Exemplo de configuração de atribuição da VLAN dinâmica com servidor RADIUS e Wireless LAN Controller

Índice

Introdução

Este documento introduz o conceito da atribuição da VLAN dinâmica. O documento descreve como configurar o controller de LAN Wireless (WLC) e um servidor RADIUS para atribuir dinamicamente os clientes da Wireless LAN (WLAN) a uma VLAN específica.

Pré-requisitos

Requisitos

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

- Ter conhecimento básico do WLC e dos Lightweight Access Points (LAPs)
- Ter conhecimento funcional do servidor AAA
- Ter conhecimento completo das redes wireless e das questões de segurança wireless

- Ter conhecimento básico do Lightweight AP Protocol (LWAPP)

Componentes Utilizados

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

- O Cisco 4400 WLC que executa firmware com release 5.2
- LAP Cisco Série 1130
- Adaptador de cliente wireless da Cisco 802.11a/b/g que executa firmware com release 4.4
- Utilitário de desktop do Cisco Aironet (ADU) que executa a versão 4.4
- CiscoSecure Access Control Server (ACS) que executa a versão 4.1
- Switch Cisco Série 2950

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Atribuição da VLAN (Rede local virtual) dinâmica com servidor Radius

Na maioria de sistemas de WLAN, cada WLAN tem uma política estática que se aplica a todos os clientes associados com um Service Set Identifier (SSID), ou o WLAN na terminologia do controlador. Embora poderoso, este método tem limitações porque exige que os clientes se associem com os diferentes SSID para herdar diferentes QoS e políticas de segurança.

Mas a solução de Cisco WLAN suporta identidades na rede. Isto permite a rede anuncie um único SSID, mas permite que usuários específicos herdem diferentes QoS ou políticas de segurança baseadas nas credenciais do usuário.

A atribuição da VLAN dinâmica é um recurso que coloca um usuário wireless em uma VLAN específica baseado nas credenciais fornecidas pelo usuário. Esta tarefa de atribuir usuários a uma VLAN específica é realizada por um servidor de autenticação RADIUS, como o CiscoSecure ACS. Isto pode ser usado, por exemplo, para permitir que o host wireless permaneça na mesma VLAN enquanto ele se desloca em uma rede no campus.

Logo, quando um cliente tenta associar-se a um LAP registrado em um controlador, o LAP passa as credenciais do usuário ao servidor RADIUS para validação. Quando a autenticação é bem sucedida, o servidor Radius passa determinados atributos da Internet Engineering Task Force (IETF) ao usuário. Estes atributos RADIUS decidem a ID da VLAN que deve ser atribuído ao cliente wireless. A SSID (WLAN, em termos do WLC) do cliente não importa porque o usuário sempre recebe esta identificação predeterminada da VLAN.

Os atributos do usuário do RADIUS usados para a atribuição de ID da VLAN são:

- IETF 64 (tipo de túnel) — Defina como VLAN.
- IETF 65 (tipo de meio do túnel) — Defina como 802.
- IETF 81 (ID do grupo privado do túnel) — Defina como a identificação da VLAN.

A ID da VLAN tem 12 bits, e um valor entre 1 e 4094, inclusive. Como a ID de Grupo Privado do Túnel é do tipo string, como definido na RFC2868 para uso com a IEEE 802.1X, o valor de número inteiro da ID de VLAN é codificado como uma string. Quando estes atributos de túnel são enviados, é necessário preencher o campo Tag.

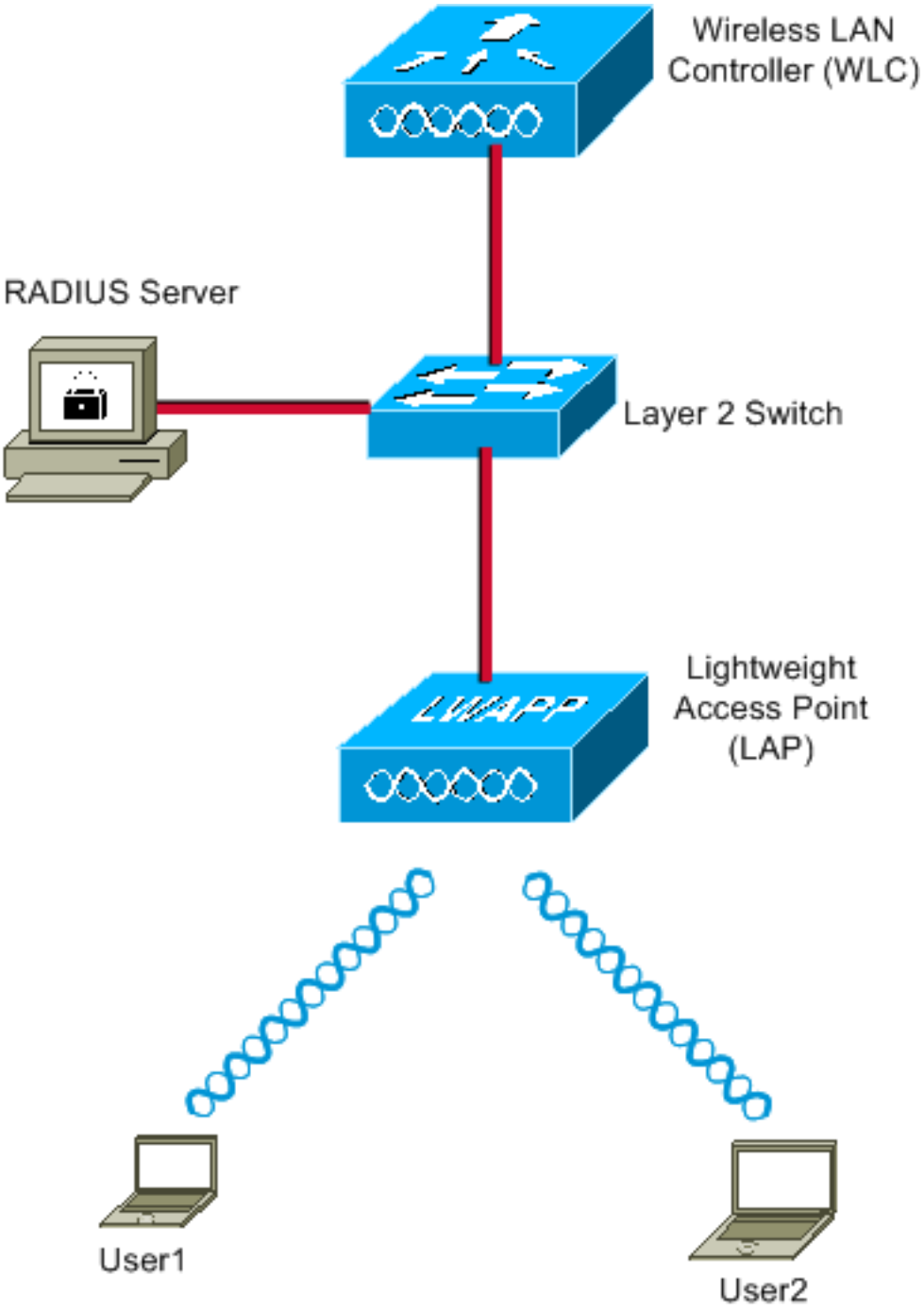
Como é explicado na RFC2868 , seção 3.1: **O campo Tag tem um octeto de comprimento e permite agrupar no mesmo pacote atributos que se referem ao mesmo túnel.** Os valores válidos para este campo são de 0x01 a 0x1F, inclusive. Se o campo Tag não for utilizado, ele deve ser zero (0x00). Consulte na RFC 2868 mais informações sobre todos os atributos de RADIUS.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Estes são os detalhes de configuração dos componentes usados neste diagrama:

- O endereço IP do servidor ACS (RADIUS) é 172.16.1.1.
- O endereço da interface de gerenciamento do WLC é 172.16.1.30.
- O endereço da relação do Gerenciador AP do WLC é 172.16.1.31.
- O endereço 172.16.1.1 do servidor DHCP é usado para atribuir IP address ao LWAPP. **O servidor DHCP interno no controlador é usado para atribuir o endereço IP aos clientes wireless.**
- A VLAN10 e a VLAN11 são usadas nesta configuração. O usuário1 é configurado para ser colocado na VLAN10 e o usuário2 é configurado para ser colocado na VLAN11 pelo servidor RADIUS.**Nota:** Este documento mostra todas as informações de configuração relativas somente ao usuário1. Faça o mesmo procedimento explicado neste documento para o usuário2.
- Este documento usa o 802.1x com LEAP como o mecanismo de segurança.**Nota:** A Cisco recomenda que você use métodos de autenticação avançados, tais como o EAP-FAST e a

autenticação EAP-TLS, para proteger a WLAN. Este documento usa somente LEAP por simplicidade.

Configuração

Antes da configuração, este documento supõe que o LEAP já está registrado no WLC. Para mais informações, consulte Exemplo de Configuração Básica de Controladores de Wireless LAN e Pontos de Acesso Lightweight. Para informações sobre o procedimento de registro envolvido, consulte Regristo do Lightweight AP (LAP em um controlador da Wireless LAN (WLC) .

Configuration Steps

Esta configuração é dividida em três categorias:

1. Configuração de servidor RADIUS
2. Configurar o Switch para várias VLANs
3. Configuração de WLC
4. Configuração de utilitário do cliente Wireless

Configuração de servidor RADIUS

Esta configuração exige estas etapas:

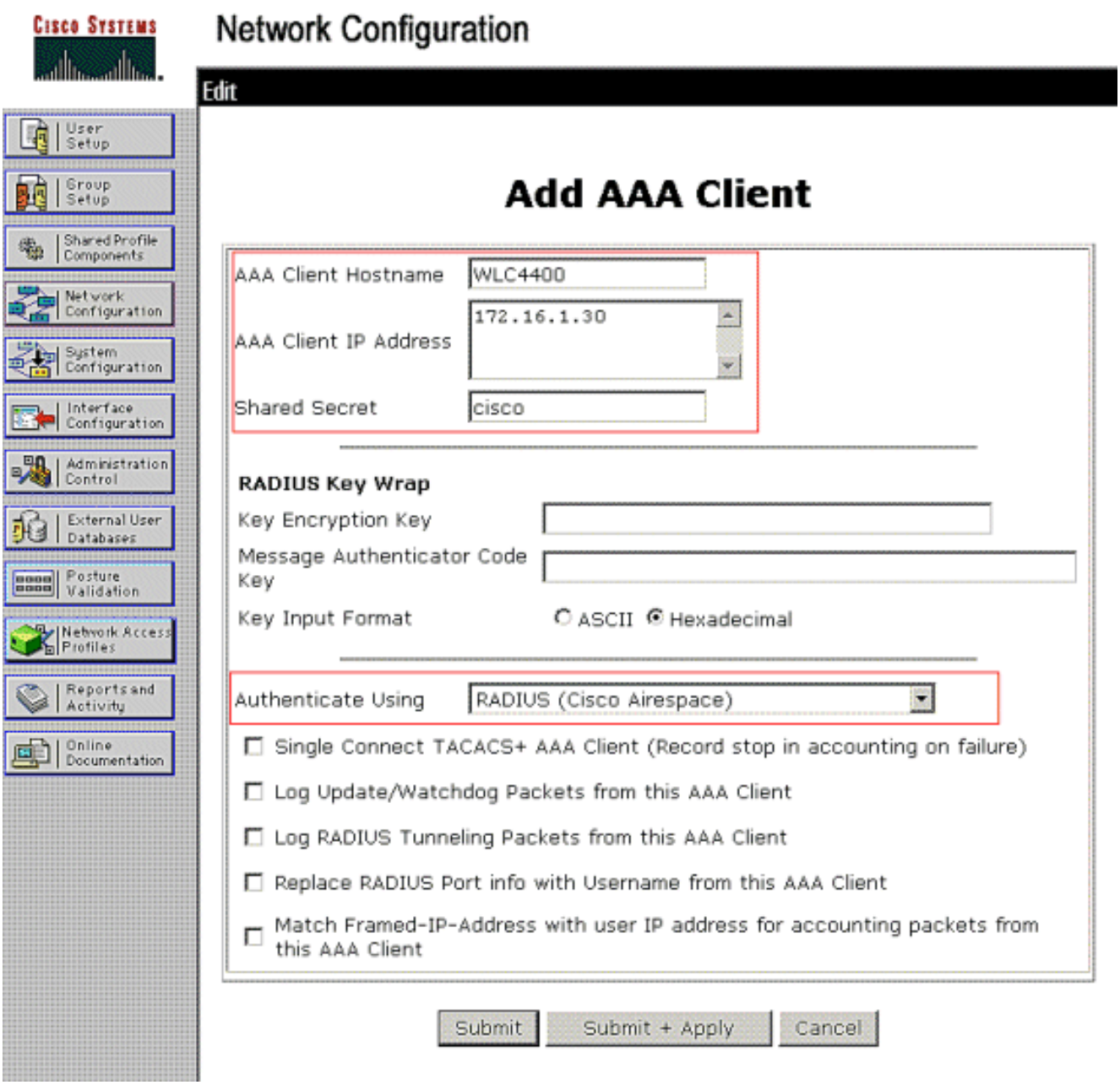
- Configurar o WLC como um cliente de AAA no servidor Radius
- Configurar os usuários e os atributos do RADIUS (IETF) usados para a atribuição da VLAN dinâmica no servidor RADIUS

Configurar o cliente de AAA para o WLC no servidor RADIUS

Este procedimento explica como adicionar o WLC como um cliente de AAA no servidor RADIUS para que o WLC possa passar as credenciais do usuário ao servidor RADIUS.

