

Wireless Domain Services FAQ

Document ID: 65346

Questions

Introduction

What is WDS?

How do I configure my AP as a WDS?

On what platforms does Cisco Structured Wireless-Aware Network (SWAN) WDS run?

How does AP-based WDS compare with switch-based WDS?

How do I set up WDS with my current wireless LAN (WLAN) network?

What is the role of the WDS device in the wireless LAN (WLAN) network?

How do the WDS and the infrastructure APs in the WLAN communicate with each other?

Can I configure the 1300 AP/Bridge as a WDS master?

How many infrastructure APs can a single WDS manage?

What is fast secure roaming (FSR)?

What is Layer 3 (L3) roaming?

What is the role of the Wireless LAN Solution Engine (WLSE) in a WDS-enabled wireless LAN (WLAN) network?

What are the advantages of the use of WDS on a Wireless LAN Services Module (WLSM)?

What is the radio management (RM) feature of WDS?

Can Cisco Aironet APs support clients while the APs scan the air/radio frequency (RF) environment?

Can WDS perform accounting functions?

In order to set up WDS with CCKM what are the cipher suites supported? Is Extensible Authentication Protocol-Flexible Authentication through Secured Tunnel (EAP-FAST) compatible with Cisco CKM? What combination do I use?

Does the authentication key-management cckm optional command work for both Aironet clients with fast roaming checked and those without fast roaming checked?

For how long does the WLSM cache user credentials?

Can I set up more than 60 APs in a WDS that uses AP-based WDS?

How many WDS backup candidates can I have? Can a WDS backup candidate still function as an AP in the WDS and report the information to the primary WDS?

If I have three WDS APs and they all fail, does the failure only affect WDS information, or all APs and clients? In other words, is the WDS a point of failure for the wireless network?

On one subnetwork, I have a WDS configured with a priority of 200 and a WDS with a priority of 100. If the WDS master with a priority of 200 fails, does the WDS with the priority of 100 become the master on the subnetwork?

Does the `show iapp rogue-ap-list` command in a Cisco 1200 AP provide any useful information when a Wireless LAN Solution Engine (WLSE) is not in place?

I have a Cisco AP1200 configured for WDS. The AP hangs and does not respond on the console or Telnet until I perform a power cycle. However, the AP does not crash. Why does this happen?

Can a repeater AP support WDS?

Can a 350 series AP be configured as WDS access point?

Related Information

Introduction

This document provides information on the most frequently asked questions (FAQ) about Wireless Domain Services (WDS).

Q. What is WDS?

A. WDS is a part of the Cisco Structured Wireless Aware Network (SWAN). WDS is a collection of Cisco IOS® Software features that enhance WLAN client mobility, and simplify WLAN deployment and management. WDS is a new feature for access points (APs) in Cisco IOS Software, and the basis of the Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM). WDS is a core function that enables other features, such as:

- ◆ Fast secure roaming (FSR)
- ◆ Wireless LAN Solution Engine (WLSE) interaction
- ◆ Radio management (RM)

Before the operation of any other WDS-based features, you must establish relationships between the APs that participate in WDS and the device that is configured as the WDS. One of the main purposes of WDS is to cache the user credentials as soon as the authentication server authenticates the client for the first time. On subsequent attempts, WDS authenticates the client on the basis of the cached information.

Q. How do I configure my AP as a WDS?

A. Refer to Wireless Domain Services Configuration for information on how to configure the AP as a WDS.

Q. On what platforms does Cisco Structured Wireless-Aware Network (SWAN) WDS run?

A. You can run SWAN WDS on Cisco Aironet APs, Cisco Catalyst switches, or Cisco routers. Here is the list of platforms that currently support SWAN WDS:

- ◆ Aironet 1230 AG Series APs
- ◆ Aironet 1240AG Series APs
- ◆ Aironet 1200 Series APs
- ◆ Aironet 1130 AG Series APs
- ◆ Aironet 1100 Series APs
- ◆ Catalyst 6500 Series Wireless LAN Services Module (WLSM)
- ◆ Cisco 3800, 3700 series Integrates Services Routers (ISR) and some models of 2800 and 2600 series ISR that run Cisco IOS version 12.3(11)T or later.

