Tipos do autenticação wireless em ISR fixo com o exemplo da configuração de SDM

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Informações de Apoio
Configurar
Diagrama de Rede
Configurar o roteador para o acesso SDM
Lance o aplicativo wireless SDM no roteador
Configurar a autenticação aberta com criptografia de WEP
Configurar o servidor DHCP interno para clientes Wireless deste VLAN
Configurar aberto com autenticação de MAC
Configurar a autenticação 802.1x/EAP
Configurar a autenticação compartilhada
Configurar a autenticação WPA
Configurar a autenticação WPA-PSK
Configuração de cliente Wireless
Configurar o cliente Wireless para a autenticação aberta com criptografia de WEP
Configurar o cliente Wireless para aberto com autenticação de MAC
Configurar o cliente Wireless para a autenticação 802.1x/EAP
Configurar o cliente Wireless para a autenticação compartilhada
Configurar o cliente Wireless para a autenticação WPA
Configurar o cliente Wireless para a autenticação WPA-PSK
Troubleshooting
Comandos para Troubleshooting
Informações Relacionadas

Introdução

Este documento fornece os exemplos de configuração que explicam como configurar vários tipos do autenticação da camada 2 em um roteador integrado Cisco Wireless da configuração fixa para a conectividade Wireless com Security Device Manager (SDM).

Pré-requisitos

Requisitos

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

- Conhecimento de como configurar os parâmetros básicos do roteador dos Serviços integrados de Cisco (ISR) com SDM
- Conhecimento de como configurar o adaptador de cliente Wireless 802.11a/b/g com o utilitário de Desktop de Aironet (ADU)

Componentes Utilizados

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

- Cisco 877W ISR que executa o Software Release 12.3(8)YI1 de Cisco IOS®
- Versão 2.4.1 de Cisco SDM instalada no ISR
- Portátil com versão 3.6 do utilitário de Desktop de Aironet
- adaptador cliente do a/b/g do 802.11 que executa a versão de firmware 3.6

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.

Informações de Apoio

Cisco SDM é uma ferramenta de Gerenciamento de dispositivos intuitiva, com base na Web para roteadores baseado em software do Cisco IOS. Cisco SDM simplifica o roteador e a configuração de segurança através dos assistentes espertos, que ajudam clientes rapidamente e os distribuem facilmente, configura, e monitora o Roteadores do ® do Cisco Systems sem exigir o conhecimento do comando line interface(cli) do Cisco IOS Software.

O SDM pode ser transferido gratuitamente do centro de software no cisco.com.

O SDM pode ser instalado independentemente enquanto uma cópia separada no cada roteadores individuais, ou podem igualmente ser instalados em um PC. Cisco SDM instalado em um PC permite que você use o SDM para controlar o outro Roteadores que executa imagens IOS apropriadas na rede. Contudo, o SDM em um PC não apoia a restauração da configuração de roteador para fabricar o padrão.

Este documento usa o SDM instalado no roteador Wireless para configurar o roteador para a autenticação wireless.

Cisco SDM comunica-se com o Roteadores para duas finalidades:

- Alcance os arquivos de aplicativo de Cisco SDM para a transferência ao PC

- Leia e escreva a configuração de roteador e o estado

Cisco SDM usa o HTTP para transferir os arquivos de aplicativo (sdm.tar, home.tar) ao PC. Uma combinação de HTTP e de telnet/SSH é usada para ler e escrever a configuração de roteador.

Refira Roteador Cisco e Security Device Manager Q&A para as últimas informações sobre do Roteadores e das IOS Software releases que apoiam o SDM.

Consulte para configurar seu roteador para apoiar o SDM para obter mais informações sobre de como usar Cisco SDM em um roteador.

Consulte para instalar os arquivos SDM para que as instruções instalem e transfiram arquivos SDM no roteador ou no PC.

Configurar

O documento explica como configurar estes tipos do autenticação com o SDM:

- Autenticação aberta com criptografia de WEP
- Abra com autenticação de MAC
- Autenticação compartilhada
- autenticação do protocolo de autenticação 802.1x/Extensible (EAP)
- Wi-Fi Protected Access (WPA) - Pre autenticação da chave compartilhada (PSK)
- Autenticação WPA

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

Note: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Esta instalação usa o servidor Radius local no Sem fio ISR para autenticar os clientes Wireless que usam a autenticação do 802.1x.

Configurar o roteador para o acesso SDM

Termine estas etapas a fim permitir que o roteador seja alcançado com o SDM:

1. Configurar o roteador para o HTTP/https que o acesso que usa o procedimento explicado dentro configura seu roteador para apoiar o SDM.
2. Atribua um endereço IP de Um ou Mais Servidores Cisco ICM NT ao roteador com estas etapas:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastEthernet 0
Router(config-if)#ip address10.77.244.197 255.255.255.224

        % IP addresses cannot be configured on L2 links.
```

No 871W Router, você pôde encontrar tal Mensagem de Erro. Este Mensagem de Erro mostra que o ethernet0 rápido é um link da camada 2 em que você não pode configurar nenhum endereço IP de Um ou Mais Servidores Cisco ICM NT.

3. A fim superar esta edição, crie uma relação da camada 3 (VLAN) e atribua um endereço IP de Um ou Mais Servidores Cisco ICM NT no mesmos com estas etapas:

```
Router(config)#interface Vlan1
Router(config-if)#ip address 10.77.244.197 255.255.255.224
```

4. Permita este VLAN na relação rápida do ethernet0 da camada 2 com estas etapas. Este documento configura a interface rápida de Ethernet como uma interface de tronco para permitir o VLAN1. Você pode igualmente configurar-lo como uma interface de acesso e permitir o VLAN1 na relação por sua instalação de rede.

