dans le campus. Des contrôleurs LAN sans fil supplémentaires peuvent être ajoutés afin de fournir une capacité et une résilience additionnelles à la conception.

Modèle de conception Cisco FlexConnect

Cisco FlexConnect est une solution sans fil destinée aux déploiements de sites distants. Grâce à cette solution, les entreprises peuvent configurer et contrôler les points d'accès des sites distants depuis le siège via le WAN, sans déployer de contrôleur sur chaque site distant. Le point d'accès Cisco FlexConnect peut commuter le trafic de données client hors de son interface filaire et utiliser les solutions de trunking 802.1Q pour segmenter plusieurs WLAN. Le VLAN natif du trunk est utilisé pour toutes les communications CAPWAP entre le point d'accès et le contrôleur. Ce mode de fonctionnement est désigné sous le nom de commutation locale FlexConnect. Il s'agit du mode de fonctionnement décrit dans ce guide.

Figure 3 - Modèle de conception Cisco FlexConnect



Cisco FlexConnect peut également retransmettre le trafic au contrôleur centralisé, spécifiquement utilisé pour l'accès invité sans fil.

Vous pouvez avoir recours à une paire de contrôleurs partagés ou à une paire de contrôleurs dédiés pour déployer Cisco FlexConnect.

Dans un modèle avec contrôleurs partagés, les points d'accès en mode local et en mode FlexConnect configurés partagent un contrôleur commun. Une architecture avec contrôleurs partagés requiert la prise en charge par le LAN sans fil de la commutation locale FlexConnect et du mode local. Les contrôleurs LAN sans fil compatibles présentés dans ce guide de conception validée par Cisco (CVD) sont les contrôleurs sans fil des gammes Cisco WiSM2, 5500 et 2500. Si vous utilisez déjà une paire de contrôleurs en mode local sur le même site que l'agrégation WAN et que cette paire possède une capacité supplémentaire suffisante pour prendre en charge les points d'accès Cisco FlexConnect, vous pouvez effectuer un déploiement partagé.

Si l'environnement ne répond pas aux exigences associées à un contrôleur partagé, vous pouvez déployer une paire de contrôleurs HA dédiés en utilisant un contrôleur de cloud de la gamme Cisco Flex 7500, un contrôleur Cisco 5500 ou WiSM2. Les contrôleurs doubles résilients configurés dans un modèle de redondance N+1 peuvent être utilisés : avec le contrôleur LAN sans fil de la gamme Cisco 2500 ou le contrôleur LAN sans fil virtuel Cisco. Le contrôleur doit résider dans le data center.

Si **toutes** les affirmations suivantes sont correctes concernant un site, déployez Cisco FlexConnect sur ce site :

- Le LAN du site se compose d'une pile de commutateurs ou d'un seul commutateur de couche d'accès.
- Le site possède moins de 50 points d'accès.
- Le site présente une latence WAN inférieure à 100 ms (aller-retour vers le contrôleur partagé).

Haute disponibilité

Avec l'influence grandissante de la mobilité tant dans nos vies personnelle que professionnelle, la disponibilité du réseau reste une priorité. Dans le réseau du guide de conception d'un LAN de campus sans fil, la haute disponibilité est assurée via l'utilisation de contrôleurs résilients au sein d'un même groupe de mobilité.

Cisco AireOS prend en charge la commutation avec état des points d'accès et la commutation avec état du client. Ces deux fonctions sont rassemblées sous le terme SSO haute disponibilité (SSO HA). Avec le modèle de licence économique SSO HA, les déploiements sans fil Cisco améliorent la disponibilité du réseau sans fil et, en cas de perturbation du contrôleur LAN, garantissent des délais de reprise inférieurs à la seconde. En outre, la fonction SSO HA permet au contrôleur LAN sans fil résilient de bénéficier de licences économiques de contrôleur de secours résilient. Le nombre de licences de point d'accès est automatiquement hérité du contrôleur LAN sans fil principal qui lui est appairé. Pour en profiter, achetez un contrôleur de secours résilient en utilisant la référence HA disponible pour les contrôleurs LAN sans fil des gammes Cisco 5500, 7500 et WiSM2. Pour bénéficier de la prise en charge de la fonction SSO HA avec la famille de contrôleurs WiSM2, vous devez déployer les deux contrôleurs LAN sans fil WiSM2 dans l'une des configurations suivantes :

- Dans une paire de commutateurs de la gamme Cisco Catalyst 6500 configurés pour fonctionner dans un système de commutation virtuelle (VSS)
- Dans le même châssis de commutateurs de la gamme Cisco Catalyst 6500
- Dans un autre châssis de commutateurs de la gamme Cisco Catalyst 6500 en cas d'extension du VLAN de redondance de couche 2

Les mises à niveau logicielles et la configuration du contrôleur LAN sans fil principal sont synchronisées automatiquement avec le contrôleur LAN sans fil de secours résilient.

Le tableau suivant présente les contrôleurs compatibles avec la fonction SSO HA.

Tableau 2 - Prise en charge des fonctions de haute disponibilité

Modèle Cisco WLC	SSO HA	Redondance N+1	Groupe d'agrégation de liaisons (LAG)
vWLC	Non	Oui	Oui (via VMWare)
2500	Non	Oui	Oui
5500	Oui	Oui	Oui
WiSM2	Oui	Oui	S/O
5760	Oui[1]	Oui	Oui
7500 Flex	Oui	Oui	Oui

[1]Le contrôleur LAN sans fil de la gamme Cisco 5760 prend en charge la commutation avec état des points d'accès (AP SSO) grâce au câble d'empilage.