Q. How does AP-based WDS compare with switch-based WDS?

A. When you use AP-based WDS, Cisco SWAN supports:

- ◆ Layer 2 (L2) fast secure roaming (FSR)
- ◆ Scalable wireless LAN (WLAN) management
- ◆ Advanced radio management (RM) capabilities
- ◆ Enhanced wireless security

When you use switch-based WDS, SWAN supports:

- ◆ L2/Layer 3 (L3) FSR
- ◆ Advanced RM capabilities
- ◆ End-to-end security
- ◆ End-to-end quality of service (QoS) in campus WLAN deployments.

Q. How do I set up WDS with my current wireless LAN (WLAN) network?

A. In order to set up WDS, you must designate one AP or the Wireless LAN Services Module (WLSM) as the WDS. The WDS AP must establish a relationship to an authentication server through authentication with a WDS user name and password. The authentication server can be either an external Remote Authentication Dial-In User Service (RADIUS) server or the local RADIUS server feature in the WDS AP. The WLSM must have a relationship with the authentication server, even though the WLSM does not need to authenticate to the server.

Q. What is the role of the WDS device in the wireless LAN (WLAN) network?

A. The WDS device performs these tasks on your WLAN:

- ◆ Advertises WDS capability and participates in an election of the best WDS device for your WLAN.

When you configure your WLAN for WDS, you set up one device as the main WDS candidate and one or more additional devices as backup WDS candidates. If the main WDS device goes offline, one of the backup WDS devices takes the place of the main device.

- ◆ Authenticates all APs in the subnetwork and establishes a secure communication channel with each of the APs.
- ◆ Collects radio data from APs in the subnetwork, aggregates the data, and forwards the data to the Wireless LAN Solution Engine (WLSE) device on your network.
- ◆ Registers all client devices in the subnetwork, establishes session keys for the client devices, and caches the client security credentials.

When a client roams to another AP, the WDS device forwards the client security credentials to the new AP.

Q. How do the WDS and the infrastructure APs in the WLAN communicate with each other?

A. The WDS and the infrastructure APs communicate over a multicast protocol called the Wireless LAN Context Control Protocol (WLCCP). These multicast messages cannot be routed. Therefore, a WDS and the associated infrastructure APs must be in the same IP subnetwork and on the same LAN segment. Between the WDS and the Wireless LAN Solution Engine (WLSE), WLCCP uses Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) on port 2887. When the WDS and WLSE are on different subnetworks, packet translation with a protocol like Network Address Translation (NAT) cannot occur.

Q. Can I configure the 1300 AP/Bridge as a WDS master?

A. You cannot configure the Cisco Aironet 1300 AP/Bridge as a WDS master. The 1300 AP/Bridge does not support this functionality. The 1300 AP/Bridge can participate in a WDS

network in which some other AP or WLSM acts as the WDS master.

Q. How many infrastructure APs can a single WDS manage?

A. A single WDS AP can support a maximum of 60 infrastructure APs when the radio interface is disabled. The number drops to 30 if the AP that acts as the WDS AP also accepts client associations.

A Wireless LAN Services Module (WLSM)–equipped switch supports up to 300 APs.

Q. What is fast secure roaming (FSR)?

A. FSR is one of the features that WDS offers. FSR is supported by Cisco Aironet 1200 and 1100 Series APs in conjunction with Cisco client devices or Cisco–compatible client devices. With FSR, authenticated client devices can roam securely at Layer 2 (L2) from one AP to another without any perceptible delay during re–association. FSR supports latency–sensitive applications, such as:

- ◆ Wireless Voice over IP (VoIP)
- ◆ Enterprise resource planning (ERP)
- ◆ Citrix–based solutions

WDS provides fast, secure handoff services to APs, without the drop of connections. The services are for applications, such as voice, that require roaming times that are less than 150 ms.

Q. What is Layer 3 (L3) roaming?

A. With Layer 2 (L2) roaming, the wireless client roams between two APs that are part of the same subnetwork on the wired side. AP–based WDS provides this functionality. With AP–based WDS, you must configure the APs to be in the same VLAN.

With L3 roaming, the wireless client roams between two APs that reside in two different subnetworks. Therefore, the client roams between two different VLANs on the wired side. This removes the creation of VLANs that span the entire campus, which the AP–based WDS create. Client devices use multipoint generic routing encapsulation (mGRE) tunnels in order to roam to APs that reside on different L3 subnetworks. The roaming clients remain connected to your network without the need to change IP addresses.

