

無線域服務配置

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[無線域服務](#)

[WDS裝置的角色](#)

[使用WDS裝置的接入點的角色](#)

[組態](#)

[將AP指定為WDS](#)

[將WLSM指定為WDS](#)

[將AP指定為基礎設施裝置](#)

[定義客戶端身份驗證方法](#)

[驗證](#)

[疑難排解](#)

[疑難排解指令](#)

[相關資訊](#)

簡介

本檔案介紹無線網域服務(WDS)的概念。本檔案還說明如何將一個存取點(AP)或無線LAN服務模組([Wireless LAN Services Module, WLSM](#))設定為WDS，以及至少將另一個設定為基礎架構AP。本文檔中的過程將引導您找到功能正常的WDS，並允許客戶端關聯到WDS AP或基礎架構AP。本文檔旨在建立一個基礎，您可以根據此基礎配置[快速安全漫遊](#)，或將無線LAN解決方案引擎([WLSE](#))引入網路，以便使用這些功能。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 全面瞭解無線LAN網路和無線安全問題。
- 瞭解當前的可擴展身份驗證協定(EAP)安全方法。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 使用Cisco IOS®軟體的AP
- Cisco IOS軟體版本12.3(2)JA2或更新版本
- Catalyst 6500系列無線LAN服務模組

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從介面BVI1上的已清除 (預設) 組態和IP位址啟動，因此可從Cisco IOS軟體GUI或命令行介面(CLI)存取裝置。如果您在即時網路中工作，請確保您瞭解任何命令的潛在影響。

慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

無線域服務

WDS是Cisco IOS軟體中AP的新功能，是Catalyst 6500系列WLSM的基礎。WDS是一個核心功能，支援其他功能，例如：

- 快速安全漫遊
- WLSE互動
- 無線電管理

必須先在參與WDS的AP和WLSM之間建立關係，其他任何基於WDS的功能才能工作。WDS的用途之一是消除驗證伺服器驗證使用者憑據的需要，並減少客戶端驗證所需的時間。

要使用WDS，必須指定一個AP或WLSM作為WDS。WDS AP必須使用WDS使用者名稱和密碼與身份驗證伺服器建立關係。身份驗證伺服器可以是外部RADIUS伺服器，也可以是WDS AP中的本地RADIUS伺服器功能。WLSM必須與身份驗證伺服器建立關係，即使WLSM不需要向伺服器進行身份驗證。

其他AP (稱為基礎設施AP) 與WDS通訊。在進行註冊之前，基礎設施AP必須向WDS驗證其自身。WDS上的基礎結構伺服器組定義此基礎結構身份驗證。

WDS上的一個或多個客戶端伺服器組定義客戶端身份驗證。

當客戶端嘗試關聯到基礎設施AP時，基礎設施AP會將使用者的憑證傳遞到WDS進行驗證。如果WDS第一次看到憑證，則WDS會轉到身份驗證伺服器來驗證憑證。然後WDS快取憑證，以便消除相同使用者再次嘗試身份驗證時返回身份驗證伺服器的需要。重新身份驗證的示例包括：

- 重新鍵入
- 漫遊
- 使用者啟動客戶端裝置時

任何基於RADIUS的EAP身份驗證協定都可以通過WDS進行隧道傳輸，如下所示：

- 輕量EAP(LEAP)
- 受保護的EAP(PEAP)
- EAP — 傳輸層安全(EAP-TLS)
- 通過安全通道的EAP-Flexible Authentication(EAP-FAST)

MAC地址身份驗證還可以通過隧道連線到外部身份驗證伺服器，或針對WDS AP的本地清單進行身份驗證。WLSM不支援MAC地址身份驗證。

WDS和基礎架構AP通過稱為WLAN情景控制協定(WLCCP)的組播協定進行通訊。這些組播消息無

法路由，因此WDS和相關基礎設施AP必須位於同一個IP子網和同一個LAN網段上。在WDS和WLSE之間，WLCCP在埠2887上使用TCP和使用者資料包協定(UDP)。當WDS和WLSE位於不同的子網中時，網路地址轉換(NAT)等協定無法轉換資料包。

配置為WDS裝置的AP最多支援60個參與的AP。配置為WDS裝置的整合服務路由器(ISR)最多支援100個參與的AP。配備WLSM的交換機支援多達600個參與的AP和240個移動組。單個AP最多支援16個移動組。

注意：思科建議基礎設施AP運行與WDS裝置相同版本的IOS。如果您使用較舊版本的IOS，AP可能無法向WDS裝置進行身份驗證。此外，Cisco建議您使用最新版本的IOS。您可以在[Wireless downloads](#)頁面中找到最新版本的IOS。

