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. Quel est WDS ?

A. Le WDS est une partie du réseau averti de radio structuré par Cisco (CYGNE). Le WDS est une collection de caractéristiques de logiciel de Cisco IOS® qui améliorent la mobilité de client WLAN, et simplifie le déploiement et la Gestion WLAN. Le WDS est une nouvelle caractéristique pour les Points d'accès (aps) dans le logiciel de Cisco IOS, et la base du module de services LAN sans fil (WLSM) de la gamme Cisco 6500. Le WDS est une principale fonction qui active d'autres caractéristiques, comme :

- Jeûnent l'itinérance sécurisée (FSR)
- Interaction du Wireless LAN Solution Engine (WLSE)
- Gestion par radio (RM)

Avant l'exécution de toutes les autres caractéristiques basées sur WDS, vous devez établir des relations entre les aps qui participent au WDS et au périphérique qui est configuré comme WDS. Un des buts principaux du WDS est de cacher les identifiants utilisateurs dès que le serveur d'authentification authentifiera le client pour la première fois. Sur des tentatives ultérieures, le WDS authentifie le client sur la base des informations en cache.

Q. Comment est-ce que je configure mon AP comme WDS ?

A. Référez-vous à la configuration Sans fil de services de domaine pour les informations sur la façon dont configurer AP comme WDS.

Q. Sur quelles Plateformes fait Cisco a structuré le réseau sans fil (CYGNE) WDS s'exécutent ?

A. Vous pouvez exécuter le CYGNE WDS sur des Routeurs de Cisco Aironet aps, de commutateurs Cisco Catalyst, ou de Cisco. Voici la liste de Plateformes qui prennent en charge actuellement le CYGNE WDS :

- Aironet 1230 gammes aps AG
- Gamme aps de l'Aironet 1240AG
- Gamme 1200 aps d'Aironet
- Aironet 1130 gammes aps AG
- AP de la gamme Aironet 1100

- Module de services Sans fil réseau local de gamme Catalyst 6500 (WLSM)
- Le 3800 de Cisco, gamme 3700 intègre les Routeurs de services (ISR) et quelques modèles des gammes 2800 et 2600 ISR cette version 12.3(11)T ou ultérieures de Cisco IOS de passage.

Q. Comment le WDS basé sur AP rivalise-t-il avec le WDS basé sur commutateur ?

A. Quand vous utilisez le WDS basé sur AP, le CYGNE de Cisco le prend en charge :

- Posez 2 (L2) jeûnent l'itinérance sécurisée (FSR)
- Gestion Sans fil extensible du RÉSEAU LOCAL (WLAN)
- Capacités par radio avancées de Gestion (RM)
- Sécurité Sans fil améliorée

Quand vous utilisez le WDS basé sur commutateur, le CYGNE le prend en charge :

- L2/Layer 3 (L3) FSR
- Capacités avancées de RM
- Sécurité de bout en bout
- Qualité de service de bout en bout (QoS) dans des déploiements du campus WLAN.

Q. Comment est-ce que j'installe le WDS avec mon réseau Sans fil en cours du RÉSEAU LOCAL (WLAN) ?

A. Afin d'installer le WDS, vous devez indiquer un AP ou le Module de services Sans fil de RÉSEAU LOCAL (WLSM) comme WDS. Le WDS AP doit établir des relations à un serveur d'authentification par l'authentification avec un nom d'utilisateur et le mot de passe WDS. Le serveur d'authentification peut être un serveur externe de Service RADIUS (Remote Authentication Dial-In User Service) ou la caractéristique locale de serveur de RADIUS dans le WDS AP. Le WLSM doit avoir des relations avec le serveur d'authentification, quoique le WLSM n'ait pas besoin d'authentifier au serveur.