Conclua estes passos:

1. Na interface gráfica do usuário do ACS, clique em **Network Configuration**.
2. Clique na seção **Add Entry** sob o campo AAA Clients.
3. Digite a chave (Key) e o endereço IP do cliente do AAA (AAA Client IP Address).O endereço IP deve ser o endereço IP da interface de gerenciamento do WLC.Certifique-se que a chave que você digitar é a mesma configurada no WLC na janela Security. Esta é a chave secreta usada para uma comunicação entre o cliente de AAA (WLC) e o servidor RADIUS.
4. Escolha **RADIUS (Cisco Airespace)** no campo Authenticate Using como o tipo do autenticação.

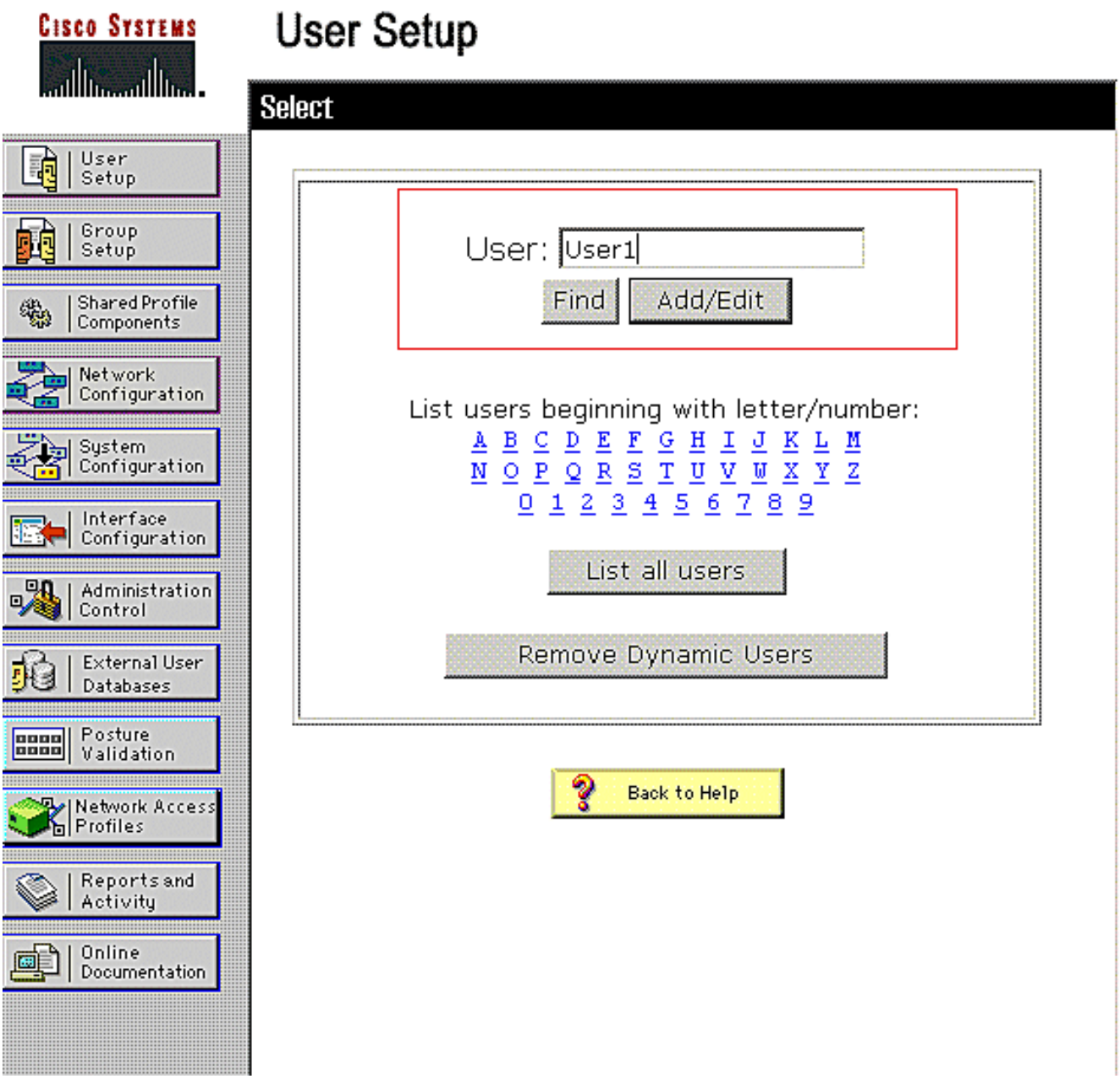


Configurar os usuários e os atributos do RADIUS (IETF) usados para a atribuição da VLAN dinâmica no servidor RADIUS

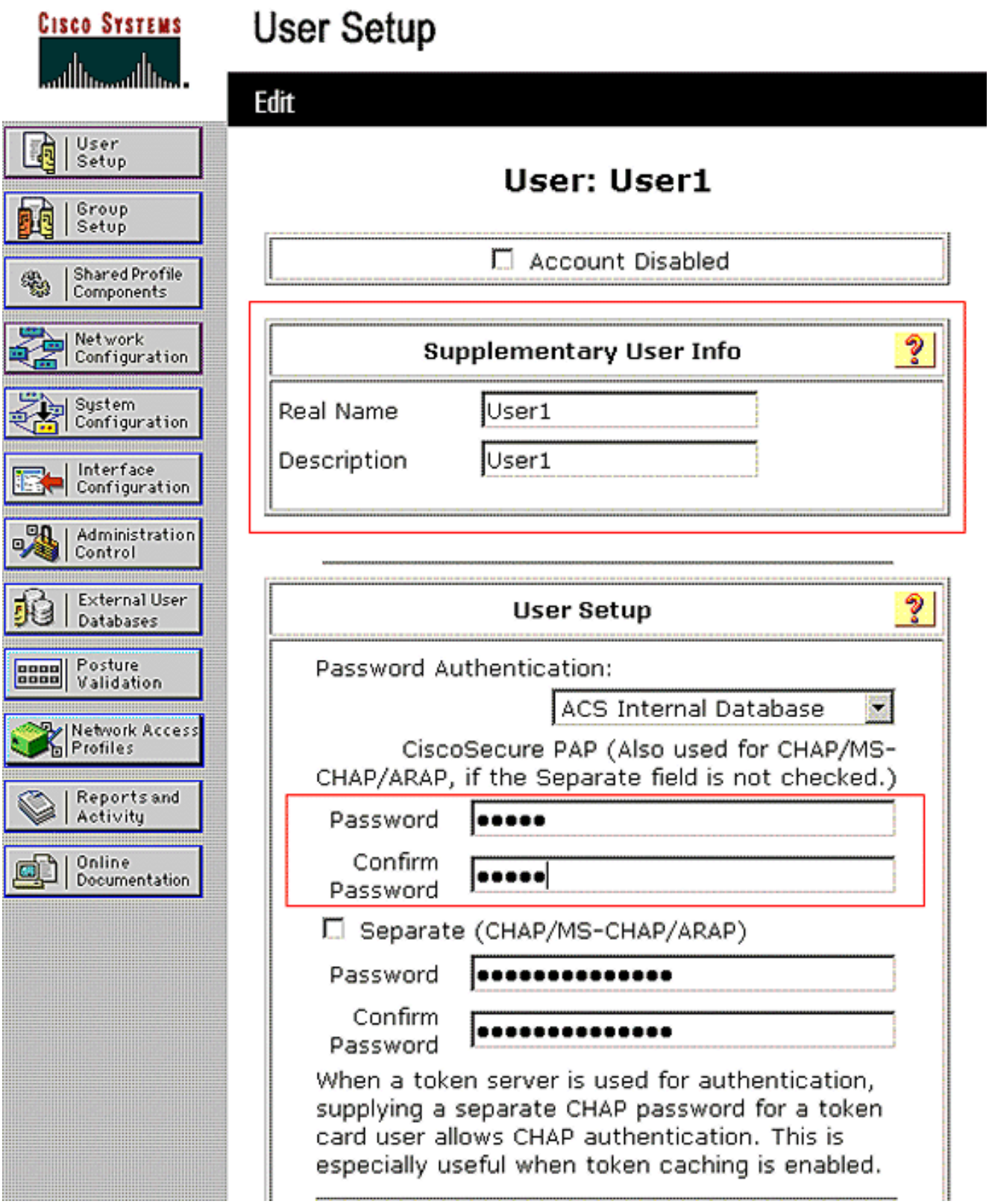
Este procedimento explica como configurar os usuários no servidor RADIUS e nos atributos do RADIUS (IETF) usados para atribuir IDs da VLAN a estes usuários.

Conclua estes passos:

1. Na interface gráfica do usuário do ACS, clique em **User Setup**.
2. Na janela User Setup, digite um nome de usuário no campo User e clique em **Add/Edit**.