WDS裝置的角色

WDS裝置在無線LAN上執行多項任務：

- 通告其WDS功能並參與為您的無線LAN選擇最佳WDS裝置。為WDS配置無線LAN時，需要將一台裝置設定為主要WDS候選裝置，將一台或多台其他裝置設定為備用WDS候選裝置。如果主WDS裝置離線，則其中一個備份WDS裝置將取而代之。
- 對子網中的所有AP進行身份驗證，並與其中每個AP建立安全通訊通道。
- 從子網中的AP收集無線電資料，聚合資料並將其轉發到網路上的WLSE裝置。
- 充當與參與的AP關聯的所有802.1x身份驗證客戶端裝置的傳遞過程。
- 註冊子網中使用動態金鑰的所有客戶端裝置，為其建立會話金鑰，並快取其安全憑據。當客戶端漫遊到另一個AP時，WDS裝置會將客戶端的安全憑證轉發到新AP。

使用WDS裝置的接入點的角色

在以下活動中，無線LAN上的AP與WDS裝置互動：

- 發現並跟蹤當前WDS裝置，並將WDS通告中繼到無線LAN。
- 向WDS裝置驗證並建立與WDS裝置的安全通訊通道。
- 向WDS裝置註冊關聯的客戶端裝置。
- 向WDS裝置報告無線電資料。

組態

WDS以有序的模組化方式顯示配置。每個概念都建立在先前的概念之上。WDS省略了密碼、遠端訪問和無線電設定等其他配置專案，以清晰度並專注於核心主題。

本節提供設定本檔案中所述功能所需的資訊。

註：使用[Command Lookup Tool](#)([僅供](#)已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

將AP指定為WDS

第一步是指定一個AP作為WDS。WDS AP是唯一與身份驗證伺服器進行通訊的接入點。

完成以下步驟，將AP指定為WDS：

1. 要在WDS AP上配置身份驗證伺服器，請選擇**Security > Server Manager**以轉至「伺服器管理器」頁籤：在Corporate Servers下，在Server欄位中鍵入身份驗證伺服器的IP地址。指定共用金鑰和埠。在Default Server Priorities下，將Priority 1欄位設定為相應身份驗證型別下的該伺服器IP地址。

The screenshot shows the Cisco 1200 Access Point configuration page for the Server Manager section. The interface includes a navigation menu on the left with categories like HOME, EXPRESS SET-UP, SECURITY, SERVICES, and WIRELESS SERVICES. The main content area is divided into several sections:

- SERVER MANAGER** (selected) and **GLOBAL PROPERTIES** tabs.
- Hostname**: WDS_AP
- Security: Server Manager** section with a **Backup RADIUS Server** configuration area containing fields for **Backup RADIUS Server** (Hostname or IP Address), **Shared Secret**, and buttons for **Apply**, **Delete**, and **Cancel**.
- Corporate Servers** section with a **Current Server List** (RADIUS) and a **Server** configuration area. The **Server** field is set to 10.0.0.3. Other fields include **Shared Secret**, **Authentication Port (optional)** (1645), and **Accounting Port (optional)** (1646). Buttons for **Apply** and **Cancel** are present.
- Default Server Priorities** section with three columns of priority settings:
 - EAP Authentication**: Priority 1 is set to 10.0.0.3, Priority 2 and 3 are set to < NONE >.
 - MAC Authentication**: Priority 1, 2, and 3 are all set to < NONE >.
 - Accounting**: Priority 1, 2, and 3 are all set to < NONE >.
 - Admin Authentication (RADIUS)**: Priority 1, 2, and 3 are all set to < NONE >.
 - Admin Authentication (TACACS+)**: Priority 1, 2, and 3 are all set to < NONE >.
 - Proxy Mobile IP Authentication**: Priority 1, 2, and 3 are all set to < NONE >.Buttons for **Apply** and **Cancel** are at the bottom right.

或者，也可以從CLI發出以下命令：

2. 下一步是將身份驗證伺服器中的WDS AP配置為身份驗證、授權和記帳(AAA)客戶端。為此，您需要將WDS AP新增為AAA客戶端。請完成以下步驟：**注意**：本文檔使用Cisco Secure ACS伺服器作為身份驗證伺服器。在Cisco Secure Access Control Server(ACS)中，這發生在 [Network Configuration](#) 頁面上，您可以在該頁面中為WDS AP定義以下屬性：名稱IP 位址共用

金鑰認證方法RADIUS Cisco AironetRADIUS Internet工程任務組[IETF]按一下**Submit**。對於其它非ACS身份驗證伺服器，請參閱製造商提供的文檔。

The screenshot shows the 'Add AAA Client' configuration page in the Cisco Secure ACS interface. The page is titled 'Network Configuration' and has a 'Cisco Systems' logo. On the left is a navigation menu with options like 'User Setup', 'Group Setup', 'Shared Profile Components', 'Network Configuration', 'System Configuration', 'Interface Configuration', 'Administration Control', 'External User Databases', 'Reports and Activity', and 'Online Documentation'. The main content area is titled 'Add AAA Client' and contains the following fields and options:

- AAA Client Hostname: WDS_AP
- AAA Client IP Address: 10.0.0.102
- Key: sharedsecret
- Authenticate Using: RADIUS (Cisco Aironet)


Below these fields are four unchecked checkboxes:

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

At the bottom are three buttons: 'Submit', 'Submit + Restart', and 'Cancel'. On the right side, there is a 'Help' section with a list of links: 'AAA Client Hostname', 'AAA Client IP Address', 'Key', 'Network Device Group', 'Authenticate Using', 'Single Connect TACACS+ AAA Client', 'Log Update/Watchdog Packets from this AAA Client', 'Log RADIUS Tunneling Packets from this AAA Client', and 'Replace RADIUS Port info with Username from this AAA Client'. Below the links, there are two sections: 'AAA Client Hostname' with the text 'The AAA Client Hostname is the name assigned to the AAA client.' and a '[Back to Top]' link; and 'AAA Client IP Address' with the text 'The AAA Client IP Address is the IP address assigned to the AAA client.'

此外，在Cisco Secure ACS中，請確保在[System Configuration - Global Authentication Setup](#)頁面上配置ACS以執行LEAP身份驗證。首先，按一下**System Configuration**，然後按一下**Global Authentication Setup**。

CISCO SYSTEMS **System Configuration**

Select	Help
<ul style="list-style-type: none">User SetupGroup SetupShared Profile ComponentsNetwork ConfigurationSystem ConfigurationInterface ConfigurationAdministration ControlExternal User DatabasesReports and ActivityOnline Documentation	<ul style="list-style-type: none">Service ControlLoggingDate Format ControlLocal Password ManagementCiscoSecure Database ReplicationACS BackupACS RestoreACS Service ManagementIP Pools ServerIP Pools Address RecoveryACS Certificate SetupGlobal Authentication Setup <p></p>
	<p>Service Control</p> <p>Select to open the page from which you can stop or restart Cisco Secure ACS services.</p> <p>[Back to Top]</p>

向下滾動頁面至LEAP設定。選中此框時，ACS會驗證LEAP。

CISCO SYSTEMS System Configuration

Edit

Global Authentication Setup

EAP Configuration

PEAP

Allow EAP-MSCHAPv2

Allow EAP-GTC

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

EAP-FAST

Allow EAP-FAST

Active master key TTL:

Retired master key TTL:

PAC TTL:

Client initial message:

Authority ID Info:

Allow automatic PAC provisioning:

EAP-FAST master server:

Actual EAP-FAST server status: **Master**

EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

LEAP

Allow LEAP (For Aironet only)

EAP-MD5

Allow EAP-MD5

AP EAP request timeout (seconds):

MS-CHAP Configuration

Allow MS-CHAP Version 1 Authentication

Allow MS-CHAP Version 2 Authentication

[Back to Help](#)

Help

- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP EAP request timeout](#)
- [MS-CHAP Configuration](#)

This page specifies settings for various authentication protocols.

[\[Back to Top\]](#)

PEAP

Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have

3. 要在WDS AP上配置WDS設定，請在WDS AP上選擇**Wireless Services > WDS**，然後按一下**General Set-Up**頁籤。請執行以下步驟：在WDS-Wireless Domain Services - Global Properties下，選中**Use this AP as Wireless Domain Services**。將Wireless Domain Services

Priority欄位的值設定為大約254，因為這是第一個值。您可以將一個或多個AP或交換機配置為提供WDS的候選裝置。具有最高優先順序的裝置提供WDS。

The screenshot shows the Cisco 1200 Access Point configuration interface. The left sidebar contains a navigation menu with options like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, AP, WDS, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled 'Cisco 1200 Access Point' and has tabs for 'WDS STATUS', 'SERVER GROUPS', and 'GENERAL SET-UP'. The 'GENERAL SET-UP' tab is active, showing the 'WDS - Wireless Domain Services - Global Properties' section. In this section, the checkbox 'Use this AP as Wireless Domain Services' is checked. Below it, the 'Wireless Domain Services Priority' is set to 254, which is circled in red. The 'Wireless Network Manager - Global Configuration' section is also visible, with the 'Configure Wireless Network Manager' checkbox unchecked and the 'Wireless Network Manager IP Address' field set to 'DISABLED'. The bottom right corner has 'Apply' and 'Cancel' buttons.

或者，也可以從CLI發出以下命令：

4. 選擇Wireless Services > WDS，然後轉到Server Groups頁籤：定義驗證其他AP的伺服器組名稱，即基礎結構組。將Priority 1設定為先前配置的身份驗證伺服器。按一下Use Group For:Infrastructure Authentication單選按鈕。將設定應用到相關的服務集識別符號(SSID)。

Cisco Systems
Cisco 1200 Access Point

WDS STATUS | SERVER GROUPS | GENERAL SET-UP

Hostname WDS_AP 16:26:44 Fri Apr 23 2004

Wireless Services: WDS - Server Groups

Server Group List

< NEW >
Infrastructure

Delete

Server Group Name: Infrastructure

Group Server Priorities: [Define Servers](#)

Priority 1: 10.0.0.3

Priority 2: < NONE >

Priority 3: < NONE >

Use Group For:

Infrastructure Authentication

Client Authentication

Authentication Settings

EAP Authentication

LEAP Authentication

MAC Authentication

Default (Any) Authentication

SSID Settings

Apply to all SSIDs

Restrict SSIDs (Apply only to listed SSIDs)

SSID: DISABLED Add

Remove

Apply Cancel

或者，也可以從CLI發出以下命令：

5. 將WDS使用者名稱和密碼配置為身份驗證伺服器中的使用者。在Cisco Secure ACS中，這發生在 [User Setup](#) 頁面上，您可以在該頁面中定義WDS使用者名稱和密碼。對於其它非ACS身份驗證伺服器，請參閱製造商提供的文檔。**注意：**不要將WDS使用者放在分配了許多許可權和許可權的組中 — WDS只需要有限的身份驗證。

User Setup

User: WDSUser (New User)

Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Submit Cancel

Help

- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

6. 選擇 **Wireless Services > AP**，然後為 Participate in SWAN infrastructure 選項按一下 **Enable**。然後鍵入 WDS 使用者名稱和密碼。必須在身份驗證伺服器上為指定 WDS 成員的所有裝置定義 WDS 使用者名稱和密碼。

Cisco Systems
Cisco 1200 Access Point

Hostname WDS_AP 16:00:29 Fri Apr 23 2004

Wireless Services: AP

Participate in SWAN Infrastructure: Enable Disable

WDS Discovery: Auto Discovery
 Specified Discovery: (IP Address)

Username:
Password:
Confirm Password:

L3 Mobility Service via IP/GRE Tunnel: Enable Disable

Apply Cancel

或者，也可以從CLI發出以下命令：

7. 選擇**Wireless Services > WDS**。在「WDS AP WDS狀態」頁籤上，檢查WDS AP是否出現在「WDS資訊」區域的「活動狀態」中。AP還必須出現在AP資訊區域中，其狀態為已註冊。如果AP未顯示「已註冊」或「活動」，請檢查身份驗證伺服器是否有任何錯誤或身份驗證嘗試失敗。當AP正確註冊時，新增基礎設施AP以使用WDS的服務。

Cisco 1200 Access Point

WDS STATUS | SERVER GROUPS | GENERAL SET-UP

Hostname WDS_AP 16:30:08 Fri Apr 23 2004

Wireless Services: WDS - Wireless Domain Services - Status

WDS Information			
MAC Address	IP Address	Priority	State
0005.9a38.429f	10.0.0.102	254	Administratively StandAlone - ACTIVE

WDS Registration

APs: 1 Mobile Nodes: 0

AP Information		
MAC Address	IP Address	State
0005.9a38.429f	10.0.0.102	REGISTERED