Prise en charge de la multidiffusion

L'utilisation des applications voix et vidéo continue à progresser en raison du nombre toujours croissant de smartphones, de tablettes et d'ordinateurs connectés aux réseaux sans fil, et ce, dans tous les domaines de la vie quotidienne. Dans chacun des modèles de conception sans fil, la prise en charge de la multidiffusion, courante sur un réseau filaire, est désormais possible. La multidiffusion est une condition requise pour mettre en œuvre la fourniture efficace de certaines applications de type un à plusieurs, comme la vidéo et les communications groupées utilisant la fonction « push to talk ». Grâce à l'extension de la prise en charge de la multidiffusion au-delà du campus et du data center, les utilisateurs mobiles peuvent désormais utiliser des applications de multidiffusion.

Le LAN de campus sans fil prend en charge la transmission multidiffusion du contrôleur sur site via l'utilisation du mode multidiffusion-multidiffusion, qui utilise une adresse IP de multidiffusion afin de transmettre plus efficacement les flux de multidiffusion aux points d'accès sur lesquels des utilisateurs sans fil sont abonnés à un groupe de multidiffusion particulier. Le mode multidiffusion-multidiffusion est pris en charge dans cette conception validée par Cisco avec les contrôleurs LAN sans fil des gammes Cisco 2500, 5500, WiSM2 et 5760.

Les sites distants utilisant le contrôleur de cloud de la gamme Cisco Flex 7500 ou Cisco vWLC avec Cisco FlexConnect en mode de commutation locale peuvent également bénéficier de l'utilisation d'applications de multidiffusion. Sur les sites distants, la multidiffusion tire parti de la prise en charge du trafic de multidiffusion par le WAN et le LAN sous-jacents. Lorsque cette méthode est combinée à des points d'accès en mode FlexConnect avec commutation locale, les abonnés aux flux de multidiffusion reçoivent les données directement par le réseau WAN ou LAN, sans frais supplémentaires au niveau du contrôleur LAN sans fil.

Band Select

Avec l'apparition d'appareils personnels fonctionnant sur la fréquence 2,4 GHz jusque-là utilisée par les appareils industriels, scientifiques et médicaux, le niveau de bruit entraînant des interférences sur cette bande s'est considérablement accru. De même, nombre d'appareils sans fil disponibles aujourd'hui sont des appareils bibandes pouvant fonctionner sur la bande 2,4 GHz ou 5 GHz.

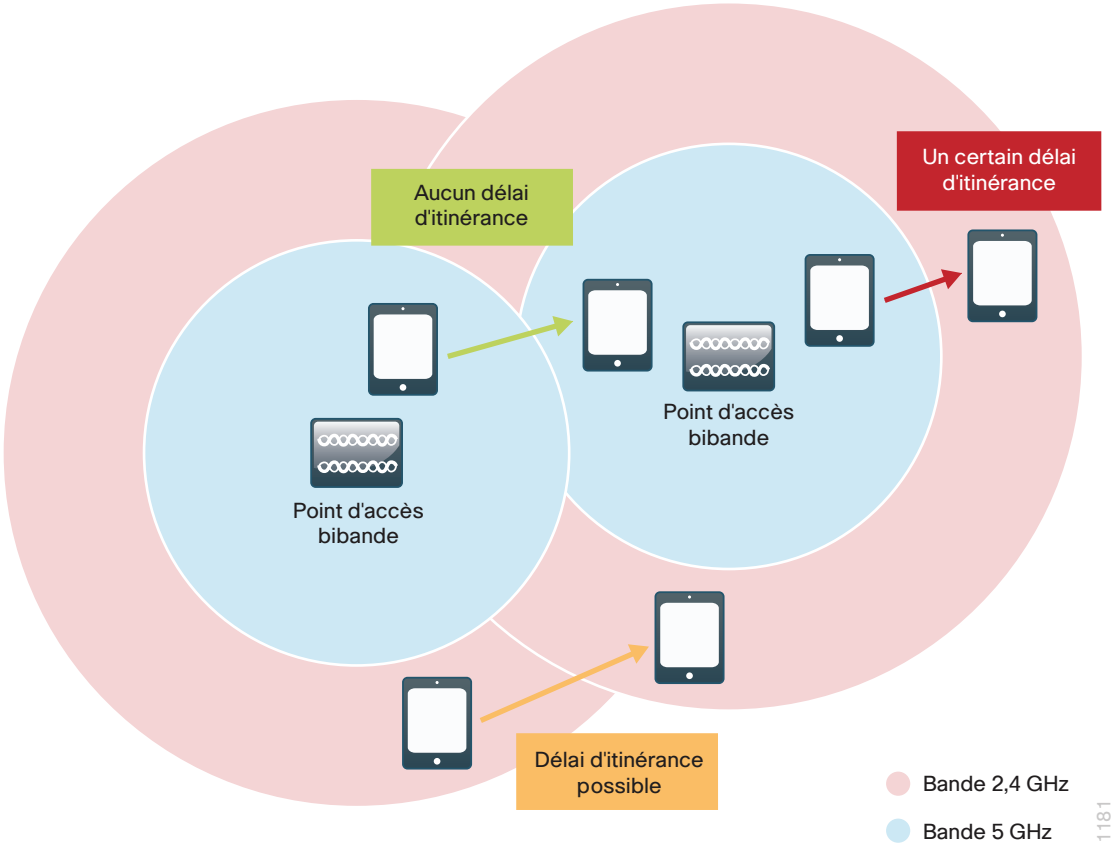
Avec des appareils professionnels critiques, il serait avantageux de forcer une utilisation de la bande 5 GHz, afin de générer moins d'interférences et par conséquent de faire bénéficier les utilisateurs d'une meilleure expérience.

Lorsque les appareils bibandes recherchent un point d'accès, ils envoient souvent d'abord une demande de la sonde sur la bande 2,4 GHz, puis sur la bande 5 GHz quelques millisecondes plus tard. La réponse de la sonde 2,4 GHz est habituellement reçue en premier. De ce fait, de nombreux appareils se connectent en utilisant la bande 2,4 GHz, même si un point d'accès 5 GHz est disponible.

