Glossaire des termes relatifs aux points d'accès sans fil

Objectif

Cet article contient la liste des termes utilisés dans la configuration et le dépannage des points d'accès sans fil Cisco (WAP).

Périphériques pertinents

- Points d'accès sans fil

Liste des termes généraux

- VLAN basé sur la norme 802.1Q - La spécification IEEE 802.1Q établit une méthode standard pour étiqueter les trames Ethernet avec les informations d'appartenance VLAN et définit le fonctionnement des ponts VLAN qui permettent la définition, le fonctionnement et l'administration des topologies VLAN au sein d'une infrastructure LAN pontée. La norme 802.1Q vise à résoudre le problème de la division des grands réseaux en parties plus petites, de sorte que le trafic de diffusion et de multidiffusion n'utilise pas plus de bande passante que nécessaire. La norme contribue également à fournir un niveau de sécurité plus élevé entre les segments des réseaux internes.

- 802.1X Supplicant : le demandeur est l'un des trois rôles de la norme IEEE 802.1X. La norme 802.1X a été développée pour assurer la sécurité de la couche 2 du modèle OSI. Il se compose des composants suivants : demandeur, authentificateur et serveur d'authentification. Un demandeur est le client ou le logiciel qui se connecte à un réseau afin de pouvoir accéder aux ressources de ce réseau. Il doit fournir des informations d’identification ou des certificats pour obtenir une adresse IP et faire partie de ce réseau particulier. Un demandeur ne peut pas accéder aux ressources du réseau tant qu'il n'a pas été authentifié.

- ACL : une liste de contrôle d'accès (ACL) est une liste de filtres de trafic réseau et d'actions corrélées utilisées pour améliorer la sécurité. Elle bloque ou permet aux utilisateurs d'accéder à des ressources spécifiques. Une liste de contrôle d’accès contient les hôtes auxquels l’accès au périphérique réseau est autorisé ou refusé. Les listes de contrôle d'accès peuvent être définies de deux manières : par adresse IPv4 ou par adresse IPv6.

- Band Steer : l'équilibrage de charge avancé, mieux connu sous le nom de « Band Steering », est une fonctionnalité qui détecte les périphériques capables de transmettre à la bande 5 GHz. La bande 2,4 GHz est souvent encombrée et subit des interférences de la part de différents périphériques tels que le Bluetooth et même les fours à micro-ondes. Cette fonctionnalité permet à votre point d'accès de diriger et de diriger les périphériques vers une fréquence radio plus optimale, améliorant ainsi les performances du réseau.

- Bandwidth Utilization : l'utilisation de la bande passante vous permet de placer un seuil sur la moyenne des transferts de données réussis via un chemin de communication. Certaines des techniques utilisées pour améliorer cela sont le formatage, la gestion, le plafonnement et l'allocation de la bande passante.

- Bonjour — Bonjour permet de détecter un point d'accès et ses services à l'aide du DNS de multidiffusion. Il annonce ses services au réseau et répond aux demandes des types de services qu'il prend en charge, ce qui simplifie la configuration du réseau dans les environnements de petites entreprises. Lorsque Bonjour est activé sur un périphérique WAP pris en charge, n'importe quel client Bonjour peut découvrir et accéder à l'utilitaire Web sans configuration préalable. Bonjour fonctionne sur les réseaux IPv4 et IPv6.

- Captive Portal : la méthode Captive Portal oblige les utilisateurs ou hôtes du réseau local à afficher une page Web spéciale avant de pouvoir accéder normalement au réseau public. Captive Portal transforme un navigateur Web en périphérique d'authentification. La page Web nécessite une interaction ou une authentification de l'utilisateur avant que l'accès ne soit autorisé à utiliser le réseau.

- Isolation de canal : un périphérique avec la gestion de canal activée attribue automatiquement des canaux radio sans fil aux autres périphériques WAP dans le cluster. L'attribution automatique de canaux réduit les interférences avec d'autres points d'accès en dehors de son cluster et optimise la bande passante Wi-Fi pour aider à maintenir l'efficacité des communications sur le réseau sans fil.

