Häufig gestellte Fragen zu Wireless Domain Services

Inhalt

Einführung

Dieses Dokument enthält Informationen zu den am häufigsten gestellten Fragen (FAQs) zu Wireless Domain Services (WDS).

F. Was ist WDS?

Antwort: WDS ist Teil des Cisco Structured Wireless Aware Network (SWAN). WDS ist eine Sammlung von Cisco IOS® Software-Funktionen, die die Mobilität von WLAN-Clients erhöhen und die Bereitstellung und Verwaltung von WLANs vereinfachen. WDS ist eine neue Funktion für Access Points (APs) in der Cisco IOS-Software und die Grundlage des Cisco Catalyst Wireless LAN Services Module (WLSM) der Serie 6500. WDS ist eine Kernfunktion, die andere Funktionen ermöglicht, z. B.:

- Schnelles sicheres Roaming (FSR)
- Interaktion mit Wireless LAN Solution Engine (WLSE)
- Funkverwaltung (RM)

Vor dem Betrieb anderer WDS-basierter Funktionen müssen Sie Beziehungen zwischen den APs herstellen, die am WDS teilnehmen, und dem Gerät, das als WDS konfiguriert ist. WDS dient in erster Linie dazu, die Benutzeranmeldeinformationen zu zwischenspeichern, sobald der Authentifizierungsserver den Client zum ersten Mal authentifiziert. Bei nachfolgenden Versuchen authentifiziert WDS den Client anhand der zwischengespeicherten Informationen.

F. Wie konfiguriere ich meinen Access Point als WDS?

Antwort: Weitere Informationen zur Konfiguration des Access Points als WDS finden Sie unter Konfiguration von Wireless Domain Services.

F. Auf welchen Plattformen wird der Cisco Structured Wireless-Aware Network (SWAN) WDS ausgeführt?

Antwort: Sie können SWAN WDS auf Cisco Aironet APs, Cisco Catalyst Switches oder Cisco Routern ausführen. Die folgende Liste enthält Plattformen, die derzeit SWAN WDS unterstützen:

- APs der Aironet Serie 1230 AG
- APs der Aironet Serie 1240AG
- APs der Aironet Serie 1200
- APs der Aironet Serie 1130 AG
- Aironet APs der Serie 1100
- Catalyst Wireless LAN Services Module (WLSM) der Serie 6500
- Die Cisco Serien 3800 und 3700 integrieren Services Router (ISR) sowie einige ISR-Modelle der Serien 2800 und 2600, auf denen die Cisco IOS-Version 12.3(11)T oder höher ausgeführt

wird.

F. Wie schneidet AP-basiertes WDS im Vergleich zu Switch-basiertem WDS ab?

Antwort: Wenn Sie AP-basierte WDS verwenden, unterstützt Cisco SWAN Folgendes:

- Layer 2 (L2) Fast Secure Roaming (FSR)
- Skalierbares WLAN-Management
- Erweiterte Funkverwaltungsfunktionen
- Verbesserte Wireless-Sicherheit

Wenn Sie ein Switch-basiertes WDS verwenden, unterstützt SWAN Folgendes:

- L2/Layer 3 (L3) FSR
- Erweiterte RM-Funktionen
- End-to-End-Sicherheit
- End-to-End Quality of Service (QoS) in Campus-WLAN-Bereitstellungen.

F. Wie richte ich WDS mit meinem aktuellen WLAN-Netzwerk ein?

Antwort: Um WDS einzurichten, müssen Sie einen Access Point oder das Wireless LAN Services Module (WLSM) als WDS festlegen. Der WDS AP muss durch Authentifizierung mit einem WDS-Benutzernamen und -Kennwort eine Beziehung zu einem Authentifizierungsserver herstellen. Beim Authentifizierungsserver kann es sich entweder um einen externen RADIUS-Server (Remote Authentication Dial-In User Service) oder um die lokale RADIUS-Serverfunktion im WDS AP handeln. Das WLSM muss über eine Beziehung zum Authentifizierungsserver verfügen, obwohl das WLSM keine Authentifizierung für den Server benötigt.

