PEAP sob redes sem fio unificadas com o Internet Authentication Service da Microsoft (IAS)

Índice

Introdução

Este original fornece um exemplo de configuração para configurar o Protected Extensible Authentication Protocol (PEAP) com a autenticação Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) versão 2 em uma rede Cisco Unified Wireless com o Microsoft Internet Authentication Service (IAS) como um servidor RADIUS.

Pré-requisitos

Requisitos

Há uma suposição que o leitor tem a instalação de Windows 2003 do conhecimento do gerenciamento de recursos básicos e a instalação do controlador de Cisco desde que este documento cobre somente as configurações específicas para facilitar os testes.

Nota: Este documento é pretendido dar aos leitores um exemplo na configuração exigida no server MS para o PEAP – autenticação chap MS. A configuração de servidor Microsoft apresentada nesta seção foi testada no laboratório e encontrada trabalhar como esperado. Se você tem o problema que configura o servidor Microsoft, contacte Microsoft para a ajuda. O tac Cisco não apoia a configuração do Microsoft Windows server.

Para a instalação inicial e a informação de configuração para os controladores do Cisco 4400 Series, refira o guia de início rápido: Controladores de LAN sem fio Cisco série 4400.

Microsoft Windows 2003 Guias de Instalação e Configuração pode ser encontrado em instalar Windows Server 2003 R2 .

Antes que você comece, instale o Microsoft Windows server 2003 com sistema operacional SP1 em cada um dos server no laboratório de teste e atualize todos os pacotes de serviços. Instale os controladores e o Lightweight Access Points (regaços) e assegure-se de que as atualizações de software mais recente estejam configuradas.

Componentes Utilizados

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

- Controlador do Cisco 4400 Series que executa a versão de firmware 4.0
- Protocolo do Access point do peso leve de Cisco 1131 (LWAPP) AP
- Servidor de empreendimento de Windows 2003 (SP1) com Internet Authentication Service (IAS), Certificate Authority (CA), DHCP, e serviços do Domain Name System (DNS) instalados
- Profissional de Windows XP com SP2 (e os pacotes de serviços actualizados) e a placa de interface da rede Wireless do Cisco Aironet 802.11a/b/g (NIC)
- Versão 4.0 do utilitário de Desktop de Aironet
- Cisco 3560 Switch

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.

Vista geral PEAP

Segurança do nível do transporte dos usos PEAP (TLS) para criar um canal cifrado entre um cliente PEAP de autenticação, tal como um portátil wireless, e um autenticador PEAP, tal como o Internet Authentication Service de Microsoft (IAS) ou o algum servidor Radius. O PEAP não especifica um método de autenticação, mas fornece a segurança adicional para outros protocolos de autenticação de EAP, tais como o EAP-MSCHAPv2, que pode se operar através do canal cifrado TLS fornecido pelo PEAP. O processo de autenticação de PEAP consiste em duas fases principal:

PEAP fase um: Canal cifrado TLS

Os associados do cliente Wireless com o AP. Uma associação da IEEE 802.11-based fornece um sistema aberto ou a autenticação de chave compartilhada antes de uma associação segura é criada entre o cliente e o Access point (REGAÇO). Depois que a associação da IEEE 802.11-based é estabelecida com sucesso entre o cliente e o Access point, a sessão TLS está negociada com o AP. Depois que a autenticação é terminada com sucesso entre o cliente Wireless e o servidor de IAS, a sessão TLS está negociada entre eles. A chave que é derivada dentro desta negociação é usada para cifrar toda a comunicação subsequente.

Fase dois PEAP: uma comunicação EAP-autenticada

Uma comunicação EAP, que inclua a negociação EAP, ocorre dentro do canal TLS criado pelo PEAP dentro da primeira fase do processo de autenticação de PEAP. O servidor de IAS autentica o cliente Wireless com EAP-MS-CHAP v2. O REGAÇO e as mensagens dianteiras do controlador somente entre o cliente Wireless e o servidor Radius. O WLC e o REGAÇO não podem decifrar estas mensagens porque não é o ponto final TLS.