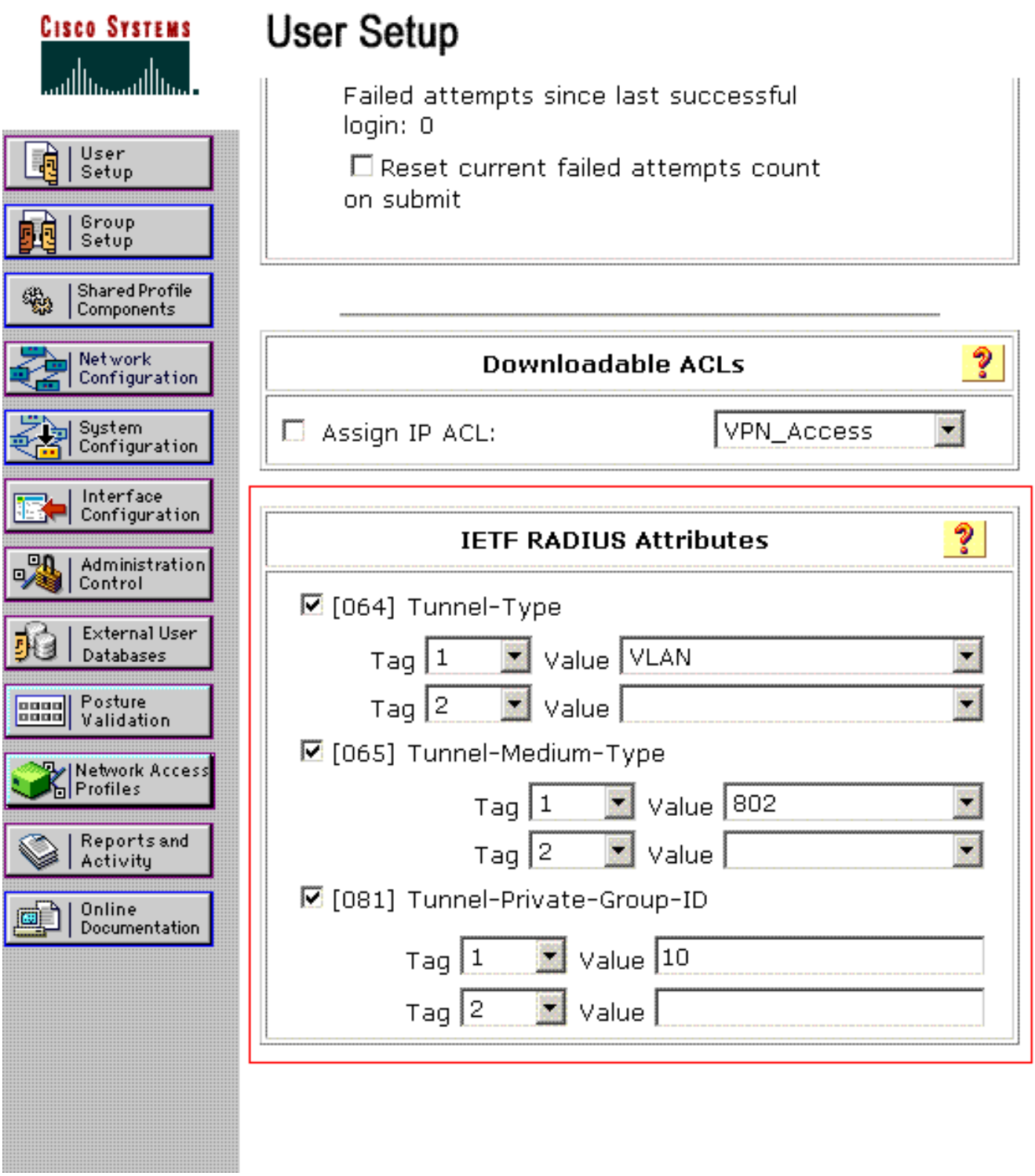


3. Na página Edit, digite as informações necessárias do usuário, como mostrado aqui:

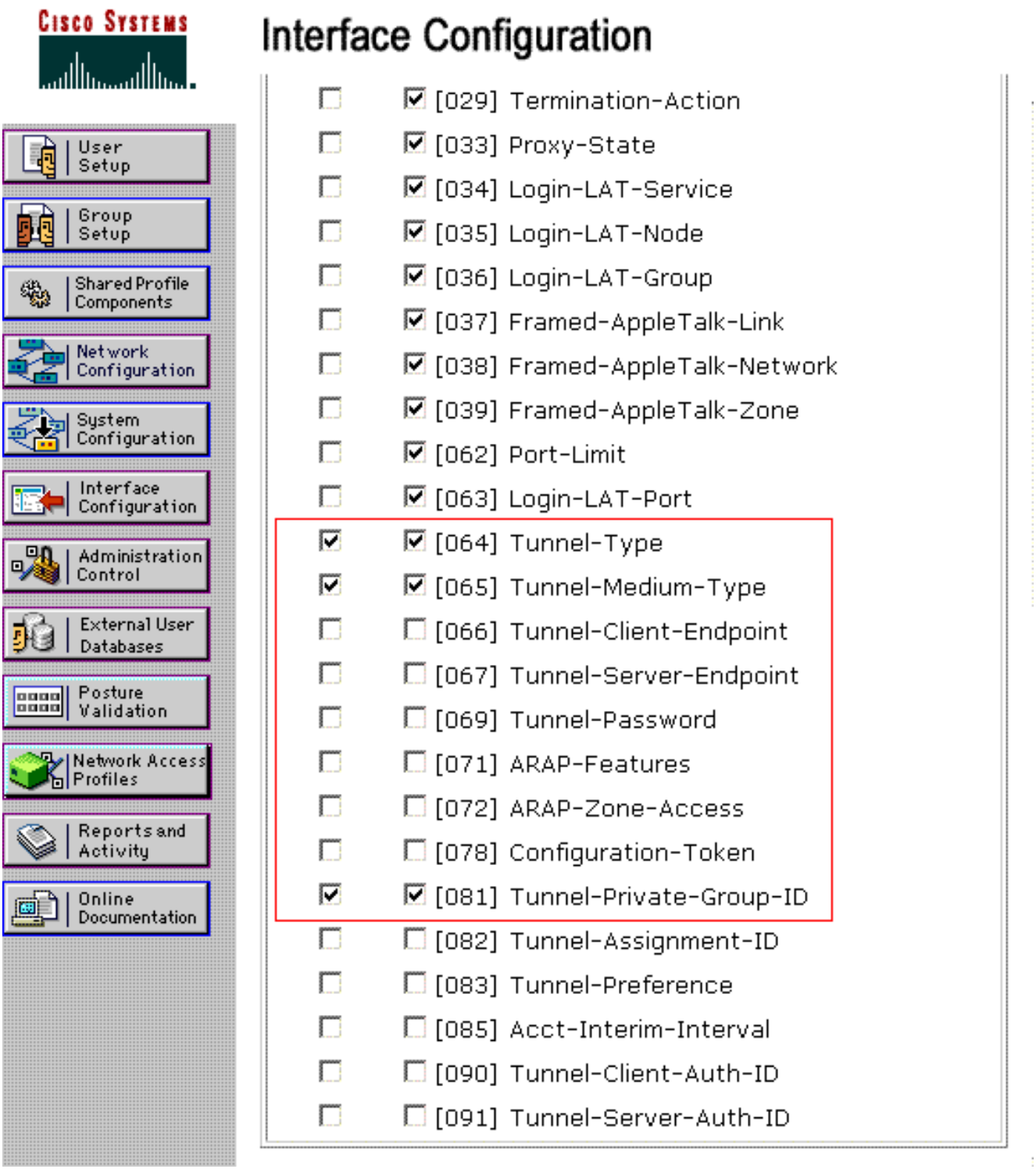


Neste diagrama, observe que a senha que você fornece na seção User Setup deve ser a mesma fornecida no lado do cliente durante a autenticação de usuário.

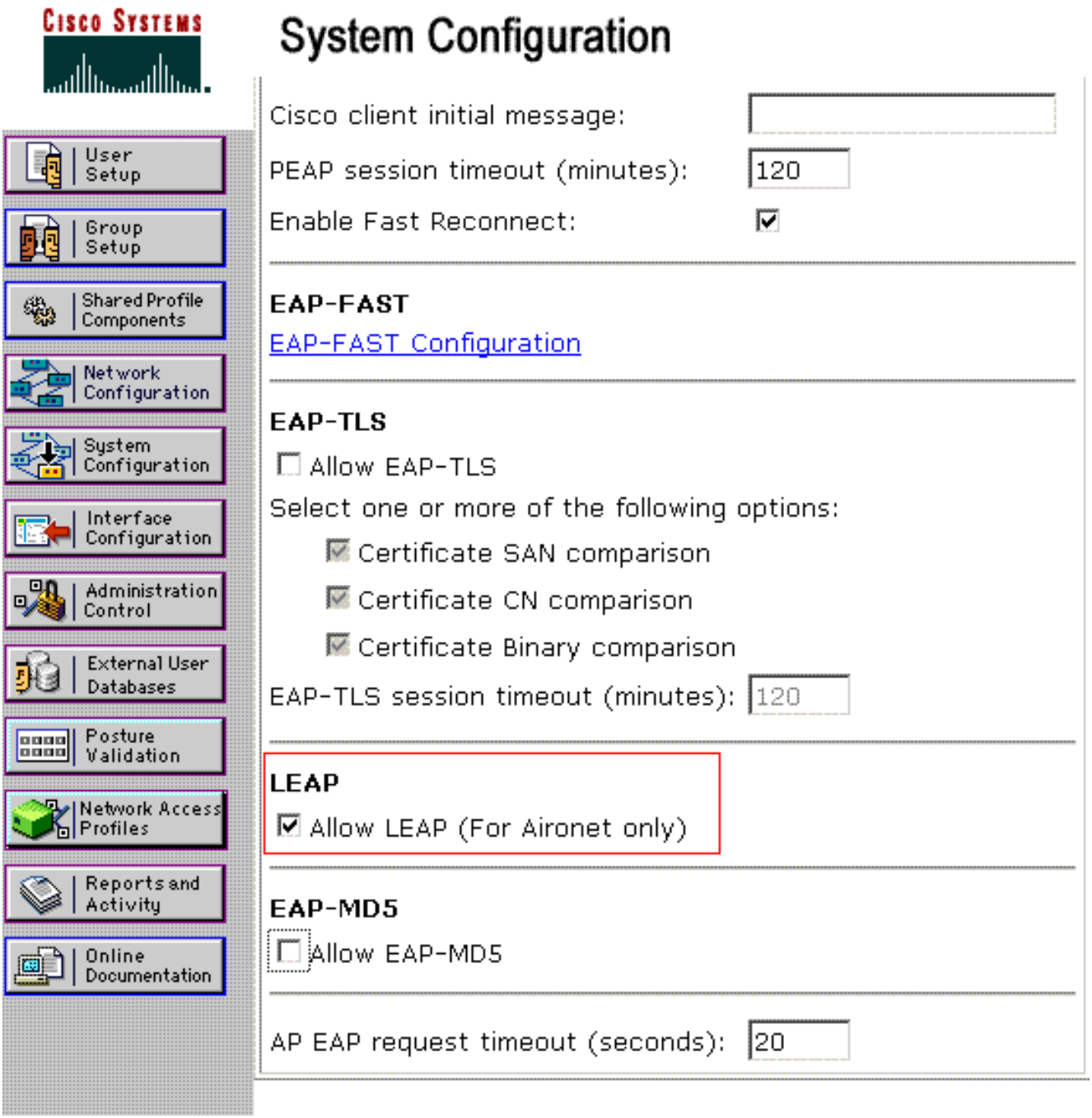
4. Role para baixo a página Edit e encontre o campo **IETF RADIUS Attributes**.
5. No campo IETF RADIUS Attributes, marque as caixas de seleção junto aos três atributos de túnel e configure os valores de atributo como mostrado
   aqui:



Nota: Na configuração inicial do servidor ACS, os atributos do IETF RADIUS não puderam ser exibidos.Escolha **Interface Configuration > RADIUS (IETF)** para habilitar os atributos do IETF na janela de configuração do usuário.Depois marque as caixas de seleção dos atributos **64, 65 e 81** nas colunas User e
Group.



Nota: Para que o servidor RADIUS atribua dinamicamente o cliente a uma VLAN específica, **a ID de VLAN configurada no campo IETF 81 (Tunnel-Private-Group-ID) do servidor RADIUS deve existir no WLC.**Marque a caixa de seleção do atributo **Per User TACACS+/RADIUS** em Interface Configuration > Advanced Options para habilitar o servidor RADIUS para as configurações por usuário.Da mesma forma, como se usa o LEAP como o protocolo de autenticação, assegure-se de que o LEAP esteja habilitado na janela Configuration do servidor RADIUS, como mostrado
aqui:



Configurar o ACS com atributos de Cisco Airespace VSA para a atribuição da VLAN dinâmica

Nas mais recentes versões do ACS, você também pode configurar o atributo Cisco Airespace [VSA (Vendor-Specific)] para atribuir um usuário autenticado com sucesso com um nome da interface da VLAN (não a ID da VLAN) como a configuração do usuário no ACS. Para isso, execute as etapas nesta seção.

Nota: Esta seção usa a versão ACS 4.1 para configurar o atributo Cisco Airespace VSA.

