Services de domaine sans fil - Forum Aux Questions

Contenu

Introduction

Ce document fournit des renseignements sur les questions fréquemment posées (FAQ) sur Wireless Domain Services (WDS).

Q. Qu'est-ce que WDS ?

A. WDS fait partie du réseau SWAN (Structured Wireless Aware Network) de Cisco. WDS est un ensemble de fonctionnalités du logiciel Cisco IOS® qui améliorent la mobilité des clients WLAN et simplifient le déploiement et la gestion WLAN. WDS est une nouvelle fonctionnalité pour les points d'accès (AP) dans le logiciel Cisco IOS, et la base du module WLSM (Wireless LAN Services Module) de la gamme Cisco Catalyst 6500. WDS est une fonction centrale qui permet d'autres fonctionnalités, telles que :

- Itinérance sécurisée rapide (FSR)
- Interaction WLSE (Wireless LAN Solution Engine)
- Gestion de la radio (RM)

Avant d'utiliser d'autres fonctionnalités basées sur WDS, vous devez établir des relations entre les AP qui participent au WDS et le périphérique configuré en tant que WDS. L'un des principaux objectifs de WDS est de mettre en cache les informations d'identification de l'utilisateur dès que le serveur d'authentification authentifie le client pour la première fois. Lors de tentatives ultérieures, WDS authentifie le client sur la base des informations mises en cache.

Q. Comment configurer mon AP en tant que WDS ?

A. Référez-vous à Configuration des services de domaine sans fil pour plus d'informations sur la façon de configurer l'AP en tant que WDS.

Q. Sur quelles plates-formes le WDS (Structured Wireless-Aware Network) de Cisco fonctionne-t-il ?

A. Vous pouvez exécuter SWAN WDS sur les points d'accès Cisco Aironet, les commutateurs Cisco Catalyst ou les routeurs Cisco. Voici la liste des plates-formes qui prennent actuellement en charge le WDS SWAN :

- Points d'accès de la gamme Aironet 1230 AG
- Points d'accès de la gamme Aironet 1240AG
- AP de la gamme Aironet 1200
- Points d'accès de la gamme Aironet 1130 AG
- AP de la gamme Aironet 1100
- Module de services LAN sans fil (WLSM) de la gamme Catalyst 6500

- Les gammes Cisco 3800 et 3700 intègrent des routeurs à services (ISR) et certains modèles des gammes 2800 et 2600 ISR qui exécutent Cisco IOS version 12.3(11)T ou ultérieure.

Q. Comment les WDS basés sur AP se comparent-ils aux WDS basés sur les commutateurs ?

A. Lorsque vous utilisez un WDS basé sur un point d'accès, Cisco SWAN prend en charge :

- Itinérance sécurisée rapide (FSR) de couche 2 (L2)
- Gestion WLAN (Wireless LAN) évolutive
- Fonctionnalités de gestion radio avancées
- Sécurité sans fil améliorée

Lorsque vous utilisez un WDS basé sur des commutateurs, le réseau étendu prend en charge :

- FSR de couche 2/couche 3 (L3)
- Fonctionnalités RM avancées
- Sécurité de bout en bout
- Qualité de service (QoS) de bout en bout dans les déploiements WLAN de campus.

Q. Comment configurer WDS avec mon réseau LAN sans fil (WLAN) actuel ?

A. Pour configurer WDS, vous devez désigner un point d'accès ou le module de services LAN sans fil (WLSM) comme WDS. Le point d'accès WDS doit établir une relation avec un serveur d'authentification par authentification avec un nom d'utilisateur et un mot de passe WDS. Le serveur d'authentification peut être soit un serveur RADIUS (Remote Authentication Dial-In User Service) externe, soit la fonctionnalité de serveur RADIUS local dans l'AP WDS. Le WLSM doit avoir une relation avec le serveur d'authentification, même si le WLSM n'a pas besoin de s'authentifier auprès du serveur.