Mobile Node Information

MAC Address	IP Address	State	SSID	VLAN ID	BSSID

Wireless Network Manager Information

IP Address	Authentication Status

Refresh

或者，也可以從CLI發出以下命令：**注意**：您無法測試客戶端關聯，因為客戶端身份驗證還沒有設定。

將WLSM指定為WDS

本節說明如何將WLSM配置為WDS。WDS是唯一與身份驗證伺服器進行通訊的裝置。

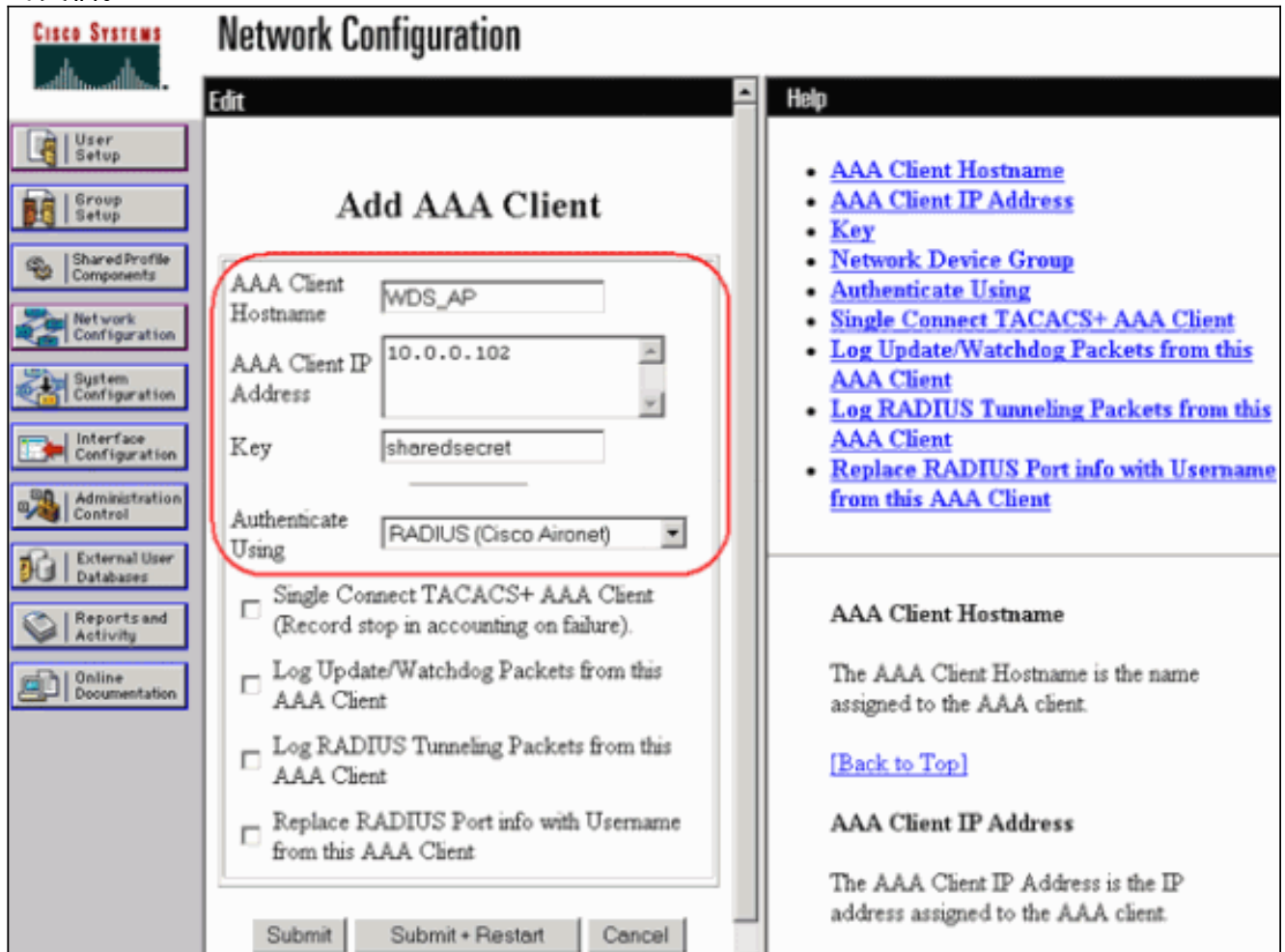
註：在WLSM的`enable`命令提示符下發出這些命令，而不是Supervisor Engine 720的命令。若要進入WLSM的命令提示符，請在Supervisor Engine 720的`enable`命令提示符下發出以下命令：

```
c6506#session slot x proc 1
!--- In this command, x is the slot number where the
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>
wlan>enable
Password: <enable password>
wlan#
```

注意：為了更輕鬆地排除故障和維護WLSM，請配置對WLSM的Telnet遠端訪問。請參閱[配置Telnet遠端訪問](#)。

若要將WLSM指定為WDS:

1. 在WLSM的CLI上，發出以下命令，並與身份驗證伺服器建立關係：**注意**：WLSM中沒有優先順序控制。如果網路包含多個WLSM模組，則WLSM會使用[冗餘配置](#)來確定主模組。
2. 將身份驗證伺服器中的WLSM配置為AAA客戶端。在Cisco Secure ACS中，這發生在[Network Configuration](#)頁面上，您可以在該頁面中為WLSM定義以下屬性：名稱IP 位址共用金鑰認證方法RADIUS Cisco AironetRADIUS IETF對於其它非ACS身份驗證伺服器，請參閱製造商提供的文檔。



Network Configuration

Add AAA Client

AAA Client Hostname: WDS_AP

AAA Client IP Address: 10.0.0.102

Key: sharedsecret

Authenticate Using: RADIUS (Cisco Aironet)

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Submit Submit + Restart Cancel

Help

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

此外，在Cisco Secure ACS中，將ACS配置為在[System Configuration - Global Authentication Setup](#)頁面上執行LEAP身份驗證。首先，按一下**System Configuration**，然後按一下**Global Authentication Setup**。

CISCO SYSTEMS **System Configuration**

Select	Help
<ul style="list-style-type: none">User SetupGroup SetupShared Profile ComponentsNetwork ConfigurationSystem ConfigurationInterface ConfigurationAdministration ControlExternal User DatabasesReports and ActivityOnline Documentation	<ul style="list-style-type: none">Service ControlLoggingDate Format ControlLocal Password ManagementCiscoSecure Database ReplicationACS BackupACS RestoreACS Service ManagementIP Pools ServerIP Pools Address RecoveryACS Certificate SetupGlobal Authentication Setup <p>Back to Help</p>
	<p>Service Control</p> <p>Select to open the page from which you can stop or restart Cisco Secure ACS services.</p> <p>[Back to Top]</p>

向下滾動頁面至LEAP設定。選中此框時，ACS會驗證LEAP。

CISCO SYSTEMS System Configuration

Edit

Global Authentication Setup

EAP Configuration

PEAP

Allow EAP-MSCHAPv2

Allow EAP-GTC

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

EAP-FAST

Allow EAP-FAST

Active master key TTL:

Retired master key TTL:

PAC TTL:

Client initial message:

Authority ID Info:

Allow automatic PAC provisioning:

EAP-FAST master server:

Actual EAP-FAST server status: **Master**

EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

LEAP

Allow LEAP (For Aironet only)

EAP-MD5

Allow EAP-MD5

AP EAP request timeout (seconds):

MS-CHAP Configuration

Allow MS-CHAP Version 1 Authentication

Allow MS-CHAP Version 2 Authentication

[Back to Help](#)

Submit Submit + Restart Cancel

Help

- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP EAP request timeout](#)
- [MS-CHAP Configuration](#)

This page specifies settings for various authentication protocols.

