

Configuração dos serviços do domínio sem fio

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Serviços do domínio Wireless](#)

[Papel do dispositivo WDS](#)

[Papel dos Access point usando o dispositivo WDS](#)

[Configuração](#)

[Designe um AP como o WDS](#)

[Designe um WLSM como o WDS](#)

[Designe um AP como o dispositivo de infraestrutura](#)

[Defina o método de autenticação do cliente](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento introduz o conceito de serviços de domínio sem fio (WDS). O original igualmente descreve como configurar um Access Point (AP) ou o [Módulo de serviços do Wireless LAN \(WLSM\)](#) como o WDS e pelo menos um outro como uma infraestrutura AP. O procedimento neste documento fornece orientações sobre um WDS que é funcional e permite que clientes associem ao WDS AP ou a um AP de infraestrutura. Este original pretende estabelecer uma base de que você pode configurar [rapidamente vaguear seguro](#) ou introduzir um [motor das soluções LAN Wireless](#) (WLSE) na rede, assim que você pode usar as características.

[Pré-requisitos](#)

[Requisitos](#)

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Tenha o conhecimento completo das redes de Wireless LAN e das edições de segurança Wireless.
- Tenha métodos de segurança do Extensible Authentication Protocol (EAP) do conhecimento dos atuais.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- AP com software de Cisco IOS®
- Cisco IOS Software Release 12.3(2)JA2 ou Mais Recente
- Módulo de serviços do Wireless LAN do Catalyst 6500 Series

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste original começaram com uma configuração esclarecida (PADRÃO) e um endereço IP de Um ou Mais Servidores Cisco ICM NT na relação BVI1, assim que a unidade são acessíveis do Cisco IOS Software GUI ou do comando line interface(cli). Se você trabalha em uma rede viva, assegure-se de que você compreenda o impacto potencial do comando any.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Serviços do domínio Wireless

O WDS é uns novos recursos para AP no Cisco IOS Software e na base do Catalyst 6500 Series WLSM. O WDS é uma função do núcleo que permita outros recursos como estes:

- Rápido fixe vaguear
- Interação WLSE
- Gerenciamento de rádio

Você deveu estabelecer relacionamentos entre os AP que participam no WDS e no WLSM, antes que qualquer outro WDS-basearam o trabalho das características. Uma das finalidades do WDS é eliminar a necessidade de validação de credenciais de usuário pelo servidor de autenticação e reduzir o tempo necessário para as autenticações de cliente.

A fim usar o WDS, você deve designar um AP ou o WLSM como o WDS. UM WDS AP deve usar um nome de usuário e a senha WDS para estabelecer um relacionamento com um Authentication Server. O Authentication Server pode ser um servidor de raio externo ou a característica local do servidor Radius no WDS AP. O WLSM deve ter um relacionamento com o Authentication Server, mesmo que o WLSM não precise de autenticar ao server.

Outros AP, chamados a infraestrutura AP, comunicam-se com o WDS. Antes que o registro ocorra, a infraestrutura AP deve autenticar-se ao WDS. Um grupo de servidor da infraestrutura no WDS define esta autenticação de infraestrutura.

Uns ou vários grupos de servidor cliente no WDS definem a autenticação do cliente.

Quando um cliente tenta associar a uma infraestrutura AP, a infraestrutura AP passa as credenciais do usuário ao WDS para a validação. Se o WDS vê as credenciais pela primeira vez, o WDS gerencie para o Authentication Server para validar as credenciais. O WDS põe em esconderijo então as credenciais, a fim eliminar a necessidade de retornar ao Authentication Server quando o mesmo usuário tenta a autenticação outra vez. Os exemplos da reautenticação incluem:

- Re-fechar
- Vaguear
- Quando o usuário puser em andamento o dispositivo do cliente

Alguns protocolos de autenticação de EAP Raio-baseado podem ser escavados um túnel com o WDS tal como estes:

- EAP de pouco peso (PULO)
- PEAP (EAP Protegido)
- Segurança da camada do EAP-transporte (EAP-TLS)
- Autenticação Flexível de EAP com o Tunelamento seguro (EAP-FAST)

A autenticação do MAC address pode igualmente escavar um túnel a um servidor de autenticação externa ou contra uma lista local a um WDS AP. O WLSM não apoia a autenticação do MAC address.

