Índice

Introdução

Este documento introduz o conceito de serviços de domínio sem fio (WDS). O documento 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 documento 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 documento começado 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 registo 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 authenticação 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 gira 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 protocolo 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). Estes 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 o 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.

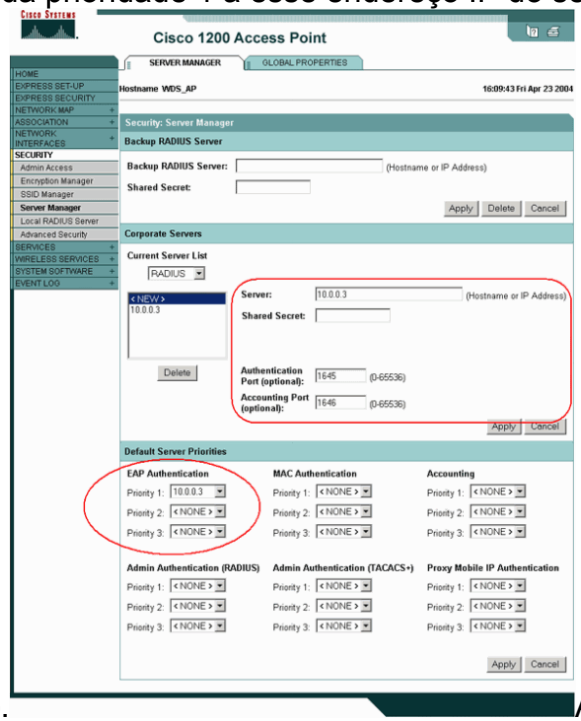
Esta seção apresenta a informação necessária configurar as características descritas neste documento.

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.

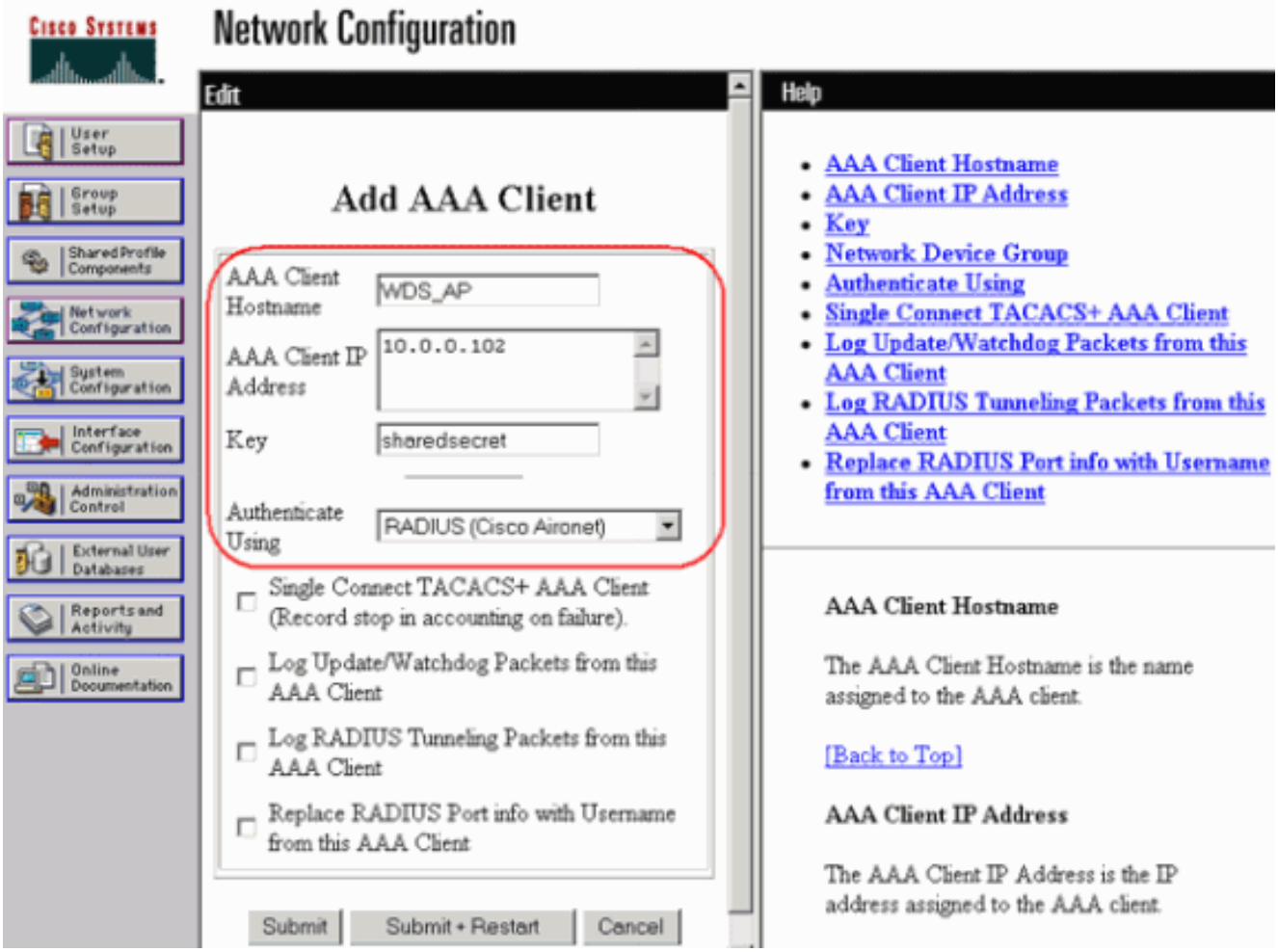
Termine estas etapas a fim designar um AP como o WDS:

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. 

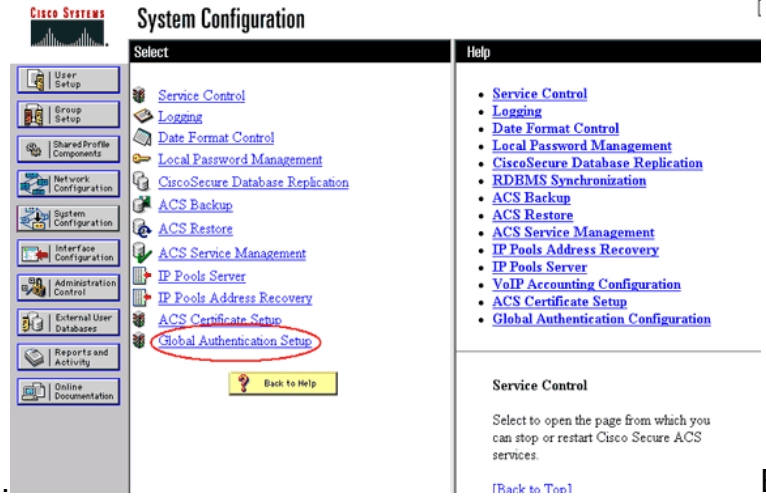
Alternativamente, emita

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 documento 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.