La fonction de sélection de fréquence hertzienne Band Select retarde la réponse de la sonde 2,4 GHz de quelques centaines de millisecondes. Ainsi, le point d'accès peut déterminer si l'appareil sans fil est de type bibande. Un appareil sans fil bibande est détecté lorsqu'une demande de sonde 2,4 GHz et 5 GHz est envoyée depuis le même appareil. En retardant la réponse de la sonde 2,4 GHz et en envoyant en premier celle de la bande 5 GHz, il est possible de forcer le client sans fil à se connecter à la bande de 5 GHz (à privilégier).

Il n'est pas recommandé d'utiliser la fonction Band Select avec les appareils voix et vidéo, car elle cause des retards de réponse aux demandes de la sonde sur la bande 2,4 GHz. Pour les appareils de diffusion en continu en temps réel passant d'une zone 5 GHz à une zone de couverture 2,4 GHz, ou les clients itinérants naviguant entre des points d'accès 2,4 GHz, ce délai peut entraîner une interruption momentanée de la connectivité. Avec les flux de trafic de données uniquement, ce délai est négligeable et il n'a généralement aucune incidence sur l'accès aux applications.

Figure 4 - L'impact de Band Select sur les applications en temps réel



ClientLink

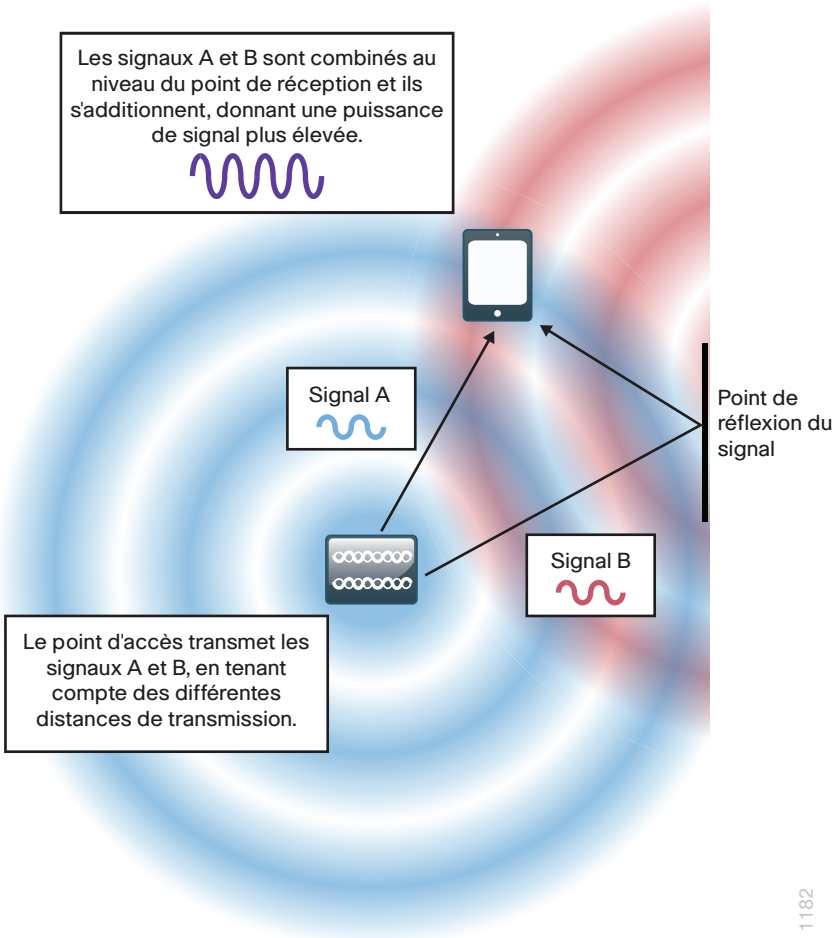
La technologie Cisco ClientLink de connectivité de réseau sans fil utilise la formation de faisceaux (beamforming) pour améliorer le rapport signal/bruit des clients sans fil, sans se limiter à ceux qui prennent en charge le 802.11n. ClientLink améliore le débit entre le point d'accès et le client en réduisant les retransmissions et en facilitant des débits de données plus élevés. En outre, en réduisant la durée d'utilisation du canal RF par tous les clients sans fil, les performances globales du réseau sans fil s'en voient améliorées.

Sur un contrôleur LAN sans fil donné, ClientLink est activé sur une bande radio entière (802.11b ou 802.11a, par exemple) ou par point d'accès.

Tableau 3 - Configuration par défaut et prise en charge de ClientLink

Version ClientLink	Prise en charge des points d'accès	Configuration ClientLink par défaut
3.0	Routeurs d'accès multiservices de la gamme Cisco Aironet 3700	Activée
2.0	Cisco Aironet 1600, 2600 et 3600	Activée
1.0	Cisco Aironet 1140, 3500, 1250 et 1260	Désactivée

Figure 5 - Optimisation ClientLink



Performances de la bande passante 802.11ac

C'est la première fois dans l'histoire de la technologie sans fil basée sur Wi-Fi que de telles améliorations ont été observées en termes de performances : tout cela depuis l'introduction du 802.11ac. En 1997, le standard 802.11 initial a permis d'atteindre des performances théoriques de couche physique (PHY) de 2 Mbit/s. Aujourd'hui, avec l'introduction de la technologie 802.11ac Wave 1 à 3 flux spatiaux (3SS), les performances théoriques maximales passent à 1,3 Gbit/s.