O WDS e a infraestrutura AP comunicam-se sobre um protocolo de transmissão múltipla chamado o protocolo de controle do contexto WLAN (WLCCP). Estas mensagens de transmissão múltipla não podem ser distribuídos, assim que um WDS e a infraestrutura associada AP devem estar na mesma sub-rede IP e no mesmo segmento LAN. Entre o WDS e os usos TCP WLSE, WLCCP e o User Datagram Protocol (UDP) na porta 2887. Quando o WDS e o WLSE estão em sub-redes diferentes, um protocolo como o Network Address Translation (NAT) não pode traduzir os pacotes.

Um AP configurado como os suportes do dispositivo WDS até 60 AP de participação. Um roteador dos Serviços integrados (ISR) configurado como os dispositivos WDS apoia até 100 AP de participação. E um interruptor WLSM-equipado apoia até 600 AP de participação e até 240 Grupos de mobilidade. Um único AP apoia até 16 Grupos de mobilidade.

Nota: Cisco recomenda que a infraestrutura AP executa a mesma versão de IOS que o dispositivo WDS. Se você usa uma versão de IOS mais velha, os AP puderam não autenticam ao dispositivo WDS. Além, Cisco recomenda que você usa a versão a mais atrasada dos IO. Você pode encontrar a versão de IOS a mais atrasada na página [wireless das transferências](#).

Papel do dispositivo WDS

O dispositivo WDS executa diversas tarefas em seu Wireless LAN:

- Anuncia sua capacidade WDS e participa em eleger o melhor dispositivo WDS para seu Wireless LAN. Quando você configura seu Wireless LAN para o WDS, você estabelece um dispositivo como o candidato principal WDS e uns ou vários dispositivos adicionais como candidatos WDS de backup. Se o dispositivo principal WDS vai off line, um dos dispositivos do backup WDS toma seu lugar.
- Autentica todos os AP na sub-rede e estabelece um canal de comunicação segura com o cada um deles.
- Recolhe os dados de rádio dos AP na sub-rede, agrega-os os dados, e para a frente ao dispositivo WLSE em sua rede.
- Atua como a passagem-através para de todos os dispositivos do cliente 802.1x-authenticated associados aos AP de participação.
- Registra todos os dispositivos do cliente na sub-rede que usam fechar dinâmico, estabelece chaves de sessão para elas, e põe em esconderijo suas credenciais de segurança. Quando

um cliente vaguear a um outro AP, as credenciais de segurança do dispositivo WDS para a frente do cliente ao AP novo.

Papel dos Access point usando o dispositivo WDS

Os AP em seu Wireless LAN interagem com o dispositivo WDS nestas atividades:

- Descubra e siga as propagandas atuais do dispositivo e do relé WDS WDS ao Wireless LAN.
- Autentique com o dispositivo WDS e estabeleça um canal de comunicação segura ao dispositivo WDS.
- Registrar dispositivos do cliente associados com o dispositivo WDS.
- Relate os dados de rádio ao dispositivo WDS.

Configuração

O WDS apresenta a configuração em uma forma pedida, modular. Construções de cada conceito no conceito que precede. O WDS omite outros itens de configuração tais como senhas, Acesso remoto, e configurações de rádio para maior clareza e foco no assunto do núcleo.

Esta seção apresenta a informação necessária configurar as características descritas neste original.

Nota: Use a [Command Lookup Tool \(somente clientes registrados\)](#) para obter mais informações sobre os comandos usados nesta seção.

Designe um AP como o WDS

A primeira etapa é designar um AP como o WDS. O WDS AP é único que se comunica com o Authentication Server.

Termine estas etapas a fim designar um AP como o WDS:

1. A fim configurar o Authentication Server no WDS AP, escolha a **Segurança > o gerenciador do servidor** a ir à aba do gerenciador do servidor: Sob servidores corporativos, datilografe o endereço IP de Um ou Mais Servidores Cisco ICM NT do Authentication Server no campo do server. Especifique o segredo compartilhado e as portas. Sob prioridades do server do padrão, ajuste o campo da prioridade 1 a esse endereço IP do servidor sob o tipo do autenticação apropriado.