Q. Quel est le rôle du périphérique WDS dans le réseau LAN sans fil (WLAN) ?

A. Le périphérique WDS effectue les tâches suivantes sur votre WLAN :

- Annonce la fonctionnalité WDS et participe à la sélection du meilleur périphérique WDS pour votre WLAN.Lorsque vous configurez votre WLAN pour WDS, vous configurez un périphérique en tant que candidat WDS principal et un ou plusieurs périphériques supplémentaires en tant que candidat WDS de secours. Si le périphérique WDS principal est hors connexion, l'un des périphériques WDS de sauvegarde remplace le périphérique principal.
- Authentifie tous les points d’accès du sous-réseau et établit un canal de communication sécurisé avec chacun des points d’accès.
- Collecte les données radio des points d'accès du sous-réseau, agrège les données et les transmet au périphérique WLSE (Wireless LAN Solution Engine) de votre réseau.
- Inscrit tous les périphériques clients dans le sous-réseau, établit les clés de session pour les périphériques clients et met en cache les informations d'identification de sécurité du client.Lorsqu'un client se déplace vers un autre point d'accès, le périphérique WDS transfère les informations d'identification de sécurité du client au nouveau point d'accès.

Q. Comment le WDS et les points d’accès d’infrastructure du WLAN communiquent-ils entre eux ?

A. Le WDS et les AP d'infrastructure communiquent via un protocole de multidiffusion appelé WLCCP (Wireless LAN Context Control Protocol). Ces messages de multidiffusion ne peuvent pas être routés. Par conséquent, un WDS et les AP d'infrastructure associés doivent se trouver dans le même sous-réseau IP et sur le même segment de réseau local. Entre le WDS et le WLSE (Wireless LAN Solution Engine), le WLCCP utilise le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol) sur le port 2887. Lorsque le WDS et le WLSE se trouvent sur différents sous-réseaux, la traduction de paquets avec un protocole tel que la traduction d'adresses de réseau (NAT) ne peut pas se produire.

Q. Puis-je configurer le point d'accès/pont 1300 en tant que WDS principal ?

A. Vous ne pouvez pas configurer le point d'accès/pont Cisco Aironet 1300 en tant que WDS principal. Le point d'accès/pont 1300 ne prend pas en charge cette fonctionnalité. Le point d'accès/pont 1300 peut participer à un réseau WDS dans lequel d'autres points d'accès ou WLSM agissent en tant que WDS principal.

Q. Combien de points d'accès d'infrastructure un seul WDS peut-il gérer ?

A. Un seul point d'accès WDS peut prendre en charge un maximum de 60 points d'accès d'infrastructure lorsque l'interface radio est désactivée. Le nombre passe à 30 si le point d'accès qui agit en tant que point d'accès WDS accepte également les associations de clients.

Un commutateur équipé d'un module de services LAN sans fil (WLSM) prend en charge jusqu'à 300 points d'accès.

Q. Qu'est-ce que l'itinérance sécurisée rapide (FSR) ?

A. FSR est l'une des fonctionnalités offertes par WDS. Le FSR est pris en charge par les points d'accès Cisco Aironet 1200 et 1100 conjointement avec les périphériques clients Cisco ou les périphériques clients compatibles Cisco. Avec FSR, les périphériques clients authentifiés peuvent circuler en toute sécurité au niveau de la couche 2 (L2) d'un point d'accès à un autre sans délai perceptible pendant la réassociation. FSR prend en charge les applications sensibles à la latence, telles que :

- Voix sur IP sans fil (VoIP)
- Planification des ressources d'entreprise
- Solutions Citrix

WDS fournit des services de transfert rapides et sécurisés aux points d'accès, sans perte de connexions. Les services sont destinés aux applications, telles que la voix, qui nécessitent des temps d'itinérance inférieurs à 150 ms.

Q. Qu’est-ce que l’itinérance de couche 3 (L3) ?

A. Avec l'itinérance de couche 2 (L2), le client sans fil circule entre deux points d'accès qui font partie du même sous-réseau côté câblé. WDS basé sur AP fournit cette fonctionnalité. Avec le WDS basé sur AP, vous devez configurer les AP pour qu'ils soient dans le même VLAN.