[\[Back to Top\]](#)

PEAP

Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have

3. 在WLSM上，定義驗證其他AP（基礎結構伺服器組）的方法。
4. 在WLSM上，定義驗證客戶端裝置（客戶端伺服器組）以及這些客戶端使用的EAP型別的方法。
。註：此步驟無需執行定義客戶端驗證方法流程。

5. 在Supervisor Engine 720和WLSM之間定義唯一的VLAN，以允許WLSM與外部實體（如AP和身份驗證伺服器）通訊。此VLAN在網路中的其他任何位置或用於任何其他用途。首先在Supervisor Engine 720上建立VLAN，然後發出以下命令：在Supervisor Engine 720上：在WLSM上：
6. 使用以下命令驗證WLSM的功能：在WLSM上：在Supervisor Engine 720上：

將AP指定為基礎設施裝置

接下來，您必須指定至少一個基礎架構AP並將該AP關聯到WDS。客戶端與基礎設施AP關聯。基礎架構AP請求WDS AP或WLSM為其執行身份驗證。

完成以下步驟，以便新增使用WDS服務的基礎架構AP：

注意：此配置僅適用於基礎設施AP，而不適用於WDS AP。

1. 選擇**Wireless Services > AP**。在基礎架構AP上，選擇**Enable**以啟用無線服務選項。然後鍵入WDS使用者名稱和密碼。必須在身份驗證伺服器上為要成為WDS成員的所有裝置定義WDS使用者名稱和密碼。

The screenshot displays the configuration interface for a Cisco 1200 Access Point. The main heading is "Cisco 1200 Access Point" with a sub-heading "Wireless Services: AP". The hostname is "Infrastructure_AP" and the time is "10:00:26 Mon Apr 26 2004". The configuration is divided into several sections:

- Participate in SWAN Infrastructure:** The "Enable" radio button is selected, indicated by a red arrow.
- WDS Discovery:** The "Auto Discovery" radio button is selected. The "Specified Discovery" option is disabled, with the text "DISABLED (IP Address)" in a greyed-out box.
- WDS Credentials:** A red box highlights the "Username" field containing "infrastructureap", the "Password" field, and the "Confirm Password" field.
- L3 Mobility Service via IP/GRE Tunnel:** The "Disable" radio button is selected.

At the bottom right, there are "Apply" and "Cancel" buttons.

或者，也可以從CLI發出以下命令：

2. 選擇**Wireless Services > WDS**。在WDS AP WDS狀態頁籤上，新的基礎架構AP出現在WDS資訊區域中，狀態為活動，在AP資訊區域中，狀態為註冊。如果AP未顯示為ACTIVE和/或REGISTERED，請檢查身份驗證伺服器是否有任何錯誤或身份驗證嘗試失敗。在AP顯示ACTIVE和/或REGISTERED後，向WDS新增客戶端身份驗證方法。

Cisco 1200 Access Point

Hostname: WDS_AP | 10:02:01 Mon Apr 26 2004

Wireless Services: WDS - Wireless Domain Services - Status

WDS Information

MAC Address	IP Address	Priority	State
0005.9a38.429f	10.0.0.102	254	Administratively StandAlone - ACTIVE

WDS Registration

APs: 2 | Mobile Nodes: 0

AP Information

MAC Address	IP Address	State
000c.8547.b6c7	10.0.0.108	REGISTERED
0005.9a38.429f	10.0.0.102	REGISTERED

Mobile Node Information

MAC Address	IP Address	State	SSID	VLAN ID	BSSID

Wireless Network Manager Information

IP Address	Authentication Status

Refresh

或者，也可以從CLI發出以下命令：或者，從WLSM發出以下命令：然後在基礎架構AP上發出以下命令：**注意：您無法測試客戶端關聯，因為客戶端身份驗證還沒有設定。**

定義客戶端身份驗證方法

最後，定義客戶端身份驗證的方法。

完成以下步驟以新增客戶端身份驗證方法：

1. 選擇**Wireless Services > WDS**。在WDS AP伺服器組頁籤上執行以下步驟：定義驗證客戶端的伺服器組（客戶端組）。將Priority 1設定為先前配置的身份驗證伺服器。設定適用的身份驗證型別（LEAP、EAP、MAC等）。將設定應用到相關SSID。

The screenshot displays the Cisco 1200 Access Point configuration interface for the 'WDS STATUS' tab. The main content area is titled 'Wireless Services: WDS - Server Groups'. A 'Server Group List' shows 'Client' selected. The configuration for the 'Client' group includes a 'Server Group Name' of 'Client' and 'Group Server Priorities' of '10.0.0.3', '<NONE>', and '<NONE>'. The 'Use Group For' section has 'Client Authentication' selected. Under 'Authentication Settings', 'EAP Authentication' and 'LEAP Authentication' are checked. Under 'SSID Settings', 'Apply to all SSIDs' is selected, and the 'SSID' field is set to 'DISABLED'. The page includes a navigation menu on the left and 'Apply' and 'Cancel' buttons at the bottom right.

