Domande frequenti su Servizi di dominio wireless

Sommario

Introduzione

In questo documento vengono fornite informazioni sulle domande più frequenti (FAQ) relative a Servizi di dominio wireless (WDS).

D. Che cos'è WDS?

R. WDS fa parte di Cisco Structured Wireless Aware Network (SWAN). WDS è una raccolta di funzionalità software di Cisco IOS® che migliorano la mobilità dei client WLAN e semplificano l'installazione e la gestione della WLAN. WDS è una nuova funzionalità per gli access point (AP) nel software Cisco IOS e alla base di Cisco Catalyst serie 6500 Wireless LAN Services Module (WLSM). WDS è una funzione di base che consente di utilizzare altre funzionalità, ad esempio:

- Roaming sicuro rapido (FSR)
- Interazione Wireless LAN Solution Engine (WLSE)
- Gestione radio (RM)

Prima di utilizzare altre funzionalità basate su Servizi di distribuzione Windows, è necessario stabilire relazioni tra gli access point che partecipano a Servizi di distribuzione Windows e il dispositivo configurato come Servizi di distribuzione Windows. Uno degli scopi principali di Servizi di distribuzione Windows è memorizzare nella cache le credenziali utente non appena il server di autenticazione autentica il client per la prima volta. Nei tentativi successivi, WDS autentica il client in base alle informazioni memorizzate nella cache.

D. Come configurare l'access point come servizio di distribuzione Windows?

R. Per informazioni su come configurare l'access point come servizio WDS, consultare il documento sulla configurazione di Servizi di dominio wireless.

D. Su quali piattaforme vengono eseguiti i servizi WDS Cisco Structured Wireless-Aware Network (SWAN)?

R. È possibile eseguire SWAN WDS su Cisco Aironet AP, switch Cisco Catalyst o router Cisco. Di seguito è riportato l'elenco delle piattaforme che attualmente supportano SWAN WDS:

- Aironet serie 1230 AG AP
- Aironet serie 1240AG AP
- Aironet serie 1200 AP
- Aironet serie 1130 AG AP
- Aironet serie 1100 AP
- Catalyst serie 6500 Wireless LAN Services Module (WLSM)
- Cisco serie 3800, 3700 Integra Services Router (ISR) e alcuni modelli di ISR serie 2800 e 2600 con Cisco IOS versione 12.3(11)T o successive.

D. Quali sono le differenze tra WDS basati su AP e WDS basati su switch?

R. Quando si utilizza un WDS basato su AP, Cisco SWAN supporta:

- Roaming sicuro veloce (FSR) di layer 2 (L2)
- Gestione scalabile di LAN wireless (WLAN)
- Funzionalità avanzate di gestione della radio (RM)
- Sicurezza wireless migliorata

Quando utilizzate WDS basato su switch, SWAN supporta:

- FSR L2/Layer 3 (L3)
- Funzionalità RM avanzate
- Sicurezza completa
- Quality of Service (QoS) completo nelle implementazioni WLAN negli campus.

D. Come configurare WDS con la rete WLAN corrente?

R. Per configurare WDS, è necessario designare un access point o il modulo WLSM (Wireless LAN Services Module) come WDS. L'access point Servizi di distribuzione Windows deve stabilire una relazione con un server di autenticazione tramite l'autenticazione con un nome utente e una password di Servizi di distribuzione Windows. Il server di autenticazione può essere un server RADIUS (Remote Authentication Dial-In User Service) esterno o la funzionalità server RADIUS locale nel punto di accesso di Servizi di distribuzione Windows. Il modulo WLSM deve avere una relazione con il server di autenticazione, anche se non deve eseguire l'autenticazione nel server.