Depois que a fase uma PEAP ocorre, e o canal TLS está criado entre o servidor de IAS e o cliente Wireless do 802.1X, porque uma tentativa da autenticação bem sucedida onde o usuário forneça credenciais senha-baseadas válidas com o PEAP-MS-CHAP v2, a sequência do mensagem de RADIUS é esta:

1. O servidor de IAS envia um mensagem request da identidade ao cliente: EAP-pedido/identidade.
2. O cliente responde com um mensagem de resposta da identidade: EAP-resposta/identidade.
3. O servidor de IAS envia um mensagem de desafio MS-CHAP v2: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (desafio).
4. O cliente responde com um desafio e resposta MS-CHAP v2: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (resposta).
5. O servidor de IAS envia para trás um pacote do sucesso MS-CHAP v2 quando o server autenticou com sucesso o cliente: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (sucesso).
6. O cliente responde com um pacote do sucesso MS-CHAP v2 quando o cliente autenticou com sucesso o server: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (sucesso).
7. O servidor de IAS envia um EAP-TLV que indique a autenticação bem sucedida.
8. O cliente responde com um mensagem de sucesso do estado EAP-TLV.
9. O server termina a autenticação e envia uma mensagem do EAP-sucesso usando o texto simples. Se os VLAN são distribuídos para o isolamento do cliente, os atributos VLAN estão incluídos nesta mensagem.

Configurar

Este documento fornece um exemplo para a configuração de PEAP MS-CHAP v2.

Nota: 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:

Nesta instalação, um server de Microsoft Windows 2003 executa estes papéis:

- Controlador de domínio para o domínio **Wireless.com**
- Server DHCP/DNS
- Server do Certificate Authority (CA)
- Diretório ativo – para manter a base de dados de usuário
- Internet Authentication Service (IAS) – para autenticar os usuários Wireless

Este server conecta à rede ligada com fio através de um switch de Camada 2 como mostrado.

O controlador do Wireless LAN (WLC) e o REGAÇO registrado igualmente conectam à rede através do switch de Camada 2.

Os clientes Wireless C1 e C2 usarão o acesso protegido por wi-fi 2 (WPA2) - autenticação PEAP MSCHAP v2 para conectar à rede Wireless.

O objetivo é configurar o server de Microsoft 2003, o controlador do Wireless LAN, e o AP de pouco peso para autenticar os clientes Wireless com autenticação PEAP MSCHAP v2.

A próxima seção explica como configurar os dispositivos para esta instalação.

Configurações

Esta seção olha a configuração exigida setup a autenticação PEAP MS-CHAP v2 neste WLAN:

- Configurar o server de Microsoft Windows 2003
- Configurar o controlador do Wireless LAN (WLC) e os AP de pouco peso
- Configurar os clientes Wireless

Comece com a configuração do server de Microsoft Windows 2003.

Configurar o server de Microsoft Windows 2003

Configurar o server de Microsoft Windows 2003

Como mencionado na seção da instalação de rede, use o server de Microsoft Windows 2003 na rede para executar estas funções.

- **Controlador de domínio** – para o **Sem fio do** domínio
- **Server DHCP/DNS**
- **Server do Certificate Authority (CA)**
- **Internet Authentication Service (IAS)** – para autenticar os usuários Wireless

- **Diretório ativo** – para manter a base de dados de usuário

Configurar o server de Microsoft Windows 2003 para estes serviços. Comece com a configuração do server de Microsoft Windows 2003 como um controlador de domínio.