The screenshot shows the Cisco 1200 Access Point configuration page. The left sidebar contains navigation options like HOME, EXPRESS SET-UP, SECURITY, SERVICES, and WIRELESS SERVICES. The main content area is divided into several sections:

- SERVER MANAGER / GLOBAL PROPERTIES:** Shows Hostname WDS_AP and the date/time 16:09:43 Fri Apr 23 2004.
- Security: Server Manager:** Contains a section for Backup RADIUS Server with fields for Backup RADIUS Server (Hostname or IP Address) and Shared Secret, and buttons for Apply, Delete, and Cancel.
- Corporate Servers:** Includes a Current Server List with a RADIUS dropdown and a list containing < NEW > and 10.0.0.3. A red circle highlights the configuration details for the 10.0.0.3 server:
 - Server: 10.0.0.3 (Hostname or IP Address)
 - Shared Secret: [Empty field]
 - Authentication Port (optional): 1645 (0-65536)
 - Accounting Port (optional): 1646 (0-65536)
- Default Server Priorities:** A table of priority settings for various authentication methods. A red circle highlights the EAP Authentication section:

Authentication Method	Priority 1	Priority 2	Priority 3
EAP Authentication	10.0.0.3	< NONE >	< NONE >
MAC Authentication	< NONE >	< NONE >	< NONE >
Accounting	< NONE >	< NONE >	< NONE >
Admin Authentication (RADIUS)	< NONE >	< NONE >	< NONE >
Admin Authentication (TACACS+)	< NONE >	< NONE >	< NONE >
Proxy Mobile IP Authentication	< NONE >	< NONE >	< NONE >

Alternativamente, emita estes comandos do CLI:

2. A próxima etapa é configurar o WDS AP no Authentication Server como um cliente do Authentication, Authorization, and Accounting (AAA). Para isto, você precisa de adicionar o WDS AP como um cliente de AAA. Conclua estes passos:**Nota:** Este original usa o server do Cisco Secure ACS como o Authentication Server.No Serviço de controle de acesso Cisco Secure (ACS), isto ocorre na página da [configuração de rede](#) onde você define estes atributos para o WDS AP:NomeEndereço IPShared secretMétodo de autenticaçãoRADIUS Cisco AironetInternet Engineering Task Force [IETF] de RADIUSClique **submetem-se** sobre.Para outros Authentication Server NON-ACS, refira a documentação do

fabricante.

The screenshot shows the Cisco Network Configuration interface. The main heading is "Add AAA Client". The form contains the following fields and options:

- AAA Client Hostname:
- AAA Client IP Address:
- Key:
- Authenticate Using:

Below the form are several 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 of the form 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](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

Below the links, there are two sections of help text:

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.

Também, no Cisco Secure ACS, assegure-se de que você configure o ACS para executar a autenticação de leap na [configuração de sistema - página de instalação da autenticação global](#). Primeiramente, a **configuração de sistema** do clique, clica então a **instalação da autenticação global**.

CISCO SYSTEMS **System Configuration**

Select	Help
<ul style="list-style-type: none"> User Setup Group Setup Shared Profile Components Network Configuration System Configuration Interface Configuration Administration Control External User Databases Reports and Activity Online Documentation 	<ul style="list-style-type: none"> Service Control Logging Date Format Control Local Password Management CiscoSecure Database Replication ACS Backup ACS Restore ACS Service Management IP Pools Server IP Pools Address Recovery ACS Certificate Setup Global Authentication Setup <p style="text-align: center;">Back to Help</p>
	<ul style="list-style-type: none"> • Service Control • Logging • Date Format Control • Local Password Management • CiscoSecure Database Replication • RDBMS Synchronization • ACS Backup • ACS Restore • ACS Service Management • IP Pools Address Recovery • IP Pools Server • VoIP Accounting Configuration • ACS Certificate Setup • Global Authentication Configuration <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>

Enrole para baixo a página o ajuste do PULO. Quando a caixa é marcada, o ACS autentica o 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. A fim configurar os settings WDS no WDS AP, escolha **Serviços sem fio > WDS no WDS AP**, e clique sobre a aba **geral da instalação**. Execute estas etapas: Sob serviços do domínio do WDS-Sem fio - Propriedades globais, **uso da verificação este AP como serviços do**

domínio Wireless. Ajuste o valor para o campo de prioridade dos serviços do domínio Wireless a um valor de aproximadamente **254**, porque este é primeiro. Você pode configurar uns ou vários AP ou Switches como candidatos para fornecer o WDS. O dispositivo com a prioridade mais alta fornece o WDS.