D. Qual è il ruolo del dispositivo WDS nella rete WLAN (Wireless LAN)?

R. Il dispositivo WDS esegue le seguenti attività sulla WLAN:

- Pubblicizza la funzionalità WDS e partecipa alla scelta del dispositivo WDS più adatto per la tua WLAN.Quando si configura la WLAN per WDS, si imposta un dispositivo come candidato principale per WDS e uno o più dispositivi aggiuntivi come candidati per WDS di backup. Se il dispositivo WDS principale non è in linea, uno dei dispositivi WDS di backup sostituisce il dispositivo principale.
- Autentica tutti gli access point nella sottorete e stabilisce un canale di comunicazione sicuro con ciascuno di essi.
- Raccoglie i dati radio dai punti di accesso della sottorete, li aggrega e li inoltra al dispositivo Wireless LAN Solution Engine (WLSE) della rete.
- Registra tutti i dispositivi client nella sottorete, stabilisce le chiavi di sessione per i dispositivi client e memorizza nella cache le credenziali di sicurezza del client.Quando un client esegue il roaming in un altro punto di accesso, il dispositivo WDS inoltra le credenziali di sicurezza del client al nuovo punto di accesso.

D. In che modo le WDS e i punti di accesso all'infrastruttura della WLAN comunicano tra loro?

R. Il WDS e i punti di accesso dell'infrastruttura comunicano tramite un protocollo multicast denominato Wireless LAN Context Control Protocol (WLCCP). Impossibile instradare questi

messaggi multicast. Pertanto, un WDS e i punti di accesso dell'infrastruttura associati devono trovarsi nella stessa sottorete IP e sullo stesso segmento LAN. Tra WDS e Wireless LAN Solution Engine (WLSE), WLCCP utilizza il protocollo TCP (Transmission Control Protocol) e il protocollo UDP (User Datagram Protocol) sulla porta 2887. Quando WDS e WLSE si trovano su sottoreti diverse, non è possibile eseguire la conversione dei pacchetti con un protocollo come NAT (Network Address Translation).

D. È possibile configurare l'access point/bridge 1300 come sistema WDS principale?

R. Non è possibile configurare Cisco Aironet 1300 AP/Bridge come WDS primario. 1300 AP/Bridge non supporta questa funzionalità. Il 1300 AP/Bridge può far parte di una rete WDS in cui altri AP o WLSM fungono da WDS principale.

D. Quanti access point per l'infrastruttura è in grado di gestire un singolo WDS?

R. Un singolo WDS AP può supportare un massimo di 60 punti di accesso all'infrastruttura quando l'interfaccia radio è disabilitata. Il numero scende a 30 se anche l'access point che funge da access point Servizi di distribuzione Windows accetta associazioni client.

Uno switch dotato di Wireless LAN Services Module (WLSM) supporta fino a 300 access point.

D. Che cos'è il roaming protetto veloce (FSR)?

R. FSR è una delle funzionalità offerte da WDS. FSR è supportato dai Cisco Aironet serie 1200 e 1100 AP in combinazione con dispositivi client Cisco o dispositivi client compatibili con Cisco. Con FSR, i dispositivi client autenticati possono spostarsi in modo sicuro al layer 2 (L2) da un access point all'altro senza alcun ritardo visibile durante la riassociazione. FSR supporta applicazioni sensibili alla latenza, ad esempio:

- VoIP (Wireless Voice over IP)
- ERP (Enterprise Resource Planning)
- Soluzioni basate su Citrix

WDS fornisce servizi di handoff rapidi e sicuri agli access point, senza interruzione delle connessioni. I servizi sono destinati ad applicazioni, ad esempio la voce, che richiedono tempi di roaming inferiori a 150 ms.

D. Che cos'è il roaming di layer 3 (L3)?

R. Con il roaming di layer 2 (L2), il client wireless esegue il roaming tra due access point che fanno parte della stessa sottorete sul lato cablato. WDS basato su AP fornisce questa funzionalità. Con le WDS basate su AP, è necessario configurare gli AP in modo che si trovino sulla stessa VLAN.