F. Welche Rolle spielt das WDS-Gerät im WLAN-Netzwerk?

Antwort: Das WDS-Gerät führt diese Aufgaben im WLAN aus:

- Werbt für WDS-Funktionalität aus und nimmt an der Auswahl des besten WDS-Geräts für Ihr WLAN teil.Wenn Sie Ihr WLAN für WDS konfigurieren, richten Sie ein Gerät als WDS-Hauptkandidat und ein oder mehrere zusätzliche Geräte als Backup-WDS-Kandidaten ein. Wenn das Haupt-WDS-Gerät offline geht, übernimmt eines der Backup-WDS-Geräte die Stelle des Hauptgeräts.
- Authentifiziert alle APs im Subnetz und stellt einen sicheren Kommunikationskanal zu jedem der APs her.
- Sammelt Funkdaten von APs im Subnetzwerk, aggregiert die Daten und leitet sie an das WLSE-Gerät (Wireless LAN Solution Engine) im Netzwerk weiter.
- Registriert alle Clientgeräte im Subnetz, erstellt Sitzungsschlüssel für die Client-Geräte und legt die Client-Sicherheitsanmeldeinformationen im Cache ab.Wenn ein Client zu einem anderen AP wechselt, leitet das WDS-Gerät die Client-Sicherheitsanmeldeinformationen an den neuen AP weiter.

F. Wie kommunizieren WDS und die Infrastruktur-APs im WLAN miteinander?

Antwort: Der WDS und die Infrastruktur-APs kommunizieren über ein Multicast-Protokoll, das als

WLCCP (Wireless LAN Context Control Protocol) bezeichnet wird. Diese Multicast-Nachrichten können nicht geroutet werden. Daher müssen sich ein WDS und die zugehörigen Infrastruktur-APs im gleichen IP-Subnetz und im gleichen LAN-Segment befinden. Zwischen dem WDS und der Wireless LAN Solution Engine (WLSE) verwendet WLCCP das Transmission Control Protocol (TCP) und das User Datagram Protocol (UDP) an Port 2887. Wenn sich WDS und WLSE in unterschiedlichen Subnetzen befinden, kann keine Paketübersetzung mit einem Protokoll wie Network Address Translation (NAT) erfolgen.

F. Kann ich die 1300 AP/Bridge als primäres WDS konfigurieren?

Antwort: Sie können den Cisco Aironet 1300 AP/Bridge nicht als primäres WDS konfigurieren. Diese Funktionalität wird von der 1300 AP/Bridge nicht unterstützt. Die 1300 AP/Bridge kann an einem WDS-Netzwerk teilnehmen, in dem ein anderer AP oder WLSM als primäres WDS fungiert.

F. Wie viele Infrastruktur-APs kann ein einzelnes WDS verwalten?

Antwort: Ein einzelner WDS AP kann bis zu 60 Infrastruktur-APs unterstützen, wenn die Funkschnittstelle deaktiviert ist. Die Zahl fällt auf 30, wenn der Access Point, der als WDS-Access Point fungiert, auch Clientzuordnungen akzeptiert.

Ein mit WLSM (Wireless LAN Services Module) ausgestatteter Switch unterstützt bis zu 300 APs.

F. Was ist schnelles sicheres Roaming (FSR)?

Antwort: FSR ist eine der Funktionen, die WDS bietet. FSR wird von den Cisco Aironet APs der Serien 1200 und 1100 in Verbindung mit Cisco Client-Geräten oder mit Cisco kompatiblen Client-Geräten unterstützt. Mit FSR können authentifizierte Client-Geräte sicher auf Layer 2 (L2) von einem Access Point zum anderen wechseln, ohne dass es zu spürbaren Verzögerungen während der Neuzuordnung kommt. FSR unterstützt latenzempfindliche Anwendungen wie:

- Wireless Voice over IP (VoIP)
- Enterprise Resource Planning (ERP)
- Citrix-basierte Lösungen

WDS bietet schnelle und sichere Übergabe von Services an APs ohne Verbindungsunterbrechung. Die Services sind für Anwendungen wie Sprache bestimmt, die Roaming-Zeiten von weniger als 150 ms erfordern.

F. Was ist Layer-3-Roaming (L3)?

Antwort: Beim Layer-2-Roaming (L2) wechselt der Wireless-Client zwischen zwei APs, die Teil desselben Subnetzwerks sind, auf der kabelgebundenen Seite. AP-basiertes WDS stellt diese Funktionalität bereit. Bei AP-basiertem WDS müssen Sie die APs so konfigurieren, dass sie sich im selben VLAN befinden.

Beim L3-Roaming wechselt der Wireless-Client zwischen zwei APs, die sich in zwei verschiedenen Subnetzen befinden. Daher wechselt der Client zwischen zwei verschiedenen VLANs auf der kabelgebundenen Seite. Dadurch entfällt die Erstellung von VLANs, die den gesamten Campus umfassen, den das AP-basierte WDS erstellt. Client-Geräte verwenden mGRE-Tunnel (Multipoint Generic Routing Encapsulation), um zu APs zu wechseln, die sich in verschiedenen L3-Subnetzen befinden. Die Roaming-Clients bleiben mit Ihrem Netzwerk

verbunden, ohne dass IP-Adressen geändert werden müssen.