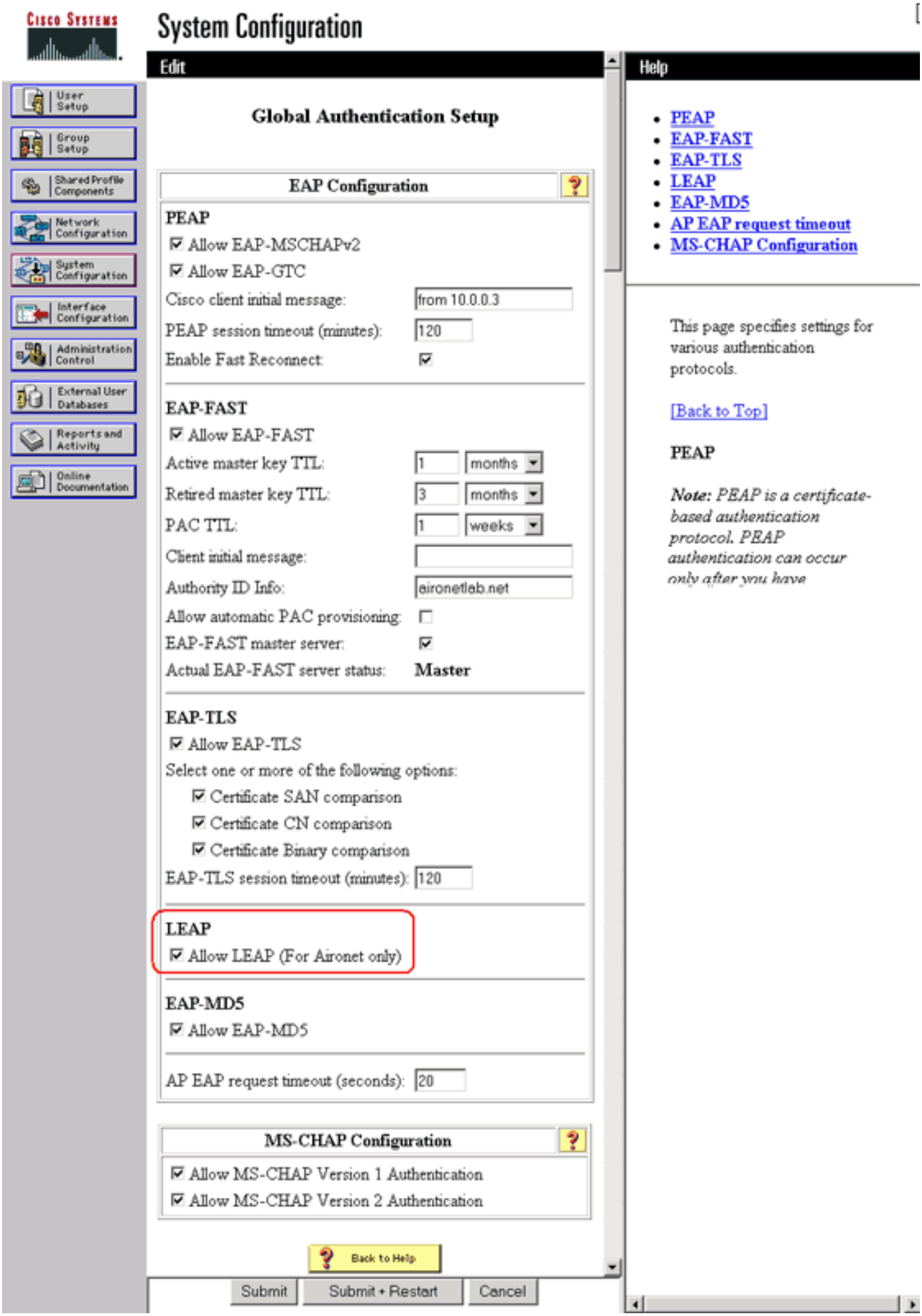


Também, no Cisco Secure ACS, assegure-se de que você configure o ACS para executar a autenticação de leap na configuração de sistema - página de instalação da autenticação global. Primeiramente, a **configuração de sistema do** clique, clica então a **instalação da autenticação global**.



Enrole para baixo a

página o ajuste do PULO. Quando a caixa é marcada, o ACS autentica o LEAP.

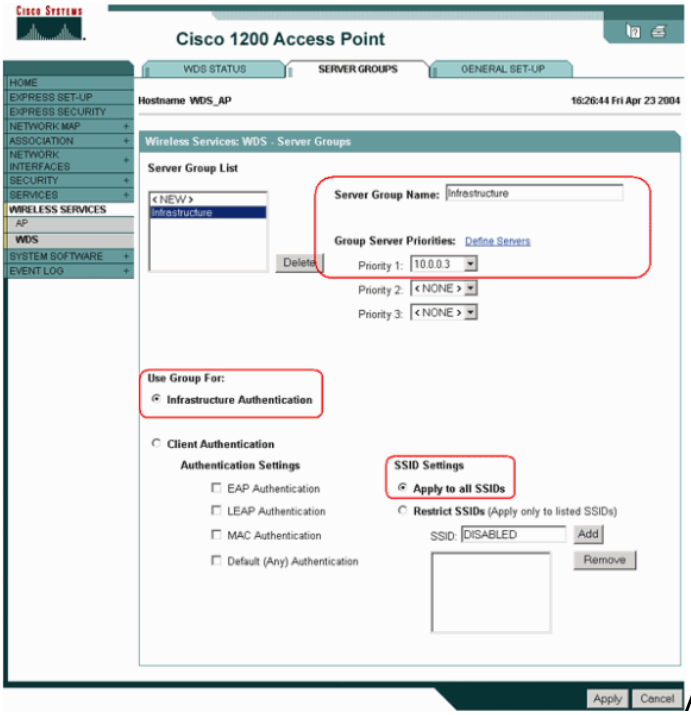


3. A fim configurar os setttings WDS no WDS AP, escolha **Serviços sem fio > WDS no** WDS

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:

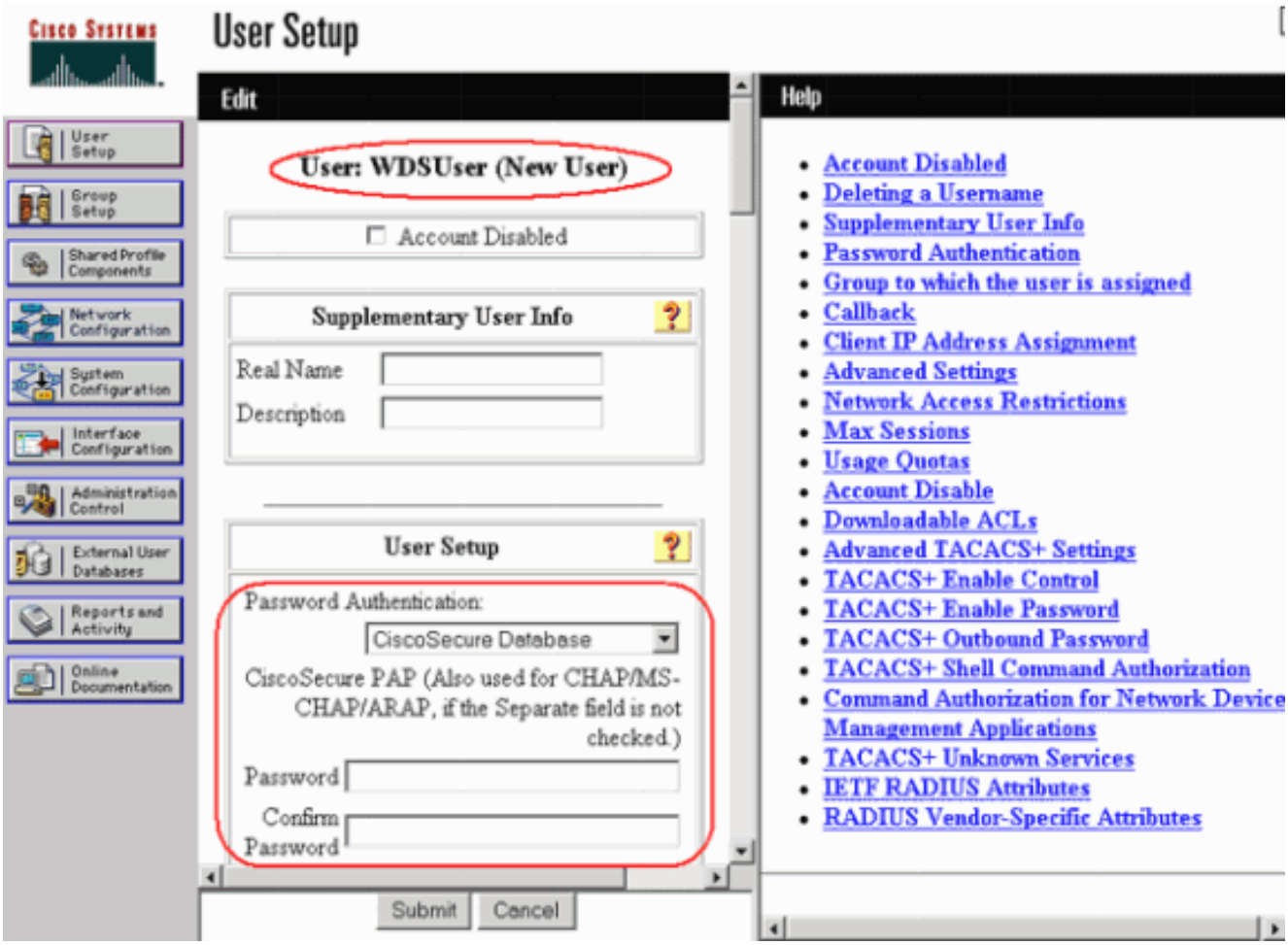
4. Escolha **Serviços sem fio > WDS**, e vá à aba dos **grupos de servidor**:Defina um nome de grupo de servidor que autentique os outros AP, um grupo da infraestrutura.Defina a prioridade 1 para o servidor de autenticação configurado anteriormente.Clique o **grupo do uso para:** Botão de rádio da **autenticação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



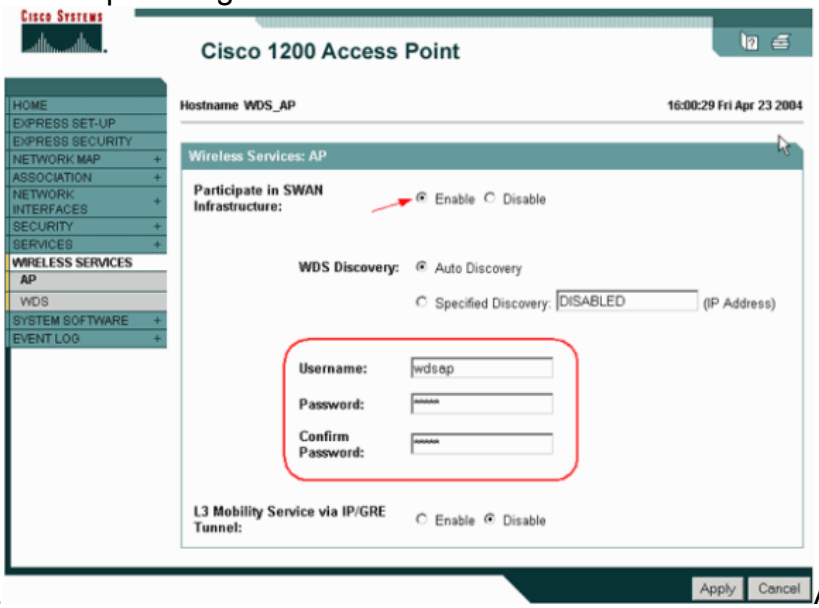
(SSID). Alternativamente, emita estes

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 põem o usuário WDS em um grupo que seja atribuído muitos direitos e privilégios? O WDS exige somente autenticação limitada.