Q. Quel est le rôle du périphérique WDS dans le réseau Sans fil du RÉSEAU LOCAL (WLAN) ?

A. Le périphérique WDS effectue ces tâches sur votre WLAN :

- Annonce la capacité WDS et participe à une élection du meilleur périphérique WDS pour votre WLAN.Quand vous configurez votre WLAN pour le WDS, vous installez un périphérique en tant que le candidat principal WDS et un ou plusieurs périphériques supplémentaires en tant que candidats de sauvegarde WDS. Si le périphérique principal WDS va off-line, un des périphériques de la sauvegarde WDS remplace le périphérique principal.
- Authentifie tous les aps dans le sous-réseau et établit un canal de communication protégée avec chacun des aps.
- Collecte les données par radio des aps dans le sous-réseau, agrège les données, et en avant les données au périphérique du Wireless LAN Solution Engine (WLSE) sur votre réseau.
- Enregistre tous les périphériques de client dans le sous-réseau, établit des clés de session pour les périphériques de client, et cache les qualifications de Sécurité de client.Quand un client erre à un autre AP, le périphérique WDS en avant les qualifications de Sécurité de client

à nouvel AP.

Q. Comment est-ce que le WDS et l'infrastructure aps dans le WLAN communiquent les uns avec les autres ?

A. Le WDS et l'infrastructure aps communiquent au-dessus d'un protocole de Multidiffusion appelé le Control Protocol Sans fil de contexte de RÉSEAU LOCAL (WLCCP). Ces messages multicasts ne peuvent pas être conduits. Par conséquent, un WDS et l'infrastructure associée aps doivent être dans le même sous-réseau IP et sur le même segment de RÉSEAU LOCAL. Entre le WDS et le Wireless LAN Solution Engine (WLSE), Protocole TCP (Transmission Control Protocol) et Protocole UDP (User Datagram Protocol) d'utilisations WLCCP sur le port 2887. Quand le WDS et les WLSE sont sur différents sous-réseaux, la traduction de paquet avec un protocole comme le Traduction d'adresses de réseau (NAT) ne peut pas se produire.

Q. Est-ce que je peux configurer les 1300 AP/Bridge comme maître WDS ?

A. Vous ne pouvez pas configurer Cisco Aironet 1300 AP/Bridge comme maître WDS. Les 1300 AP/Bridge ne prennent en charge pas cette fonctionnalité. Les 1300 AP/Bridge peuvent participer à un réseau WDS dans lequel quelque autre AP ou WLSM agit en tant que maître WDS.

Q. Combien l'infrastructure aps peut-elle un WDS simple gérer ?

A. Un WDS simple AP peut prendre en charge un maximum 60 de l'infrastructure aps quand l'interface par radio est désactivée. Le nombre chute à 30 si AP qui agit en tant que WDS AP également reçoit des associations de client.

Un Module de services Sans fil de RÉSEAU LOCAL (WLSM) - commutateur équipé prend en charge jusqu'à 300 aps.

Q. Quelle est l'itinérance sécurisée rapide (FSR) ?

A. FSR est l'une des caractéristiques que le WDS offre. FSR est pris en charge par les gammes 1200 et 1100 aps de Cisco Aironet en même temps que des périphériques de client de Cisco ou des périphériques Cisco-compatibles de client. Avec FSR, les périphériques authentifiés de client peuvent errer sécurisé à la couche 2 (L2) d'un AP à l'autre sans n'importe quel retard perceptible pendant la rassociation. FSR prend en charge des applications sensibles à la latence, comme :

- Voix sur ip Sans fil (VoIP)
- Planification des ressources d'entreprise (ERP)
- solutions basées sur Citrix

Le WDS fournit des services rapides et sécurisés de transfert aux aps, sans baisse des connexions. Les services sont pour les applications, telles que la Voix, qui ont besoin de les temps d'itinérance qui sont moins de 150 ms.

Q. Quelle est itinérance de la couche 3 (L3) ?

A. Avec l'itinérance de la couche 2 (L2), le client sans fil erre entre deux aps qui font partie du même sous-réseau du côté de câble. le WDS basé sur AP fournit cette fonctionnalité. Avec le WDS basé sur AP, vous devez configurer les aps pour être dans le même VLAN.