Con il roaming L3, il client wireless effettua il roaming tra due access point che risiedono in due sottoreti diverse. Pertanto, il client effettua il roaming tra due VLAN diverse sul lato cablato. In questo modo viene rimossa la creazione di VLAN che si estendono sull'intero campus e vengono create da WDS basato su AP. I dispositivi client utilizzano i tunnel mGRE (Multipoint Generic Routing Encapsulation) per eseguire il roaming verso gli access point che risiedono in sottoreti L3 diverse. I client in roaming rimangono connessi alla rete senza la necessità di modificare gli

indirizzi IP.

D. Qual è il ruolo del Wireless LAN Solution Engine (WLSE) in una rete WLAN (Wireless LAN) abilitata per WDS?

R. I punti di accesso e, facoltativamente, i dispositivi client Cisco o i dispositivi client compatibili con Cisco eseguono misurazioni a radiofrequenza (RF) all'interno di una singola sottorete. Cisco SWAN WDS aggrega le misure e le inoltra a CiscoWorks WLSE per analizzarle. Sulla base di queste misurazioni, CiscoWorks WLSE può:

- Rilevare punti di accesso non autorizzati e interferenze da altri dispositivi.**Nota:** in WLSE è possibile visualizzare un massimo di 5000 righe. Se il WLSE ha raggiunto questo limite anomalo, viene visualizzato il messaggio di errore `Limite di rilevamento di errori di infrastruttura/ad-hoc`. In questi casi, per eliminare i router da WLSE, selezionare **IDS > Manage Rogues** (ID > Gestisci server non autorizzati), scegliere l'opzione **"Select *ALL*"** *& '**Delete**' (Seleziona *TUTTI*" & **Elimina**) per eliminare i router.Se il numero di radio sconosciuto (non autorizzato) è superiore a 5000 nell'ambiente in uso, premere nuovamente questo numero e viene visualizzato lo stesso messaggio di avviso. L'unico modo per ovviare a questo problema è gestire queste radio o contrassegnarle come facili da usare.
- Effettuare indagini in loco
- Supporto della risoluzione automatica WLAN per un canale ottimale e impostazioni del livello di potenza

D. Quali sono i vantaggi dell'uso di WDS su un modulo WLSM (Wireless LAN Services Module)?

R. L'introduzione del WDS basato su switch e del WLSM facilita il roaming sicuro veloce (FSR) Layer 3 (L3) e fornisce una soluzione altamente scalabile per la mobilità L3 nel campus. WDS basato su switch centralizza la funzionalità di WDS nel blade WLSM in uno switch centrale e offre i seguenti vantaggi:

- Maggiore scalabilità WDS: la scalabilità aumenta fino a 300 punti di accesso e 6000 utenti su una rete WLAN (Wireless LAN) del campus.
- Progettazione e implementazione semplificate: nessuna VLAN si estende sulla rete del campus. Con l'architettura mGRE (Multipoint Generic Routing Encapsulation), non sono necessarie modifiche all'infrastruttura cablata di rete corrente.
- Gestibilità per un'installazione WLAN di grandi dimensioni: questa soluzione fornisce un unico punto di ingresso sia per il controllo WLAN che per i dati utente nella rete cablata per cui applicare le policy di sicurezza e qualità del servizio (QoS).
- Mobilità L3 tra piani e tra più edifici
- Possibilità di utilizzare le funzionalità avanzate di Cisco Catalyst 6500, che include altri Catalyst 6500 Service Module
- Sicurezza end-to-end e QoS migliorate grazie all'integrazione con la piattaforma Catalyst 6500

D. Qual è la funzione di gestione della radio (RM) di WDS?

A. Un punto di accesso abilitato per WDS funge anche da aggregatore per le statistiche sulle

radiofrequenze (RF) provenienti dagli altri punti di accesso. Il punto di accesso abilitato per WDS trasmette queste statistiche al Wireless LAN Solution Engine (WLSE) per evidenziare i punti di accesso non autorizzati. Il monitor di RF consente al WLSE di creare una mappa di copertura wireless. Il WLSE utilizza anche i punti di accesso attuali per effettuare indagini in loco e identificare le aree senza copertura. È possibile importare le planimetrie sul software per rendere le aree in cui sono necessari punti di accesso aggiuntivi facilmente individuabili.