Configurar o server de Microsoft Windows 2003 como um controlador de domínio

A fim configurar o server de Microsoft Windows 2003 como um controlador de domínio, termine estas etapas:

1. Clique o **começo**, **corrida do** clique, o tipo **dcpromo.exe, e** clique então o começo OKTO o assistente de instalação de diretório ativo.
2. Clique **ao lado de** executam o assistente de instalação de diretório ativo.
3. A fim criar um domínio novo, escolha o **controlador de domínio da** opção para um domínio novo.
4. O clique **ao lado de** cria uma floresta nova das árvores de domínio.
5. Se o DNS não é instalado no sistema, o assistente fornece-lhe as opções com que para configurar o DNS. Escolha o **nenhum, apenas instale e configurar o DNS n**este computador. Clique em Next.
6. Datilografe o nome de DNS completo para o domínio novo. Neste exemplo **Wireless.com** é usado e clique **em seguida**.
7. Dê entrada com o nome de netbios para o domínio e clique-o **em seguida**. Este exemplo usa o **SEM FIO**.
8. Escolha o base de dados e registre lugar para o domínio. Clique em Next.
9. Escolha um lugar para o dobrador de Sysvol. Clique em Next.
10. Escolha as permissões padrão para os usuários e os grupos. Clique em Next.
11. Ajuste a senha de administrador e o clique **em seguida**.
12. O clique **ao lado de** aceita as opções de domínio ajustadas previamente.
13. **Revestimento do** clique para fechar o assistente de instalação de diretório ativo.
14. Reinicie o server para que as mudanças tomem o efeito.

Com esta etapa, você configurou o server de Microsoft Windows 2003 como um controlador de domínio e criou um domínio novo **Wireless.com**. Configurar em seguida serviços DHCP no server.

Instale e configurar serviços DHCP no server de Microsoft Windows 2003

O serviço DHCP no server de Microsoft 2003 é usado para fornecer endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes Wireless. A fim instalar e configurar serviços DHCP neste server, termine estas etapas:

1. O clique **adiciona ou remove programas no** Control Panel.
2. O clique **adiciona/remove componentes do Windows**.
3. Escolha **serviços de rede** e clique **detalhes**.
4. Escolha o **protocolo de configuração dinâmica host (DHCP)** e clique a **APROVAÇÃO**.
5. O clique **ao lado de** instala o serviço DHCP.
6. Clique em **Concluir** para concluir a instalação.
7. A fim configurar serviços DHCP, clique o **iniciar > programas > ferramentas administrativas** e clique o **DHCP pressão-**em.
8. Escolha o servidor DHCP - **tsweb-lapt.wireless.com** (neste exemplo).
9. Clique a **ação** e clique-a então **autorizam** para autorizar o serviço DHCP.
10. Na árvore de console, clicar com o botão direito **tsweb-lapt.wireless.com** e clique então o

espaço novo para definir um intervalo de endereço IP para os clientes Wireless.
11. Na boa vinda à página nova do wizard de escopo do wizard de escopo novo, clique **em seguida**.
12. Na página do nome do espaço, datilografe o nome do escopo de DHCP. Neste exemplo, use **clientes DHCP** como o nome do espaço. Clique em Next.
13. Na página do intervalo de endereço IP, incorpore o começo e termine endereços IP de Um ou Mais Servidores Cisco ICM NT para o espaço, e clique-os **em seguida**.
14. Adicionar as exclusões paginam, mencionam que o endereço IP de Um ou Mais Servidores Cisco ICM NT que você gostaria de reservar/exclui do escopo de DHCP. Clique em Next.
15. Mencione a duração de aluguel na página da duração de aluguel, e clique-a **em seguida**.
16. Configurar as opções de DHCP paginam, escolhem **sim, eu quero configurar agora a opção de DHCP**, e clico **em seguida**.
17. Se há roteador do gateway padrão, mencione o endereço IP de Um ou Mais Servidores Cisco ICM NT do gateway router na página do roteador (gateway padrão), e clique-o **em seguida**.
18. Na página do Domain Name e dos servidores DNS, datilografe o nome do domínio que foi configurado previamente. No exemplo, use **Wireless.com**. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do server. Clique em Add.
19. Clique em Next.
20. Na página do servidor das VITÓRIAS, clique **em seguida**.
21. Na página do espaço da ativação, escolha **sim, eu quero ativar agora o espaço**, e clico **em seguida**.
22. Ao terminar o wizard de escopo novo, **revestimento do** clique.
23. No indicador Snapin DHCP, verifique que o escopo de DHCP que foi criado é ativo.