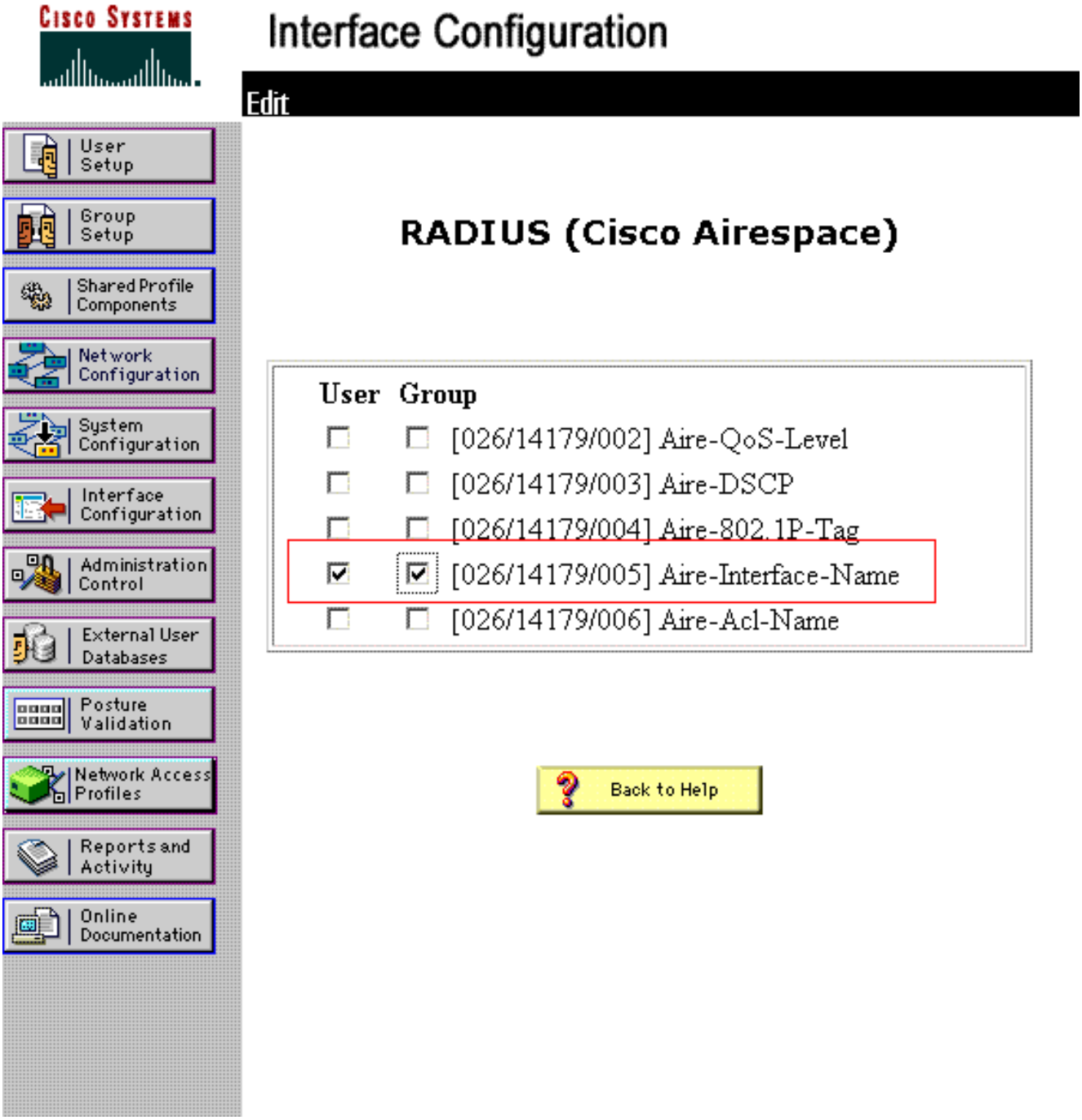
Configurar o Grupo do ACS com a opção do atributo Cisco Airespace VSA

Conclua estes passos:

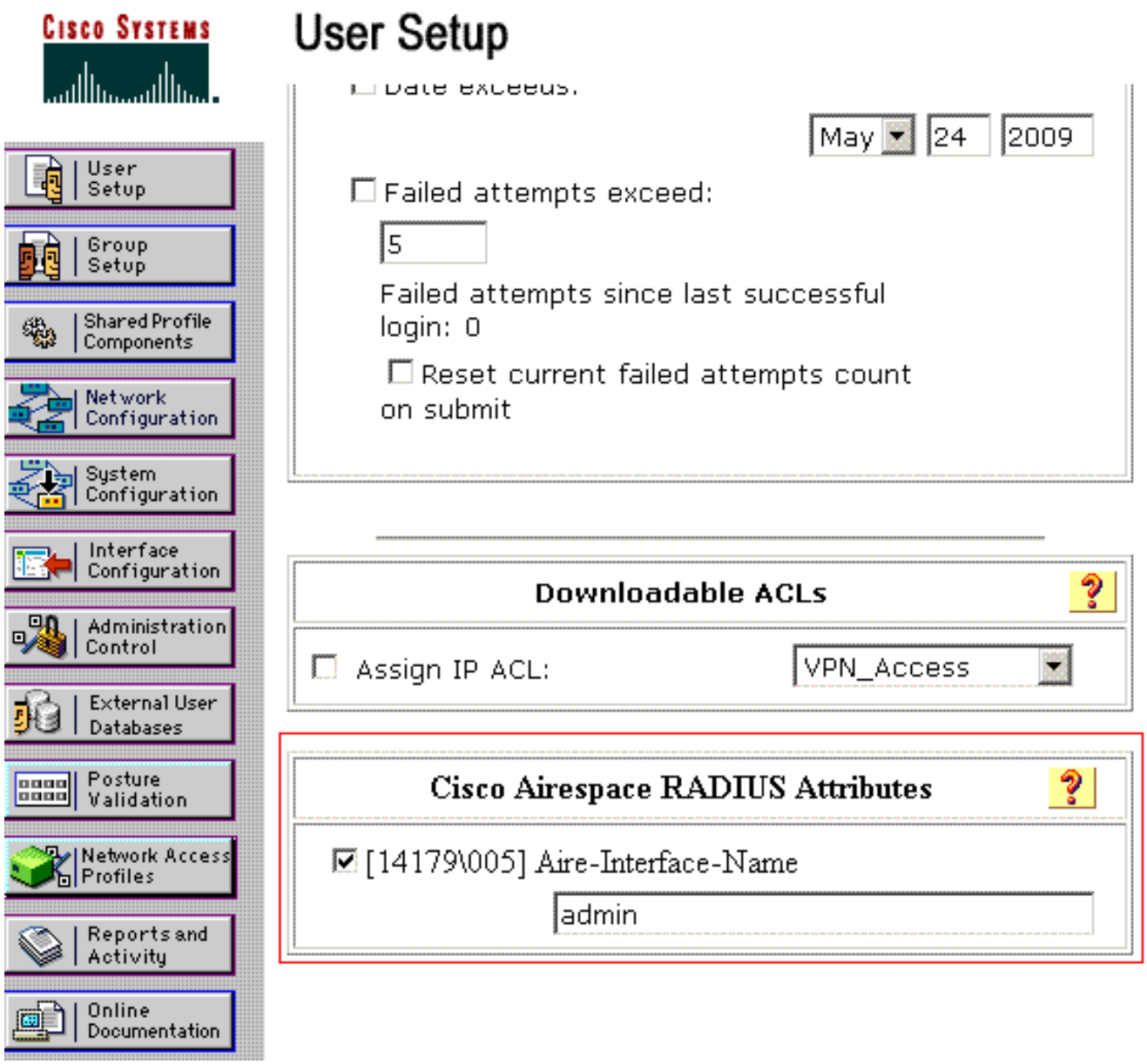
1. Na interface gráfica do usuário do ACS 4.1, clique em **Interface Configuration** na barra de

navegação. Depois selecione **RADIUS (Cisco Airespace)** na página Interface Configuration para configurar a opção do atributo Cisco Airespace.

2. Na janela RADIUS (Cisco Airespace), marque a caixa de seleção User (e a caixa de seleção Group, se necessário) junto a **Aire-Interface-Name** para exibi-lo na página User Edit. Depois, clique em
Submit.



3. Vá para a página User Edit do usuário1.
4. Na página User Edit, role para baixo para a seção **Cisco Airespace RADIUS Attributes**. Marque a caixa de seleção junto ao atributo **Aire-Interface-Name** e especifique o nome da interface dinâmica a ser atribuída quando da autenticação de usuário bem-sucedida.Este exemplo atribui o usuário a **admin**
VLAN.



5. Clique em Submit.

Configurar o Switch para várias VLANs

Para permitir várias VLANs no switch, você deve emitir estes comandos para configurar a porta do switch conectada ao controlador:

1. Switch(config-if)#switchport **mode trunk**
2. Switch(config-if)#switchport **trunk encapsulation dot1q**

Nota: Por padrão, a maioria dos switches permitem todas as VLAN criadas nesse switch através da porta de tronco.

Estes comandos variam de um switch do Catalyst Operating System (CatOS) para outro.

Se uma rede com fio é conectada ao switch, então esta mesma configuração pode ser aplicada à porta do switch conectada à rede com fio. Isto permite a comunicação entre as mesmas VLANs nas redes com e sem fio.

Nota: Este documento não discute a comunicação entre VLANs. Isto vai além do escopo deste documento. Você deve compreender que para o roteamento entre VLANs, é necessário um

switch de camada 3 ou um roteador externo com configurações apropriadas de VLAN e de entroncamento. Há diversos documentos que explicam a configuração do roteamento entre VLANs.

Configuração de WLC

Esta configuração exige estas etapas:

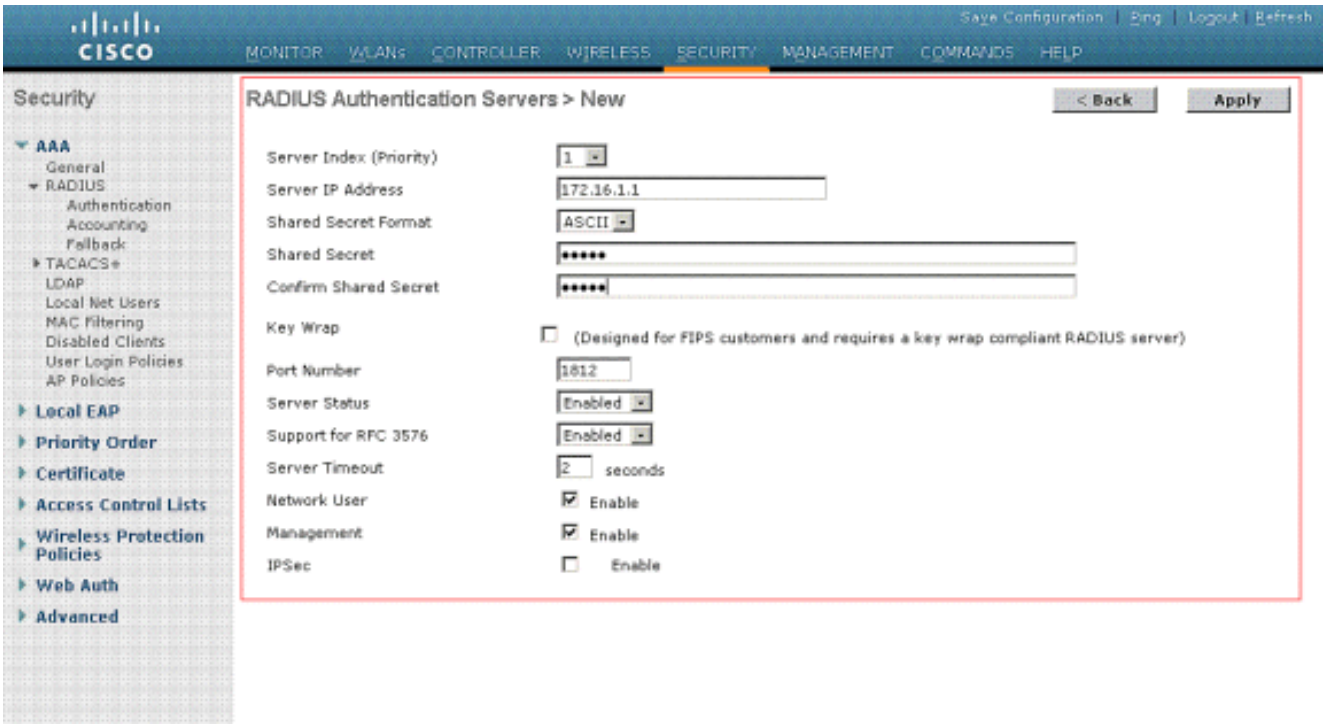
- Configurar o WLC com os detalhes do Servidor de Autenticação
- Configurar as interfaces dinâmicas (VLANs)
- Configurar as WLANs (SSID)

Configurar o WLC com os detalhes do Servidor de Autenticação

Énecessário configurar o WLC para que ele possa comunicar-se com o servidor RADIUS para autenticar os clientes, e também para todas as outras transações.