Tableau 4 - Performances de la bande passante 802.11ac

Année	Technologie	Performances PHY théoriques	Performances utilisateur prévues
1997	802.11	2 Mbit/s	1 Mbit/s
1999	802.11b	11 Mbit/s	6 Mbit/s
1999	802.11a	54 Mbit/s	25 Mbit/s
2003	802.11g	54 Mbit/s	25 Mbit/s
2003	802.11a/g	54 Mbit/s	13-25 Mbit/s
2007	802.11n	450 Mbit/s avec 3SS	180-220 Mbit/s
2013	802.11ac Wave 1	1,3 Gbit/s avec 3SS	Jusqu'à 750 Mbit/s
Avenir	802.11ac Wave 2	2,4-3,5 Gbit/s	À définir

Les performances sans fil réelles dépendent d'un certain nombre de variables, comme la distance, l'adaptateur sans fil et l'environnement RF global. En outre, les cellules mixtes adjacentes utilisant le standard 802.11a peuvent entraîner une utilisation plus longue des canaux en raison d'une vitesse de transmission réduite. Lorsqu'un canal 802.11a/n adjacent lié de 40 MHz est déployé avec un canal principal mal aligné, vous ne profitez pas des bénéfices du mécanisme Clear Channel Assessment (CCA).

La spécification 802.11ac Wave 1 inclut un certain nombre de technologies (détaillées ci-dessous) responsables de cette amélioration considérable des performances.

- La spécification 802.11ac est mise en œuvre uniquement sur la bande 5 GHz, plus calme et moins encombrée.
- La technologie 802.11ac utilise une modulation d'amplitude en quadrature 256QAM, ce qui permet d'atteindre 8 bits par symbole et de multiplier les performances par quatre. En d'autres termes, la QAM est une technique de modulation utilisant la phase et l'amplitude des formes d'onde pour encoder les données. La modulation 256QAM utilise 256 symboles, ce qui augmente le débit.
- La technologie 802.11ac étend la largeur des canaux : elle permet d'atteindre des largeurs de 20, 40 et 80 MHz avec la Wave 1 et des largeurs de 20, 40, 80, 80+80 et 160 MHz avec la Wave 2.
- La technique de beamforming, améliorée depuis la spécification 802.11ac Wave 1 et incluse dans la technologie de réseau sans fil Cisco ClientLink, permet au point d'accès d'*orienter le faisceau* ou de diriger une concentration de signaux au niveau du récepteur, qui s'additionnent pour améliorer la qualité et le niveau du signal de ce récepteur. Avec la Wave 2, le beamforming multi-utilisateur permet à un point d'accès unique de transmettre un signal vers quatre clients sans fil simultanément et sur la même fréquence. Chaque client possède ainsi son propre faisceau spatial dédié.

Planification des canaux 802.11ac

Avec l'utilisation des fonctions RRM (Radio Resource Management, gestion des ressources radio) et d'attribution dynamique de canal, l'affectation des canaux est plus simple qu'aux premiers jours du 802.11. Malgré tout, vous devez prendre en compte certains facteurs avant de décider de lier les canaux. Même si le réseau du guide de conception d'un LAN de campus sans fil suppose que vous effectuez un nouveau déploiement, certains administrateurs réseau d'environnements sans fil existants pourraient vouloir procéder plus prudemment et s'assurer que les facteurs de planification des canaux sont pris en compte.

Si votre environnement se limite à des canaux de 20 MHz standard, Cisco vous recommande de procéder par étapes pour passer aux canaux de 80 MHz. La première étape consiste à activer un ensemble de canaux avec sélection de fréquence dynamique (DFS). Pour pouvoir utiliser des canaux DFS, le point d'accès doit rechercher l'utilisation de fréquences radar. Si de tels signaux sont détectés, le point d'accès passe sur un autre canal ou réduit la puissance de transmission. Les canaux DFS permettent l'utilisation d'un spectre RF plus large, en fonction de votre domaine de réglementation. Cela permet ensuite un plus grand choix en termes de liaison des canaux par attribution dynamique.

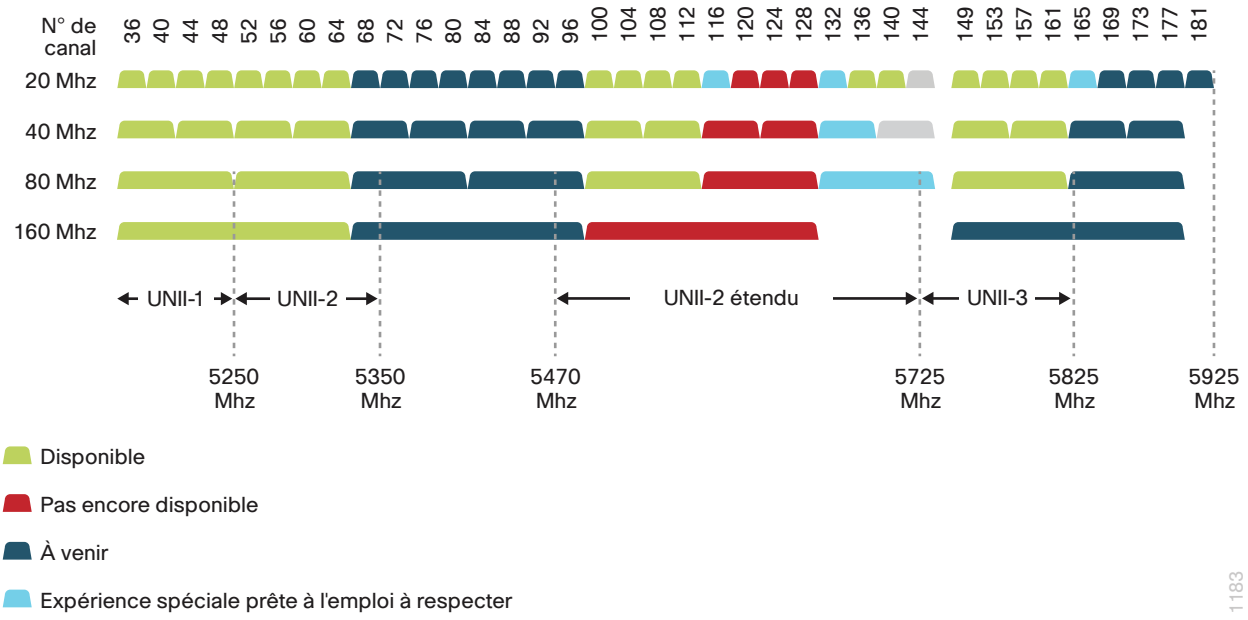
Lorsque les canaux DFS sont activés, quatre canaux de 80 MHz et huit de 40 MHz sont disponibles aux États-Unis.