Agora que o DHCP DNS é permitido no server, configurar o server como um server do Certificate Authority (CA) da empresa.

Instale e configurar o server de Microsoft Windows 2003 como um server do Certificate Authority (CA)

O PEAP com EAP-MS-CHAPv2 valida o servidor Radius baseado no certificado atual no server. Adicionalmente, o certificado de servidor deve ser emitido por um Certification Authority (CA) público que é confiado pelo computador de cliente (isto é, o certificado de CA público já existe no dobrador da Autoridade de certificação de raiz confiável na loja do certificado do computador de cliente). Neste exemplo, configurar o server de Microsoft Windows 2003 como um Certificate Authority (CA) que emite o certificado ao Internet Authentication Service (IAS).

A fim instalar e configurar os serviços certificados no server, termine estas etapas:

1. O clique **adiciona ou remove programas no Control Panel**.
2. O clique **adiciona/remove componentes do Windows**.
3. **Serviços certificados do** clique.
4. O clique **sim ao** mensagem de advertência, **após ter instalado serviços certificados, o computador não pode ser rebatizado e o computador não pode juntar-se ou ser removido de um domínio. Você quer continuar?**
5. Sob o tipo do Certificate Authority, escolha a **CA raiz da empresa**, e clique-a **em seguida**.
6. Dê entrada com um nome para identificar CA. Este exemplo usa Sem fio-**CA**. Clique em Next.

7. “Um diretório do log CERT” é criado para o armazenamento do base de dados do certificado. Clique em Next.
8. Se o IIS é permitido, deve ser parado antes que você continue. Clique a **APROVAÇÃO ao** mensagem de advertência que o IIS deve ser parado. Reinicia automaticamente depois que CA é instalado.
9. Clique o **revestimento** para terminar a instalação de serviços do Certificate Authority (CA).

A próxima etapa é instalar e configurar o Internet Authentication Service no server de Microsoft Windows 2003.

Conecte clientes ao domínio

A próxima etapa é conectar os clientes à rede ligada com fio e transferir a informação específica do domínio do domínio novo. Ou seja conecte os clientes ao domínio. Para isso, conclua essas etapas:

1. Conecte os clientes à rede ligada com fio com um cabo do Ethernet direto reto.
2. Carreg acima do cliente e do início de uma sessão com a senha username do cliente.
3. Clique o **começo**; clique a **corrida**; datilografe o **Cmd**; e **APROVAÇÃO do** clique.
4. No comando prompt, datilografe o **ipconfig**, e o clique **entra** para verificar que o DHCP trabalha corretamente e o cliente recebeu um endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP.
5. A fim juntar-se ao cliente ao domínio, clicar com o botão direito o **meu computador**, e escolha **propriedades**.
6. Clique a aba do **nome de computador**.
7. Clique a **mudança**.
8. Clique o **domínio**; datilografe **wireless.com**; e **APROVAÇÃO do** clique.
9. Datilografe o **administrador username** e o específico da senha ao domínio a que o cliente se junta. (Esta é a conta de administrador no diretório ativo no server.)
10. Clique em **OK**.
11. Clique **sim** para reiniciar o computador.
12. Uma vez que o computador reinicia, entre com esta informação: Username = **administrador**; **Password> da** senha = do <domain; Domínio = **Sem fio**.
13. Clicar com o botão direito o **meu computador**, e clique **propriedades**.
14. Clique a aba do **nome de computador** para verificar que você está no domínio de Wireless.com.
15. A próxima etapa é verificar que o cliente recebeu o certificado de CA (confiança) do server.
16. **Começo do** clique; **corrida do** clique; datilografe o **mmc**, e clique a **APROVAÇÃO**.
17. Clique o **arquivo**, e o clique **adiciona/remove pressão-**em.
18. Clique em Add.
19. Escolha o **certificado**, e o clique **adiciona**.
20. Escolha a **conta do computador**, e clique-a **em seguida**.
21. Clique o **revestimento** para aceitar o computador local do padrão.
22. Clique **perto**, e clique a **APROVAÇÃO**.
23. Expanda **Certificados (computador local)**; expanda **Autoridades de certificação de raiz confiável**; e **Certificados do** clique. **Sem fio do** achado na lista.
24. Repita este procedimento para adicionar mais clientes ao domínio.

