Fiche technique

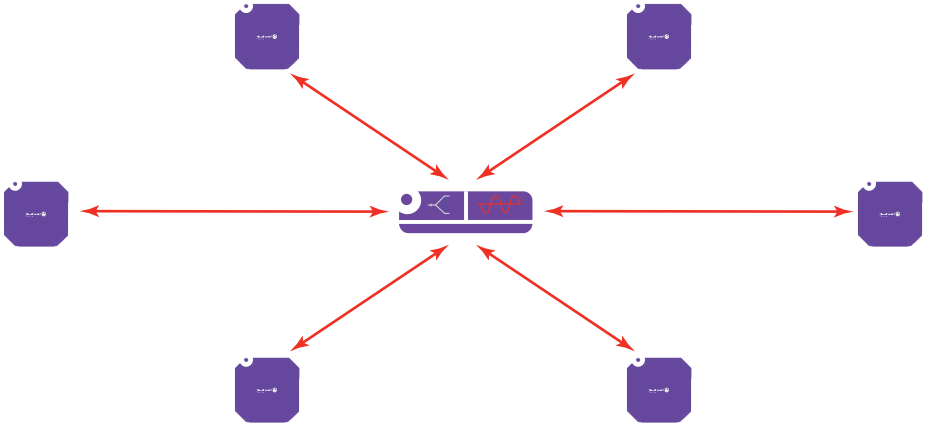
Architecture de contrôle Wi-Fi distribuée

Pourquoi faut-il opter pour le contrôle Wi-Fi distribué

Alcatel·Lucent Enterprise

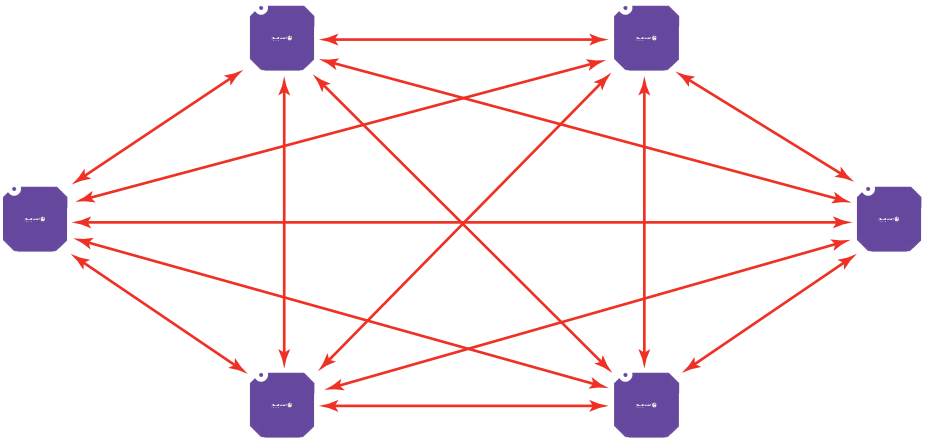
Lors de ses premiers pas sur le marché sans fil, l'entreprise proposait des points d'accès complets ou autonomes. Ces derniers convenaient parfaitement aux réseaux sans fil à petite échelle avec des clients limités par point d'accès. En effet, les paramètres radio, les services d'accès, la sécurité et le contrôle de chaque point d'accès complet devaient être configurés individuellement. Cette approche ne convenait pas aux déploiements dans les moyennes ou grandes entreprises/organisations. Il était clairement nécessaire de développer un type de contrôle de point d'accès centralisé. C'est pourquoi le contrôleur WLAN a été développé.

Le contrôleur WLAN (un appareil ou un serveur monté sur un rack) fonctionne à l'aide de points d'accès allégés qui permettent de récupérer leur micrologiciel et leur configuration à partir du contrôleur WLAN, ce qui offre ainsi un point de gestion unique pour l'ensemble du réseau sans fil. Le contrôleur WLAN agit également en tant que commutateur et pare-feu pour l'ensemble du trafic sans fil tunnelisé via le contrôleur. Il offre un point de contrôle et une terminaison unique pour l'ensemble du trafic sans fil. Les contrôleurs WLAN requièrent des appareils performants pour exécuter des fonctions avancées telles que la configuration automatique des paramètres radio (sélection des chaînes, émission de puissance, etc.), la détection et la prévention des intrusions, la surveillance et l'analyse du spectre, etc.



Cela dit, l'option « contrôleur » n'a jamais été une fin en soi. Au début des années 2000, il s'agissait de la seule option pour convaincre les plus grands clients d'opter pour la technologie WLAN et de déployer des réseaux WLAN susceptibles de relever les défis auxquels ils étaient confrontés dans les domaines du contrôle centralisé, de la sécurité et de la résilience. À cette époque, bien sûr, les limitations et les coûts des composants physiques dans les points d'accès ne pouvaient mener qu'à une approche centralisée. Par la suite, les puces, les mémoires et les processeurs ont évolué pour devenir plus puissants et plus économiques. Aujourd'hui, il est possible de virtualiser le contrôleur, de le déployer et de l'exécuter de manière distribuée dans les points d'accès de façon coordonnée. Voici le choix effectué par Alcatel-Lucent Enterprise (ALE) : les points d'accès intelligents et avancés sont gérés en tant que système ou cluster unique et prennent en charge les plans de contrôle et de routage de manière distribuée et coordonnée.