```
Router(config)#interface fastEthernet 0
Router(config-if)#switchport trunk encapsulation dot1q
Router(config-if)#switchport trunk allowed vlan add vlan1
!--- This command allows VLAN1 through the fast ethernet interface. !--- In order to allow
all VLANs through this interface, issue the !--- switchport trunk allowed vlan add all
command on this interface.
```

Note: Este exemplo supõe que o roteador básico e as configurações sem fio estão executados já no roteador. Consequentemente, a próxima etapa é diretamente lançar o aplicativo wireless no roteador configurar parâmetros de autenticação.

Lance o aplicativo wireless SDM no roteador

Termine estas etapas a fim lançar o aplicativo wireless:

1. Comece o SDM abrindo um navegador e incorporando o endereço IP de Um ou Mais Servidores Cisco ICM NT de seu roteador.Você é alertado aceitar ou diminuir um indicador da alerta de segurança do navegador da Web que olhe como este:
2. Clique **sim** para continuar.
3. No indicador que aparece, incorpore o nome de usuário e senha do privilégio level_15 a fim alcançar o roteador.Este exemplo usa o **admin** como o nome de usuário e senha:
4. Clique em OK para continuar. Incorpore a mesma informação onde quer que se exige.
5. Clique **sim** e **ESTÁ BEM** como apropriado nas páginas resultantes a fim lançar o aplicativo SDM.Enquanto o aplicativo SDM abre, você está alertado por um indicador da alerta de segurança aceitar um Security Certificate assinado.
6. Clique **sim** para aceitar o certificado assinado.O roteador Cisco resultante e a página principal SDM olham como este:
7. Nesta página, o clique **configura no** superior a fim lançar o roteador configura o indicador do modo.
8. No indicador do modo configurar, selecione **relações e conexões da** coluna das tarefas que aparece no lado esquerdo desta página.
9. No indicador das relações e das conexões, clique a aba da **conexão da criação**.Isto alista todas as relações disponíveis para ser configurado no roteador.
10. A fim lançar o aplicativo wireless, escolha o **Sem fio da** lista de relações. Então, **aplicativo do Sem fio do lançamento do** clique.Este tiro de tela explica as etapas 8, 9 e 10:Isto lança o aplicativo wireless SDM em uma janela separada onde os vários tipos do autenticação

possam ser configurados.O Home Page wireless do aplicativo SDM olha como este:Observe que o status de software **está desabilitado** e o status de hardware da relação (wireless) de rádio está **para baixo** porque nenhum SSID é configurado na relação. Em seguida, você configura os SSID e os tipos do autenticação nesta interface de rádio de modo que os clientes Wireless possam se comunicar através desta relação.

Configurar a autenticação aberta com criptografia de WEP

A autenticação aberta é um algoritmo da autenticação nula. O Access Point (AP) concederá todo o pedido para a autenticação. A autenticação aberta permite todo o acesso de rede do dispositivo. Se o no encryption é permitido na rede, todo o dispositivo que conhecer o SSID do AP pode aceder à rede. Com a criptografia de WEP permitida em um AP, a chave de WEP própria torna-se meios do controle de acesso. Se um dispositivo não tem a chave de WEP correta, mesmo que a autenticação seja bem sucedida, o dispositivo será incapaz de transmitir dados com o AP. Também, não pode decifrar os dados enviados do AP.

Refira a autenticação aberta ao Access point para mais informação.

Este exemplo usa estes parâmetros de configuração para a autenticação aberta com criptografia de WEP:

- Nome SSID: **openwep**
- Identificação VLAN: **1**
- Endereço IP de Um ou Mais Servidores Cisco ICM NT VLAN: **10.1.1.1/16**
- Escala de endereço de DHCP para os clientes Wireless deste VLAN/SSID: **10.1.1.5/16 - 10.1.1.10/16**

Termine estas etapas a fim configurar a autenticação aberta com WEP:

1. No Home Page wireless do aplicativo, clique **Serviços sem fio > VLAN** a fim configurar um VLAN.
2. Selecione o **roteamento dos** serviços: Página VLAN.
3. Nos serviços: A página de roteamento vlan, cria o VLAN e atribui-o à interface de rádio.Esta é a janela de configuração do VLAN1 na interface de rádio. O VLAN1 é o VLAN nativo aqui:
4. No Home Page wireless do aplicativo, selecione a **segurança Wireless** > o **gerenciador de SSID** a fim configurar o SSID e o tipo do autenticação.
5. Na Segurança: A página do gerenciador de SSID, configura o SSID e atribui o SSID ao VLAN criado em step1 a fim permitir o SSID na interface de rádio.
6. Sob a seção dos ajustes da autenticação desta página, escolha a **autenticação aberta**.Está aqui a janela de configuração que explica estas etapas:
7. Clique em Apply.**Note**: A caixa suspensa que corresponde à caixa de verificação de autenticação aberta implica que a autenticação aberta pode ser configurada além com diversos tipos do autenticação adicionais, tais como o EAP ou a autenticação de MAC. Esta seção discute somente a autenticação aberta sem a ADIÇÃO (sem tipo do autenticação adicional).
8. Configurar a criptografia de WEP para este SSID/VLAN. No Home Page wireless, selecione a **segurança Wireless** > o **gerenciador de criptografia** a fim configurar as configurações de criptografia.Na Segurança: A página do gerenciador de criptografia, ajustou o modo de criptografia e as chaves para o **VLAN1**.Escolha a **criptografia de WEP: Imperativo** como o modo de criptografia.Ajuste a chave de criptografia para este VLAN.Esta seção usa estes

ajustes da chave de criptografia:Slot1 da chave de criptografia: usado como a chave transmissoraTamanho da chave de criptografia: bit 40Chave de criptografia no valor hexadecimal: 1234567890**Note**: O mesmo entalhe da chave de criptografia (1, neste caso) deve ser usado como a chave transmissora no cliente Wireless. Também, o cliente Wireless deve ser configurado com o mesmo valor chave (1234567890 neste caso) para que o cliente Wireless comunique-se com esta rede de WLAN.Esta janela de configuração explica estas etapas:Esta página da segurança Wireless representa a configuração completa:

Configurar o servidor DHCP interno para clientes Wireless deste VLAN

Termine estas etapas a fim configurar um servidor DHCP interno no roteador. Este é um opcional, embora recomendado, método atribuir o endereço IP de Um ou Mais Servidores Cisco ICM NT aos clientes Wireless.

1. No SDM configurar o indicador do modo, selecionam **tarefas adicionais** sob a coluna das tarefas que está no lado esquerdo do indicador.
2. **Nas tarefas adicionais** pagine, expanda a árvore **DHCP** e escolha **conjuntos de DHCP** segundo as indicações deste exemplo. Na coluna dos conjuntos de DHCP mostrada no lado direito desta página, o clique **adiciona** para criar um conjunto de DHCP novo.
3. Na página do conjunto de DHCP adicionar, especifique o nome do conjunto de DHCP, rede do conjunto de DHCP, máscara de sub-rede, começando o endereço IP de Um ou Mais Servidores Cisco ICM NT, terminando parâmetros do endereço IP de Um ou Mais Servidores Cisco ICM NT e do roteador padrão segundo as indicações deste exemplo:
4. Click **OK**.O servidor DHCP interno é configurado no roteador.

Configurar aberto com autenticação de MAC

Neste tipo de autenticação, estará permitido ao cliente Wireless alcançar a rede de WLAN somente se o MAC address do cliente está sob a lista de endereços permitidos MAC no Authentication Server. O AP retransmite o MAC address do dispositivo do cliente Wireless a um servidor de autenticação RADIUS em sua rede, e o server verifica o endereço contra uma lista de endereços permitidos MAC. A autenticação com base em MAC fornece um método de autenticação alternativo para os dispositivos do cliente que não têm a capacidade EAP.