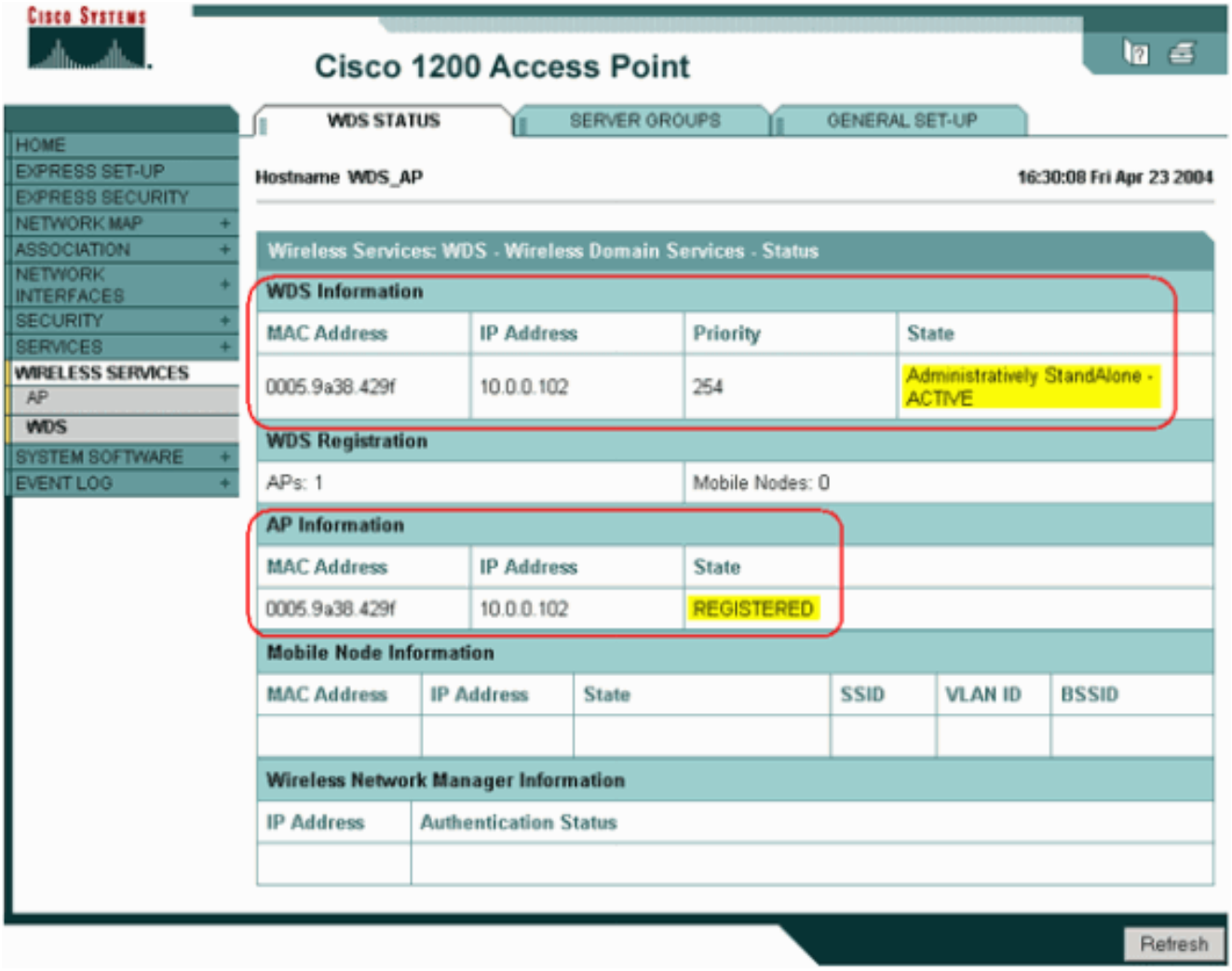
6. Escolha **Serviços sem fio > AP**, e o clique **permite** para a participação na opção da infraestrutura de swan. Datilografe então o nome de usuário e senha WDS.Você deve definir um nome de usuário e uma senha WDS no servidor de autenticação para todos os diapositivos que designam membros do



WDS. Alternativamente, emita estes

comandos do CLI:

7. 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.



Alternativamente, emita estes comandos do CLI:**Nota:** Você não pode associações do cliente de teste porque a authenticação 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:

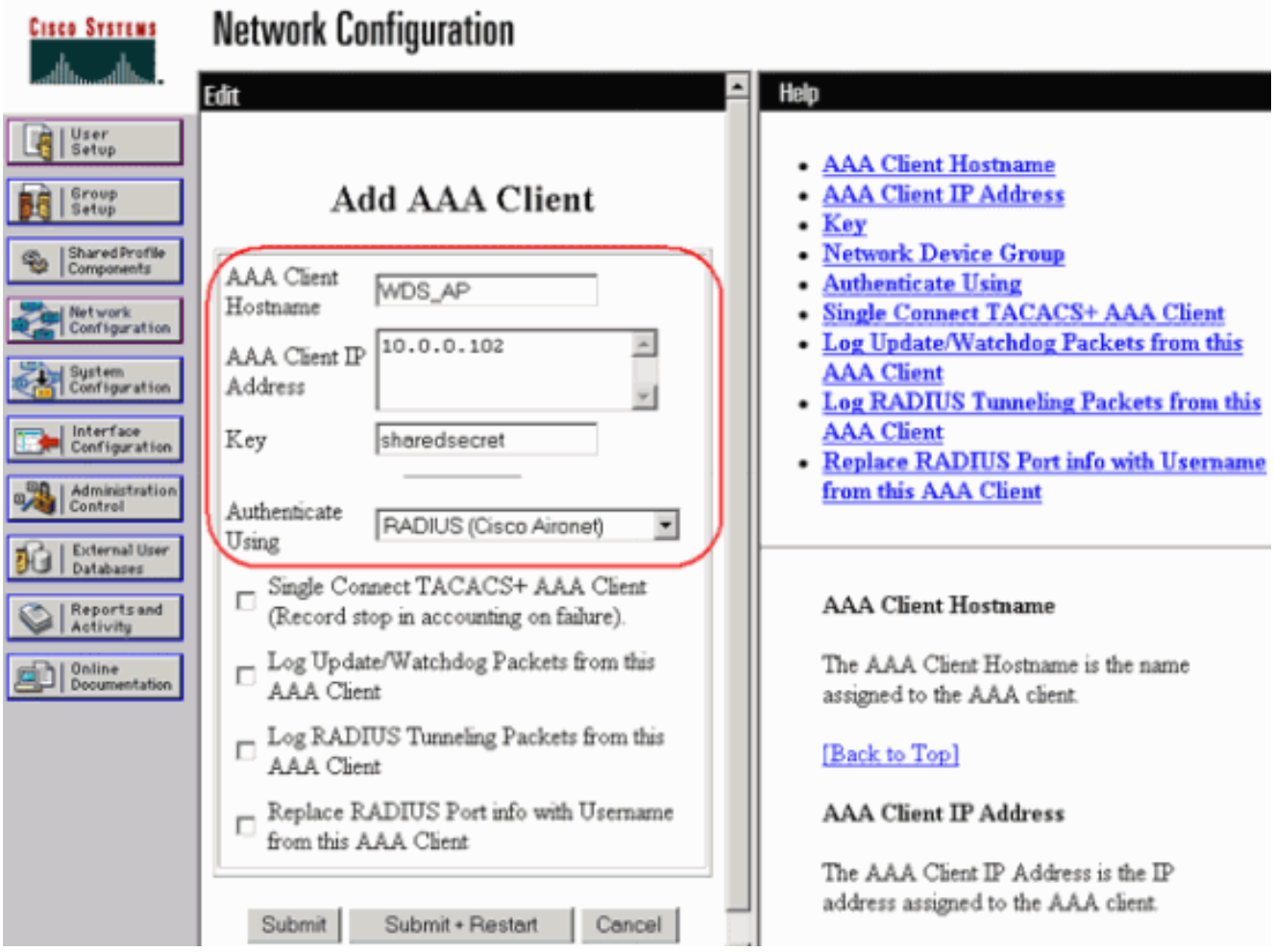
```
c6506#session slot x proc 1!--- In this command, x is
the slot number where the WLSM resides. The default
escape character is Ctrl-^, then x.You can also type
'exit' at the remote prompt to end the sessionTrying
127.0.0.51 ... OpenUser Access VerificationUsername:
```

```
<username>Password: <password>wlan>enablePassword:
<enable password>wlan#
```