Instale o Internet Authentication Service no server de Microsoft Windows 2003 e

peça um certificado

Nesta instalação, o Internet Authentication Service (IAS) é usado como um servidor Radius para autenticar clientes Wireless com autenticação de PEAP.

Termine estas etapas para instalar e configurar IAS no server.

1. O clique **adiciona ou remove programas no** Control Panel.
2. O clique **adiciona/remove componentes do Windows**.
3. Escolha **serviços de rede**, e clique **detalhes**.
4. Escolha o **Internet Authentication Service**; clique a **APROVAÇÃO**; e clique **em seguida**.
5. **Revestimento do** clique para terminar a instalação de IAS.
6. A próxima etapa é instalar o certificado do computador para o Internet Authentication Service (IAS).
7. **Começo do** clique; **corrida do** clique; datilografe o **mmc**; e **APROVAÇÃO do** clique.
8. Clique o **console no** menu de arquivo, e escolha-o então **adicionam/removem pressão-**em.
9. O clique **adiciona** para adicionar a pressão-em.
10. Escolha **Certificados da** lista de pressão-INS, e o clique **adiciona**.
11. Escolha a **conta do computador**, e clique-a **em seguida**.
12. Escolha o **computador local**, e clique o **revestimento**.
13. Clique **perto**, e clique a **APROVAÇÃO**.
14. Expanda **Certificados (computador local)**; clicar com o botão direito a **pasta pessoal**; escolha **todas as tarefas** e **peça** então o **certificado novo**.
15. Clique **em seguida na** *boa vinda ao assistente do pedido do certificado*.
16. Escolha o molde de certificado do **controlador de domínio** (se você pede um certificado do computador em um server a não ser o DC, escolhe um molde de certificado do **computador**), e clique-o **em seguida**.
17. Datilografe um nome e uma descrição para o certificado.
18. Clique o **revestimento** para terminar o assistente do pedido da certificação.

Configurar o Internet Authentication Service para a autenticação PEAP-MS-CHAP v2

Agora que você instalou e pediu um certificado para IAS, configurar IAS para a autenticação.

Conclua estes passos:

1. Clique o **iniciar > programas > ferramentas administrativas**, e clique o **Internet Authentication Service pressão-**em.
2. Clicar com o botão direito o **Internet Authentication Service (IAS)**, e clique então o **serviço do registro no diretório ativo**.
3. **O Internet Authentication Service do registro na** caixa de diálogo do **diretório ativo** aparece; **APROVAÇÃO do** clique. Isto permite IAS de autenticar usuários no diretório ativo.
4. **APROVAÇÃO do** clique na caixa de diálogo seguinte.
5. Adicionar o controlador do Wireless LAN como um cliente de AAA no servidor de IAS MS.
6. Clicar com o botão direito **clientes RADIUS**, e escolha o **cliente RADIUS novo**.
7. Datilografe o nome do cliente (WLC neste caso), e incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do WLC. Clique em Next.