或者，也可以從CLI發出以下命令：**注意**：示例WDS AP是專用的，不接受客戶端關聯。**注意**：請勿在基礎架構AP上配置伺服器組，因為基礎架構AP會將任何請求轉發到WDS以進行處理。

2. 在基礎架構AP或AP上：在**Security > Encryption Manager**選單項下，根據您使用的身份驗證協定的要求，按一下**WEP Encryption**或**Cipher**。

CISCO SYSTEMS

Cisco 1200 Access Point

RADIO0-802.11B RADIO1-802.11A

Hostname Infrastructure_AP 10:36:59 Mon Apr 26 2004

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY
Admin Access
Encryption Manager
SSID Manager
Server Manager
Local RADIUS Server
Advanced Security
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

Security: Encryption Manager - Radio0-802.11B

Encryption Modes

None

WEP Encryption Mandatory

Cisco Compliant TKIP Features: Enable MIC Enable Per Packet Keying

Cipher WEP 128 bit

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

在Security > SSID Manager選單項下，選擇您使用的身份驗證協定所需的身份驗證方法。

The screenshot displays the Cisco 1200 Access Point configuration interface. The top navigation bar includes the Cisco Systems logo and the title "Cisco 1200 Access Point". Below this, there are tabs for "RADIO0-802.11B" and "RADIO1-802.11A". The main content area is divided into several sections:

- Left Sidebar:** A vertical menu with options like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, Admin Access, Encryption Manager, SSID Manager (highlighted), Server Manager, Local RADIUS Server, Advanced Security, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG.
- Header:** "Hostname Infrastructure_AP" and "10:38:39 Mon Apr 26 2004".
- Security: SSID Manager - Radio0-802.11B:**
 - SSID Properties:** A section for managing SSIDs.
 - Current SSID List:** A list box containing "< NEW >" and "infraSSID".
 - Form Fields:** "SSID:" is set to "infraSSID", "VLAN:" is set to "< NONE >", and "Network ID:" is empty. There are buttons for "Delete-Radio0" and "Delete-All".
- Authentication Settings:** A section with "Methods Accepted:" and three options:
 - Open Authentication: with EAP
 - Shared Authentication: < NO ADDITION >
 - Network EAP: < NO ADDITION >

3. 現在，您可以成功測試客戶端是否對基礎架構AP進行身份驗證。WDS狀態頁籤中(在**Wireless Services** > **WDS**選單項下)的WDS的AP指示客戶端出現在「移動節點資訊」區域中，並且具有「已註冊」狀態。如果客戶端沒有出現，請檢查身份驗證伺服器是否存在任何錯誤或客戶端的身分驗證嘗試失敗。

Cisco 1200 Access Point

WDS STATUS | SERVER GROUPS | GENERAL SET-UP

Hostname WDS_AP 10:49:24 Mon Apr 26 2004

Wireless Services: WDS - Wireless Domain Services - Status

WDS Information

MAC Address	IP Address	Priority	State
0005.9a38.429f	10.0.0.102	254	Administratively StandAlone - ACTIVE

WDS Registration

APs: 2 Mobile Nodes: 1

AP Information

MAC Address	IP Address	State
000c.8547.b6c7	10.0.0.108	REGISTERED
0005.9a38.429f	10.0.0.102	REGISTERED

Mobile Node Information

MAC Address	IP Address	State	SSID	VLAN ID	BSSID
0030.6527.f74a	10.0.0.25	REGISTERED	infraSSID	-	0007.85b4.113b

Wireless Network Manager Information

IP Address	Authentication Status

Refresh

或者，也可以從CLI發出以下命令：注意：如果需要調試身份驗證，請確保在WDS AP上進行調試，因為WDS AP是與身份驗證伺服器通訊的裝置。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。此清單顯示與WDS命令相關的一些常見問題，以便進一步說明這些命令的用途：

- 問題：在WDS AP上，這些專案的建議設定是什麼？radius-server timeoutradius-server deadtime臨時金鑰完整性協定(TKIP)消息完整性檢查(MIC)故障保持時間客戶端暫停時間EAP或MAC重新身份驗證間隔EAP客戶端超時（可選）答案：建議您將配置保留為有關這些特殊設定的預設設定，並且僅在時間方面出現問題時使用它們。以下是WDS AP的建議設定：禁用radius-server timeout。這是AP在重新傳送請求之前等待回覆RADIUS請求的秒數。預設值為5秒。禁用radius-server deadtime。除非所有伺服器都標籤為停用，否則會在數分鐘內由其他要求跳過RADIUS。預設情況下，TKIP MIC故障保持時間啟用為60秒。如果啟用暫停時間，可以輸入時間間隔（以秒為單位）。如果AP在60秒內檢測到兩個MIC故障，它將在此處指定的暫