Tableau 5 - Disponibilité mondiale des canaux 5 GHz

Nombre de canaux disponibles	U.S.A.	UE	Chine	Inde	Japon	Russie
Canaux 20 MHz	18	16	5	13	19	16
Canaux 40 MHz	8	8	2	6	9	8
Canaux 80 MHz	4	4	1	3	4	4

Avec l'arrivée des canaux de 80 MHz dans le 802.11ac Wave 1 et les canaux de 160 MHz à venir avec la Wave 2, vous devez prendre certains facteurs en compte lors de la planification des canaux. Les canaux de 20 MHz se retrouvent en nombre sur la bande 5 GHz, mais cette tendance pourrait s'inverser avec le déploiement de canaux de 80 MHz et de 160 MHz (Wave 2) dans les entreprises. Figure 6 explique les effets de la sélection des canaux de 40 MHz et 80 MHz.

Figure 6 - Utilisation des canaux aux États-Unis



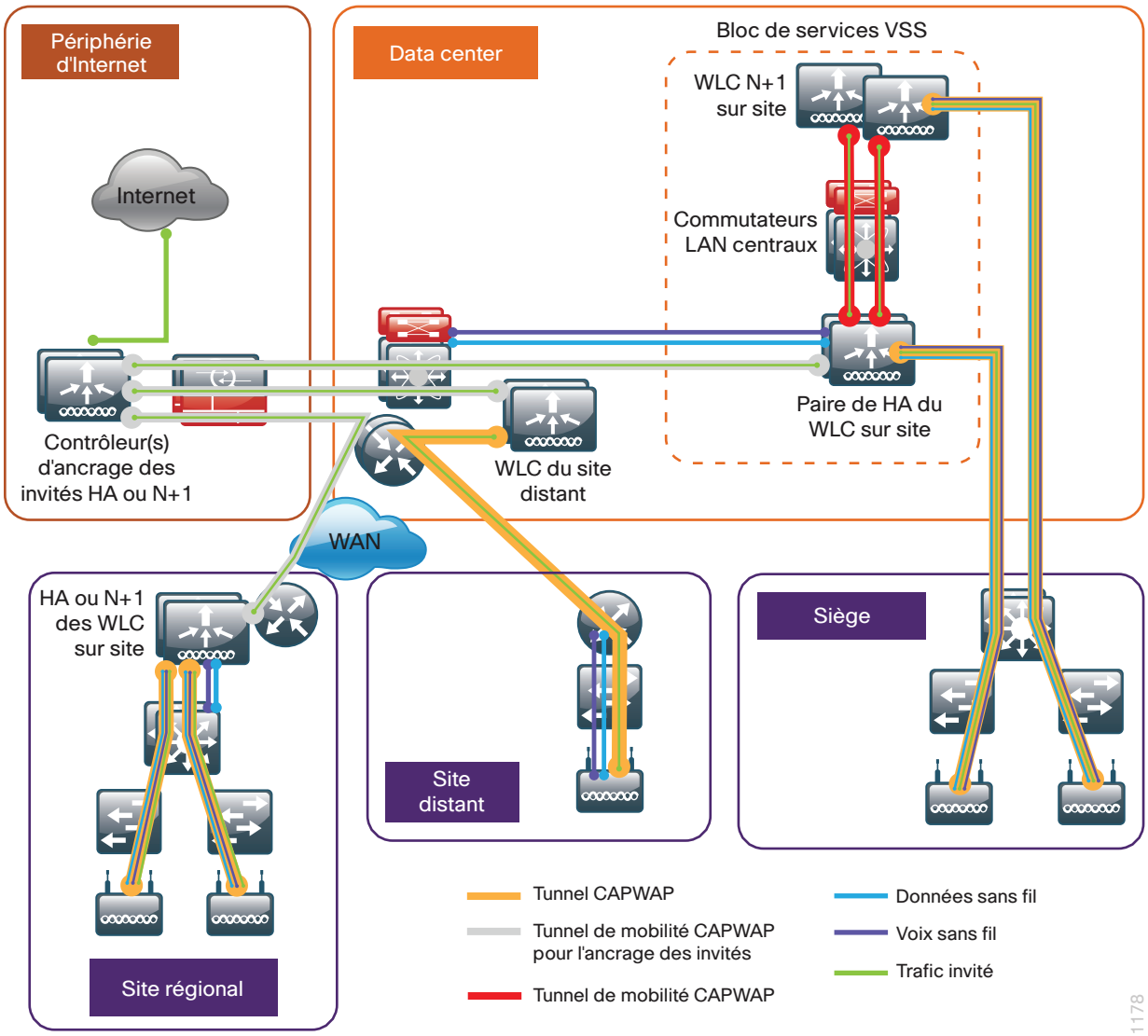
Avec la fonction RRM, le contrôle de puissance de transmission (TPC) et l'attribution dynamique de canal, la sélection de canaux est automatisée et optimisée.

Invité sans fil

L'utilisation du LAN de campus sans fil existant pour fournir l'accès invité est un moyen pratique et économique de permettre aux visiteurs et aux prestataires de se connecter à Internet. Le réseau invité sans fil offre les fonctionnalités suivantes :

- Il fournit un accès à Internet aux invités via un SSID sans fil ouvert, avec un contrôle d'accès web.
- Il prend en charge la création par un utilisateur interne autorisé d'informations d'authentification temporaires pour chaque invité.
- Il isole le trafic du réseau invité de celui du réseau interne afin d'empêcher les invités d'accéder aux ressources réseau internes.
- Il prend en charge les modèles de conception en mode local et Cisco FlexConnect.