Conclua estes passos:

1. Na interface gráfica do usuário, clique em **Security**.
2. Digite o endereço IP do servidor RADIUS e a chave secreta compartilhada usados entre o servidor RADIUS e o WLC.Esta chave secreta compartilhada deve ser a mesma que foi configurada no servidor RADIUS em Network Configuration > AAA Clients > Add Entry. Este é um exemplo de janela do
WLC:

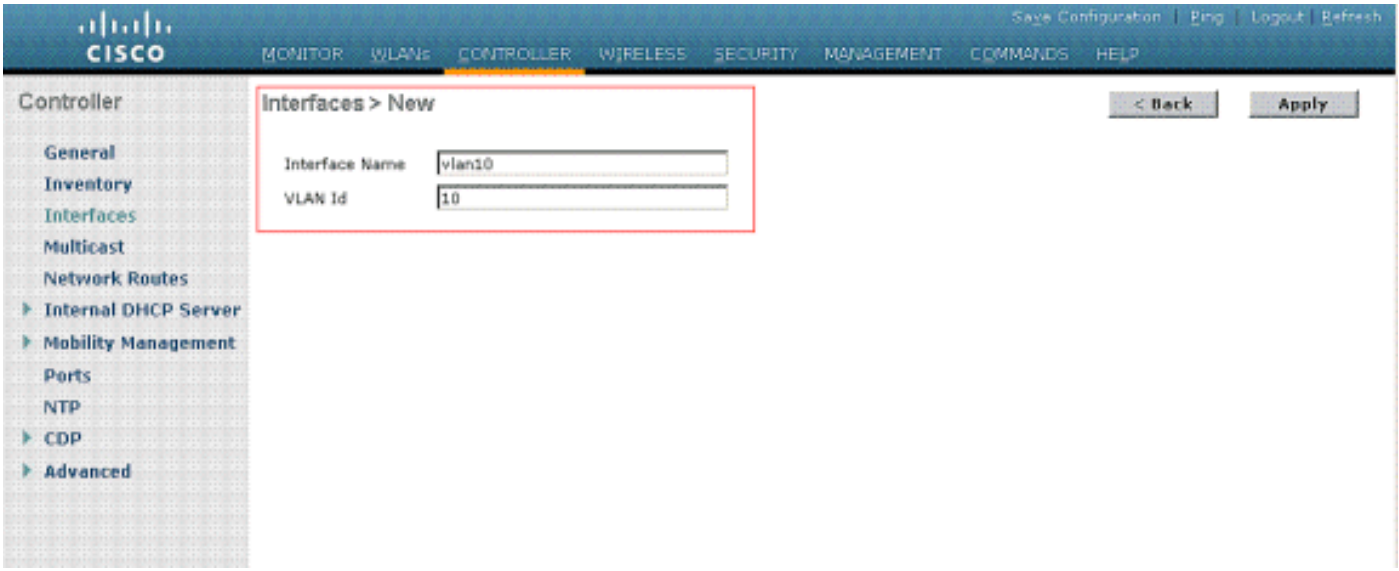


Configurar as interfaces dinâmicas (VLANs)

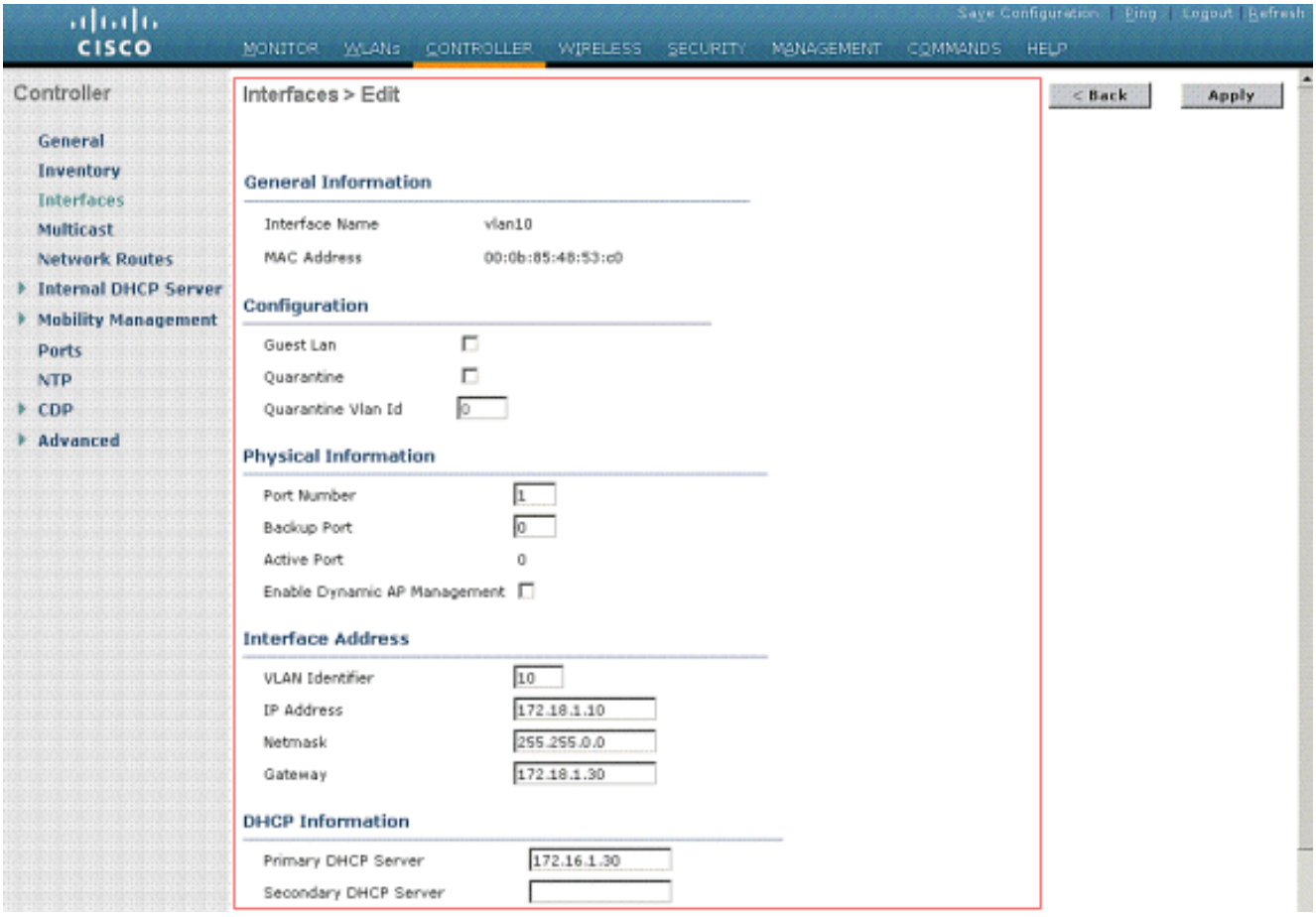
Este procedimento explica como configurar interfaces dinâmicas no WLC. Como explicado antes neste documento, a ID de VLAN especificada sob o atributo Tunnel-Private-Group ID do servidor RADIUS deve igualmente existir no WLC.

No exemplo, o usuário1 é especificado com **Tunnel-Private-Group ID of 10 (VLAN =10)** no servidor RADIUS. Veja a seção IETF RADIUS Attributes na janela User Setup do usuário1.

Você pode ver a mesma interface dinâmica (VLAN=10) configurada no WLC neste exemplo. A interface dinâmica é configurada na interface gráfica do controlador, na janela Controller > Interfaces.



1. Clique em **Apply** nesta janela.Isto abre a janela Edit desta interface dinâmica (VLAN 10 aqui).
2. Digite o endereço IP e o gateway padrão desta interface dinâmica.



Nota: Como este documento usa um servidor DHCP interno no controlador, o campo primary DHCP server desta janela indica a própria interface de gerenciamento do WLC. Você

também pode usar um servidor de DHCP externo, um roteador, ou o próprio servidor RADIUS como um servidor DHCP para os clientes wireless. Nesses casos, o campo primary DHCP server indica o endereço IP desse dispositivo usado como o servidor DHCP. Para mais informações, consulte a documentação do servidor DHCP.

3. Clique em Apply.Agora você está configurado com uma interface dinâmica em seu WLC. Similarmente, você pode configurar diversas interfaces dinâmicas em seu WLC. Mas lembre-se de que a mesma ID de VLAN também deve existir no servidor RADIUS para que essa VLAN específica seja atribuída ao cliente.

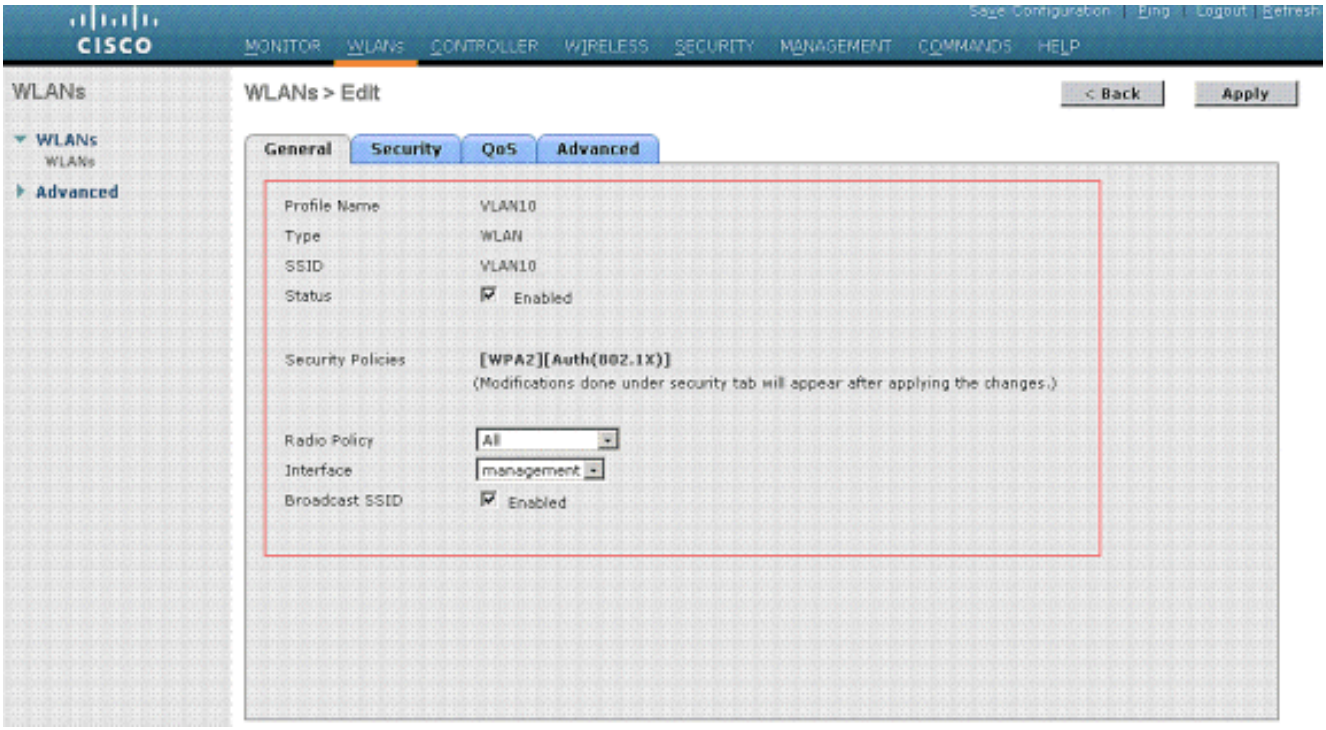
Configurar as WLANs (SSID)