Alternativamente, emita estes comandos do CLI:

4. Escolha **Serviços sem fio > WDS**, e vá à aba dos **grupos de servidor**: Defina um nome de grupo de servidor que autentique os outros AP, um grupo da infraestrutura. Defina a prioridade 1 para o servidor de autenticação configurado anteriormente. Clique o **grupo do uso para**: Botão de rádio da **autenticação de infraestrutura**. Aplique os ajustes aos service set identifier relevantes (SSID).

The screenshot displays the Cisco 1200 Access Point configuration interface. The main configuration area is titled "Wireless Services: WDS - Server Groups". It features a "Server Group List" table with one entry, "Infrastructure". To the right of the table, there are fields for "Server Group Name" (Infrastructure), "Group Server Priorities" (Priority 1: 10.0.0.3, Priority 2: <NONE>, Priority 3: <NONE>), and "Use Group For" (Infrastructure Authentication). Below these are "Authentication Settings" (EAP, LEAP, MAC, Default) and "SSID Settings" (Apply to all SSIDs, Restrict SSIDs). The bottom right has "Apply" and "Cancel" buttons.

Alternativamente, emita estes comandos do CLI:

5. Configurar o nome de usuário e a senha WDS como um usuário em seu Authentication Server.No Cisco Secure ACS, isto ocorre na página da [instalação de usuário](#), onde você define o nome de usuário e a senha WDS. Para outros Authentication Server NON-ACS, refira a documentação do fabricante.**Nota:** Não põe o usuário WDS em um grupo que seja atribuído muitos direitos e privilégios — o WDS exige somente autenticação limitada.

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

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. Escolha **Serviços sem fio > AP**, e o clique **permite** para a participação na opção da infraestrutura de swan. Datilografe então o nome de usuário e senha WDS. Você deve definir um nome de usuário e uma senha WDS no servidor de autenticação para todos os dispositivos que designam membros do WDS.

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

Alternativamente, emita estes comandos do CLI:

- Escolha **Serviços sem fio > WDS**. Na aba do Status WDS WDS AP, verificação se o WDS AP aparece na área de informação de WDS, no estado ATIVO. O AP deve igualmente aparecer na área de informação AP, com estado como REGISTRADO. Se o AP não parece REGISTRADO ou ATIVO, verifique o Authentication Server para ver se há todos os erros ou a autenticação falha tenta. Quando o AP se registra apropriadamente, adicionar uma infraestrutura AP para usar os serviços do WDS.

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

Alternativamente, emita estes comandos do CLI: **Nota:** Você não pode associações do cliente de teste porque a autenticação do cliente não tem disposições ainda.

Designe um WLSM como o WDS

Esta seção explica como configurar um WLSM como um WDS. O WDS é o único dispositivo que se comunica com o Authentication Server.

Nota: Emita estes comandos na alerta de comando enable do WLSM, não do Supervisor Engine 720. A fim obter ao comando prompt do WLSM, emita estes comandos em uma alerta de comando enable no Supervisor Engine 720:

```
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#
```

Nota: A fim pesquisar defeitos mais facilmente e manter seu WLSM, configurar o Acesso remoto do telnet ao WLSM. Consulte a [Configuração de Acesso Remoto de Telnet](#).

A fim designar um WLSM como o WDS:

1. Do CLI do WLSM, emita estes comandos, e estabeleça um relacionamento com o Authentication Server:**Nota:** Não há controle de prioridade no WLSM. Se a rede contém os módulos WLSM múltiplos, o WLSM usa a [configuração de redundância](#) a fim determinar o módulo principal.
2. Configurar o WLSM no Authentication Server como um cliente de AAA.No Cisco Secure ACS, isto ocorre na página da [configuração de rede](#) onde você define estes atributos para o WLSM:NomeEndereço IPShared secretMétodo de autenticaçãoRADIUS Cisco AironetRAIO IETFPPara outros Authentication Server NON-ACS, refira a documentação do fabricante.

The screenshot shows the 'Add AAA Client' configuration page in the Cisco Secure ACS web interface. The page is titled 'Network Configuration' and has a 'Help' sidebar on the right. The main content area is titled 'Add AAA Client' and contains the following fields and options:

- AAA Client Hostname:
- AAA Client IP Address:
- Key:
- Authenticate Using:

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 of the form are three buttons: 'Submit', 'Submit + Restart', and 'Cancel'. The 'Help' sidebar on the right contains 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.'