D. I Cisco Aironet AP possono supportare i client durante la scansione dell'ambiente a radiofrequenza (RF)?

R. Sì, i Cisco AP sono multifunzionali. I Cisco AP servono i client e monitorano anche l'aria/RF. Si consiglia sempre di avere meno client associati all'access point configurati come Servizi di distribuzione Windows.

D. WDS è in grado di eseguire funzioni di contabilità?

R. No. WDS può eseguire l'autenticazione ma non l'accounting. L'accounting è completamente indipendente ed è necessario disporre di un server RADIUS per questa funzione.

D. Per configurare WDS con CCKM, quali sono le suite di cifratura supportate? Extensible Authentication Protocol-Flexible Authentication through Secured Tunnel (EAP-FAST) è compatibile con Cisco CKM? Quale combinazione si utilizza?

R. Per utilizzare Cisco CKM, è necessario usare una suite di cifratura. Queste combinazioni di suite di cifratura sono supportate dalla CCKM.

- crittografia wep128
- crittografia, modalità cifratura wep40
- crittografia, modalità ciphers ckip
- crittografia, modalità cifratura ckip-cmic
- crittografia, modalità cifratura cmic
- tkip modalità crittografia

EAP-FAST/Cisco CKM è supportato con le schede Cisco Aironet 350 e presto sarà supportato con le schede Aironet CB21AG. Di seguito è riportato il comando per abilitare la cifratura:

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

EAP-FAST non utilizza la chiave WEP impostata. EAP-FAST utilizza una chiave dinamica.

D. Il comando authentication key-management cckm optional funziona sia per i client Aironet con roaming veloce selezionato che per quelli senza roaming veloce selezionato?

R. Se Cisco Centralized Key Management (CKM) è impostato su facoltativo, l'impostazione funziona sia per i client Aironet con roaming veloce selezionato che per i client senza roaming veloce selezionato.

D. Per quanto tempo vengono memorizzate nella cache le credenziali utente di WLSM?

R. Il tempo di cache può dipendere dal tipo di client. Tra il punto di accesso e il nodo mobile (MN) è presente un keep-alive, che dipende dalla configurazione del punto di accesso e dal tipo di client. Se si tratta di un client Cisco, l'access point rileva rapidamente l'assenza del client e lascia il relativo elenco di associazioni. In tal caso, il client rimane nell'elenco MN di WDS in uno stato disconnesso per circa 10 minuti.

Se si tratta di un client di terze parti, il timeout di keep-alive su un access point può essere molto lungo, fino a 30 minuti.

Fondamentalmente, se il client Cisco non si trova nella tabella delle associazioni dot11 in un punto di accesso per 10 minuti, è necessaria la riautenticazione, ossia l'invio al server di autenticazione anziché all'access point dell'infrastruttura basato sull'utente memorizzato nella cache. Se un client non Cisco non si trova nella tabella delle associazioni dot11 in un access point per un periodo compreso tra 10 e 30 minuti, è necessaria una riautenticazione.

D. È possibile configurare più di 60 punti di accesso in un servizio di distribuzione Windows che utilizza servizi di distribuzione Windows basati su punti di accesso?

R. Non utilizzare più di 60 access point su un WDS primario. È possibile riscontrare problemi di utilizzo della CPU con più di 60 punti di accesso. È possibile avere più WDS primari, ma è necessario che si trovino in sottoreti diverse. Un esempio è l'utilizzo di:

- Un WDS principale e 30 AP sulla versione 10.10.10.10
- Un altro WDS primario e 30 AP alla 10.10.20.20

In questo caso, il problema è che non è possibile eseguire il roaming veloce tra i domini di Servizi di distribuzione Windows.

D. Quanti candidati di backup WDS posso avere? Un candidato di backup di Servizi di distribuzione Windows può ancora funzionare come punto di accesso in Servizi di distribuzione Windows e segnalare le informazioni al Servizio di distribuzione Windows principale?