F. Welche Rolle spielt die Wireless LAN Solution Engine (WLSE) in einem WDS-fähigen WLAN-Netzwerk?

Antwort: APs und optional Cisco Client-Geräte oder Cisco-kompatible Client-Geräte nehmen Hochfrequenzmessungen in einem einzelnen Subnetz vor. Cisco SWAN WDS aggregiert die Messwerte und leitet diese zur Analyse an CiscoWorks WLSE weiter. Anhand dieser Messungen kann CiscoWorks WLSE:

- Erkennung von nicht autorisierten APs und Interferenzen von anderen Geräten**Hinweis:** Die maximale Anzahl von unberechtigten Benutzern, die in WLSE angezeigt werden können, beträgt 5.000. Wenn die WLSE diesen Grenzwert erreicht hat, wird die Fehlermeldung `Limit of Infrastructure/Ad-hoc rogues Tracking (Begrenzt der Infrastruktur-/Ad-hoc-` Fehlerverfolgung) angezeigt. Um diese unberechtigten Benutzer aus WLSE zu löschen, navigieren Sie zu **IDS > Manage Rogues**, wählen Sie die **Option "Select *ALL*"** *& **"Delete"** aus, um die unberechtigten Benutzer zu löschen.Wenn die Anzahl der unbekannten (nicht autorisierten) Funkmodule in Ihrer Umgebung über 5000 liegt, drücken Sie erneut diese Nummer, und die gleiche Warnmeldung wird angezeigt. Die einzige Möglichkeit, dies zu überwinden, besteht darin, diese Funkgeräte entweder zu verwalten oder diese Funkgeräte als freundlich zu kennzeichnen.
- Durchführung von Standortgutachten
- Unterstützung von WLAN-Self-Healing-Funktionen für optimale Kanaleinstellung und Einstellung auf Leistungsebene

F. Welche Vorteile bietet die Verwendung von WDS auf einem Wireless LAN Services Module (WLSM)?

Antwort: Die Einführung eines Switch-basierten WDS und des WLSM vereinfacht Layer 3 (L3) Fast Secure Roaming (FSR) und bietet eine hochskalierbare Lösung für L3-Mobilität im Campus. Switch-basiertes WDS zentralisiert die Funktionalität von WDS im WLSM-Blade in einem zentralen Switch und bietet folgende Vorteile:

- Verbesserte WDS-Skalierbarkeit - Die Skalierbarkeit erhöht sich auf 300 APs und 6.000 Benutzer in einem Campus Wireless LAN (WLAN)-Netzwerk.
- Vereinfachtes Design und vereinfachte Implementierung - im Campus-Netzwerk sind keine VLANs vorhanden. Bei Verwendung der mGRE-Architektur (Multipoint Generic Routing Encapsulation) sind keine Änderungen an der aktuellen kabelgebundenen Netzwerkinfrastruktur erforderlich.
- Verwaltbarkeit für eine große WLAN-Bereitstellung - Diese Lösung bietet einen zentralen Eingangspunkt für die WLAN-Steuerung und die Benutzerdaten in das kabelgebundene Netzwerk, für die Sicherheits- und Quality of Service (QoS)-Richtlinien angewendet werden sollen.
- L3-Mobilität zwischen Etagen und über mehrere Gebäude hinweg
- Erweiterte Funktionen des Cisco Catalyst 6500, einschließlich anderer Catalyst 6500-Servicemodule
- Verbesserte End-to-End-Sicherheit und QoS durch Integration mit der Catalyst 6500-Plattform

F. Welche Funkverwaltungsfunktion (Radio Management, RM) bietet WDS?

Antwort: Ein WDS-fähiger Access Point fungiert außerdem als Aggregator für Hochfrequenzstatistiken der anderen Access Points. Der WDS-fähige AP leitet diese Statistiken an die Wireless LAN Solution Engine (WLSE) weiter, um nicht autorisierte APs hervorzuheben. Mit dem HF-Monitor kann die WLSE eine Karte der Wireless-Abdeckung erstellen. Die WLSE verwendet außerdem aktuelle APs, um Standortuntersuchungen durchzuführen und Gebiete ohne Abdeckung zu identifizieren. Sie können Raumpläne in die Software importieren, um Bereiche, in denen zusätzliche APs benötigt werden, einfach zu identifizieren.