- Client QoS : l'association de qualité de service (QoS) client est une section qui fournit des options supplémentaires pour la personnalisation de la QoS d'un client sans fil. Ces options incluent la bande passante autorisée à envoyer, recevoir ou garantie. L'association de qualité de service client peut également être manipulée à l'aide de listes de contrôle d'accès (ACL).

- Journalisation des événements : les événements système sont des activités du système qui peuvent nécessiter une attention particulière et des actions nécessaires afin d'exécuter le système en douceur et d'éviter les pannes. Ces événements sont enregistrés sous forme de journaux. Les journaux système permettent à l'administrateur d'effectuer le suivi d'événements particuliers qui se produisent sur le périphérique. Les journaux d’événements sont utiles pour le dépannage réseau, le débogage du flux de paquets et la surveillance des événements.

- Itinérance rapide : l'itinérance rapide entre les points d'accès sans fil permet une connectivité sans fil rapide, sécurisée et ininterrompue pour une expérience mobile transparente pour les applications en temps réel telles que FaceTime, Skype et Cisco Jabber.

- HTTPS : le protocole HTTPS (Hyper Text Transfer Protocol Secure) est un protocole de transfert plus sécurisé que le protocole HTTP. Le point d'accès peut être géré via des connexions HTTP et HTTPS lorsque les serveurs HTTP/HTTPS sont configurés. Certains navigateurs Web utilisent HTTP tandis que d'autres utilisent HTTPS. Un point d'accès doit disposer d'un certificat SSL (Secure Socket Layer) valide pour utiliser le service HTTPS.

- IPv4 : IPv4 est un système d'adressage 32 bits utilisé pour identifier un périphérique dans un réseau. Il s'agit du système d'adressage utilisé dans la plupart des réseaux informatiques, y compris Internet.

- IPv6 : IPv6 est un système d'adressage 128 bits utilisé pour identifier un périphérique dans un réseau. Il s'agit du successeur d'IPv4 et de la version la plus récente du système d'adressage utilisé dans les réseaux informatiques. IPv6 est actuellement déployé dans le monde entier. Une adresse IPv6 est représentée par huit champs de nombres hexadécimaux, chaque champ contenant 16 bits. Une adresse IPv6 est divisée en deux parties, chacune composée de 64 bits. La première partie correspond à l'adresse réseau et la seconde à l'adresse hôte.

- LLDP : le protocole LLDP (Link Layer Discovery Protocol) est un protocole de détection défini dans la norme IEEE 802.1AB. Le protocole LLDP permet aux périphériques réseau d'annoncer des informations les concernant aux autres périphériques du réseau. Le protocole LLDP utilise les services LLC (Logical Link Control) pour transmettre et recevoir des informations à destination et en provenance d'autres agents LLDP. LLC fournit un point d'accès de service de liaison (LSAP) pour l'accès au protocole LLDP. Chaque trame LLDP est transmise en tant que requête de service MAC unique. Chaque trame LLDP entrante est reçue au niveau du point d'accès au service MAC (MSAP) par l'entité LLC en tant qu'indication de service MAC.

- Équilibrage de charge : l'équilibrage de charge est une terminologie réseau utilisée pour répartir la charge de travail sur plusieurs ordinateurs, liaisons réseau et diverses autres ressources afin d'obtenir une utilisation appropriée des ressources, d'optimiser le débit, le temps de réponse et d'éviter principalement la surcharge.

- MAC ACL : le contrôle d'accès au support (MAC) basé sur la liste de contrôle d'accès (ACL) est une liste d'adresses MAC source. Si un paquet provient d'un point d'accès sans fil vers un port LAN ou vice versa, ce périphérique vérifie si l'adresse MAC source du paquet correspond à une entrée de cette liste et vérifie les règles de liste de contrôle d'accès par rapport au contenu de la trame. Il utilise ensuite les résultats correspondants pour autoriser ou refuser ce paquet. Cependant, les paquets du LAN au port LAN ne seront pas vérifiés.

- SSID multiples : vous pouvez configurer plusieurs SSID (Service Set Identifier) ou points d'accès virtuels (VAP) sur votre point d'accès et attribuer différents paramètres de configuration à chaque SSID. Tous les SSID peuvent être actifs simultanément. Les périphériques clients peuvent s'associer au point d'accès à l'aide de n'importe quel SSID.