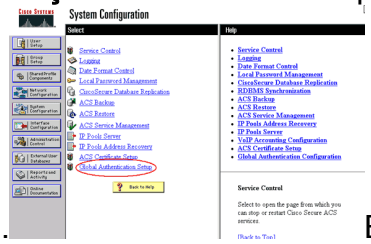
Nota: A fim pesquisar defeitos mais facilmente e manter seu WLSM, configurar o Acesso remoto do telnet ao WLSM. Consulte a Configuração de Acesso Remoto de Telnet.

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 IETFPara outros Authentication Server NON-ACS, refira a documentação do fabricante.

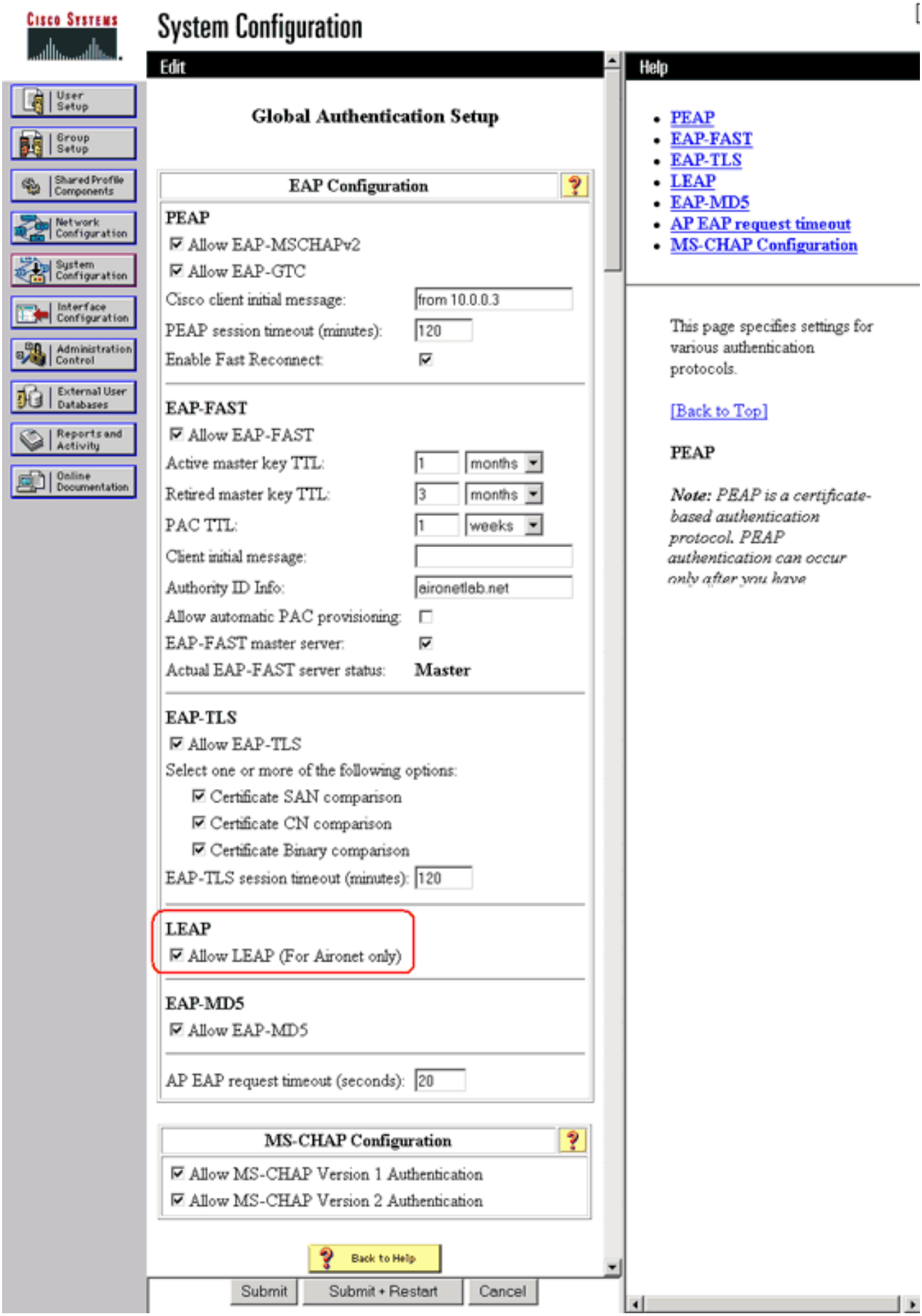


Também, no Cisco Secure ACS, configurar o ACS para executar a autenticação de leap na configuração de sistema - página de instalação da autenticação global. Primeiramente, a **configuração de sistema do** clique, clica então a **instalação da autenticação global**.