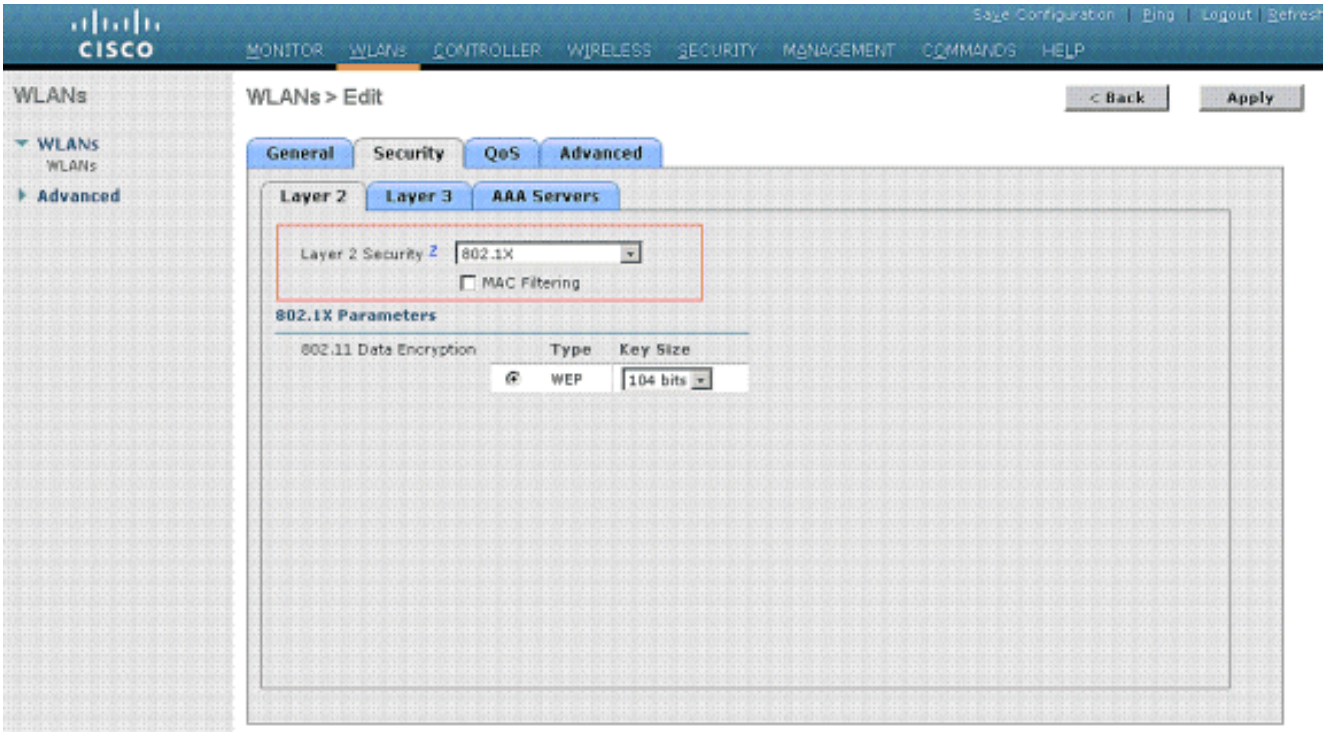
Este procedimento explica como configurar as WLANs no WLC.

Conclua estes passos:

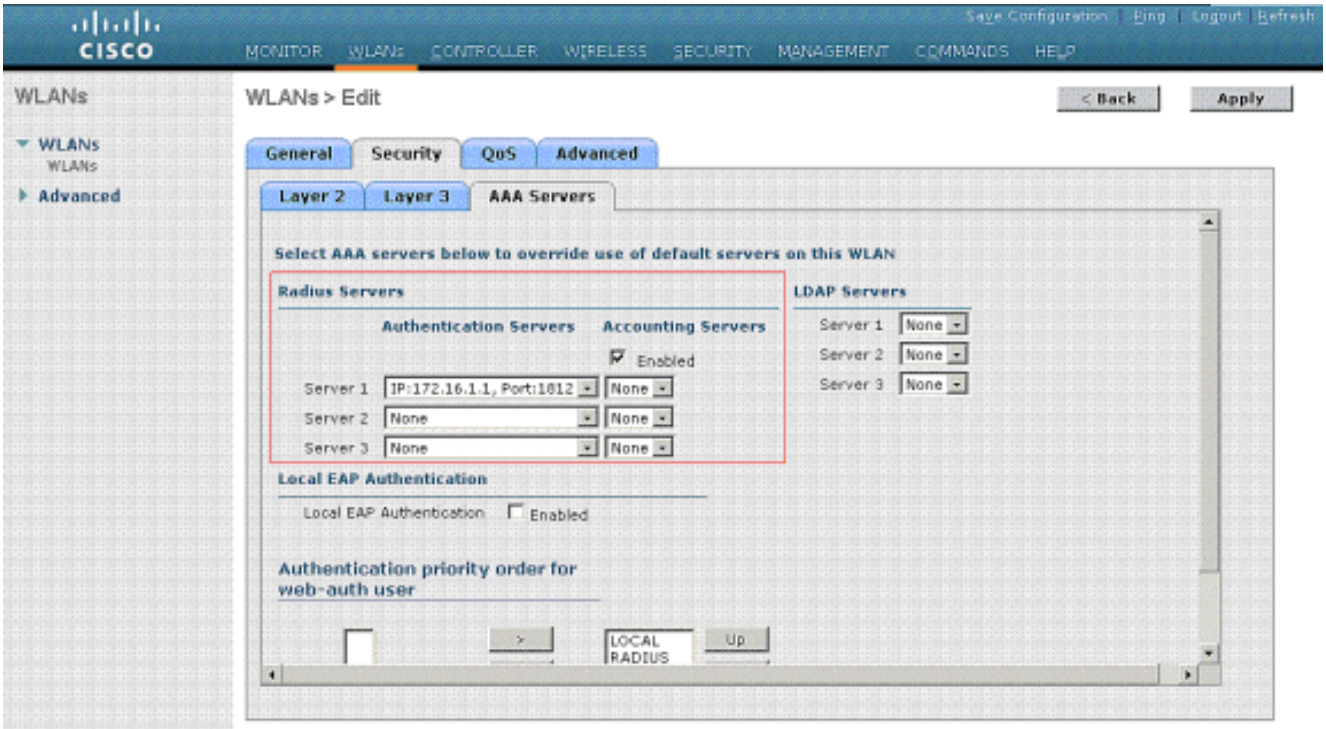
1. Na interface gráfica do controlador, escolha **WLANs > New** para criar uma nova WLAN.A janela New WLANs é exibida.
2. Digite a ID da WLAN e a SSID da WLAN.Você pode digitarqualquer nome como SSID da WLAN. Este exemplo usa a VLAN10 como a SSID da WLAN.

3. Clique em **Apply** para abrir a janela Edit da SSID10 da WLAN.





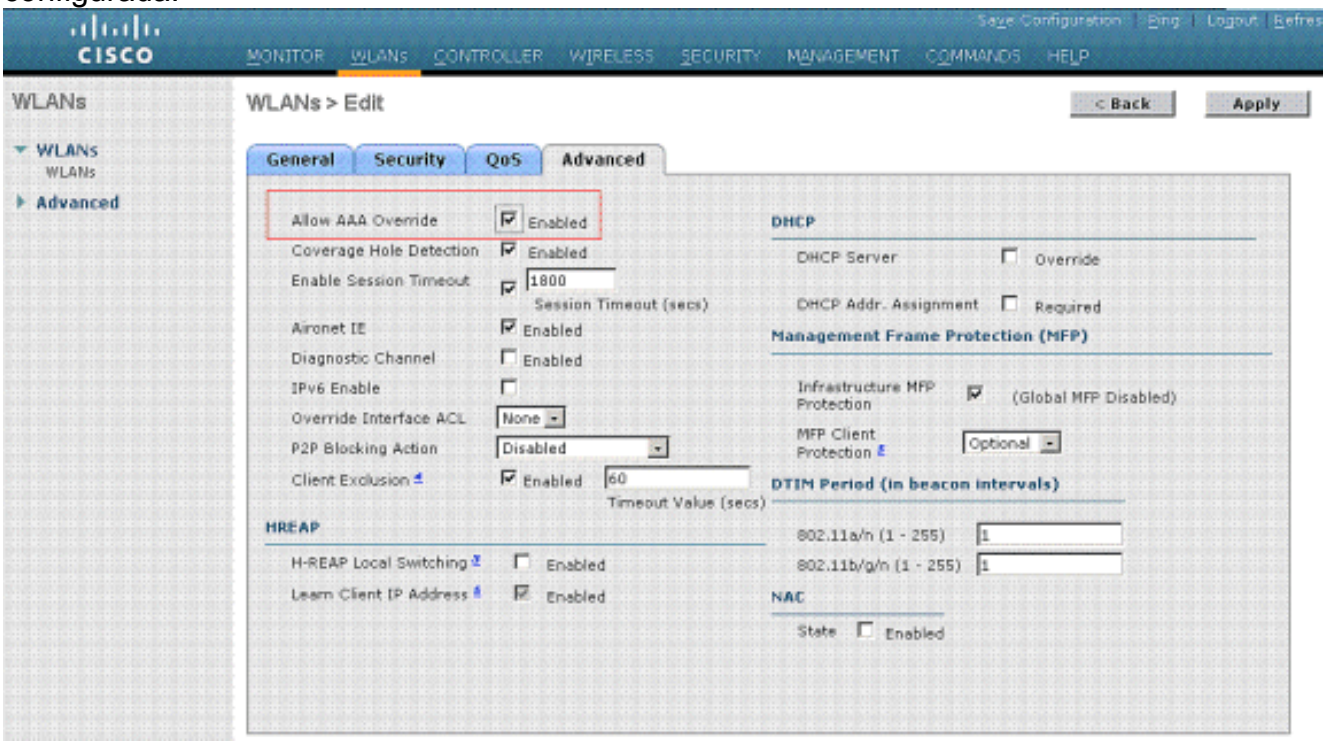
Normalmente, em um controlador de LAN Wireless, cada WLAN é mapeada para uma VLAN específica (SSID) de modo que determinado usuário que pertença a essa WLAN esteja colocado na VLAN específica mapeada. Esse mapeamento normalmente ocorre no campo Interface Name da janela WLAN
SSID.



No exemplo fornecido, é função do servidor RADIUS atribuir um cliente wireless a uma VLAN específica para uma autenticação bem-sucedida. As WLANs não precisam estar mapeadas para uma interface dinâmica específica no WLC. Ou, mesmo que o mapeamento da WLAN para a interface dinâmica seja feito no WLC, o servidor RADIUS cancela este mapeamento e atribui o usuário que vem por essa WLAN para a VLAN especificada sob o campo de usuário **Tunnel-Group-Private-ID** no servidor RADIUS.