Figure 7 - L'essentiel de l'architecture sans fil



Les deux modèles de déploiement de paires de contrôleurs (partagés et dédiés) de la zone démilitarisée (DMZ) en périphérie d'Internet sont pris en charge pour les services invités sans fil présentés dans ce guide CVD.

Si vous utilisez une seule paire de contrôleurs dans toute l'entreprise, et que cette paire est connectée au même commutateur de distribution que le pare-feu en périphérie d'Internet, vous pouvez effectuer un déploiement partagé.

Dans ce type de déploiement, un VLAN est créé sur le commutateur de distribution afin de connecter le trafic invité des contrôleurs LAN sans fil à la zone DMZ de manière logique. Le VLAN invité de la zone DMZ n'est associé à aucune interface virtuelle de commutateur ni interface de couche 3. De ce fait, chaque client sans fil du réseau invité utilise le pare-feu en périphérie d'Internet comme passerelle par défaut.

Si votre environnement ne remplit pas les conditions d'un déploiement partagé, vous pouvez utiliser les contrôleurs LAN sans fil de la gamme Cisco 5500 ou Cisco 2500 pour déployer un contrôleur invité dédié. Le contrôleur se connecte directement à la zone DMZ en périphérie d'Internet, et le trafic invité provenant de tous les autres contrôleurs de l'organisation est transmis vers ce dernier. Les autres contrôleurs LAN sans fil (de la gamme Cisco WiSM2 et Cisco 5760 par exemple) peuvent fournir les services d'ancrage décrits, mais la plupart des entreprises ont recours à d'autres modèles. Par conséquent, ces modèles de déploiement ne sont pas abordés dans le présent guide.

Avec les deux modèles de conception de réseau sans fil invité (partagé et dédié), le pare-feu en périphérie d'Internet restreint l'accès du réseau invité. Ce dernier ne peut accéder qu'à Internet et aux serveurs DHCP et DNS internes.

Ce guide aborde l'utilisation du contrôleur LAN sans fil de la gamme Cisco 5760 en tant que WLC de campus centralisé. Ce contrôleur peut être déployé suivant différents modèles. L'arrivée de l'accès convergent a également permis d'introduire un certain nombre de nouvelles fonctions : Mobility Controller (MC), Mobility Agent (MA) et Mobility Oracle (MO).

Le modèle de déploiement présenté dans ce guide CVD pour le contrôleur LAN sans fil de la gamme Cisco 5760 est similaire à celui de Cisco AireOS (réseau sans fil unifié Cisco). Dans cette architecture, les contrôleurs maintiennent l'utilisation des fonctions MC et MA sur le contrôleur. Les versions à venir sépareront ces fonctions afin de proposer des fonctionnalités d'évolutivité supplémentaires. Cette approche convient à de nombreux déploiements de contrôleurs LAN sans fil de la gamme Cisco 5760, lorsqu'il s'agit de déplacer le MA sur les commutateurs de la gamme Cisco Catalyst 3850/3650, car les commutateurs de couche d'accès sont mis à niveau.

Conceptions de LAN sans fil supplémentaires

Validés dans l'environnement du guide de conception d'un LAN de campus sans fil, le guide de conception de la technologie CleanAir de campus sans fil permet de réduire les interférences RF dans le LAN sans fil, alors que le guide de conception Cisco OfficeExtend favorise la productivité des télétravailleurs.

Technologie CleanAir sans fil de campus

Les utilisateurs sans fil s'attendent à bénéficier d'un accès à Internet sans fil sans problème, atteignant des performances similaires à celles d'un accès filaire. Les interférences RF nuisant aux performances sans fil sont généralement transitoires. Il est souvent impossible de contacter immédiatement un ingénieur IT spécialisé dans les technologies sans fil. À peine le temps de signaler le problème que ce dernier s'est résolu de lui-même.

La technologie Cisco CleanAir, désormais disponible dans chaque point d'accès Cisco CleanAir, analyse le spectre en temps réel pour identifier et localiser les sources des interférences. Cisco CleanAir peut également prendre des mesures en temps réel pour réduire les effets des interférences et ainsi améliorer l'expérience utilisateur sur le réseau sans fil. En cas d'interférences, Cisco CleanAir peut forcer les points d'accès à changer de canal afin de les éviter.

Les événements d'interférence sont automatiquement enregistrés sur le moteur de services de mobilité pour analyse ultérieure. Où que se trouve l'administrateur réseau, il peut accéder aux informations d'analyse du spectre avancée en temps réel et à un historique de ces dernières.

Le guide de conception de la technologie CleanAir de campus sans fil décrit l'installation et l'utilisation du logiciel MetaGeek Chanalyzer, qui permet à l'administrateur réseau d'obtenir une intelligence spectrale Cisco CleanAir détaillée, en temps réel.

Technologie Cisco CleanAir

La technologie Cisco CleanAir permet d'intégrer l'intelligence spectrale RF en temps réel et historique obtenue directement à partir des points d'accès Cisco CleanAir. Avant l'introduction de la technologie CleanAir, les opérateurs devaient porter sur eux un instrument de détection de signaux d'intérêt et localiser eux-mêmes l'emplacement physique de l'appareil qui en était à l'origine. Cisco CleanAir automatise ces tâches en ajoutant des informations détaillées dans les analyseurs de spectre autonomes. Avec l'ajout de l'appareil virtuel Cisco Mobility Services Engine, les opérateurs réseau peuvent accéder aux informations historiques de CleanAir. Une meilleure connaissance des événements RF en dehors des heures de bureau s'avère très utile pour les environnements dont le spectre RF doit être géré en continu, comme les hôpitaux et les environnements de production.

Une solution Cisco CleanAir de base se compose du contrôleur LAN sans fil Cisco et de points d'accès des gammes Cisco Aironet 2600, 3600 ou 3700. Pour profiter de l'ensemble des fonctionnalités CleanAir, l'infrastructure Cisco Prime peut afficher en temps réel les données provenant de CleanAir. Les points d'accès des gammes Cisco 3500 et 1550 peuvent également fournir une intelligence spectrale CleanAir, mais ces modèles ne sont pas décrits dans le guide de conception de la technologie CleanAir de campus sans fil.