Avec l'itinérance L3, le client sans fil erre entre deux aps qui résident dans deux sous-réseaux différents. Par conséquent, le client erre entre deux VLAN différents du côté de câble. Ceci retire la création des VLAN qui répartissent le campus entier, que le WDS basé sur AP créent. Les périphériques de client utilisent les tunnels génériques multipoints d'encapsulation de routage (mGRE) afin d'errer aux aps qui résident sur les différents sous-réseaux L3. Les clients d'itinérance restent connectés à votre réseau sans nécessité de changer des adresses IP.

Q. Quel est le rôle du Wireless LAN Solution Engine (WLSE) dans un réseau Sans fil WDS-activé du RÉSEAU LOCAL (WLAN) ?

A. Les périphériques de client aps et, sur option, de Cisco ou les périphériques Cisco-compatibles de client prennent des mesures de Radiofréquence (RF) dans un sous-réseau simple. Le CYGNE WDS de Cisco agrège les mesures et en avant les mesures aux CiscoWorks WLSE pour l'analyse. Avec ces mesures comme base, boîte des CiscoWorks WLSE :

- Détectez les aps escrocs et l'interférence d'autres périphériques.**Remarque:** Le nombre maximal d'escrocs qui peuvent être affichés dans WLSE a 5000 ans. Si le WLSE a atteint cette limite escroc, la `limite de l'infrastructure/ad hoc des escrocs dépistant le` message d'erreur apparaît. En pareil cas, pour supprimer ces escrocs de WLSE, naviguez vers des **ID > gèrent des escrocs**, choisissent l'option de « **effacement** » de *& **« *ALL* choisi »** afin de supprimer les escrocs.Si le compte (escroc) inconnu de radio est plus de 5000 dans votre environnement, vous frappez de nouveau ce nombre et le même message d'avertissement apparaît. La seule manière de surmonter ceci est à gèrent ces radios ou marquent ces radios comme amicale.
- Provide a aidé des analyses de site
- Prenez en charge le WLAN autocuratif pour la configuration optimale de canal et de niveau de puissance

Q. Quels sont les avantages de l'utilisation du WDS sur un Module de services Sans fil de RÉSEAU LOCAL (WLSM) ?

A. L'introduction du WDS basé sur commutateur et du WLSM facilite la couche 3 (L3) jeûnent l'itinérance sécurisée (FSR) et fournissent fortement une solution évolutive pour la mobilité L3 dans le campus. le WDS basé sur commutateur centralise la fonctionnalité du WDS dans la lame WLSM dans un commutateur central et fournit ces indemnités :

- Évolutivité accrue WDS — L'évolutivité grimpe jusqu'à 300 aps et à 6000 utilisateurs à travers un réseau Sans fil du RÉSEAU LOCAL de campus (WLAN).
- Conception et réalisation simplifiée — VLAN ne répartit pas le réseau campus. Avec l'utilisation de l'architecture générique multipoint d'encapsulation de routage (mGRE), aucune modification à l'infrastructure câblée de réseau en cours n'est nécessaire.
- Gestionnabilité pour un grand déploiement WLAN — Cette solution fournit un seul point d'entrée pour le contrôle WLAN et les données d'utilisateur dans le réseau câblé pour que lequel applique des stratégies de Sécurité et de Qualité de service (QoS).
- Mobilité L3 entre les planchers et à travers de plusieurs bâtiments
- La capacité d'utiliser la fonctionnalité avancée sur le Cisco Catalyst 6500, qui inclut d'autres modules de service de Catalyst 6500
- Sécurité de bout en bout améliorée et QoS par l'intégration avec la plate-forme de Catalyst 6500

Q. Quelle est la caractéristique par radio de Gestion (RM) du WDS ?

A. AP WDS-activé agit également en tant qu'agrégateur pour des statistiques de Radiofréquence (RF) des autres aps. Les passer WDS-activés AP le long des ces statistiques au Wireless LAN Solution Engine (WLSE) afin de mettre en valeur des aps escrocs. Le moniteur du rf permet au WLSE pour créer une carte de couverture Sans fil. Le WLSE emploie également le courant aps afin d'effectuer des analyses de site et identifier des zones sans la couverture. Vous pouvez importer des plans d'étage sur le logiciel pour faire des zones où vous avez besoin d'aps supplémentaires faciles à repérer.