Avec l'itinérance L3, le client sans fil se déplace entre deux points d'accès qui résident dans deux sous-réseaux différents. Par conséquent, le client se déplace entre deux VLAN différents du côté câblé. Cela supprime la création de VLAN qui s'étend sur l'ensemble du campus, que le WDS basé sur les points d'accès crée. Les périphériques clients utilisent des tunnels mGRE (Multipoint Generic Routing Encapsulation) afin de se déplacer vers les points d'accès qui résident sur différents sous-réseaux de couche 3. Les clients itinérants restent connectés à votre réseau sans avoir à modifier les adresses IP.

Q. Quel est le rôle du Wireless LAN Solution Engine (WLSE) dans un réseau WLAN (Wireless LAN) WDS ?

A. Les points d'accès et, éventuellement, les périphériques clients Cisco ou les périphériques clients compatibles Cisco prennent des mesures de radiofréquence (RF) dans un seul sous-réseau. Cisco SWAN WDS regroupe les mesures et les transmet à CiscoWorks WLSE pour analyse. Grâce à ces mesures, CiscoWorks WLSE peut :

- Détecter les points d'accès indésirables et les interférences d'autres périphériques.**Remarque :** Le nombre maximal de rogues pouvant être affiché dans WLSE est de 5 000. Si le WLSE a atteint cette limite non autorisée, le message d'erreur `Limit of Infrastructure/Ad hoc Rogues Tracer` apparaît. Dans de tels cas, pour supprimer ces rogues de WLSE, accédez à **IDS > Manage Rogues**, choisissez l'option **« Select *ALL*"** *& **'Delete'** afin de supprimer les rogues.Si le nombre d'émetteurs inconnus (non autorisés) dépasse 5 000 dans votre environnement, vous appuyez à nouveau sur ce nombre et le même message d'avertissement s'affiche. La seule façon de surmonter cela est soit de gérer ces radios, soit de marquer ces radios comme amicales.
- Fournir une assistance pour les études de site
- Prise en charge de l'autoréparation WLAN pour un réglage optimal du canal et de l'alimentation

Q. Quels sont les avantages de l'utilisation de WDS sur un module WLSM (Wireless LAN Services Module) ?

A. L'introduction du WDS basé sur les commutateurs et du WLSM facilite l'itinérance sécurisée rapide de couche 3 (L3) et fournit une solution hautement évolutive pour la mobilité de couche 3 sur le campus. WDS basé sur un commutateur centralise les fonctionnalités du WDS dans la lame WLSM dans un commutateur central et offre les avantages suivants :

- Évolutivité WDS accrue : l'évolutivité atteint 300 points d'accès et 6 000 utilisateurs sur un réseau LAN sans fil de campus.
- Conception et mise en oeuvre simplifiées : aucun VLAN n'est présent sur le réseau du campus. Avec l'utilisation de l'architecture mGRE (Multipoint Generic Routing Encapsulation), aucune modification de l'infrastructure câblée du réseau actuel n'est nécessaire.
- Facilité de gestion pour un déploiement WLAN de grande envergure : cette solution fournit un point d'entrée unique pour le contrôle WLAN et les données utilisateur dans le réseau câblé pour lequel appliquer des politiques de sécurité et de qualité de service (QoS).
- Mobilité de couche 3 entre les étages et sur plusieurs bâtiments
- Possibilité d'utiliser des fonctionnalités avancées sur le commutateur Cisco Catalyst 6500, qui inclut d'autres modules de service Catalyst 6500
- Sécurité et qualité de service de bout en bout améliorées grâce à l'intégration à la plate-forme

Catalyst 6500

Q. Quelle est la fonction de gestion radio (RM) de WDS ?

A. Un point d'accès WDS agit également comme agrégateur pour les statistiques de radiofréquence (RF) des autres points d'accès. Le point d'accès WDS transmet ces statistiques au Wireless LAN Solution Engine (WLSE) afin de mettre en évidence les points d'accès non autorisés. Le moniteur RF permet au WLSE de créer une carte de couverture sans fil. Le WLSE utilise également les points d'accès actuels afin de réaliser des études de site et d'identifier les zones sans couverture. Vous pouvez importer des plans d'étage dans le logiciel pour rendre les zones où vous avez besoin de points d'accès supplémentaires faciles à repérer.