La solution Unified Management and Distributed Control (Gestion unifiée et contrôle distribué) vous permet d'exécuter toutes les fonctions d'un contrôleur centralisé. De plus, elle permet d'éliminer la complexité de l'architecture, les points de défaillance uniques, les goulots d'étranglement, la latence et les coûts d'exploitation élevés. La suppression du contrôleur requis précédemment dans les architectures de déploiement sans fil offre de nombreux avantages potentiels aux organisations et à leurs départements informatiques.



Réduction des dépenses d'investissement

Les architectures basées sur un contrôleur impliquent des dépenses d'exploitation préalables élevées. Elles impliquent également des frais de licence et d'entretien très élevés. L'avantage le plus significatif de l'architecture de contrôle distribué est la réduction des dépenses d'investissement étant donné qu'aucun contrôleur n'est requis. Les économies sont encore plus significatives pour les déploiements qui impliquent plusieurs contrôleurs à des fins de redondance ou de partage de charge.

De plus, le modèle de licence Alcatel-Lucent Enterprise prévoit une licence unique par point d'accès dans le cadre de la gestion. Cette licence unique inclut toutes les fonctionnalités requises à l'heure actuelle pour un réseau sans fil de pointe (détection des intrusions, pare-feu, inspection approfondie de paquet), ce qui permet de réduire les coûts logiciels. Cela permet également d'apporter davantage de simplicité et de clarté par rapport aux modèles de licence traditionnels qui sont fournis avec les contrôleurs et qui facturent des frais de licence par fonctionnalité.

Réduction des coûts d'exploitation

La suppression des contrôleurs permet de réduire le nombre d'équipements à manipuler et à gérer et de bénéficier de plusieurs avantages liés à la réduction des coûts d'exploitation : réduction de l'espace occupé dans les racks, diminution des exigences en matière d'alimentation et de refroidissement, absence de frais de maintenance (plus particulièrement pour les contrôleurs de sauvegarde non utilisés) et, bien évidemment, réduction du nombre d'équipements à surveiller par le département informatique.

Meilleure résilience

Dans une architecture centralisée basée sur un contrôleur, le contrôleur constitue un point de défaillance unique pour l'ensemble du réseau sans fil. Il impacte l'ensemble du trafic sans fil lorsque le contrôleur tombe en panne. Le seul moyen de minimiser l'impact est d'ajouter des contrôleurs redondants supplémentaires, mais cela nécessite souvent un gros investissement. Avec une architecture de contrôle distribuée, ce point de défaillance unique disparaît. En effet, la fonction de contrôleur n'est plus centralisée mais elle est partagée par tous les points d'accès du domaine de gestion. Si un point d'accès tombe en panne, le point d'accès avoisinant le détecte et réagit en augmentant sa puissance de transmission, ce qui permet d'éviter la formation d'un trou dans la couverture radio. L'impact se fera sentir au niveau local uniquement : seuls les clients associés au point d'accès en panne seront associés au point d'accès avoisinant et pourront s'authentifier à nouveau.

Élimination des goulots d'étranglement et réduction de la latence

Un réseau WLAN constitue désormais un atout essentiel et indispensable d'une organisation. Le Wi-Fi n'est plus une solution de confort. Le réseau WLAN permet de connecter les applications grandes consommatrices de bande passante et/ou sensibles à la latence, telles que la voix ou la vidéo sur IP ou la diffusion de vidéos en continu. Au fil des années, la technologie s'est améliorée pour proposer de meilleurs niveaux de débit grâce aux normes IEEE 802.11a/b/g/n, puis 802.11ac qui fournissent un débit supérieur à 1 Go à distance. Afin de pouvoir exploiter pleinement les capacités des points d'accès 802.11ac, chaque point d'accès doit être connecté au LAN via IEEE 802.3bz 2.5GBase-T link, qui fournit une connectivité pouvant aller jusqu'à 2,5 G. La tunnelisation d'une telle quantité de trafic à partir de chaque point d'accès vers le contrôleur est difficile à assurer. Par conséquent, elle est susceptible de créer un goulot d'étranglement du débit, ainsi qu'une augmentation de la latence. Grâce à l'approche de contrôle distribuée, le trafic n'est plus tunnelisé vers l'équipement centralisé mais il est directement redirigé vers le commutateur Ethernet local.

Une évolutivité augmentée

Une fois que vous avez atteint le nombre maximal de points d'accès pouvant être gérés par un contrôleur, le déploiement de points d'accès supplémentaires requiert un contrôleur supplémentaire. L'architecture de contrôle distribuée offre une meilleure évolutivité : aucun contrôleur n'est requis, quelle que soit la taille du déploiement.

Enfin, l'architecture de contrôle distribuée représente certainement le chemin le plus court vers le prochain bouleversement en matière de technologie sans fil en entreprise : le Cloud Wi-Fi.

Alcatel·Lucent
Enterprise