4. Marque a caixa de seleção **Allow AAA Override** para cancelar as configurações de WLC pelo servidor RADIUS.

5. Habilite Allow AAA Override no controlador para cada WLAN (SSID) configurada.



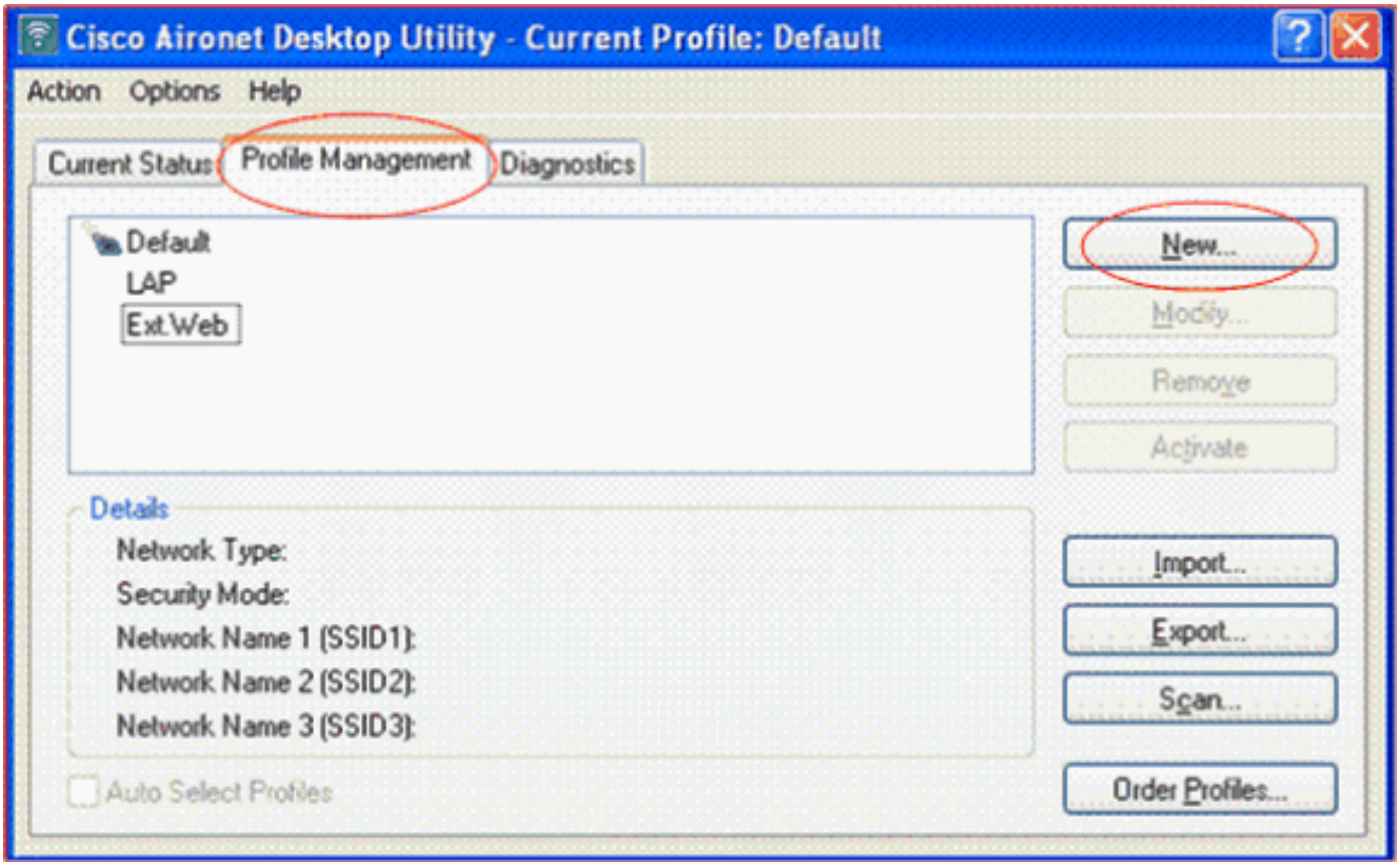
Com AAA Override habilitado, se um cliente tem o AAA e os parâmetros de autenticação do controlador WLAN em conflito, a autenticação do cliente é executada pelo servidor AAA (RADIUS). Como parte desta autenticação, o sistema operacional move os clientes para uma VLAN retornada pelo servidor AAA. Isto é predefinido na configuração da interface do controlador.Por exemplo, se a WLAN corporativa usa principalmente uma interface de gerenciamento atribuída à VLAN2, e AAA Override retorna um redirecionamento à VLAN 100, o sistema operacional redireciona todas as transmissões do cliente para a VLAN 100 mesmo se for a porta física à qual a VLAN 100 está atribuída. Com AAA Override desabilitado, todas as autenticações do cliente usam as configurações do parâmetro de autenticação do controlador, e a autenticação só é executada pelo servidor AAA se o controlador WLAN não contiver nenhum parâmetro de autenticação específico do cliente.

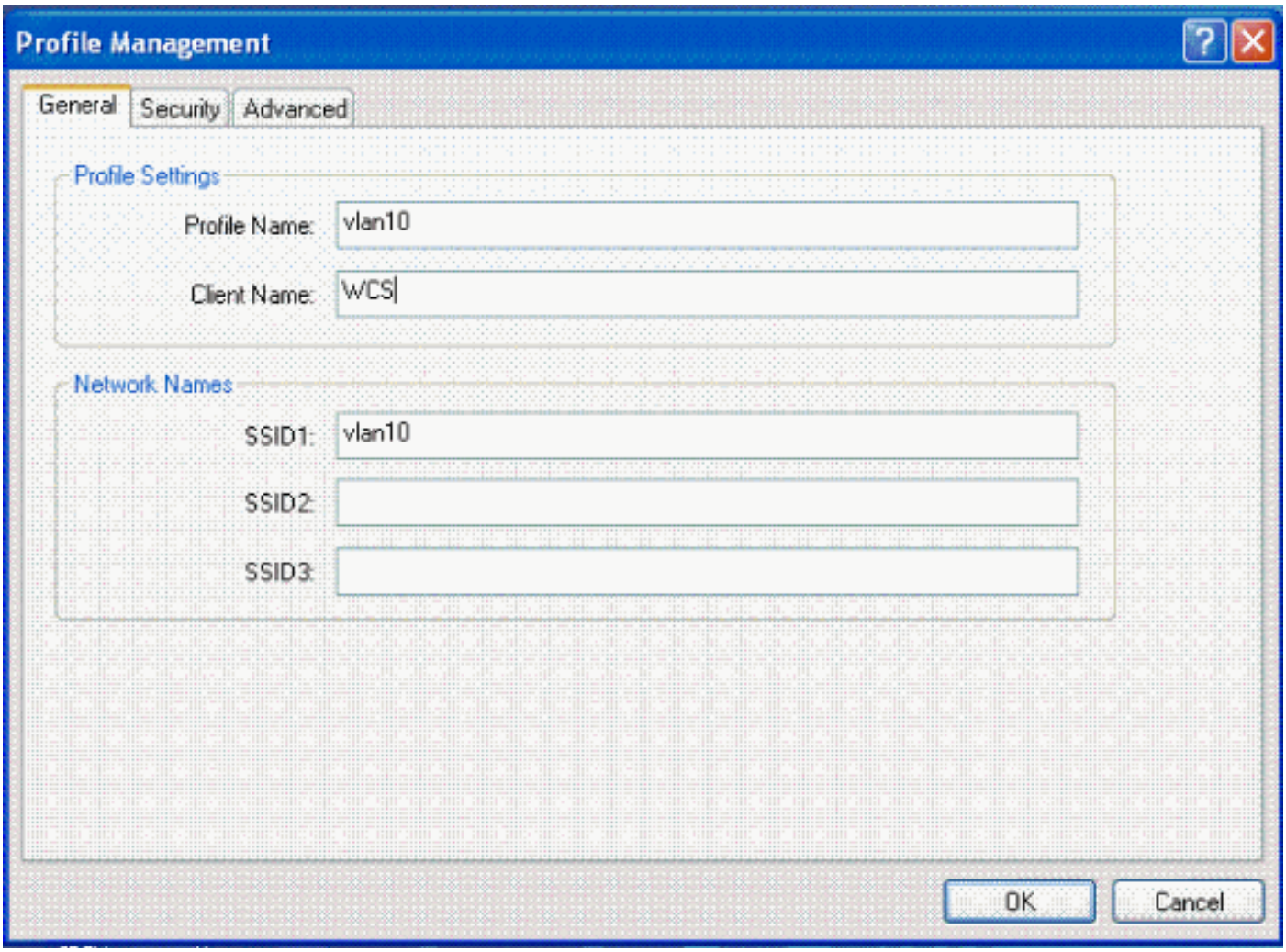
Configuração de utilitário do cliente Wireless

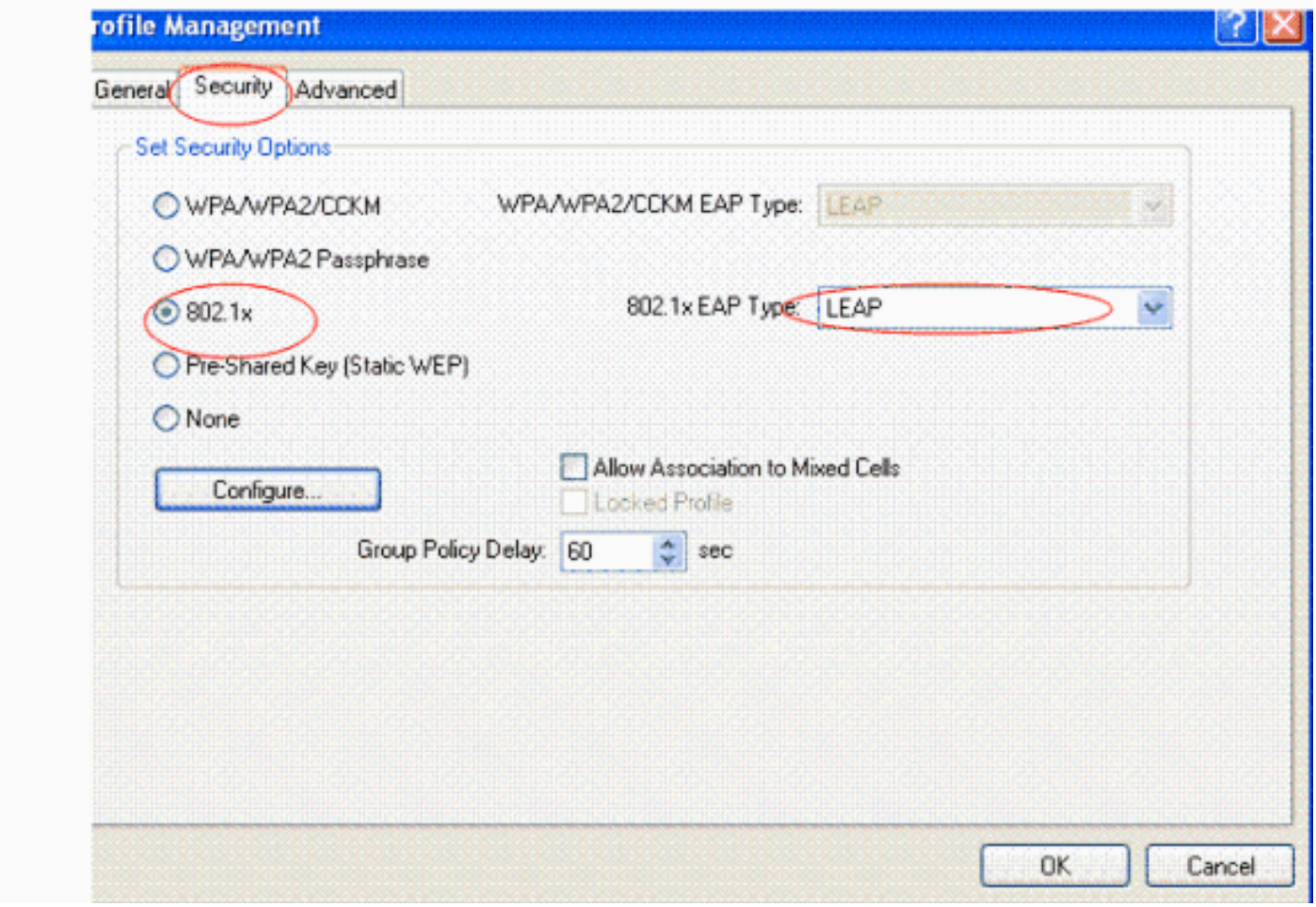
Este documento usa o ADU como o utilitário de cliente para a configuração dos perfis de usuário. Esta configuração também usa LEAP como o protocolo de autenticação. Configure o ADU segundo o exemplo nesta seção.