Q. Les points d'accès Cisco Aironet peuvent-ils prendre en charge les clients pendant que les points d'accès analysent l'environnement de radiofréquence (RF) ?

A. Oui, les points d'accès Cisco sont multifonctionnels. Les points d'accès Cisco desservent les clients et surveillent également l'air/RF. Il est toujours recommandé d'avoir moins de clients associés au point d'accès configuré en tant que WDS.

Q. WDS peut-il effectuer des fonctions comptables ?

A. Non. WDS peut effectuer l'authentification mais pas la comptabilité. La comptabilité est totalement indépendante et vous devez avoir un serveur RADIUS pour cette fonction.

Q. Pour configurer WDS avec CCKM, quelles sont les suites de chiffrement prises en charge ? Extensible Authentication Protocol-Flexible Authentication through Secure Tunnel (EAP-FAST) est-il compatible avec Cisco CKM ? Quelle combinaison utiliser ?

A. Vous devez utiliser une suite de chiffrement pour utiliser Cisco CKM. Ces combinaisons de suite Cipher sont prises en charge avec CCKM.

- cryptage mode cryptage wep128
- cryptage mode ciphers wep40
- cryptage mode ciphers ckip
- cryptage mode ciphers ckip-cmic
- cryptage mode ciphers cmic
- cryptage mode ciphers tkip

EAP-FAST/Cisco CKM est pris en charge avec les cartes Cisco Aironet 350 et bientôt avec les cartes Aironet CB21AG. Voici la commande permettant d'activer le chiffrement :

```
encryption vlan 1 mode ciphers tkip wep128
```

EAP-FAST n'utilise pas la clé WEP que vous avez définie. EAP-FAST utilise une clé dynamique.

Q. La commande authentication key-management cckm facultative fonctionne-t-elle

pour les clients Aironet dont l'itinérance rapide est vérifiée et pour ceux dont l'itinérance rapide n'est pas vérifiée ?

A. Si vous réglez la gestion centralisée des clés Cisco (CKM) sur facultatif, le paramètre fonctionne pour les clients Aironet dont l'itinérance rapide est activée et pour les clients dont l'itinérance rapide n'est pas activée.

Q. Pendant combien de temps les informations d'identification des utilisateurs du cache WLSM sont-elles mises en cache ?

A. La durée du cache peut dépendre du type de client. Il y a un maintien en vie entre l'AP et le noeud mobile (MN), qui dépend de la configuration de l'AP et du type de client. S'il s'agit d'un client Cisco, le point d'accès détecte rapidement l'absence du client et quitte sa liste d'associations. Une fois que cela se produit, le client reste dans la liste MN du WDS dans un état séparé pendant environ 10 minutes.

S'il s'agit d'un client tiers, le délai d'attente de maintien en vie sur un point d'accès peut être très long, aussi longtemps que 30 minutes.

En gros, si le client Cisco ne figure pas dans la table d'association dot11 d'un point d'accès pendant 10 minutes, une nouvelle authentification est nécessaire, ce qui signifie qu'il doit l'envoyer au serveur d'authentification plutôt qu'au point d'accès d'infrastructure basé sur l'utilisateur mis en cache. Si un client non Cisco ne figure pas dans la table d'association dot11 d'un point d'accès pendant 10 à 30 minutes, une nouvelle authentification est nécessaire.

Q. Puis-je configurer plus de 60 points d'accès dans un WDS qui utilise un WDS basé sur des points d'accès ?

A. N'utilisez pas plus de 60 points d'accès sur un seul WDS principal. Vous pouvez rencontrer des problèmes d'utilisation du CPU avec plus de 60 points d'accès. Vous pouvez avoir plusieurs WDS principaux, mais ils doivent se trouver sur différents sous-réseaux. L'utilisation de :

- Un WDS principal et 30 points d'accès sur 10.10.10.10
- Autre WDS principal et 30 points d'accès sur 10.10.20.20

Dans ce cas, le problème est que vous ne pouvez pas effectuer de itinérance rapide entre les domaines WDS.

Q. Combien de candidats de sauvegarde WDS puis-je avoir ? Un candidat de secours WDS peut-il toujours fonctionner comme un point d'accès dans le WDS et signaler les informations au WDS principal ?