Também, no Cisco Secure ACS, configurar o ACS para executar a autenticação de leap na [configuração de sistema - página de instalação da autenticação global](#). Primeiramente, a configuração de sistema do clique, clica então a instalação da autenticação global.

CISCO SYSTEMS **System Configuration**

Select	Help
<ul style="list-style-type: none"> User Setup Group Setup Shared Profile Components Network Configuration System Configuration Interface Configuration Administration Control External User Databases Reports and Activity Online Documentation 	<ul style="list-style-type: none"> Service Control Logging Date Format Control Local Password Management CiscoSecure Database Replication ACS Backup ACS Restore ACS Service Management IP Pools Server IP Pools Address Recovery ACS Certificate Setup Global Authentication Setup <p style="text-align: center;">Back to Help</p>
	<ul style="list-style-type: none"> • Service Control • Logging • Date Format Control • Local Password Management • CiscoSecure Database Replication • RDBMS Synchronization • ACS Backup • ACS Restore • ACS Service Management • IP Pools Address Recovery • IP Pools Server • VoIP Accounting Configuration • ACS Certificate Setup • Global Authentication Configuration <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>

Enrole para baixo a página o ajuste do PULO. Quando a caixa é marcada, o ACS autentica o 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. No WLSM, defina um método que autentique os outros AP (um grupo de servidor da infraestrutura).

4. No WLSM, defina um método que autentiquem os dispositivos do cliente (um grupo de

servidor cliente) e o que EAP datilografa 2 aqueles clientes o uso. **Nota:** Esta etapa elimina a necessidade para o processo do [método de autenticação do cliente da definição](#).

5. Defina um VLAN original entre o Supervisor Engine 720 e o WLSM a fim permitir que o WLSM comunique-se com as entidades exteriores como AP e Authentication Server. Esta VLAN não está sendo usada em nenhum outro lugar ou para qualquer outra finalidade na rede. Crie o VLAN no Supervisor Engine 720 primeiramente, a seguir emita estes comandos: No Supervisor Engine 720: No WLSM:
6. Verifique a função do WLSM com esses comandos: No WLSM: No Supervisor Engine 720:

Designe um AP como o dispositivo de infraestrutura

Em seguida, você deve designar pelo menos uma infraestrutura AP e relacionar o AP ao WDS. Os clientes associam à infraestrutura AP. A infraestrutura AP pede o WDS AP ou WLSM para executar a autenticação para eles.

Termine estas etapas a fim adicionar uma infraestrutura AP que use os serviços do WDS:

Nota: Esta configuração aplica-se somente à infraestrutura AP e não o WDS AP.

1. Escolha **Serviços sem fio > AP**. Na infraestrutura AP, seleta **permita** para a opção de Serviços sem fio. Datilografe então o nome de usuário e senha WDS. Você deve definir um nome de usuário e uma senha de WDS no servidor de autenticação para todos os dispositivos que serão membros do WDS.

The screenshot shows the Cisco 1200 Access Point configuration page. 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 shows the configuration for 'Wireless Services: AP'. The 'Participate in SWAN Infrastructure' section has a red arrow pointing to the 'Enable' radio button. Below it, 'WDS Discovery' is set to 'Auto Discovery'. The 'Specified Discovery' option is disabled, with the text 'DISABLED (IP Address)'. A red box highlights the 'Username' field containing 'infrastructureap', and the 'Password' and 'Confirm Password' fields. At the bottom, the 'L3 Mobility Service via IP/GRE Tunnel' is set to 'Disable'. The page includes 'Apply' and 'Cancel' buttons at the bottom right.

Alternativamente, emita estes comandos do CLI:

- Escolha **Serviços sem fio > WDS**. Na aba do Status WDS WDS AP, a infraestrutura nova AP aparece na área de informação de WDS, com o estado tão ATIVO, e na área de informação AP, com estado quanto REGISTRADA. Se o AP não parece ATIVO e/ou REGISTRADO, verifique o Authentication Server para ver se há todos os erros ou a autenticação falha tenta. Depois que o AP parece ATIVO e/ou REGISTRADO, adicionar um método de autenticação do cliente ao WDS.