8. Na página seguinte, sob Client-Vendor, escolha o **padrão RADIUS**; incorpore o segredo compartilhado; e **revestimento do** clique.
9. Observe que o WLC está adicionado como um cliente de AAA em IAS.
10. Crie uma política de acesso remoto para os clientes.
11. A fim fazer isto, clicar com o botão direito **políticas de acesso remoto**, e escolha a **política de acesso remoto nova**.
12. Datilografe um nome para a política de acesso remoto. Neste exemplo, use o nome **PEAP**. Em seguida, clique em Avançar.
13. Escolha os atributos de política baseados em suas exigências. Neste exemplo, escolha o **Sem fio**.
14. Na página seguinte, escolha o **usuário** aplicar esta política de acesso remoto para alistar dos usuários.
15. Sob métodos de autenticação, escolha **EAP protegido (PEAP)**, e o clique **configura**.
16. **Nas propriedades protegidas EAP** pagine, escolha o certificado apropriado do menu suspenso emitido certificado, e clique a **APROVAÇÃO**.
17. Verifique os detalhes da política de acesso remoto, e clique o **revestimento**.
18. A política de acesso remoto foi adicionada à lista.
19. Clicar com o botão direito a política, e clique **propriedades**. Escolha de “a **permissão de acesso remoto Grant**” sob “**se um pedido de conexão combina as circunstâncias especificadas**.”

Adicionam usuários ao diretório ativo

Nesta instalação, a base de dados de usuário é mantida no diretório ativo.

A fim adicionar usuários ao base de dados do diretório ativo, termine estas etapas:

1. Na árvore de console dos usuários e dos computadores de diretório ativo, clicar com o botão direito **usuários**; clique **novo**; e clique então o **usuário**.
2. No objeto novo – A caixa de diálogo do usuário, datilografa o nome do usuário Wireless. Este exemplo usa o nome **WirelessUser no** campo de nome e **WirelessUser no** campo de nome de logon do usuário. Clique em Next.
3. No objeto novo – A caixa de diálogo do usuário, datilografa uma senha de sua escolha na senha e confirma campos de senha. Cancele o **usuário deve mudar a senha na** caixa de verificação **seguinte do fazer logon**, e clicam **em seguida**.
4. No objeto novo – Caixa de diálogo do usuário, **revestimento do** clique.
5. Repita etapas 2 a 4 a fim criar contas de usuário adicionais.

Permita o acesso Wireless aos usuários

Conclua estes passos:

1. Na árvore de console dos **usuários e dos computadores de diretório ativo**, clique a **pasta de usuários**; clicar com o botão direito **WirelessUser**; clique **propriedades**; e vá então ao **guia de discagem de entrada**.
2. Escolha **permitem o acesso**, e clicam a **APROVAÇÃO**.

Configurar o controlador do Wireless LAN e os AP de pouco peso

Configurar agora os dispositivos Wireless para esta instalação. Isto inclui a configuração dos controladores do Wireless LAN, dos AP de pouco peso, e dos clientes Wireless.

Configurar o WLC para a autenticação RADIUS através do servidor Radius MS IAS

Configurar primeiramente o WLC para usar o MS IAS como o Authentication Server. O WLC precisa de ser configurado a fim enviar as credenciais do usuário a um servidor de raio externo. O servidor de raio externo então valida as credenciais do usuário e fornece o acesso aos clientes Wireless. A fim fazer isto, adicionar o servidor de IAS MS como um servidor Radius na página da **Segurança > da autenticação RADIUS**.

Conclua estes passos:

1. Escolha a **Segurança** e a **autenticação RADIUS do** controlador GUI indicar a página dos servidores de autenticação RADIUS. Clique então **novo** a fim definir um servidor Radius.
2. Defina os parâmetros do servidor Radius nos **servidores de autenticação RADIUS >** página **nova**. Estes parâmetros incluem o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius, o segredo compartilhado, o número de porta, e o status de servidor. O usuário de rede e as caixas de verificação de gerenciamento determinam se a autenticação Raio-baseada se aplica para o Gerenciamento e os usuários de rede. Este exemplo usa o MS IAS como o servidor Radius com endereço IP 10.77.244.198.
3. Clique em Apply.
4. O servidor de IAS MS foi adicionado ao WLC como um servidor Radius e pode ser usado para autenticar clientes Wireless.