Enrole para baixo a página o ajuste do PULO. Quando a

caixa é marcada, o ACS autentica o LEAP.



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 authenticação 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.

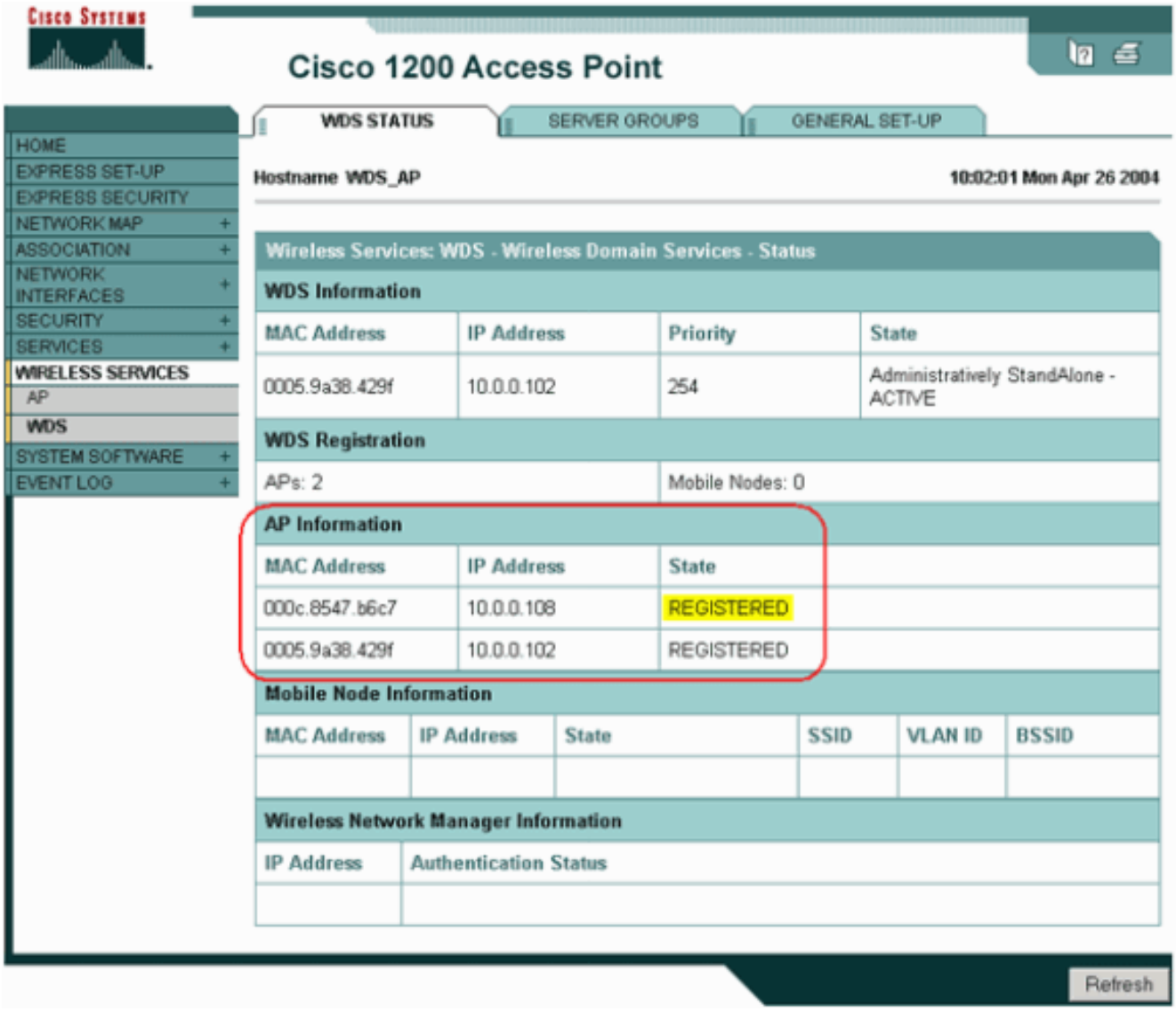
Termine estas etapas a fim adicionar uma infraestrutura AP que use os serviços do WDS:

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.

Alternativamente, emita estes comandos do CLI:

2. 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 authenticação do cliente ao
WDS.



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 authenticação do cliente não tem disposições ainda.