Q. Cisco Aironet aps peut-il prendre en charge des clients tandis que les aps balayent l'air/environnement de Radiofréquence (RF) ?

A. Oui, Cisco aps sont multifonctionnel. Cisco aps servent des clients et surveillent également l'air/RF. Il est toujours recommandé pour avoir moins de clients associés à AP configuré comme WDS.

Q. Le WDS peut-il remplir des fonctions de traçabilité ?

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

Q. Afin d'installer le WDS avec CCKM ce qui sont les suites de chiffrement prises en charge ? L'authentification Protocol-flexible d'authentification extensible par le tunnel sécurisé (EAP-FAST) compatible avec Cisco est-elle CKM ? Quelle combinaison est-ce que j'utilise ?

A. Vous devez employer une suite de chiffrement afin d'utiliser Cisco CKM. Ces combinaisons de suite de chiffrement sont prises en charge avec CCKM.

- encryption mode ciphers wep128
- encryption mode ciphers wep40
- ckip d'encryption mode ciphers
- encryption mode ciphers ckip-cmic
- encryption mode ciphers cmic
- tkip d'encryption mode ciphers

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

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

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

Q. La commande facultative de cckm d'authentication key-management fonctionne-t-elle pour les deux clients Aironet avec l'itinérance rapide vérifiée et ceux sans

itinérance rapide vérifiée ?

A. Si vous placiez le Cisco Centralized Key Management (CKM) à facultatif, la configuration fonctionne pour les deux clients Aironet qui font vérifier l'itinérance rapide et ces clients qui ne font pas vérifier l'itinérance rapide.

Q. Pendant combien de temps le WLSM cache-t-il des identifiants utilisateurs ?

A. Le temps de cache peut dépendre du type de client. Il y a une keepalive entre AP et le noeud mobile (manganèse), qui dépend de la configuration AP et du type de client. Si c'est un client de Cisco, AP détecte l'absence du client rapidement et laisse sa liste d'association. Une fois que cela se produit, le client reste dans la liste manganèse du WDS dans un état isolé pendant environ 10 minutes.

Si c'est un client de tiers, le délai d'attente de keepalive sur AP peut être très long, tant que 30 minutes.

Fondamentalement, si le client de Cisco n'est pas dans la table d'associations dot11 dans aucun AP pendant 10 minutes, la ré-authentification est nécessaire, que les moyens de l'envoyer au serveur d'authentification au lieu de à l'infrastructure AP ont basée sur l'utilisateur caché. Si un client de non-Cisco n'est pas dans la table d'associations dot11 dans aucun AP pendant entre 10 et 30 minutes, la ré-authentification est nécessaire.

Q. Est-ce que je peux installer plus de 60 aps dans un WDS qui utilise le WDS basé sur AP ?

A. N'utilisez pas plus de 60 aps sur un maître WDS. Vous pouvez rencontrer des problèmes d'utilisation du processeur avec plus de 60 aps. Vous pouvez avoir de plusieurs maîtres WDS, mais ils doivent être sur différents sous-réseaux. Un exemple est l'utilisation de :

- Un maître WDS et 30 aps sur 10.10.10.10
- Un autre maître WDS et 30 aps sur 10.10.20.20

Dans ce cas, la question est que vous ne pouvez pas jeûner errez entre les domaines WDS.