- Mode de fonctionnement : le périphérique WAP peut agir en tant que point d'accès en mode point à point unique, pont point à multipoint et répéteur. En mode point à point, un seul périphérique WAP accepte les connexions des clients et des autres périphériques du réseau. En mode pont point à multipoint, un périphérique WAP unique se comporte comme une liaison commune entre de nombreux points d'accès. Le périphérique WAP peut également servir de répéteur, où il peut établir une connexion entre des points d'accès éloignés les uns des autres. Les clients sans fil peuvent se connecter à ce répéteur. Un système de rôle WDS (Wireless Distribution System) peut être comparé de manière similaire

au rôle du répéteur.

- Capture de paquets : la capture de paquets est une fonctionnalité d'un périphérique réseau qui vous permet de capturer et de stocker les paquets transmis et reçus par le périphérique. Les paquets capturés peuvent être analysés par un analyseur de protocole réseau pour dépanner ou optimiser les performances. Le fichier de paquet capturé peut être téléchargé via HTTP/HTTPS ou un serveur TFTP. Il peut être partagé, puis analysé plus en détail pour comprendre le flux de paquets dans le réseau. La page Packet Capture permet de configurer la capture de paquets locale ou distante, de télécharger un fichier de capture de paquets ou d'afficher l'état de capture actuel.

- QoS : la qualité de service (QoS) vous permet de hiérarchiser le trafic pour différentes applications, utilisateurs ou flux de données. Il peut également être utilisé pour garantir des performances à un niveau spécifié, affectant ainsi la qualité de service du client. La qualité de service est généralement affectée par les facteurs suivants : gigue, latence et perte de paquets.

- RADIUS Server : le service RADIUS (Remote Authentication Dial-In User Service) est un mécanisme d'authentification permettant aux périphériques de se connecter et d'utiliser un service réseau. Il est utilisé à des fins d'authentification, d'autorisation et de comptabilité centralisées. Un serveur RADIUS régule l'accès au réseau en vérifiant l'identité des utilisateurs à l'aide des informations d'identification saisies. Par exemple, un réseau Wi-Fi public est installé dans un campus universitaire. Seuls les étudiants disposant du mot de passe peuvent accéder à ces réseaux. Le serveur RADIUS vérifie les mots de passe entrés par les utilisateurs et accorde ou refuse l'accès selon le cas.

- Gestion à distance : la gestion à distance manipule les paramètres d'un périphérique réseau à partir d'un emplacement distant. Cette opération est généralement effectuée sur des périphériques tels que des ordinateurs, des commutateurs, des routeurs et de nombreux autres périphériques disposant d'une adresse IP. Elle permet aux administrateurs réseau de répondre rapidement aux demandes ou aux défis, puisqu'ils n'ont pas besoin d'être physiquement sur site. L'accès aux périphériques dans la gestion à distance est presque comme le faire localement, sauf que l'adresse IP locale du périphérique est utilisée pour accéder au périphérique localement tandis que l'adresse IP WAN du périphérique est utilisée lors de l'accès sur un périphérique distant.

- Détection des points d'accès non autorisés : un point d'accès non autorisé est un point d'accès installé sur un réseau sans l'autorisation explicite d'un administrateur système. Les points d'accès non autorisés représentent une menace pour la sécurité, car toute personne ayant accès à la zone peut installer, en connaissance de cause ou non, un point d'accès sans fil qui permet à des personnes non autorisées d'accéder au réseau. La fonctionnalité Détection des points d'accès indésirables de votre point d'accès lui permet de voir ces points d'accès indésirables qui sont dans la plage et il affiche leurs informations dans l'utilitaire Web. Vous pouvez ajouter n'importe quel point d'accès autorisé à la liste des points d'accès approuvés.

- RSTP : le protocole RSTP (Rapid Spanning Tree Protocol) est une amélioration du protocole

STP. Le protocole RSTP assure une convergence Spanning Tree plus rapide après une modification de topologie. Le protocole STP peut prendre de 30 à 50 secondes pour répondre à une modification de topologie, tandis que le protocole RSTP répond dans les trois fois la durée Hello configurée. RSTP est rétrocompatible avec STP.