Q. What is the role of the Wireless LAN Solution Engine (WLSE) in a WDS–enabled wireless LAN (WLAN) network?

A. APs and, optionally, Cisco client devices or Cisco–compatible client devices take radio frequency (RF) measurements within a single subnetwork. Cisco SWAN WDS aggregates the measurements and forwards the measurements to CiscoWorks WLSE for analysis. With these measurements as a basis, CiscoWorks WLSE can:

- ◆ Detect rogue APs and interference from other devices.

Note: The maximum number of rogues that can be shown in WLSE is 5000. If the WLSE has reached this rogue limit, the `Limit of Infrastructure/Ad-hoc rogues tracking` error message appears. In such cases, to delete these rogues from WLSE, navigate to **IDS > Manage Rogues**, choose the **"Select *ALL*" * & 'Delete'** option in order to delete the rogues.

If the unknown (rogue) radio count is over 5000 in your environment, you again hit this number and the same warning message appears. The only way to overcome this is to either manage those radios or mark those radios as friendly.

- ◆ Provide assisted site surveys
- ◆ Support WLAN self-healing for optimal channel and power-level setting

Q. What are the advantages of the use of WDS on a Wireless LAN Services Module (WLSM)?

A. The introduction of switch-based WDS and the WLSM facilitates Layer 3 (L3) fast secure roaming (FSR) and provides a highly scalable solution for L3 mobility in the campus. Switch-based WDS centralizes the functionality of WDS in the WLSM blade in a central switch and provides these benefits:

- ◆ Increased WDS scalability The scalability increases to 300 APs and 6000 users across a campus wireless LAN (WLAN) network.
- ◆ Simplified design and implementation No VLANs span the campus network. With the use of multipoint generic routing encapsulation (mGRE) architecture, no changes to the current network wired infrastructure are necessary.
- ◆ Manageability for a large WLAN deployment This solution provides a single point of ingress for both WLAN control and user data into the wired network for which to apply security and quality of service (QoS) policies.
- ◆ L3 mobility between floors and across multiple buildings
- ◆ The ability to use advanced features on the Cisco Catalyst 6500, which includes other Catalyst 6500 service modules
- ◆ Enhanced end-to-end security and QoS by integration with the Catalyst 6500 platform

Q. What is the radio management (RM) feature of WDS?

A. A WDS-enabled AP also acts as an aggregator for radio frequency (RF) statistics from the other APs. The WDS-enabled AP passes along these statistics to the Wireless LAN Solution Engine (WLSE) in order to highlight rogue APs. The monitor of RF allows the WLSE to create a map of wireless coverage. The WLSE also uses current APs in order to carry out site surveys and identify areas with no coverage. You can import floor plans onto the software to make areas where you need extra APs easy to spot.

Q. Can Cisco Aironet APs support clients while the APs scan the air/radio frequency (RF) environment?

A. Yes, Cisco APs are multifunctional. Cisco APs serve clients and also monitor the air/RF. It is always recommended to have less clients associated to the AP configured as WDS.

Q. Can WDS perform accounting functions?

A. No. WDS can perform authentication but not accounting. Accounting is totally independent and you need to have a RADIUS server for this function.

Q. In order to set up WDS with CCKM what are the cipher suites supported? Is Extensible Authentication Protocol-Flexible Authentication through Secured Tunnel (EAP-FAST) compatible with

Cisco CKM? What combination do I use?

A. You need to use a cipher suite in order to use Cisco CKM. These Cipher suite combinations are supported with CCKM.

- ◆ encryption mode ciphers wep128
- ◆ encryption mode ciphers wep40
- ◆ encryption mode ciphers ckip
- ◆ encryption mode ciphers ckip-cmic
- ◆ encryption mode ciphers cmic
- ◆ encryption mode ciphers tkip

EAP-FAST/Cisco CKM is supported with the Cisco Aironet 350 cards and, soon, will be supported with the Aironet CB21AG cards. Here is the command to enable the cipher:

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

EAP-FAST does not use the WEP key that you have set. EAP-FAST uses a dynamic key.

Q. Does the authentication key-management cckm optional command work for both Aironet clients with fast roaming checked and those without fast roaming checked?

A. If you set Cisco Centralized Key Management (CKM) to optional, the setting works for both Aironet clients that have fast roaming checked and those clients that do not have fast roaming checked.