Q. Combien de candidats de sauvegarde WDS est-ce que je peux avoir ? Un candidat de sauvegarde WDS peut-il fonctionner comme AP dans le WDS et encore signaler les informations au WDS primaire ?

A. Il n'y a aucune limite au nombre de candidats de sauvegarde WDS. Oui, les candidats de sauvegarde fonctionnent toujours comme aps qui font rapport au maître WDS. En outre, seulement le WDS primaire AP établit des clés de Sécurité WLSE et s'inscrit au WLSE afin d'interagir avec le WLSE. Seulement si le WDS primaire échoue, la sauvegarde WDS prend le rôle d'un WDS actif AP et continue pour s'inscrire au WLSE et pour établir des clés de Sécurité. Tant que le WDS primaire est en activité, la sauvegarde WDS fonctionne comme AP normal qui fait rapport au maître WDS.

Q. Si j'ai trois WDS aps et ils tous échouent, la panne affecte-t-elle seulement les informations WDS, ou tous les aps et clients ? En d'autres termes, le WDS est-il par point de panne pour le réseau Sans fil ?

A. Si vos maîtres WDS échouent, tous les aps échouent aussi bien. Cependant, si les aps ont toutes les configurations qui sont nécessaires pour qu'AP fonctionne indépendamment, les aps commencent à fonctionner sans WDS quand le périphérique WDS échoue.

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 maître WDS avec une priorité de 200 échoue, le WDS avec la priorité de 100 devient-il le maître sur le sous-réseau ?

A. Dans ce cas, le maître WDS avec la priorité de 100 devient le maître si ce WDS est sur le même sous-réseau. Si ce WDS est sur un autre sous-réseau, ce ne devient pas le maître.

Q. La commande de `show iapp rogue-ap-list à` Cisco 1200 AP fournit-elle des informations utiles quand un Wireless LAN Solution Engine (WLSE) n'est pas en place ?

A. Non, cette commande fonctionne seulement en même temps que le WLSE et quand vous utilisez le gestionnaire d'emplacement dans le WLSE.

Q. J'ai Cisco AP1200 configuré pour le WDS. AP s'arrête et ne répond pas sur la console ou le telnet jusqu'à ce que j'exécute un arrêt et redémarrage. Cependant, AP ne tombe pas en panne. Que se passe-t-il ?

A. Ce problème se pose en raison de l'ID de bogue Cisco CSCsc01706 (clients enregistrés seulement). Ce problème se pose seulement sur le WDS AP quand essai de plusieurs clients sans fil pour s'associer ou errer. Cette question commencée dans la version du logiciel Cisco IOS 12.3(4)JA, mais la plupart des problèmes sont signalés dans la version du logiciel Cisco IOS 12.3(7)JA. Le Wireless LAN Solution Engine (WLSE) qui envoie la requête de Protocole SNMP (Simple Network Management Protocol) sur l'événement de mystification de MAC déclenche la question. Le WDS AP enregistre un certain nombre d'événements de mystification de MAC sur au moins deux aps. Afin de résoudre ce problème, vous devez améliorer la version du logiciel Cisco IOS à 12.3(8)JA ou à plus tard.

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

A. Les Points d'accès de répéteur ne prennent en charge pas le 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 retomber au mode répéteur en cas de panne d'Ethernets.

Q. Une gamme 350 AP peut-elle être configurée comme Point d'accès WDS ?

A. Vous ne pouvez pas configurer un Point d'accès de gamme 350 comme Point d'accès WDS. Cependant, vous pouvez configurer des Points d'accès de gamme 350 pour utiliser le Point d'accès WDS.

Informations connexes

- Configuration de services de domaine sans fil
- Support de technologie LAN sans fil

- Configurer des suites de chiffrement et le WEP
- En configurant le WDS, jeûnez itinérance sécurisée, et Gestion de radio
- Le guide de Foire aux questions et de dépannage pour les CiscoWorks WLSE et WLSE expriment, 2.13
- Support et documentation techniques - Cisco Systems