- Planificateur : le planificateur sans fil permet de planifier un intervalle de temps pour qu'un point d'accès virtuel (VAP) ou une radio soit opérationnel, ce qui permet d'économiser de l'énergie et d'améliorer la sécurité. Vous pouvez associer jusqu'à 16 profils à différents VAP ou interfaces radio, mais chaque interface n'est autorisée qu'à un seul profil. Chaque profil peut avoir un certain nombre de règles temporelles qui contrôlent la disponibilité du VAP ou du WLAN associé.

- Configuration par point unique : la configuration par point unique est une technologie de gestion simple et multipériphérique qui vous permet de déployer et de gérer un groupe de points d'accès prenant en charge cette fonctionnalité. Elle offre la commodité de configurer un groupe de points d'accès à partir d'un point unique au lieu de les configurer individuellement. Il vous permet également de gérer les points d'accès localement ou à distance.

- SNMP : le protocole SNMP (Simple Network Management Protocol) est une norme réseau permettant de stocker et de partager des informations sur les périphériques réseau. SNMP facilite la gestion, le dépannage et la maintenance du réseau.

- Spanning Tree : le protocole STP (Spanning Tree Protocol) est un protocole réseau utilisé sur un réseau local. L’objectif du protocole STP est de garantir une topologie sans boucle pour un réseau local. Le protocole STP supprime les boucles via un algorithme qui garantit qu’il n’existe qu’un seul chemin actif entre deux périphériques réseau. Le protocole STP garantit que le trafic emprunte le chemin le plus court possible au sein du réseau. Le protocole STP peut également réactiver automatiquement les chemins redondants en tant que chemins de secours en cas de défaillance d’un chemin actif.

- SSID : l'identifiant SSID (Service Set Identifier) est un identifiant unique que les clients sans fil peuvent se connecter à tous les périphériques d'un réseau sans fil ou partager entre eux. Il est sensible à la casse et ne doit pas comporter plus de 32 caractères alphanumériques. Il s'agit également du nom du réseau sans fil.

- SSID Broadcast : lorsqu'un périphérique sans fil recherche dans la zone des réseaux sans fil auxquels il peut se connecter, il détecte les réseaux sans fil à portée via leurs noms de réseau ou SSID. La diffusion du SSID est activée par défaut. Cependant, vous pouvez également choisir de le désactiver.

- TSPEC - Traffic Specification (TSPEC) est une spécification de trafic qui est envoyée depuis un client sans fil compatible QoS à un périphérique WAP demandant un certain nombre d'accès réseau pour le flux de trafic (TS) qu'il représente.

- VLAN : un réseau local virtuel (VLAN) est un réseau commuté qui est segmenté logiquement par fonction, zone ou application, sans tenir compte des emplacements physiques des utilisateurs. Les VLAN sont un groupe d’hôtes ou de ports qui peuvent être situés n’importe

où sur un réseau, mais qui communiquent comme s’ils se trouvaient sur le même segment physique. Les VLAN simplifient la gestion du réseau en vous permettant de déplacer un périphérique vers un nouveau VLAN sans modifier les connexions physiques.

- WDS : Wireless Distribution System (WDS) est une fonctionnalité qui permet l'interconnexion sans fil des points d'accès d'un réseau. Il permet à l'utilisateur d'étendre le réseau avec plusieurs points d'accès sans fil. WDS préserve également les adresses MAC des trames client sur les liaisons entre les points d’accès. Cette fonctionnalité est essentielle car elle offre une expérience transparente aux clients itinérants et permet la gestion de plusieurs réseaux sans fil.

- WMM : Wi-Fi Multimedia (WMM) est une fonctionnalité qui attribue différentes priorités de processus à différents types de trafic. WMM est également une fonctionnalité QoS qui améliore les performances du réseau sans fil en définissant la priorité du paquet de données sans fil en fonction de quatre catégories : voix, vidéo, meilleur effort et arrière-plan. Par défaut, WMM est activé. Si une application ne requiert pas WMM, elle reçoit une priorité inférieure à celle de la vidéo et de la voix.

- Wireless Isolation : empêche la communication et les transferts de fichiers entre les ordinateurs connectés à différents SSID. Le trafic sur un SSID ne sera transféré à aucun autre SSID.