The screenshot shows the Cisco 1200 Access Point configuration interface. The main content area is titled "Cisco 1200 Access Point" and has three tabs: "WDS STATUS", "SERVER GROUPS", and "GENERAL SET-UP". The "WDS STATUS" tab is selected. The page displays the hostname "WDS_AP" and the date/time "10:02:01 Mon Apr 26 2004".

The "Wireless Services: WDS - Wireless Domain Services - Status" section contains the following information:

- WDS Information:** A table with columns: MAC Address, IP Address, Priority, and State. One entry is shown: MAC Address 0005.9a38.429f, IP Address 10.0.0.102, Priority 254, and State Administratively StandAlone - ACTIVE.
- WDS Registration:** Shows APs: 2 and Mobile Nodes: 0.
- AP Information:** A table with columns: MAC Address, IP Address, and State. Two entries are shown:

MAC Address	IP Address	State
000c.8547.b6c7	10.0.0.108	REGISTERED
0005.9a38.429f	10.0.0.102	REGISTERED
- Mobile Node Information:** A table with columns: MAC Address, IP Address, State, SSID, VLAN ID, and BSSID. No data is shown.
- Wireless Network Manager Information:** A table with columns: IP Address and Authentication Status. No data is shown.

A "Refresh" button is located at the bottom right of the page.

Alternativamente, emita este comando do CLI: Alternativamente, emita este comando do WLSM: Então, emita este comando na infraestrutura AP: **Nota:** Você não pode associações do cliente de teste porque a autenticação do cliente não tem disposições ainda.

[Defina o método de autenticação do cliente](#)

Finalmente, defina um método de autenticação do cliente.

Termine estas etapas a fim adicionar um método de autenticação do cliente:

- Escolha **Serviços sem fio > WDS**. Execute estas etapas na aba dos grupos de servidor WDS AP: Defina um grupo de servidor que autentique clientes (um grupo de cliente). Defina a prioridade 1 para o servidor de autenticação configurado anteriormente. Ajuste o tipo aplicável de autenticação (PULO, EAP, MAC, e assim por diante). Aplique os ajustes aos

SSID
relevantes.

The screenshot displays the Cisco 1200 Access Point configuration page, specifically the 'SERVER GROUPS' tab. The interface includes a navigation menu on the left 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 shows 'WDS STATUS', 'SERVER GROUPS', and 'GENERAL SET-UP' tabs. The hostname is 'WDS_AP' and the time is '10:23:43 Mon Apr 26 2004'. The 'Wireless Services: WDS - Server Groups' section contains a 'Server Group List' with 'Infrastructure' and 'Client' groups. The 'Client' group is selected, and its configuration is shown in a red-bordered box. This configuration includes 'Server Group Name: Client', 'Group Server Priorities: Define Servers', and three priority dropdowns: 'Priority 1: 10.0.0.3', 'Priority 2: < NONE >', and 'Priority 3: < NONE >'. Below this, the 'Use Group For:' section has radio buttons for 'Infrastructure Authentication' and 'Client Authentication', with 'Client Authentication' selected. Under 'Client Authentication', there are 'Authentication Settings' with checkboxes for 'EAP Authentication', 'LEAP Authentication', 'MAC Authentication', and 'Default (Any) Authentication'. To the right, 'SSID Settings' has radio buttons for 'Apply to all SSIDs' (selected) and 'Restrict SSIDs (Apply only to listed SSIDs)'. The 'Restrict SSIDs' section includes an 'SSID: DISABLED' field with 'Add' and 'Remove' buttons. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Alternativamente, emita estes comandos do CLI:**Nota:** O exemplo WDS AP é dedicado e não aceita associações de cliente.**Nota:** Não configurar na infraestrutura AP para grupos de servidor porque a infraestrutura AP envia todos os pedidos ao WDS ser processado.

2. Na infraestrutura AP ou AP: Sob o item de menu da **Segurança > do gerenciador de criptografia**, a **criptografia de WEP** ou a **cifra do clique**, segundo as exigências do protocolo de autenticação você usa-se.

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

Cisco Compliant TKIP Features: Enable MIC Enable Per Packet Keying

Cipher

Encryption Keys

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

Sob o item de menu da **Segurança** > do gerenciador de **SSID**, métodos de autenticação seletos segundo as exigências do protocolo de autenticação que você se usa.