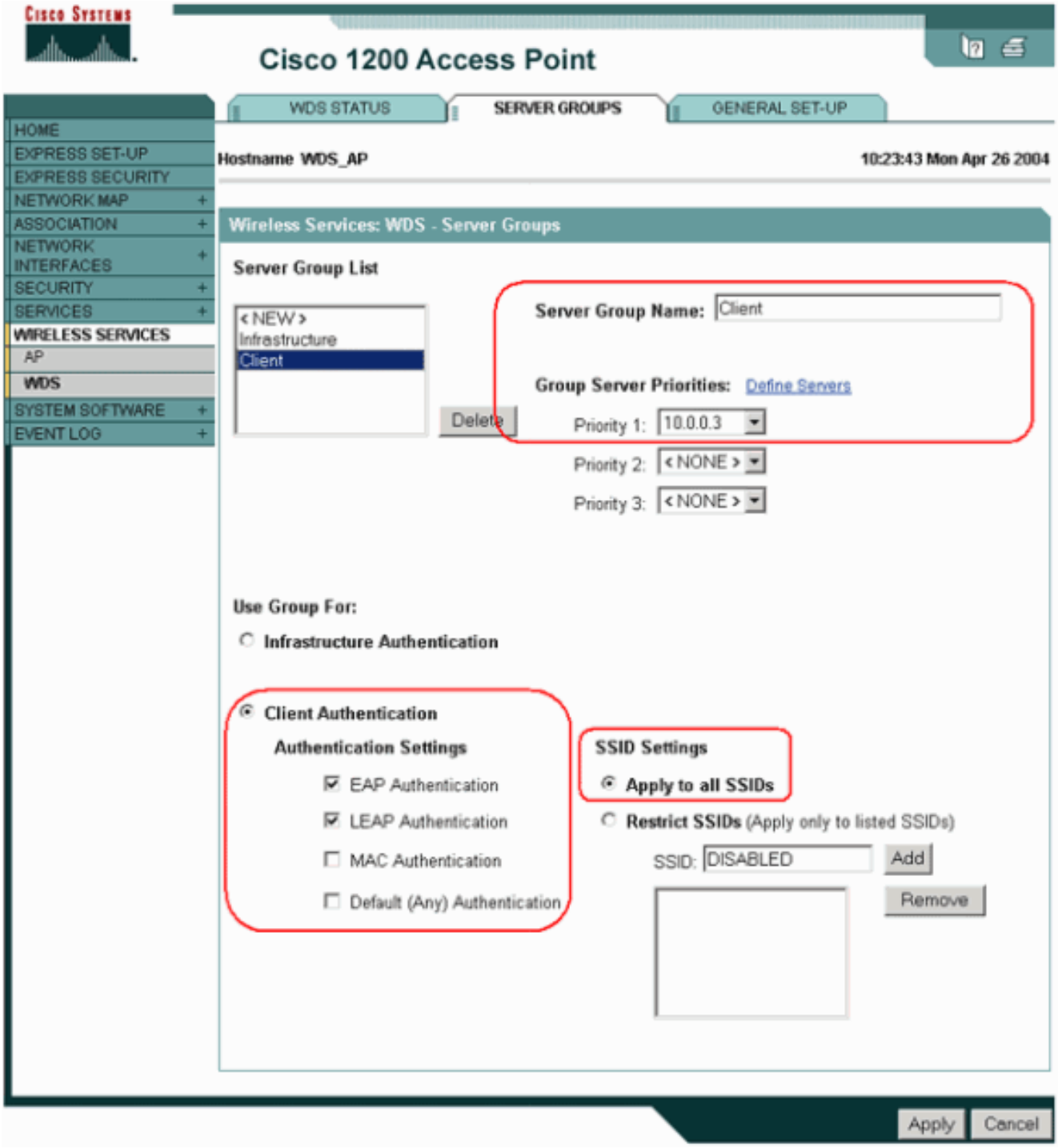
Defina o método de authenticação do cliente

Finalmente, defina um método de authenticação do cliente.

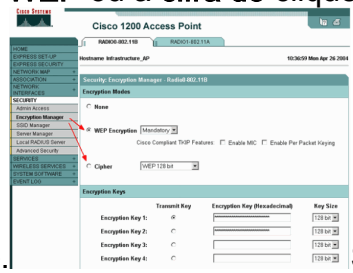
Termine estas etapas a fim adicionar um método de authenticação do cliente:

1. 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

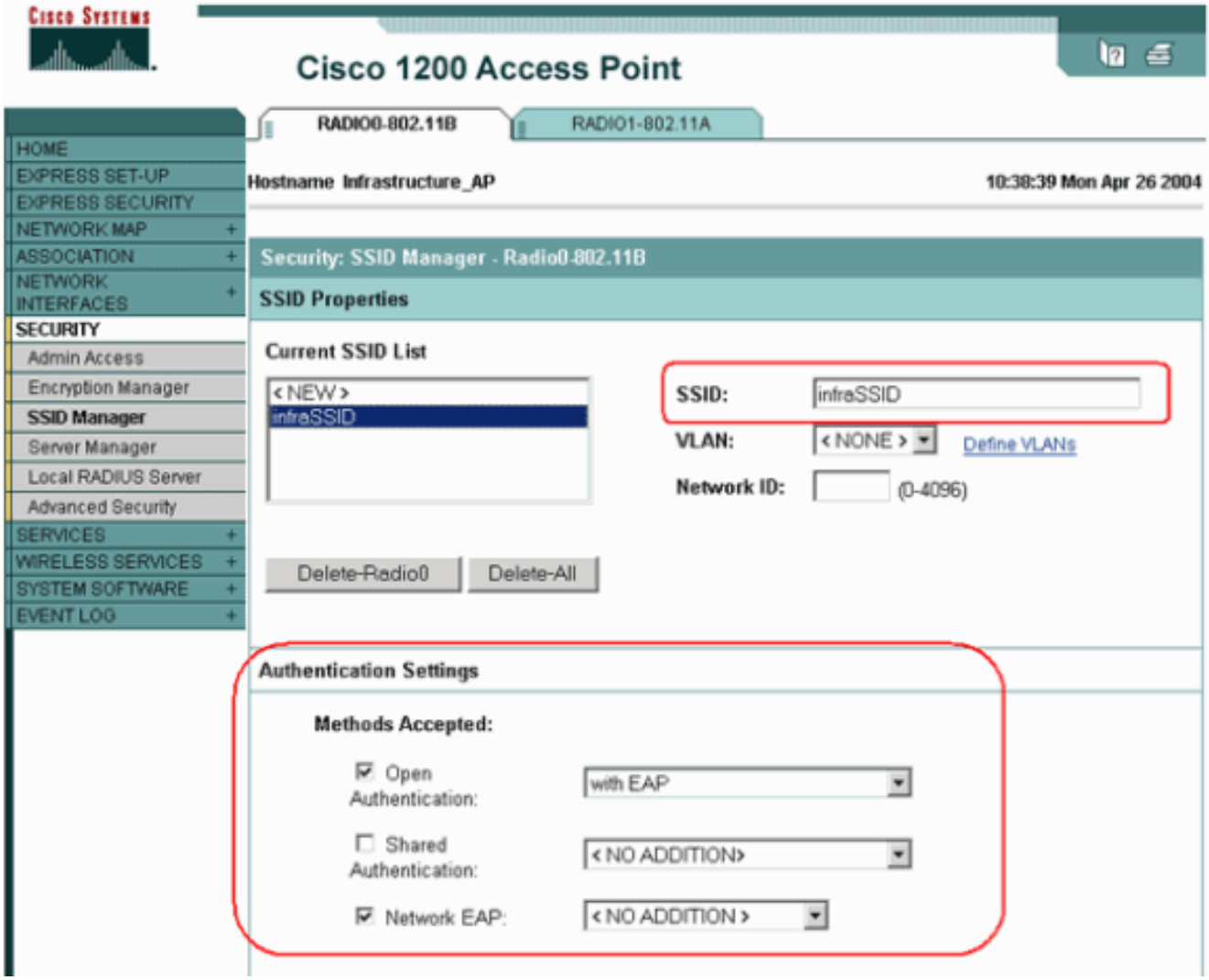
aplicável de autenticação (PULO, EAP, MAC, e assim por diante).Aplique os ajustes aos SSID
relevantes.