- WPA/WPA2 : les protocoles de sécurité WPA et WPA2 (Wi-Fi Protected Access) sont utilisés pour les réseaux sans fil afin de protéger la confidentialité en chiffrant les données transmises sur le réseau sans fil. Les protocoles WPA et WPA2 sont tous deux compatibles avec les normes IEEE 802.11e et 802.11i. Les protocoles WPA et WPA2 offrent des fonctionnalités d'authentification et de cryptage améliorées par rapport au protocole de sécurité WEP (Wired Equivalent Privacy).

Liste des termes dans les réseaux maillés

- Point d'accès : périphérique d'un réseau utilisé pour permettre aux utilisateurs de se connecter au réseau sans fil. Des étiquettes spécifiques peuvent y être ajoutées en fonction de sa fonction : principale, distante, racine, subordonnée, etc.
- Réseau maillé sans fil : type de topologie dans lequel les points d'accès sans fil se connectent entre eux pour relayer des informations. Ces réseaux fonctionnent de manière dynamique pour ajuster les besoins et maintenir la connectivité pour tous les utilisateurs.
- Point d'accès principal : le point d'accès principal assure la gestion et le contrôle du réseau sans fil et de la topologie. Il s’agit du pont vers le reste du réseau externe (généralement Internet) à l’aide d’un fournisseur d’accès Internet (FAI). Le point d’accès principal est directement relié au routeur local qui, à son tour, achemine le trafic vers l’interface WAN ISP. Le point d'accès principal est l'orchestrateur de tous les noeuds fournissant des services sans fil au sein du réseau maillé. Il gère les informations provenant des noeuds du réseau, la qualité de chaque connexion client et les informations de voisinage afin de prendre la meilleure décision sur la meilleure route pour des services sans fil optimisés vers le client mobile.

- Principal principal : point d'accès actuel chargé de la gestion du WLAN.
- Preferred Primary : paramètre dans lequel un point d'accès principal spécifique est répertorié comme préféré. Si le point d'accès principal tombe en panne, le point d'accès principal préféré prend le relais. Une fois le point d'accès préféré sauvegardé, il ne bascule pas automatiquement. Vous n'avez pas désigné de principal préféré.
- Point d'accès principal : point d'accès disposant d'une connexion câblée physique vers le réseau. Ce point d'accès doit être connecté à Ethernet et peut devenir le point d'accès principal en cas de défaillance du point d'accès principal.
- Mesh Extender : point d'accès subordonné distant du réseau qui n'est pas connecté au réseau câblé.
- Point d'accès subordonné : Terme général pouvant être appliqué à tout point d'accès maillé qui n'est pas configuré en tant que point d'accès principal.
- Point d'accès parent : un point d'accès parent est un point d'accès qui fournit la meilleure route vers le point d'accès principal.
- Point d'accès enfant : un point d'accès enfant est un extendeur de maillage qui sélectionne le point d'accès parent comme meilleure route vers le point d'accès principal.
- Point d'accès en amont : un point d'accès en amont est un terme général faisant référence à la direction des flux de données à travers les points d'accès lors du passage du client au serveur.
- Point d'accès en aval : un point d'accès en aval transporte des données d'Internet vers le client.
- Points d’accès colocalisés : extenseurs de réseau maillé situés dans la portée de diffusion du canal de liaison.
- Noeuds : dans cet article, les points d'accès sont appelés noeuds. En général, les noeuds décrivent tout périphérique qui établit une connexion ou une interaction au sein d’un réseau, ou qui a la capacité d’envoyer, de recevoir et de stocker des informations, de communiquer avec Internet et qui possède une adresse IP. Dans un réseau maillé, des paramètres radio optimisés sur tous les noeuds assurent une couverture sans fil maximale tout en réduisant les interférences radio entre les noeuds afin de fournir des débits et des débits de données supérieurs.
- Liaison : dans un réseau maillé sans fil, les informations du réseau local (LAN) doivent se rendre à un point d'accès câblé pour accéder à Internet. La liaison est le processus qui consiste à renvoyer ces informations au point d’accès filaire.

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.

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.

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.

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.