Infrastructure Cisco Prime avec Cisco CleanAir

La véritable puissance de cette infrastructure, lorsqu'elle est combinée avec les points d'accès Cisco, réside dans la possibilité pour l'administrateur réseau d'afficher une représentation visuelle de l'intégrité de l'environnement RF. Cela lui permet ainsi de mieux gérer les problèmes et de les résoudre avant qu'ils n'affectent

les utilisateurs du réseau sans fil. Grâce à l'appareil virtuel Cisco Mobility Services Engine inclus dans cette solution, l'administrateur peut afficher les problèmes RF passés. Cette fonction s'avère habituellement utile parce qu'il arrive souvent que les utilisateurs ne signalent pas immédiatement les problèmes, et parce que les équipes d'assistance de niveau 1 traitent le problème avant de le transmettre aux équipes d'assistance de niveaux 2 et 3.

L'infrastructure Cisco Prime avec Cisco CleanAir permet aux administrateurs réseau de connaître les performances du réseau sans fil, de résoudre les problèmes de connectivité du client à distance, de gérer les ressources réseau sans fil, d'analyser les appareils d'interférence, etc. Pour plus d'informations sur l'infrastructure Cisco Prime, voir la section Cisco Prime Infrastructure.

Le guide de conception de la technologie CleanAir de campus sans fil est disponible à l'adresse suivante :

www.cisco.com/go/cvd

Cisco OfficeExtend

Pour le télétravailleur à domicile, il est essentiel de pouvoir accéder aux services de manière fiable et cohérente et de profiter ainsi d'une expérience utilisateur comparable à celle dont il bénéficierait sur le campus. Cependant, sur la bande sans fil 2,4 GHz communément utilisée, les environnements résidentiels et urbains présentent de nombreuses sources potentielles de congestion : les combinés sans fil, les smartphones, les tablettes et les moniteurs pour bébé par exemple. Pour assister des utilisateurs dont les compétences techniques sont extrêmement variables, une solution pour télétravailleurs doit permettre de mettre en œuvre des appareils qui leur fournissent un accès sécurisé à l'environnement d'entreprise, de manière simple et rationalisée.

Les opérations IT sont associées à des exigences totalement différentes lorsqu'il s'agit de mettre en œuvre une solution de télétravail, notamment en ce qui concerne la sécurisation, la maintenance et la gestion correctes de l'environnement du télétravailleur de façon centralisée. Les dépenses d'exploitation constituent un élément à prendre en compte constamment. Par conséquent, le département IT doit mettre en œuvre une solution économique protégeant l'investissement de l'entreprise sans en sacrifier la qualité ou les fonctionnalités.

L'environnement décrit dans le guide de conception Cisco OfficeExtend satisfait aux exigences en termes de simplicité d'utilisation, de qualité d'expérience et de coût d'exploitation. La solution Cisco OfficeExtend repose sur deux composants principaux :

- le contrôleur LAN sans fil de la gamme Cisco 2500 ou Cisco 5500,
- le point d'accès de la gamme Cisco Aironet 600 OfficeExtend.

Contrôleurs LAN sans fil Cisco

Les contrôleurs LAN sans fil Cisco fonctionnent avec les points d'accès Cisco OfficeExtend pour prendre en charge les applications sans fil stratégiques destinées aux télétravailleurs. Ils fournissent le niveau de contrôle, d'évolutivité, de sécurité et de fiabilité dont les gestionnaires réseau ont besoin pour concevoir un environnement de télétravail sécurisé et évolutif.

Un contrôleur indépendant peut prendre en charge jusqu'à 500 sites Cisco OfficeExtend. Pour une solution résiliente, Cisco vous recommande de déployer les contrôleurs par paires.

Les contrôleurs suivants sont inclus dans l'environnement du guide de conception de Cisco OfficeExtend :

- Contrôleur LAN sans fil de la gamme Cisco 2500
- Contrôleur LAN sans fil de la gamme Cisco 5500

La flexibilité associée aux licences logicielles vous permet d'ajouter des points d'accès supplémentaires à mesure que les impératifs commerciaux évoluent. Par conséquent, vous pouvez choisir le contrôleur qui répondra à vos besoins à long terme, mais payer uniquement pour les licences dont vous vous servez, quand vous vous en servez.

Pour que les utilisateurs puissent connecter leurs terminaux sur le réseau sans fil sur site de l'entreprise ou sur le réseau sans fil de télétravail à domicile sans reconfiguration requise, le guide de conception Cisco OfficeExtend vous conseille d'utiliser les mêmes SSID sans fil au domicile des télétravailleurs que ceux prenant en charge la voix et les données au sein de l'entreprise.