停時間段內阻止該介面上的所有TKIP客戶端。預設情況下應禁用客戶端暫停時間。如果啟用暫掛，請輸入在處理後續身份驗證請求之前AP在身份驗證失敗後應等待的秒數。預設情況下，EAP或MAC重新驗證間隔處於禁用狀態。如果啟用重新身份驗證，則可以指定間隔或接受身份驗證伺服器給定的間隔。如果選擇指定時間間隔，請輸入AP在強制經過身份驗證的客戶端重新進行身份驗證之前等待的時間間隔（以秒為單位）。預設情況下，EAP客戶端超時（可選）為120秒。輸入AP應等待無線客戶端響應EAP身份驗證請求的時間。

- **問題：關於TKIP保持時間，我讀到應將其設定為100毫秒，而不是60秒。我假定它在瀏覽器中設定為一秒，因為它是您所能選擇的最低數字？****答案：**沒有將其設定為100 ms的具體建議，除非報告有故障，而唯一的解決方案就是增加此時間。一秒是最低設定。
- **問題：這兩個命令是否以任何方式幫助客戶端進行身份驗證？在WDS或基礎設施AP上是否需要這兩個命令？**`radius-server attribute 6 on-for-login-auth``radius-server attribute 6 support-multiple`**答案：**這些命令對身份驗證過程沒有幫助，WDS或AP不需要這些命令。
- **問題：在基礎結構AP上，我假設不需要伺服器管理器和全域性屬性設定，因為AP從WDS接收資訊。基礎架構AP是否需要這些特定命令？**`radius-server attribute 6 on-for-login-auth``radius-server attribute 6 support-multiple``radius-server timeout``radius-server deadtime`**答案：**基礎架構AP不需要伺服器管理器和全域性屬性。WDS負責該任務，無需進行以下設定：`radius-server attribute 6 on-for-login-auth``radius-server attribute 6 support-multiple``radius-server timeout``radius-server deadtime`預設情況下，`radius-server attribute 32 include-in-access-req format %h`設定保持不變，並且是必需的。

AP是第2層裝置。因此，當AP配置為充當WDS裝置時，AP不支援第3層移動。只有將WLSM配置為WDS裝置時，才能實現第3層移動性。請參閱[Cisco Catalyst 6500系列無線LAN服務模組](#)的[第3層行動架構](#)一節：[獲取更多資訊](#)的白皮書。

因此，將AP配置為WDS裝置時，不要使用`mobility network-id`命令。此命令適用於第3層移動性，您需要將WLSM作為WDS裝置來正確配置第3層移動性。如果您未正確使用`mobility network-id`命令，則可能會看到以下一些症狀：

- 無線客戶端無法與AP關聯。
- 無線客戶端可以與AP關聯，但不會從DHCP伺服器接收IP地址。
- 當您部署WLAN語音時，無線電話不會通過身份驗證。
- EAP身份驗證未發生。在配置`mobility network-id`後，AP會嘗試建立通用路由封裝(GRE)隧道以轉發EAP資料包。如果沒有建立通道，資料包不會到達任何地方。
- 配置為WDS裝置的AP無法按預期工作，並且WDS配置無法工作。**注意：**您不能將Cisco Aironet 1300 AP/網橋配置為WDS主裝置。1300 AP/網橋不支援此功能。1300 AP/網橋可以作為基礎設施裝置加入WDS網路，其中某些其他AP或WLSM配置為WDS主裝置。

疑難排解指令

[輸出直譯器工具](#)(僅供[已註冊](#)客戶使用)(OIT)支援某些`show`命令。使用OIT檢視`show`命令輸出的分析。

附註：使用 `debug` 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

- `debug dot11 aaa authenticator all` — 顯示客戶端通過802.1x或EAP進程進行關聯和身份驗證時經歷的各種協商。此偵錯是在Cisco IOS軟體版本12.2(15)JA中匯入。此指令在that和更新版本中取代`debug dot11 aaa dot1x all`。
- `debug aaa authentication` — 從通用AAA角度顯示身份驗證過程。
- `debug wlccp ap` — 顯示AP加入WDS時涉及的WLCCP協商。
- `debug wlccp packet` — 顯示有關WLCCP協商的詳細資訊。

- `debug wlccp leap-client` — 在基礎設施裝置加入WDS時顯示詳細資訊。

相關資訊

- [配置WDS、快速安全漫遊和無線電管理](#)
- [Catalyst 6500系列無線LAN服務模組組態說明](#)
- [配置密碼套件和WEP](#)
- [配置身份驗證型別](#)
- [無線LAN支援頁面](#)
- [技術支援與文件 - Cisco Systems](#)