A. Il n'y a pas de limite au nombre de candidats de secours WDS. Oui, les candidats de sauvegarde fonctionnent toujours comme des AP qui font rapport au WDS principal. En outre, seul le point d'accès WDS principal établit les clés de sécurité WLSE et s'enregistre auprès du WLSE afin d'interagir avec le WLSE. Ce n'est que si le WDS principal échoue que le WDS de secours prend le rôle d'un point d'accès WDS actif et s'enregistre auprès du WLSE et établit des clés de sécurité. Tant que le WDS principal est actif, le WDS de sauvegarde fonctionne comme un AP normal qui fait rapport au WDS principal.

Q. Si j'ai trois points d'accès WDS et qu'ils échouent tous, la défaillance affecte-t-

elle uniquement les informations WDS, ou tous les points d'accès et clients ? En d'autres termes, le WDS est-il un point de défaillance pour le réseau sans fil ?

A. Si vos WDS principaux échouent, tous les points d'accès échouent également. Cependant, si les points d'accès ont toutes les configurations nécessaires pour que le point d'accès fonctionne indépendamment, les points d'accès commencent à fonctionner sans le WDS lorsque le périphérique WDS tombe en panne.

Q. Sur un sous-réseau, j'ai un WDS configuré avec une priorité de 200 et un WDS avec une priorité de 100. Si le WDS principal avec une priorité de 200 échoue, le WDS avec la priorité de 100 devient-il le principal sur le sous-réseau ?

A. Dans ce cas, le WDS principal avec la priorité 100 devient le principal si ce WDS se trouve sur le même sous-réseau. Si ce WDS se trouve sur un autre sous-réseau, il ne devient pas le principal.

Q. La commande `show iapp rogue-ap-list` dans un point d'accès Cisco 1200 fournit-elle des informations utiles lorsqu'un WLSE (Wireless LAN Solution Engine) n'est pas en place ?

A. Non, cette commande fonctionne uniquement avec le WLSE et lorsque vous utilisez le Gestionnaire d'emplacements dans le WLSE.

Q. J'ai un point d'accès Cisco AP1200 configuré pour WDS. Le point d'accès est suspendu et ne répond pas sur la console ou Telnet tant que je n'ai pas effectué un cycle d'alimentation. Cependant, le point d'accès ne s'arrête pas. Que se passe-t-il ?

A. Ce problème se produit en raison de l'ID de bogue Cisco CSCsc01706 (clients enregistrés uniquement). Ce problème se produit uniquement sur le point d'accès WDS lorsque plusieurs clients sans fil tentent de s'associer ou de se déplacer. Ce problème a commencé dans le logiciel Cisco IOS Version 12.3(4)JA, mais la plupart des problèmes sont signalés dans le logiciel Cisco IOS Version 12.3(7)JA. Le WLSE (Wireless LAN Solution Engine) qui envoie la requête SNMP (Simple Network Management Protocol) sur l'événement d'usurpation MAC déclenche le problème. Le point d'accès WDS enregistre un certain nombre d'événements d'usurpation MAC sur au moins deux points d'accès. Pour résoudre ce problème, vous devez effectuer une mise à niveau vers le logiciel Cisco IOS Version 12.3(8)JA ou ultérieure.

Q. Un point d'accès répéteur peut-il prendre en charge WDS ?

A. Les points d'accès du répéteur ne prennent pas en charge WDS. Ne configurez pas un point d'accès de répéteur en tant que candidat WDS et ne configurez pas un point d'accès WDS pour revenir au mode répéteur en cas de défaillance d'Ethernet.

Q. Un point d'accès de la gamme 350 peut-il être configuré en tant que point d'accès WDS ?

A. Vous ne pouvez pas configurer un point d'accès de la gamme 350 en tant que point d'accès WDS. Cependant, vous pouvez configurer des points d'accès de la gamme 350 pour utiliser le

point d'accès WDS.

Informations connexes

- Configuration de services de domaine sans fil
- Prise en charge de la technologie sans fil, LAN (WLAN)
- Support et documentation techniques - Cisco Systems