R. Non esistono limiti al numero di candidati per il backup di Servizi di distribuzione Windows. Sì, i backup candidati funzionano ancora come punti di accesso che fanno riferimento al servizio WDS principale. Inoltre, solo l'access point WDS primario stabilisce le chiavi di sicurezza WLSE e si registra nel WLSE per interagire con quest'ultimo. Solo se il servizio di distribuzione Windows primario non funziona, il servizio di distribuzione Windows di backup assume il ruolo di un punto di accesso di Servizi di distribuzione Windows attivo e continua a registrarsi nel servizio e a stabilire le chiavi di sicurezza. Finché il servizio di distribuzione Windows principale è attivo, il servizio di distribuzione Windows di backup funziona come un normale punto di accesso che fa riferimento al servizio di distribuzione Windows principale.

D. Se si verificano errori in tre punti di accesso Servizi di distribuzione Windows, l'errore influisce solo sulle informazioni di Servizi di distribuzione Windows oppure su tutti i punti di accesso e i client? In altre parole, WDS è un punto di errore per la rete wireless?

R. Se i WDS principali hanno esito negativo, anche tutti i punti di accesso hanno esito negativo. Tuttavia, se gli access point dispongono di tutte le configurazioni necessarie per il funzionamento indipendente degli access point, questi iniziano a funzionare senza WDS in caso di guasto del dispositivo WDS.

D. In una sottorete, si dispone di una WDS configurata con priorità 200 e di una WDS con priorità 100. Se la WDS primaria con priorità 200 ha esito negativo, la WDS con priorità 100 diventa la principale nella sottorete?

R. In questo caso, il WDS primario con priorità 100 diventa il principale se il WDS si trova nella stessa sottorete. Se questo servizio di distribuzione Windows si trova in un'altra sottorete, non diventerà la rete primaria.

D. Il comando `show app rogue-ap-list` in un Cisco 1200 AP fornisce informazioni utili quando non è installato Wireless LAN Solution Engine (WLSE)?

R. No, questo comando funziona solo in combinazione con WLSE e quando si utilizza Location Manager in WLSE.

D. È stato configurato un Cisco AP1200 per WDS. L'access point si blocca e non risponde sulla console o su Telnet finché non viene eseguito un ciclo di alimentazione. Tuttavia, l'access point non si blocca. Perché questo accade?

R. Il problema è causato dall'ID bug Cisco CSCsc01706 (solo utenti registrati). Questo problema si verifica solo nel punto di accesso di Servizi di distribuzione Windows quando diversi client wireless tentano di associarsi o di spostarsi. Questo problema è stato avviato nel software Cisco IOS versione 12.3(4)JA, ma la maggior parte dei problemi è segnalata nel software Cisco IOS versione 12.3(7)JA. Il problema viene attivato dal Wireless LAN Solution Engine (WLSE) che invia la query SNMP (Simple Network Management Protocol) sull'evento di spoofing MAC. L'access point WDS registra un numero di eventi di spoofing MAC su almeno due access point. Per risolvere questo problema, è necessario aggiornare il software Cisco IOS alla versione 12.3(8)JA o successive.

D. Un punto di accesso ripetitore può supportare WDS?

R. I punti di accesso ripetitori non supportano WDS. Non configurare un punto di accesso ripetitore come candidato WDS e non configurare un punto di accesso WDS per il fallback alla modalità ripetitore in caso di errore Ethernet.

D. È possibile configurare un access point serie 350 come punto di accesso WDS?

R. Non è possibile configurare un punto di accesso serie 350 come punto di accesso WDS. Tuttavia, è possibile configurare i punti di accesso serie 350 in modo che utilizzino il punto di accesso WDS.

Informazioni correlate

- Configurazione di Servizi di dominio wireless
- Supporto della tecnologia Wireless, LAN (WLAN)
- Documentazione e supporto tecnico – Cisco Systems