Refira a autenticação do MAC address à rede para mais informação.

Note: O documento inteiro usa o servidor Radius local para a autenticação de MAC, o 802.1x/EAP, assim como a autenticação WPA.

Este exemplo usa estes parâmetros de configuração para aberto com autenticação de MAC:

- Nome SSID: **openmac**
- Identificação VLAN: **2**
- Endereço IP de Um ou Mais Servidores Cisco ICM NT VLAN: **10.2.1.1/16**
- Escala de endereço de DHCP para os clientes Wireless deste VLAN/SSID: **10.2.1.5/16 - 10.2.1.10/16**

Termine estas etapas a fim configurar aberto com autenticação de MAC:

1. No Home Page wireless do aplicativo, clique **Serviços sem fio > VLAN** a fim configurar um

VLAN.

2. Selecione o **roteamento dos** serviços: Página VLAN. Nos serviços: A página de roteamento vlan, cria o VLAN e atribui-o à interface de rádio.Está aqui a janela de configuração do **VLAN2 na** interface de rádio:
3. Configurar o servidor Radius local para a autenticação de MAC. Este servidor Radius local guardará o MAC address do cliente Wireless em seu base de dados e permitirá ou negará o cliente na rede de WLAN conforme o resultado da autenticação.No Home Page wireless, selecione a **segurança Wireless** > o **gerenciador do servidor** a fim configurar o servidor Radius local.Na página do gerenciador do servidor, configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT, o segredo compartilhado, e a autenticação e as portas de relatório do servidor Radius.Porque é um servidor Radius local, o endereço IP de Um ou Mais Servidores Cisco ICM NT especificado é o endereço desta relação wireless. A chave secreta compartilhada usada deve ser a mesma na configuração de cliente de AAA.Neste exemplo, o segredo compartilhado é **Cisco**.Clique em Apply.Enrole para baixo a página para procurar a seção de prioridades do server do padrão. Nesta seção, escolha este servidor Radius (**10.2.1.1**) como o server da prioridade padrão para a autenticação de MAC segundo as indicações deste exemplo:A fim configurar as credenciais do cliente de AAA e do usuário, selecione a **segurança Wireless > servidor Radius local do** Home Page wireless.Na página de servidor radius local, clique a **INSTALAÇÃO GERAL**.Na página de instalação GERAL, configurar o cliente de AAA e a chave secreta compartilhada como mostrado.Com uma configuração de servidor RADIUS local, o endereço IP de Um ou Mais Servidores Cisco ICM NT do server e o cliente de AAA serão o mesmo.Enrole para baixo a página de instalação GERAL para procurar a seção de configuração dos **usuários individuais**. Nos usuários individuais secione, configurar o MAC address do cliente Wireless como o nome de usuário e senha.Permita a caixa de verificação da **autenticação de MAC somente**, a seguir clique-a **aplicam-se**.A fim evitar às vezes o cliente da falha de autenticação, especifique o MAC address do cliente em um formato contínuo sem nenhuma separação segundo as indicações deste exemplo.
4. No Home Page wireless do aplicativo, selecione a **segurança Wireless** > o **gerenciador de SSID** a fim configurar o SSID e o tipo do autenticação.Na Segurança: A página do gerenciador de SSID, configura o SSID e atribui o SSID ao VLAN criado em step1 a fim permitir o SSID na interface de rádio.Sob a seção dos ajustes da autenticação desta página, escolha a **autenticação aberta** e da caixa suspensa correspondente, escolhem **com autenticação de MAC**.A fim configurar prioridades do server, escolha **personalizam** sob o MAC autenticam server e escolhem o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius local **10.2.1.1**.Este é um exemplo que explique esta etapa:
5. A fim configurar o servidor DHCP interno para clientes Wireless deste VLAN, termine as mesmas etapas explicadas no servidor DHCP interno configurar para clientes Wireless desta seção VLAN deste documento com estes parâmetros de configuração:Nome do conjunto de DHCP: VLAN2Rede do conjunto de DHCP: 10.2.0.0Máscara de sub-rede: 255.255.0.0Começando o IP: 10.2.1.5Terminando o IP: 10.2.1.10Roteador padrão: 10.2.1.1

Configurar a autenticação 802.1x/EAP

Este tipo do autenticação fornece o mais de nível elevado da Segurança para sua rede Wireless. Usando o EAP para interagir com um servidor Radius EAP-compatível, o AP ajuda um dispositivo do cliente Wireless e o servidor Radius a executar a autenticação mútua e derivar uma chave de WEP dinâmica do unicast. O servidor Radius envia a chave de WEP ao AP que a usa para todos

os sinais de dados do unicast a que envia, ou a recebe, do cliente.

Refira a autenticação de EAP à rede para mais informação.

Note: Há diversos métodos de autenticação de EAP disponíveis. Durante todo este documento, explica como configurar o protocolo lightweight extensible authentication (PULO) como a autenticação de EAP. O PULO usa o nome de usuário e senha como credenciais do usuário para a autenticação.

Note: A fim configurar a Autenticação Flexível de EAP através do Tunelamento seguro (EAP-FAST) como o tipo da autenticação de EAP, refira o manual de configuração EAP-FAST da versão 1.02 para o procedimento.

Este exemplo usa estes parâmetros de configuração para a autenticação de EAP:

- Nome SSID: **pulo**
- Identificação VLAN: **3**
- Endereço IP de Um ou Mais Servidores Cisco ICM NT VLAN: **10.3.1.1/16**
- Escala de endereço de DHCP para os clientes Wireless deste VLAN/SSID: **10.3.1.5/16 - 10.3.1.10/16**

Termine estas etapas a fim configurar a autenticação de EAP:

1. Repita etapas 1 e 2 Configure aberto com autenticação de MAC a fim criar e configurar o VLAN com estes parâmetros de configuração:Identificação VLAN: 3Endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de rádio: 10.3.1.1máscara de sub-rede: 255.255.0.0
2. Então, configurar o servidor Radius local para a authenticação do cliente. A fim executar isto, repita as etapas 3a a 3c Configure aberto com autenticação de MAC com estes parâmetros de configuração:Endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius: 10.3.1.1Segredo compartilhado: ciscoEstá aqui a tela de configuração que explica etapa 2 da autenticação de EAP:
3. Enrole para baixo a página para procurar a seção de prioridades do server do padrão. Nesta seção, escolha este servidor Radius (**10.3.1.1**) como o server da prioridade padrão para a autenticação de EAP segundo as indicações deste exemplo.
4. Repita as etapas 3e e 3f Configure abrem com autenticação de MAC.
5. Repita as etapas 3g e 3h Configure abrem com autenticação de MAC com estes parâmetros de configuração para a autenticação de EAP:Endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA: 10.3.1.1Segredo compartilhado: ciscoSob a seção dos usuários individuais, configurar o nome de usuário e senha como o **usuário1**.
6. No Home Page wireless do aplicativo, selecione a **segurança Wireless** > o **gerenciador de SSID** a fim configurar o SSID e o tipo do autenticação.Na Segurança: A página do gerenciador de SSID, configura o SSID e atribui o SSID ao VLAN criado em etapa 1 a fim permitir o SSID na interface de rádio.Sob a seção dos ajustes da autenticação desta página, escolha a **autenticação aberta** e da caixa suspensa correspondente, escolhem a **autenticação de EAP**. Também, selecione o tipo da **autenticação de EAP da rede**.A fim configurar as prioridades do server, escolha **personalizam** sob o EAP autenticam server e escolhem o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius local **10.3.1.1**.Está aqui um exemplo que explique estas etapas:
7. A fim configurar o servidor DHCP interno para clientes Wireless deste VLAN, termine as

mesmas etapas explicadas no servidor DHCP interno configurar para clientes Wireless desta seção VLAN deste documento com estes parâmetros de configuração:Nome do conjunto de DHCP: VLAN3Rede do conjunto de DHCP: 10.3.0.0Máscara de sub-rede: 255.255.0.0Começando o IP: 10.3.1.5Terminando o IP: 10.3.1.10Roteador padrão: 10.3.1.1

8. Configurar a cifra a ser usada para o Gerenciamento de chave dinâmica em cima da autenticação bem sucedida do cliente Wireless.No Home Page wireless, selecione a **segurança Wireless** > o **gerenciador de criptografia** a fim configurar as configurações de criptografia.Na tela da segurança Wireless > do gerenciador de criptografia na Segurança: A página do gerenciador de criptografia, incorpora **3** para o modo de criptografia e as chaves do grupo para o VLAN.Escolha a **cifra** como o modo de criptografia, e escolha um algoritmo de criptografia da cifra da caixa suspensa.Este exemplo usa o **TKIP** como o algoritmo da cifra:**Note**: Ao configurar a autenticação múltipla datilografa em um roteador Wireless com o SDM, às vezes ele não pôde ser possível para configurar dois tipos do autenticação diferentes ambos que usam o modo de criptografia da cifra no mesmo roteador. Nesses casos, a configuração de criptografia configurada com o SDM não pôde ser aplicada no roteador. A fim superar isto, configurar aqueles tipos do autenticação com o CLI.

Configurar a autenticação compartilhada

Cisco fornece a autenticação de chave compartilhada para seguir com o padrão do IEEE 802.11B.

Durante a autenticação de chave compartilhada, o AP envia uma corda de texto de desafio unencrypted a todo o dispositivo que tentar se comunicar com o AP. O dispositivo que pede a autenticação cifra o texto de desafio e envia-o de volta ao AP. Se o texto de desafio é cifrado corretamente, o AP permite que o dispositivo de pedido autentique. O desafio unencrypted e o desafio cifrado podem ser monitorados. Contudo, isto sae do AP aberto para atacar de um intruso que calcule a chave de WEP comparando as sequências de caracteres de texto unencrypted e cifradas.

Refira a autenticação de chave compartilhada ao Access point para mais informação.

Este exemplo usa estes parâmetros de configuração para a autenticação compartilhada:

- Nome SSID: **compartilhado**
- Identificação VLAN: **4**
- Endereço IP de Um ou Mais Servidores Cisco ICM NT VLAN: **10.4.1.1/16**
- Escala de endereço de DHCP para os clientes Wireless deste VLAN/SSID: **10.4.1.5/16 - 10.4.1.10/16**

Termine estas etapas a fim configurar a autenticação compartilhada:

1. Repita etapas 1 e 2 Configure aberto com autenticação de MAC a fim criar e configurar o VLAN com estes parâmetros de configuração:Identificação VLAN: 4Endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de rádio: 10.4.1.1máscara de sub-rede: 255.255.0.0
2. No Home Page wireless do aplicativo, selecione a **segurança Wireless** > o **gerenciador de SSID** a fim configurar o SSID e o tipo do autenticação.Na Segurança: A página do gerenciador de SSID, configura o SSID e atribui o SSID ao VLAN criado em step1 a fim permitir o SSID na interface de rádio.Sob a seção dos ajustes da autenticação desta página,

escolha a **autenticação compartilhada**.Está aqui a tela de configuração que explica estas etapas:Clique em Apply.

3. Configurar a criptografia de WEP para este SSID/VLAN. Porque é a autenticação de chave compartilhada, a mesma chave é usada para a autenticação também. No Home Page wireless, selecione a **segurança Wireless** > o **gerenciador de criptografia** a fim configurar as configurações de criptografia.Na Segurança: A página do gerenciador de criptografia, incorpora **4** para o modo de criptografia e as chaves do grupo para o VLAN.Escolha a **criptografia de WEP: Imperativo** como o modo de criptografia.Ajuste a chave de criptografia para este VLAN.Esta seção usa estes ajustes da chave de criptografia:Slot1 da chave de criptografia: usado como a chave transmissoraTamanho da chave de criptografia: bit 40Chave de criptografia no valor hexadecimal: 1234567890**Note**: O mesmo entalhe da chave de criptografia (1, neste caso) deve ser usado como a chave transmissora no cliente Wireless. Também, o cliente Wireless deve ser configurado com o mesmo valor chave (1234567890 neste caso) para que o cliente Wireless comunique-se com esta rede de WLAN.Esta tela de configuração explica estas etapas:
4. A fim configurar o servidor DHCP interno para clientes Wireless deste VLAN, termine as mesmas etapas explicadas dentro [configuram o servidor DHCP interno para clientes Wireless desta](#) seção [VLAN d](#)este documento com estes parâmetros de configuração:Nome do conjunto de DHCP: VLAN 4Rede do conjunto de DHCP: 10.4.0.0Máscara de sub-rede: 255.255.0.0Começando o IP: 10.4.1.5Terminando o IP: 10.4.1.10Roteador padrão: 10.4.1.1

Configurar a autenticação WPA

O WPA é um aprimoramento de segurança com base em padrões, interoperáveis que aumente fortemente o nível da proteção de dados e do controle de acesso para a existência e os sistemas futuros do Wireless LAN. Apoios de gerenciamento chave WPA dois tipos mutuamente exclusivos do Gerenciamento: WPA e WPA-PSK.

Refira a [utilização do gerenciamento chave WPA](#) para mais informação.

Usando o gerenciamento chave WPA, os clientes e o Authentication Server autenticam entre si usando um método de autenticação de EAP, e o cliente e servidor gerencie por pares um chave mestre (PMK). Usando o WPA, o server gerencie o PMK dinamicamente e passa-o ao AP.

Este exemplo usa estes parâmetros de configuração para a autenticação WPA:

- Nome SSID: **wpa**
- Identificação VLAN: **5**
- Endereço IP de Um ou Mais Servidores Cisco ICM NT VLAN: **10.5.1.1/16**
- Escala de endereço de DHCP para os clientes Wireless deste VLAN/SSID: **10.5.1.5/16 - 10.5.1.10/16**

Termine estas etapas a fim configurar a autenticação WPA:

1. Repita etapas 1 e 2 [Configure aberto com autenticação de MAC](#) a fim criar e configurar o VLAN com estes parâmetros de configuração:Identificação VLAN: 5Endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de rádio: 10.5.1.1máscara de sub-rede: 255.255.0.0
2. Porque o WPA é um padrão do gerenciamento chave, configurar a cifra a ser usada para o gerenciamento chave WPA.No Home Page wireless, selecione a **segurança Wireless** > o

gerenciador de criptografia a fim configurar as configurações de criptografia.Na tela da segurança Wireless > do gerenciador de criptografia na Segurança: A página do gerenciador de criptografia, incorpora **5** para o modo de criptografia e as chaves do grupo para o VLAN.Escolha a **cifra** como o modo de criptografia, e escolha um algoritmo de criptografia da cifra da caixa suspensa.Este exemplo usa o **TKIP** como o algoritmo da cifra:**Note**: Ao configurar a autenticação múltipla datilografa em um roteador Wireless com o SDM, às vezes ele não pôde ser possível para configurar dois tipos do autenticação diferentes ambos que usam o modo de criptografia da cifra no mesmo roteador. Nesses casos, a configuração de criptografia configurada com o SDM não pôde ser aplicada no roteador. A fim superar isto, configurar aqueles tipos do autenticação com o CLI.