Q. For how long does the WLSM cache user credentials?

A. The cache time can depend on the type of client. There is a keep alive between the AP and the mobile node (MN), which depends on the AP configuration and the type of client. If it is a Cisco client, the AP detects the absence of the client quickly and leaves its association list. Once that happens, the client stays in the MN list of the WDS in a detached state for about 10 minutes.

If it is a third party client, the keep alive timeout on an AP can be very long, as long as 30 minutes.

Basically, if the Cisco client is not in the dot11 association table in any AP for 10 minutes, re-authentication is needed, which means to send it to the authentication server instead of to the infrastructure AP based on the cached user. If a non-Cisco client is not in the dot11 association table in any AP for between 10 and 30 minutes, re-authentication is needed.

Q. Can I set up more than 60 APs in a WDS that uses AP-based WDS?

A. Do not use more than 60 APs on one WDS master. You can run into CPU utilization problems with more than 60 APs. You can have multiple WDS masters, but they need to be on different subnetworks. An example is the use of:

- ◆ One WDS master and 30 APs on 10.10.10.10
- ◆ Another WDS master and 30 APs on 10.10.20.20

In this case, the issue is that you cannot fast roam between WDS domains.

Q. How many WDS backup candidates can I have? Can a WDS backup candidate still function as an AP in the WDS and report the information to the primary WDS?

A. There is no limit to the number of WDS backup candidates. Yes, the backup candidates still function as APs that report to the WDS master. In addition, only the primary WDS AP establishes WLSE security keys and registers with the WLSE in order to interact with the WLSE. Only if the primary WDS fails, the backup WDS takes up the role of an active WDS AP and goes on to register with the WLSE and establish security keys. As long as the primary WDS is active, the backup WDS functions as a normal AP that reports to the WDS master.

Q. If I have three WDS APs and they all fail, does the failure only affect WDS information, or all APs and clients? In other words, is the WDS a point of failure for the wireless network?

A. If your WDS masters fail, all APs fail as well. However, if the APs have all the configurations that are necessary for the AP to function independently, the APs begin to work without the WDS when the WDS device fails.

Q. On one subnetwork, I have a WDS configured with a priority of 200 and a WDS with a priority of 100. If the WDS master with a priority of 200 fails, does the WDS with the priority of 100 become the master on the subnetwork?

A. In this case, the WDS master with the priority of 100 becomes the master if this WDS is on the same subnetwork. If this WDS is on another subnetwork, it does not become the master.

Q. Does the show iapp rogue-ap-list command in a Cisco 1200 AP provide any useful information when a Wireless LAN Solution Engine (WLSE) is not in place?

A. No, this command only works in conjunction with the WLSE and when you use the Location Manager in the WLSE.

Q. I have a Cisco AP1200 configured for WDS. The AP hangs and does not respond on the console or Telnet until I perform a power cycle. However, the AP does not crash. Why does this happen?

A. This problem occurs due to Cisco bug ID CSCsc01706 [🔗](#) (registered customers only). This problem occurs only on the WDS AP when several wireless clients try to associate or roam. This issue started in Cisco IOS Software Release 12.3(4)JA, but most problems are reported in Cisco IOS Software Release 12.3(7)JA. The Wireless LAN Solution Engine (WLSE) that sends out the Simple Network Management Protocol (SNMP) query on the MAC spoofing event triggers the issue. The WDS AP records a number of MAC spoofing events on at least two APs. In order to resolve this problem, you must upgrade to Cisco IOS Software Release 12.3(8)JA or later.

Q. Can a repeater AP support WDS?

A. Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to fall back to repeater mode in case of Ethernet failure.

Q. Can a 350 series AP be configured as WDS access point?

A. You cannot configure a 350 series access point as a WDS access point. However, you can configure 350 series access points to use the WDS access point.

Related Information

- [Wireless Domain Services Configuration](#)
- [Wireless LAN Technology Support](#)
- [Fixed and Mobile Wireless Solution Documentation](#)
- [Configuring Cipher suites and WEP](#)
- [Configuring WDS, Fast Secure Roaming, and Radio Management](#)
- [FAQ and Troubleshooting Guide for the CiscoWorks WLSE and WLSE Express, 2.13](#)
- [Fast Secure Roaming](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 21, 2008

Document ID: 65346