F. Können Cisco Aironet APs Clients unterstützen, während die APs die Luft-/Funkfrequenzumgebung (Radio Frequency, RF) scannen?

Antwort: Ja, die Cisco APs sind multifunktional. Cisco APs dienen Clients und überwachen auch die Luft/die HF. Es wird immer empfohlen, weniger Clients mit dem Access Point als WDS zu konfigurieren.

F. Kann WDS Abrechnungsfunktionen ausführen?

Antwort: Nein. WDS kann Authentifizierung, aber keine Abrechnung durchführen. Die Buchhaltung ist vollkommen unabhängig und Sie benötigen einen RADIUS-Server für diese Funktion.

F. Welche Verschlüsselungssuiten werden für die Einrichtung von WDS mit CCKM unterstützt? Ist EAP-FAST (Extensible Authentication Protocol-Flexible Authentication through Secured Tunnel) mit Cisco CKM kompatibel? Welche Kombination verwende ich?

Antwort: Um Cisco CKM verwenden zu können, müssen Sie eine Verschlüsselungssuite verwenden. Diese Cipher-Suite-Kombinationen werden von CCKM unterstützt.

- Verschlüsselungsmodus Chiffers wep128
- Verschlüsselungsmodus Chiffers wep40
- Verschlüsselungsmodus ciphes ckip
- Verschlüsselungsmodus Chiffren ckip-cmic
- Verschlüsselungsmodus Chiffren cmic
- Verschlüsselungsmodus Chiffers tkip

EAP-FAST/Cisco CKM wird von den Cisco Aironet 350-Karten unterstützt und wird demnächst von den Aironet CB21AG-Karten unterstützt. Der folgende Befehl dient zum Aktivieren der Chiffre:

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

EAP-FAST verwendet nicht den von Ihnen festgelegten WEP-Schlüssel. EAP-FAST verwendet einen dynamischen Schlüssel.

F. Funktioniert der optionale Befehl zur Schlüsselverwaltung für die Authentifizierung sowohl für Aironet-Clients mit schneller Roaming-Prüfung als auch

für Clients ohne schnelle Roaming-Prüfung?

Antwort: Wenn Sie Cisco Centralized Key Management (CKM) auf optional einstellen, funktioniert die Einstellung sowohl für Aironet-Clients, die das schnelle Roaming überprüft haben, als auch für Clients, die kein schnelles Roaming überprüft haben.

F. Für wie lange werden die Anmeldeinformationen des WLSM-Cache-Benutzers angegeben?

Antwort: Die Cache-Zeit kann vom Client-Typ abhängen. Zwischen dem AP und dem mobilen Knoten (MN) gibt es einen Keep-Alive-Modus, der von der AP-Konfiguration und dem Client-Typ abhängt. Wenn es sich um einen Cisco Client handelt, erkennt der Access Point schnell, dass der Client nicht vorhanden ist, und hinterlässt seine Zuordnungsliste. Danach verbleibt der Client etwa 10 Minuten in der MN-Liste des WDS in einem separaten Zustand.

Wenn es sich um einen Drittanbieter-Client handelt, kann die Keep-Alive-Zeitüberschreitung auf einem AP sehr lang sein, bis zu 30 Minuten.

Wenn sich der Cisco Client 10 Minuten lang nicht in der dot11-Zuordnungstabelle in einem Access Point befindet, ist eine erneute Authentifizierung erforderlich, d. h., er wird an den Authentifizierungsserver gesendet, nicht an den Infrastruktur-Access, der auf dem gecachten Benutzer basiert. Wenn ein Client eines anderen Anbieters 10 bis 30 Minuten lang nicht in der dot11-Zuordnungstabelle des Access Points aufgeführt ist, ist eine erneute Authentifizierung erforderlich.

F. Kann ich in einem WDS mit AP-basiertem WDS mehr als 60 APs einrichten?

Antwort: Verwenden Sie nicht mehr als 60 APs auf einem primären WDS. Bei mehr als 60 APs können CPU-Auslastungsprobleme auftreten. Es können mehrere primäre WDS verwendet werden, die sich jedoch in unterschiedlichen Subnetzwerken befinden müssen. Ein Beispiel ist die Verwendung von:

- Ein primärer WDS und 30 APs für 10.10.10.10
- Ein weiterer primärer WDS und 30 APs für 10.10.20.20

In diesem Fall besteht das Problem darin, dass Sie nicht schnell zwischen WDS-Domänen wechseln können.