3. A próxima etapa é configurar o servidor Radius local para a authenticação do cliente. A fim executar isto, repita as etapas 3a a 3c Configure aberto com autenticação de MAC com estes parâmetros de configuração:Endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius: 10.5.1.1Segredo compartilhado: ciscoEnrole para baixo a página do **gerenciador do servidor** para procurar a seção de prioridades do server do padrão. Nesta seção, escolha este servidor Radius (**10.5.1.1**) como o server da prioridade padrão para a autenticação de EAP segundo as indicações deste exemplo:Repita as etapas 3e e 3f Configure abrem com autenticação de MAC.Repita as etapas 3g e 3h Configure abrem com autenticação de MAC com estes parâmetros de configuração para a autenticação de EAP:Endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA: 10.5.1.1Segredo compartilhado: ciscoSob a seção dos usuários individuais, configurar o nome de usuário e senha como **user2**.
4. A fim permitir o WPA para um SSID, você precisa de permitir aberto com EAP ou a rede EAP no SSID. A fim permitir a rede EAP, no Home Page wireless do aplicativo, seleciona a **segurança Wireless** > o **gerenciador de SSID** para configurar o SSID e o tipo do autenticação.Na Segurança: A página do gerenciador de SSID, configura o SSID e atribui o SSID ao VLAN criado em step1 a fim permitir o SSID na interface de rádio.Sob a seção dos ajustes da autenticação desta página, escolha a **autenticação aberta** e da caixa suspensa correspondente, escolhem a **autenticação de EAP**. Também, selecione o tipo da **autenticação de EAP da rede**.A fim configurar prioridades do server, escolha **personalizam** sob o EAP autenticam server e escolhem o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius local **10.5.1.1**.Está aqui um exemplo que explique estas etapas:
5. Enrole para baixo a página do gerenciador de SSID para procurar a seção de **gerenciamento chave autenticada**.
6. Nesta seção, escolha **imperativo da** caixa suspensa do gerenciamento chave, e permita a **caixa de verificação WPA**.Está aqui a janela de configuração que explica estas etapas:
7. Clique em Apply.
8. A fim configurar o servidor DHCP interno para clientes Wireless deste VLAN, termine as mesmas etapas explicadas dentro configuram o servidor DHCP interno para clientes Wireless desta seção VLAN deste documento com estes parâmetros de configuração:Nome do conjunto de DHCP: VLAN 5Rede do conjunto de DHCP: 10.5.0.0Máscara de sub-rede: 255.255.0.0Começando o IP: 10.5.1.5Terminando o IP: 10.5.1.10Roteador padrão: 10.5.1.1

Configurar a autenticação WPA-PSK

O outro tipo do gerenciamento chave WPA é chamado o WPA-PSK. O WPA-PSK é usado para apoiar o WPA em um Wireless LAN onde a autenticação 802.1x-based não esteja disponível. Com este tipo, você deve configurar uma chave pré-compartilhada no AP. Você pode incorporar a

chave pré-compartilhada como o ASCII ou os caracteres hexadecimais. Se você incorpora a chave como caracteres ASCII, você entra entre 8 e 63 caráteres, e o AP expande a chave usando o processo descrito no padrão Senha-baseado da criptografia (RFC2898). Se você incorpora a chave como caracteres hexadecimais, você deve incorporar 64 caracteres hexadecimais.

Este exemplo usa estes parâmetros de configuração para a autenticação WPA-PSK:

- Nome SSID: **WPA-PSK**
- Identificação VLAN: **6**
- Endereço IP de Um ou Mais Servidores Cisco ICM NT VLAN: **10.6.1.1/16**
- Escala de endereço HCP para os clientes Wireless deste VLAN/SSID: **10.6.1.5/16 - 10.6.1.10/16**

Termine estas etapas a fim configurar o WPA-PSK:

1. Repita etapas 1 e 2 Configure aberto com autenticação de MAC a fim criar e configurar o VLAN com estes parâmetros de configuração:Identificação VLAN: 6Endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de rádio: 10.6.1.1máscara de sub-rede: 255.255.0.0
2. Porque o WPA-PSK é um padrão do gerenciamento chave, configurar a cifra a ser usada para o gerenciamento chave WPA.No Home Page wireless, selecione a **segurança Wireless** > o **gerenciador de criptografia** a fim configurar as configurações de criptografia.No indicador da **segurança Wireless** > do **gerenciador de criptografia na** Segurança: A página do gerenciador de criptografia, incorpora **6** para o modo de criptografia e as chaves do grupo para o VLAN.Escolha a **cifra** como o modo de criptografia, e escolha um algoritmo de criptografia da cifra da caixa suspensa.Este exemplo usa **TKIP+WEP 128bit** como o algoritmo da cifra.**Note**: Ao configurar a autenticação múltipla datilografa em um roteador Wireless com o SDM, às vezes ele não pôde ser possível para configurar dois tipos do autenticação diferentes ambos que usam o modo de criptografia da cifra no mesmo roteador. Nesses casos, a configuração de criptografia configurada com o SDM não pôde ser aplicada no roteador. A fim superar isto, configurar aqueles tipos do autenticação com o CLI.
3. A fim permitir o WPA-PSK para um SSID, você precisa de permitir a autenticação aberta no SSID. A fim permitir a autenticação aberta, repita a etapa 6 da autenticação aberta Configure com criptografia de WEP.Está aqui a janela de configuração do WPA-PSK:
4. Enrole para baixo a página do gerenciador de SSID para procurar a seção de **gerenciamento chave autenticada**.
5. Nesta seção, escolha **imperativo da** caixa suspensa do gerenciamento chave, permita a **caixa de verificação WPA** e incorpore a chave pré-compartilhada WPA ao ASCII ou ao formato hexadecimal.Este exemplo usa o formato ASCII. O mesmo formato deve ser usado na configuração do lado do cliente. Está aqui a janela de configuração que explica a etapa 5:A chave pré-compartilhada WPA usada nesta configuração é 1234567890.
6. Clique em Apply.
7. A fim configurar o servidor DHCP interno para clientes Wireless deste VLAN, termine as mesmas etapas explicadas dentro configuram o servidor DHCP interno para clientes Wireless desta seção VLAN deste documento com estes parâmetros de configuração:Nome do conjunto de DHCP: VLAN 6Rede do conjunto de DHCP: 10.6.0.0Máscara de sub-rede: 255.255.0.0Começando o IP: 10.6.1.5Terminando o IP: 10.6.1.10Roteador padrão: 10.6.1.1

Configuração de cliente Wireless

Depois que você configura o ISR com o SDM, você precisa de configurar o cliente Wireless para os tipos do autenticação diferentes de modo que o roteador possa autenticar estes clientes Wireless e fornecer o acesso à rede de WLAN. Este documento usa o ADU para a configuração do lado do cliente.

Configurar o cliente Wireless para a autenticação aberta com criptografia de WEP

Conclua estes passos:

1. Na janela de gerenciamento do perfil no ADU, clique **novo** a fim criar um perfil novo.Indicadores de uma nova janela onde você pode ajustar a configuração para a autenticação aberta.
2. Sob o **tab geral**, incorpore o nome de perfil e o SSID que o adaptador cliente usará.Neste exemplo, o nome de perfil e o SSID são **openwep**.**Note**: O SSID deve combinar o SSID que você configurou no ISR para a autenticação aberta.
3. Clique a **ABA de segurança** e deixe a opção de segurança como a chave pré-compartilhada (WEP estático) para a criptografia de WEP.
4. O clique **configura** e define a chave pré-compartilhada segundo as indicações deste exemplo:
5. Clique o **guia avançada na** página do Gerenciamento do perfil e ajuste o modo de autenticação do 802.11 como **aberto** para a autenticação aberta.
6. A fim verificar aberto com autenticação WEP, ative o **openwep** SSID configurado.
7. Verifique que o cliente Wireless está associado com sucesso com o roteador. Isto pode ser verificado em detalhe do roteador Wireless usando o **comando show dot11 associations**.Aqui está um exemplo:

```
Router#show dot11 associations
802.11 Client Stations on Dot11Radio0:

SSID [openwep] :

MAC Address    IP address      Device        Name            Parent         State
0040.96ac.e657 10.1.1.5        CB21AG/PI21AG client          self           Assoc


Others:  (not related to any ssid)
```

Configurar o cliente Wireless para aberto com autenticação de MAC

Conclua estes passos:

1. Na janela de gerenciamento do perfil no ADU, clique **novo** a fim criar um perfil novo.Indicadores de uma nova janela onde você pode ajustar a configuração para a autenticação aberta.
2. Sob o **tab geral**, incorpore o nome de perfil e o SSID que o adaptador cliente usará.Neste exemplo, o nome de perfil e o SSID são **openmac**.**Note**: O SSID deve combinar o SSID que você configurou no ISR para a autenticação aberta.
3. Clique a **ABA de segurança** e deixe a opção de segurança como **nenhuns** para aberto com a autenticação de MAC. Então, **APROVAÇÃO do** clique.

4. A fim verificar aberto com autenticação de MAC, ative o **openmac** SSID configurado.
5. Verifique que o cliente Wireless está associado com sucesso com o roteador. Isto pode ser verificado em detalhe do roteador Wireless usando o **comando show dot11 associations**.Aqui está um exemplo:

```
Router#show dot11 associations
802.11 Client Stations on Dot11Radio0:

SSID [openmac] :

MAC Address    IP address      Device        Name            Parent         State
0040.96ac.e657 10.2.1.5        CB21AG/PI21AG client1         self           MAC-Assoc

SSID [openwep] :


Others:  (not related to any ssid)
```

Configurar o cliente Wireless para a autenticação 802.1x/EAP

Conclua estes passos:

1. Na janela de gerenciamento do perfil no ADU, clique **novo** a fim criar um perfil novo.Indicadores de uma nova janela onde você pode ajustar a configuração para a autenticação aberta.
2. Sob o **tab geral**, incorpore o nome de perfil e o SSID que o adaptador cliente usará.Neste exemplo, o nome de perfil e o SSID são **pulo**.**Note**: O SSID deve combinar o SSID que você configurou no ISR para a autenticação 802.1x/EAP.
3. Sob o Gerenciamento do perfil, clique a **ABA de segurança**, ajuste a opção de segurança como o **802.1x** e escolha o tipo apropriado EAP.Este documento usa o **PULO** como o tipo EAP para a autenticação.
4. O clique **configura** a fim configurar os ajustes do nome de usuário e senha do PULO.Sob os ajustes do nome de usuário e senha, este exemplo escolhe **alertar manualmente para o nome de usuário e a senha** de modo que o cliente seja alertado incorporar o nome de usuário e senha correto ao tentar conectar à rede.
5. Click **OK**.
6. A fim verificar a autenticação de EAP, ative o **pulo** SSID configurado. Você é alertado incorporar um nome de usuário e senha do PULO. Incorpore ambas as credenciais como o **usuário1** e clique a **APROVAÇÃO**.
7. Verifique que o cliente Wireless está autenticado com sucesso e atribuído com um endereço IP de Um ou Mais Servidores Cisco ICM NT. Isto pode ser verificado claramente da janela de status ADU.Está aqui a saída equivalente do CLI do roteador:

```
Router#show dot11 associations
802.11 Client Stations on Dot11Radio0:

SSID [leap] :

MAC Address    IP address      Device        Name            Parent         State
0040.96ac.e657 10.3.1.5        CB21AG/PI21AG client2         self           EAP-Assoc