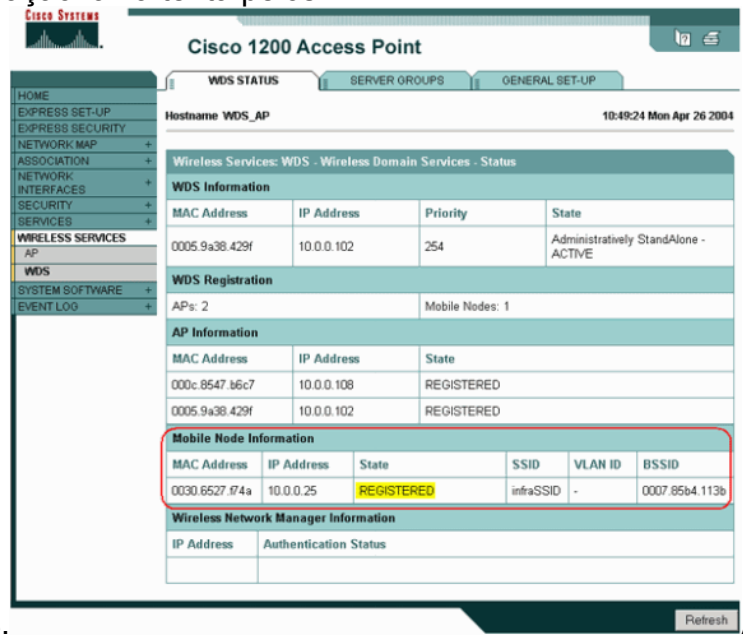
Alternativamente, emita estes comandos do CLI:**Nota:** O exemplo WDS AP é dedicado e não aceita associações de cliente.**Nota:** Não configurar na infraestrutura AP para grupos de servidor porque a infraestrutura AP envia todos os pedidos ao WDS ser processado.

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.  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.



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. 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-serverdeadtime do raio-serverTempo do holdoff da falha do Message Integrity Check do Temporal Key Integrity Protocol (TKIP) (MIC)Tempo do holdoff de clienteIntervalo do Reauthentication EAP ou MACIntervalo 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 são as configurações recomendadas para o WDS AP:**Intervalo do raio-server do** desabilitação. Este é o número de segundos esperas AP para uma resposta a uma requisição RADIUS antes que envie novamente o pedido. O padrão é os segundos 5.**Deadtime do raio-server do** desabilitação. O RAIO está saltado por pedidos adicionais para a duração dos minutos a menos que todos os server forem marcados absolutamente.O tempo do holdoff da falha TKIP MIC é permitido à revelia a 60 segundos. Se você permite o tempo do holdoff, você pode incorporar o intervalo aos segundos. Se o AP detecta duas falhas MIC dentro de 60 segundos, obstrui todos os clientes TKIP nessa relação para o período de tempo do holdoff especificado aqui.O tempo do holdoff de cliente deve ser desabilitado à revelia. Se você permite o holdoff, incorpore o número de segundos que o AP deve esperar depois que uma falha de autenticação antes de um pedido da autenticação subsequente é processada.O intervalo do Reauthentication EAP ou MAC é desabilitado à revelia. Se você permite o reauthentication, você pode especificar o intervalo ou aceitar o intervalo dado pelo Authentication Server. Se você escolhe especificar o intervalo, incorpore o intervalo aos segundos que o AP espera antes que force um cliente autenticado a reauthenticate.O intervalo do cliente EAP (opcional) é 120 segundos à revelia. Incorpore a quantidade de tempo que o AP deve esperar clientes Wireless para responder aos pedidos da autenticação de EAP.
- **Pergunta: Com respeito ao tempo do holdoff TKIP, eu li que este deve ser ajustado à Senhora 100 e aos não 60 segundos. Eu suponho que está ajustado ao segundo do navegador porque aquele é o mais baixo número que você pode seleto?Resposta:** Não há nenhuma recomendação específica ajustá-la à Senhora 100 a menos que houver uma falha relatada onde a única solução é aumentar este tempo. O segundo é o mais baixo ajuste.
- **Pergunta: Faz a authenticação do cliente destes dois comandos help em alguma maneira e são precisados no WDS ou na infraestrutura AP?em-para-início de uma sessão-AUTH do atributo 6 do raio-serveratributo 6 do raio-server apoio-múltiploResposta:** Estes comandos não ajudam o processo de autenticação e não são precisados no WDS ou no AP.

- **Pergunta: Na infraestrutura AP, eu suponho que nenhuns dos ajustes do gerenciador do servidor e das Propriedades globais estão precisados porque o AP recebe a informação do WDS. Qualquens um comandos específicos são precisados para a infraestrutura AP?em-para-início de uma sessão-AUTH do atributo 6 do raio-serveratributo 6 do raio-server apoio-múltiplointervalo do raio-serverdeadtime do raio-serverResposta:** Não há nenhuma necessidade de ter o gerenciador do servidor e as Propriedades globais para a infraestrutura AP. O WDS toma dessa tarefa e não há nenhuma necessidade de ter estes ajustes:**em-para-início de uma sessão-AUTH do atributo 6 do raio-serveratributo 6 do raio-server apoio-múltiplointervalo do raio-serverdeadtime do raio-server**As sobras do ajuste do **formato %h do incluir-em-acesso-req do atributo 32 do raio-server** à revelia e são exigidas.

Um AP é um dispositivo da camada 2. Consequentemente, o AP não apoia a mobilidade da camada 3 quando o AP é configurado para atuar como um dispositivo WDS. Você pode conseguir a mobilidade da camada 3 somente quando você configura o WLSM como o dispositivo WDS. Refira a seção da *arquitetura da mobilidade da camada 3 do* Módulo de serviços do Wireless LAN do Cisco Catalyst 6500 Series: White Paper para mais informação.

Consequentemente, quando você configura um AP como um dispositivo WDS, não use o **comando mobility network-id**. Este comando aplica-se para mergulhar 3 mobilidade e você precisa de ter um WLSM enquanto seu dispositivo WDS a fim configurar corretamente a mobilidade da camada 3. Se você usa o **comando mobility network-id** incorretamente, você pode ver alguns destes sintomas:

- 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, jejue 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