F. Wie viele WDS-Sicherungskandidaten kann ich haben? Kann ein WDS-Sicherungskandidat weiterhin als AP im WDS fungieren und die Informationen an das primäre WDS weiterleiten?

Antwort: Die Anzahl der WDS-Sicherungskandidaten ist unbegrenzt. Ja, die Sicherungskandidaten fungieren weiterhin als APs, die dem primären WDS Bericht erstatten. Darüber hinaus stellt nur der primäre WDS AP WLSE-Sicherheitsschlüssel her und registriert sich beim WLSE, um mit dem WLSE zu interagieren. Nur wenn das primäre WDS ausfällt, übernimmt das Backup-WDS die Rolle eines aktiven WDS-Access Points und registriert sich dann beim WLSE und stellt die Sicherheitsschlüssel her. Solange das primäre WDS aktiv ist, fungiert das Backup-WDS als normaler WAP, der dem primären WDS meldet.

F. Wenn ich drei WDS-APs habe, die alle ausfallen, betrifft der Ausfall nur WDS-

Informationen oder alle APs und Clients? Mit anderen Worten, stellt das WDS einen Fehlerpunkt für das Wireless-Netzwerk dar?

Antwort: Wenn Ihre primären WDS ausfallen, schlagen auch alle APs fehl. Wenn die APs jedoch über alle Konfigurationen verfügen, die für eine unabhängige Funktion des Access Points erforderlich sind, können die Access Points auch ohne WDS arbeiten, wenn das WDS-Gerät ausfällt.

F. In einem Subnetzwerk ist ein WDS mit der Priorität 200 und ein WDS mit der Priorität 100 konfiguriert. Wenn das primäre WDS mit der Priorität 200 ausfällt, wird das WDS mit der Priorität 100 zum primären WDS im Subnetzwerk?

Antwort: In diesem Fall wird das primäre WDS mit der Priorität 100 zum primären WDS, wenn sich dieses WDS im gleichen Subnetz befindet. Wenn sich dieses WDS in einem anderen Subnetz befindet, wird es nicht zum primären Netzwerk.

F. Gibt der Befehl `show iapp rogue-ap-list` in einem Cisco 1200 AP nützliche Informationen, wenn keine Wireless LAN Solution Engine (WLSE) vorhanden ist?

Antwort: Nein, dieser Befehl funktioniert nur in Verbindung mit der WLSE und wenn Sie den Location Manager in der WLSE verwenden.

F. Ich habe einen Cisco AP1200 für WDS konfiguriert. Der Access Point reagiert auf der Konsole oder auf Telnet erst, wenn ich ein- und ausgeschaltet habe. Der Access Point stürzt jedoch nicht ab. Warum geschieht das?

Antwort: Dieses Problem tritt aufgrund der Cisco Bug ID CSCsc01706 (nur registrierte Kunden) auf. Dieses Problem tritt nur auf dem WDS-AP auf, wenn mehrere Wireless-Clients versuchen, eine Verbindung herzustellen oder zu roamen. Dieses Problem wurde in der Cisco IOS Software-Version 12.3(4)JA gestartet, aber die meisten Probleme werden in der Cisco IOS-Softwareversion 12.3(7)JA gemeldet. Die Wireless LAN Solution Engine (WLSE), die die SNMP-Abfrage (Simple Network Management Protocol) für das MAC-Spoofing-Ereignis sendet, löst das Problem aus. Der WDS AP zeichnet eine Reihe von MAC-Spoofing-Ereignissen auf mindestens zwei APs auf. Um dieses Problem zu beheben, müssen Sie ein Upgrade auf die Cisco IOS Software Release 12.3(8)JA oder höher durchführen.

F. Kann ein Repeater-AP WDS unterstützen?

Antwort: Repeater-Access Points unterstützen WDS nicht. Konfigurieren Sie einen Repeater-Access Point nicht als WDS-Kandidat, und konfigurieren Sie keinen WDS-Access Point so, dass er bei einem Ethernet-Ausfall in den Repeater-Modus zurückfällt.

F. Kann ein Access Point der Serie 350 als WDS Access Point konfiguriert werden?

Antwort: Ein Access Point der Serie 350 kann nicht als WDS-Access Point konfiguriert werden. Sie können jedoch Access Points der Serie 350 für die Verwendung des WDS Access Points konfigurieren.

Zugehörige Informationen

- Konfiguration von Wireless-Domänenservices
- Unterstützung von Wireless-, LAN- (WLAN)-Technologie
- Technischer Support und Dokumentation - Cisco Systems