SSID [openmac] :

SSID [openwep] :
```

```
Others:  (not related to any ssid)
```

Configurar o cliente Wireless para a autenticação compartilhada

Conclua estes passos:

1. Na janela de gerenciamento do perfil no ADU, clique **novo** a fim criar um perfil novo.Indicadores de uma nova janela onde você pode ajustar a configuração para a autenticação aberta.
2. Sob o **tab geral**, incorpore o nome de perfil e o SSID que o adaptador cliente usará.Neste exemplo, o nome de perfil e o SSID **são compartilhados**.**Note**: O SSID deve combinar o SSID que você configurou no ISR para a autenticação aberta.
3. Clique a **ABA de segurança** e deixe a opção de segurança como a chave pré-compartilhada (WEP estático) para a criptografia de WEP. Então, o clique **configura**.
4. Defina a chave pré-compartilhada segundo as indicações deste exemplo:
5. Click **OK**.
6. Sob o Gerenciamento do perfil, clique o modo de autenticação do 802.11 do **guia avançada** e do grupo como **compartilhado** para a autenticação compartilhada.
7. A fim verificar compartilhou da autenticação, ativa o SSID **compartilhado** configurado.
8. Verifique que o cliente Wireless está associado com sucesso com o roteador. Isto pode ser verificado em detalhe do roteador Wireless usando o **comando show dot11 associations**.Aqui está um exemplo:

```
Router#show dot11 associations
802.11 Client Stations on Dot11Radio0:


SSID [shared] :

MAC Address    IP address      Device        Name            Parent         State
0040.96ac.e657 10.4.1.5        CB21AG/PI21AG WCS             self           Assoc
```

Configurar o cliente Wireless para a autenticação WPA

Conclua estes passos:

1. Na janela de gerenciamento do perfil no ADU, clique **novo** a fim criar um perfil novo.Indicadores de uma nova janela onde você pode ajustar a configuração para a autenticação aberta.
2. Sob o **tab geral**, incorpore o nome de perfil e o SSID que o adaptador cliente usará.Neste exemplo, o nome de perfil e o SSID são **wpa**.**Note**: O SSID deve combinar o SSID que você configurou no ISR para a autenticação WPA (com EAP).
3. Sob o Gerenciamento do perfil, clique a **ABA de segurança**, ajuste a opção de segurança como **WPA/WPA2/CCKM** e escolha o tipo apropriado WPA/WPA2/CCKM EAP.Este documento usa o **PULO** como o tipo EAP para a autenticação.
4. O clique **configura** a fim configurar os ajustes do nome de usuário e senha do PULO.Sob os ajustes do nome de usuário e senha, este exemplo escolhe **alertar manualmente para o nome de usuário e a senha** de modo que o cliente seja alertado incorporar o nome de usuário e senha correto ao tentar conectar à rede.
5. Click **OK**.

6. A fim verificar a autenticação de EAP, ative o pulo SSID configurado. Você é alertado incorporar um nome de usuário e senha do PULO. Incorpore ambas as credenciais como **user2**, a seguir clique a **APROVAÇÃO**.
7. Verifique que o cliente Wireless está autenticado com sucesso e atribuído com um endereço IP de Um ou Mais Servidores Cisco ICM NT. Isto pode ser verificado claramente da janela de status ADU.

Configurar o cliente Wireless para a autenticação WPA-PSK

Conclua estes passos:

1. Na janela de gerenciamento do perfil no ADU, clique **novo** a fim criar um perfil novo.Indicadores de uma nova janela onde você pode ajustar a configuração para a autenticação aberta.
2. Sob o **tab geral**, incorpore o nome de perfil e o SSID que o adaptador cliente usará.Neste exemplo, o nome de perfil e o SSID são WPA-**PSK**.**Note**: O SSID deve combinar o SSID que você configurou no ISR para a autenticação WPA-PSK.
3. Sob o Gerenciamento do perfil, clique a **ABA de segurança** e ajuste a opção de segurança como a **frase de passagem WPA/WPA2**. Então, o clique **configura** a fim configurar a frase de passagem WPA.
4. Defina uma chave pré-compartilhada WPA. A chave deve ser 8 a 63 caracteres ASCII de comprimento. Então, **APROVAÇÃO do** clique.
5. A fim verificar o WPA-PSK, ative o WPA-**PSK** SSID configurado.
6. Verifique que o cliente Wireless está associado com sucesso com o roteador. Isto pode ser verificado em detalhe do roteador Wireless usando o **comando show dot11 associations**.

Troubleshooting

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

Comandos para Troubleshooting

Você pode usar estes **comandos debug** pesquisar defeitos sua configuração.

- **debugar o autenticador todo aaa do dot11** — Ativa a eliminação de erros do MAC e dos pacotes da autenticação de EAP.
- **debugar a autenticação RADIUS** — Indica as negociações de RADIUS entre o server e o cliente.
- **debugar pacotes do Servidor local do raio** — Indica o índice dos pacotes de informação de RADIUS que são enviados e recebidos.
- **debugar o cliente do Servidor local do raio** — Indica Mensagens de Erro sobre authenticações do cliente falhadas.

Informações Relacionadas

- Autenticação em exemplos de configuração dos controladores do Wireless LAN

- Configurando VLANs
- Roteador Wireless de 1800 ISR com exemplo de configuração interno DHCP e de autenticação aberta
- Cisco Wireless ISR e de configuração do ponto de acesso HWIC guia
- Conectividade do Wireless LAN usando um ISR com exemplo de configuração da criptografia de WEP e da autenticação de leap
- Configurando tipos de autenticação
- Conectividade do Wireless LAN usando um ISR com exemplo de configuração da criptografia de WEP e da autenticação de leap
- Suporte Técnico e Documentação - Cisco Systems