Points d'accès Cisco OfficeExtend

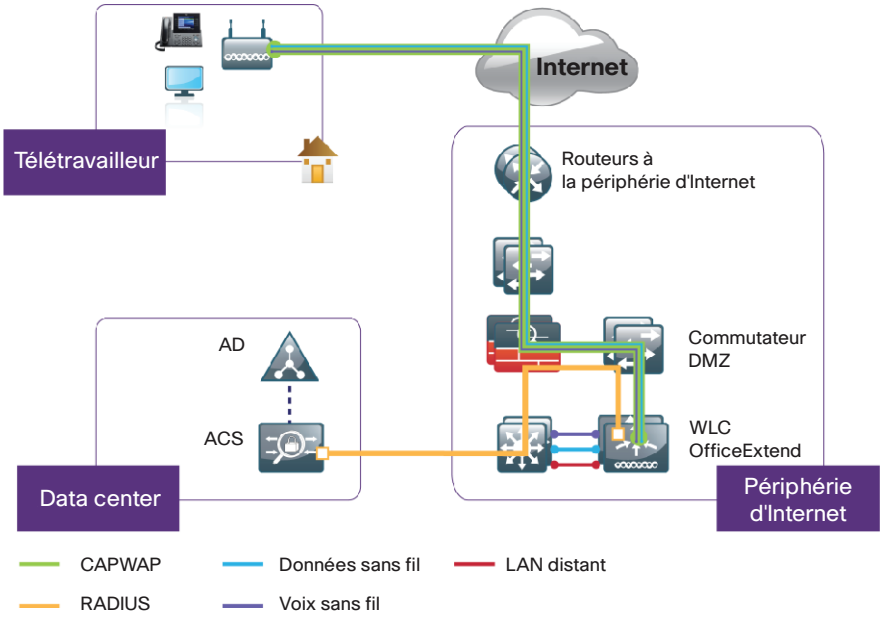
Le point d'accès de la gamme Cisco Aironet 600 est un point d'accès léger. En d'autres termes, il ne peut pas fonctionner indépendamment d'un contrôleur LAN sans fil. Pour fournir une connectivité WLAN à distance à l'aide du même profil que celui utilisé en entreprise, le point d'accès valide tout le trafic par rapport aux politiques de sécurité centralisées. En utilisant des contrôleurs LAN sans fil pour centraliser les politiques, Cisco OfficeExtend minimise les frais de gestion supplémentaires associés aux pare-feu domestiques. Les communications entre le point d'accès et le contrôleur LAN sans fil sont sécurisées via une connexion DTLS (Datagram Transport Layer Security, Sécurité de couche de transport datagramme).

Cisco OfficeExtend offre des performances sans fil 802.11n complètes et permet d'éviter la congestion causée par les appareils résidentiels, car il fonctionne simultanément sur les bandes de radiofréquences 2,4 GHz et 5 GHz. Le point d'accès fournit également une connectivité Ethernet filaire en plus du sans fil. Le point d'accès Cisco OfficeExtend fournit une segmentation filaire et sans fil du trafic domestique et d'entreprise, qui permet de bénéficier d'une connectivité des appareils à domicile sans introduire de risques de sécurité dans les politiques de l'entreprise.

Modèles de conception

Pour effectuer un déploiement le plus flexible et sécurisé possible de Cisco OfficeExtend, déployez une paire de contrôleurs LAN sans fil de la gamme Cisco 5500 ou 2500 dédiés à Cisco OfficeExtend. Dans le modèle de conception dédié, le contrôleur est directement connecté à la zone DMZ en périphérie d'Internet et le trafic provenant d'Internet se termine dans la zone démilitarisée et non dans le réseau interne, alors que le trafic client est quant à lui toujours directement connecté au réseau interne.

Figure 8 - Modèle de conception dédié Cisco OfficeExtend



Le guide de conception de Cisco OfficeExtend est disponible à l'adresse suivante :

www.cisco.com/go/cvd/campus

Commentaires

Utilisez le Formulaire de commentaires pour donner votre avis et envoyer des suggestions concernant le guide.

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose. CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site Web de Cisco, à l'adresse : www.cisco.com/go/offices.

TOUTES LES CONCEPTIONS, SPÉCIFICATIONS, DÉCLARATIONS, INFORMATIONS ET RECOMMANDATIONS (APPELÉES COLLECTIVEMENT « CONCEPTIONS ») PRÉSENTÉES DANS CE MANUEL LE SONT « EN L'ÉTAT », AVEC LEURS IMPERFECTIONS. CISCO ET SES FOURNISSEURS EXCLUENT TOUTES LES GARANTIES, Y COMPRIS, MAIS SANS S'Y LIMITER, TOUTE GARANTIE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER, D'ABSENCE DE CONTREFAÇON OU TOUTE AUTRE GARANTIE DÉCOULANT DE PRATIQUES OU DE RÈGLES COMMERCIALES. EN AUCUN CAS, CISCO OU SES FOURNISSEURS NE SERONT TENUS POUR RESPONSABLES DE TOUT DOMMAGE INDIRECT, PARTICULIER, CONSÉCUTIF OU ACCESSOIRE INCLUANT, MAIS N'ÉTANT PAS LIMITÉ, AUX PERTES DE PROFITS OU PERTE OU DOMMAGE DE DONNÉES RÉSULTANT DE L'UTILISATION OU DE L'INCAPACITÉ À UTILISER LES CONCEPTIONS, MÊME SI CISCO OU SES FOURNISSEURS ONT ÉTÉ AVISÉS DE LA POSSIBILITÉ DE TELS DOMMAGES. LES CONCEPTIONS PEUVENT ÊTRE MODIFIÉES SANS PRÉAVIS. SEULS LES UTILISATEURS SONT RESPONSABLES DE LEUR APPLICATION DES CONCEPTIONS. LES CONCEPTIONS NE REPRÉSENTENT PAS DES CONSEILS TECHNIQUES OU PROFESSIONNELS DISPENSÉS PAR CISCO, SES FOURNISSEURS OU PARTENAIRES. LES UTILISATEURS DOIVENT CONSULTER LEURS PROPRES CONSEILLERS TECHNIQUES AVANT DE METTRE EN ŒUVRE LEURS CONCEPTIONS. LES RÉSULTATS PEUVENT VARIER EN FONCTION DE DIVERS FACTEURS NON TESTÉS PAR CISCO.

Les adresses de protocole Internet (IP) utilisées dans ce document ne sont pas censées être des adresses réelles. Tous les exemples, résultats d'affichage de commandes et chiffres auxquels il est fait référence dans ce document sont donnés à titre d'illustration uniquement. L'utilisation de toute adresse IP réelle à titre d'exemple est non intentionnelle et fortuite.

© 2013 Cisco Systems, Inc. Tous droits réservés.

Cisco et le logo Cisco sont des marques commerciales ou des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales Cisco, visitez le site : www.cisco.com/go/trademarks. Les autres marques mentionnées dans les présentes sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat commercial entre Cisco et d'autres entreprises. (1110R)

B-0000225-1 04/14