Na barra de menus do ADU, escolha **Profile Management > New** para criar um novo perfil.

O cliente do exemplo é configurado para ser parte da SSID VLAN10. Estes diagramas mostram como configurar um perfil de usuário em um cliente:


Cisco Aironet Desktop Utility - Current Profile: Default
Action Options Help
Current Status
Profile Management
Diagnostics
Default
LAP
Ext.Web
New...
Modify...
Remove
Activate
Details
Network Type:
Security Mode:
Network Name 1 (SSID1):
Network Name 2 (SSID2):
Network Name 3 (SSID3):
Import...
Export...
Scan...
Auto Select Profiles
Order Profiles...


Profile Management
General
Security
Advanced
Profile Settings
Profile Name:
vlan10
Client Name:
WCS
Network Names
SSID1:
vlan10
SSID2:
SSID3:
OK
Cancel



Verificar

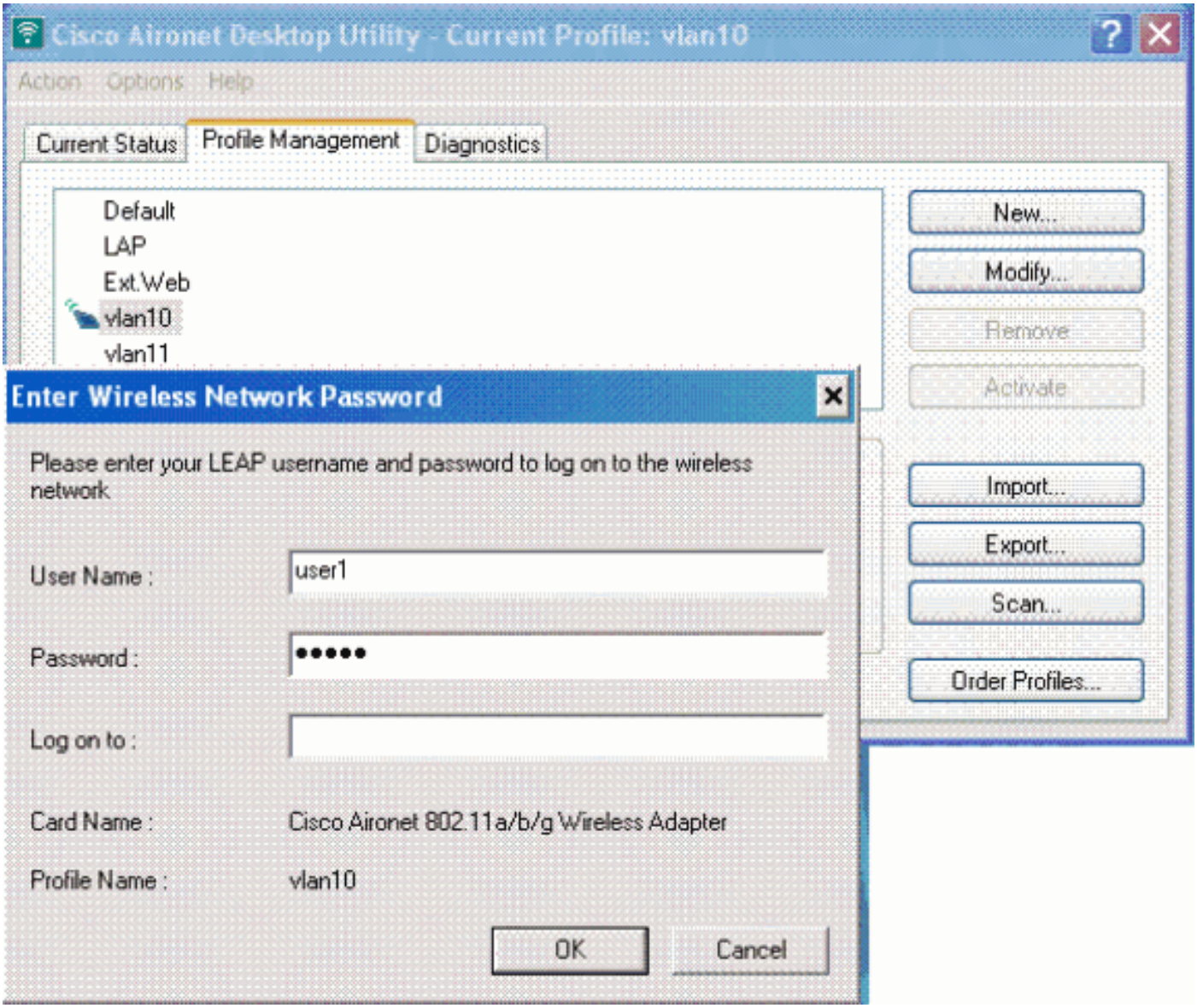
Ative o perfil de usuário que você configurou no ADU. Com base na configuração, você é solicitado a inserir um nome de usuário e senha. Você também pode instruir o ADU para usar o nome de usuário e a senha do Windows para a autenticação. Existem várias opções das quais o cliente pode receber autenticação. Você pode configurar estas opções sob a guia Security > Configure do perfil de usuário que você criou.

No exemplo anterior, observe que o usuário1 está atribuído à VLAN10 como especificado no servidor RADIUS.

Este exemplo usa este nome de usuário e senha do lado do cliente para receber a autenticação e para ser atribuído a uma VLAN pelo servidor RADIUS:

- User Name = user1
- Password = user1

Este exemplo mostra como a SSID VLAN10 é solicitada a informar o nome e senha de usuário. O nome de usuário e a senha são digitados neste exemplo:



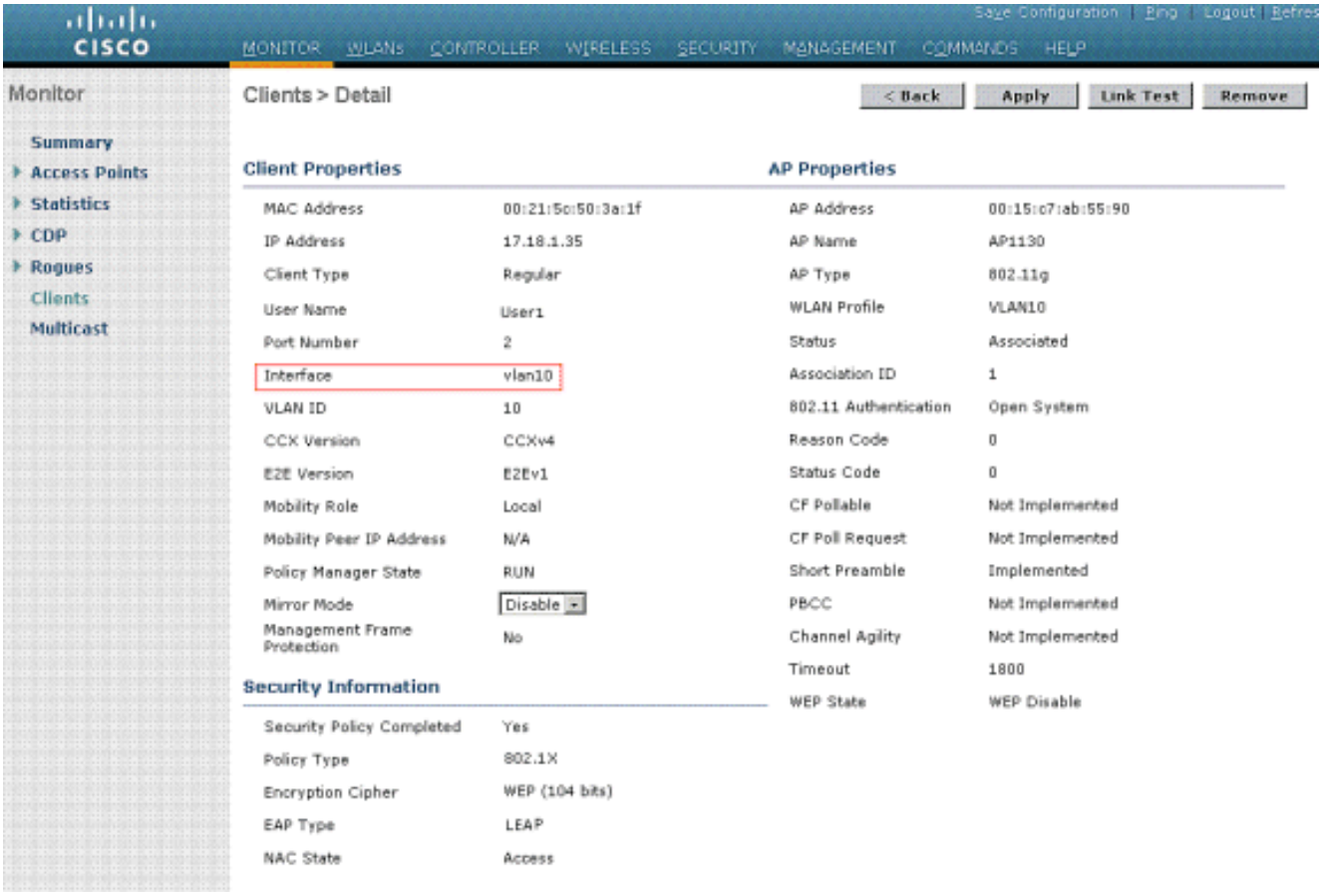
Se a autenticação e a validação correspondente forem bem-sucedidas, você recebe uma mensagem de status que informa isso.

Depois você deve verificar se seu cliente está atribuído à VLAN apropriada conforme os atributos RADIUS enviados. Conclua estas etapas para fazer isso:

1. Na interface gráfica do usuário do controlador, escolha **Wireless > AP**.
2. Clique em **Clients**, exibido no canto esquerdo da janela Access Points (APs).As estatísticas do cliente são
   exibidas.

3. Clique em **Details** para identificar e concluir os detalhes do cliente, como endereço IP, a VLAN à qual está atribuído etc.Este exemplo mostra estes detalhes do cliente,

usuário1:



Nesta janela você pode observar que este cliente está atribuído à VLAN10 conforme os atributos RADIUS configurados no servidor RADIUS.**Nota:** Se a atribuição da VLAN dinâmica for baseada na configuração do **atributo Cisco Airespace VSA**, o nome da interface será exibido como admin conforme este exemplo na página de detalhes do cliente.

Use esta seção para confirmar se a sua configuração funciona corretamente.

- **debug aaa events enable** — Este comando pode ser usado para garantir a transferência bem-sucedida dos atributos RADIUS ao cliente através do controlador. Esta parte da saída do debug garante uma transmissão bem-sucedida dos atributos RADIUS:

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:
attribute 64, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:
attribute 65, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:
attribute 81, vendorId 0, valueLen 3
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
attribute 79, vendorId 0, valueLen 32
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
4a 27 65 69 6d e4 05 f5
........J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c
........44 a9 da 6c 36 94 0a f3  <D..l6...
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]:
attribute 1, vendorId 9, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]:
attribute 25, vendorId 0, valueLen 28
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
attribute 80, vendorId 0, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Type 16777229
should be 13 for STA 00:40:96:ac:e6:57
```

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222
should be 6 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57
setting dot1x reauth timeout = 1800
```

- Estes comandos também podem ser úteis:**debug dot1x aaa enabledebug aaa packets enable**

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Nota: A atribuição do VLAN dinâmico não trabalha para a autenticação da Web de um WLC.

Informações Relacionadas

- Autenticação de EAP com servidor RADIUS
- Cisco LEAP
- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- Suporte Técnico e Documentação - Cisco Systems