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

- Security: SSID Manager - Radio0-802.11B**: This section contains the "SSID Properties" configuration. It features a "Current SSID List" table with a single entry "infraSSID" selected. To the right of the table, there are input fields for "SSID:" (containing "infraSSID"), "VLAN:" (set to "< NONE >"), and "Network ID:" (set to "0-4096"). A "Define VLANs" link is also present.
- Authentication Settings**: This section is highlighted with a red box and contains the "Methods Accepted" configuration. It includes three rows of settings:
 - Open Authentication: with EAP
 - Shared Authentication: < NO ADDITION >
 - Network EAP: < NO ADDITION >

On the left side of the interface, there is a vertical navigation menu with options such as 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, and EVENT LOG.

3. Você pode agora com sucesso testar se os clientes autenticam à infraestrutura AP. O AP do WDS na aba do Status WDS (sob os **Serviços sem fio** > o item de menu **WDS**) indica que o cliente aparece na área de informação do nó móvel e tem um estado REGISTRADO. Se o cliente não aparece, verifique o Authentication Server para ver se há todos os erros ou a autenticação falha tenta pelos clientes.

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

Alternativamente, emita estes comandos do CLI: **Nota:** Se você precisa o debug authentication, assegure-se de que você debugue no WDS AP, porque o WDS AP é o dispositivo que se comunica com o Authentication Server.

[Verificar](#)

No momento, não há procedimento de verificação disponível para esta configuração.

[Troubleshooting](#)

Esta seção fornece informações que você pode utilizar para fazer troubleshooting de configuração. Esta lista mostra algumas das perguntas comum relativas ao comando WDS a fim esclarecer mais a utilidade destes comandos:

- Pergunta: No WDS AP, que são as configurações recomendadas para estes artigos? intervalo do raio-server deadtime do raio-server Tempo do holdoff da falha do Message Integrity Check do Temporal Key Integrity Protocol (TKIP) (MIC) Tempo do holdoff de cliente Intervalo do Reauthentication EAP ou MAC Intervalo do cliente EAP (opcional) Resposta: Sugere-se que você mantenha a configuração com configurações padrão em relação a estes ajustes especiais, e usa-se somente os quando há um problema em relação ao sincronismo. Estas

- Os clientes Wireless não podem se associar ao AP.
- Os clientes Wireless podem associar ao AP, mas não recebem um endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP.
- Um telefone wireless não é autenticado quando você tem uma Voz sobre a distribuição de WLAN.
- A autenticação de EAP não ocorre. Com a rede-**identificação da mobilidade** configurada, o AP tenta construir um túnel de encapsulamento de roteamento genérico (GRE) para enviar pacotes EAP. Se nenhum túnel é estabelecido, os pacotes não vão em qualquer lugar.
- Um AP configurado como um dispositivo WDS não funciona como esperado, e a configuração de WDS não trabalha. **Nota:** Você não pode configurar o AP/bridge do Cisco Aironet 1300 como um mestre WDS. O AP/bridge 1300 não apoia esta funcionalidade. O AP/bridge 1300 pode participar em uma rede WDS enquanto um dispositivo de infraestrutura em que algum outro AP ou WLSM estão configurados como um mestre WDS.

Comandos para Troubleshooting

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- **debugar o autenticador todo aaa do dot11** — Mostra às várias negociações que um cliente vai completamente enquanto o cliente associa e autentica com o 802.1x ou o processo EAP. Isto debuga foi introduzido no Cisco IOS Software Release 12.2(15)JA. Esse comando torna obsoleto `debug dot11 aaa dot1x all` nesta versão e em versões posteriores.
- **debugar a autenticação aaa** — Mostra o processo de autenticação de uma perspectiva genérica AAA.
- **debugar o wlccp ap** — Mostra que as negociações de WLCCP envolvidas como um AP se juntam a um WDS.
- **debugar o pacote do wlccp** — Mostra a informação detalhada sobre negociações de WLCCP.
- **debugar o pulo-cliente do wlccp** — Mostra os detalhes enquanto um dispositivo de infraestrutura se junta a um WDS.

Informações Relacionadas

- [Configurando o WDS, jejeue vaguear seguro, e Gerenciamento do rádio](#)
- [Nota de configuração do Módulo de serviços do Wireless LAN do Catalyst 6500 Series](#)
- [Configurando conjuntos de cifras e o WEP](#)
- [Configurando tipos de autenticação](#)
- [Páginas de Suporte de Wireless LAN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)