Configurar um WLAN para os clientes

Configurar o SSID (o WLAN) a que os clientes Wireless conectam. Neste exemplo, crie o SSID, e nomeie-o **PEAP**.

Defina a autenticação da camada 2 como o WPA2 de modo que os clientes executem a autenticação baseada EAP (PEAP-MSCHAPv2 neste caso) e o uso AES como o mecanismo de criptografia. Deixe todos valores restantes em seus padrões.

Nota: Este documento liga o WLAN com as interfaces de gerenciamento. Quando você tem vlan múltiplos em sua rede, você pode criar um VLAN separado e ligá-lo ao SSID. Para obter informações sobre de como configurar VLAN em WLC, refira VLAN no exemplo de configuração dos controladores do Wireless LAN.

A fim configurar um WLAN no WLC termine estas etapas:

1. Clique **WLAN do** GUI do controlador a fim indicar a página WLAN. Esta página alista os WLAN que existem no controlador.
2. Escolha **novo** a fim criar um WLAN novo. Incorpore o ID de WLAN e o WLAN SSID para o WLAN, e o clique **aplica-se**.
3. Uma vez que você cria um WLAN novo, o **WLAN > edita a** página para o WLAN novo

aparece. Nesta página você pode definir os vários parâmetros específicos a este WLAN que incluem políticas gerais, servidores Radius, políticas de segurança, e parâmetros do 802.1x.
4. Verifique o **status administrativo** sob políticas gerais a fim permitir o WLAN. Se você quer o AP transmitir o SSID em seus beacon frame, verifique a **transmissão SSID**.
5. Sob a Segurança da camada 2, escolha **WPA1+WPA2**. Isto permite o WPA no WLAN. Enrole para baixo a página e escolha a política WPA. Este exemplo usa o WPA2 e a criptografia de AES. Escolha o servidor Radius apropriado do menu de destruição sob servidores Radius. Neste exemplo, use **10.77.244.198** (endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de IAS MS). Os outros parâmetros podem ser alterados basearam na exigência da rede de WLAN.
6. Clique em Apply.

Configurar os clientes Wireless

Configurar os clientes Wireless para a autenticação PEAP-MS CHAPv2

Este exemplo fornece a informação em como configurar o cliente Wireless com utilitário de desktop do Cisco Aironet. Antes que você configure o adaptador cliente, assegure isso que a versão a mais atrasada do firmware e a utilidade são usadas. Encontre a versão a mais atrasada do firmware e utilidades na página wireless das transferências no cisco.com.

A fim configurar o adaptador de cliente Wireless do a/b/g do 802.11 do Cisco Aironet com o ADU, termine estas etapas:

1. Abra o utilitário de Desktop de Aironet.
2. Clique o **Gerenciamento do perfil**, e clique-o **novo** para definir um perfil.
3. Sob o tab geral, incorpore o nome de perfil e o SSID. Neste exemplo, use o SSID que você configurou no WLC (PEAP).
4. Escolha a ABA de segurança; escolha **WPA/WPA2/CCKM**; sob WPA/WPA2/CCKM EAP, o tipo escolhe **PEAP [EAP-MSCHAPv2]**, e o clique **configura**.
5. Escolha **validam o certificado de servidor**, e escolhem Sem fio-**CA** sob o menu suspenso das autoridades de certificação do root confiável.
6. Clique a **APROVAÇÃO**, e ative o perfil.**Nota:** Quando você usar a versão 2 protegida do protocolo de autenticação de cumprimento do desafio de EAP-Microsoft (PEAP-MSCHAPv2) com Microsoft XP SP2, e a placa Wireless está controlada pela configuração do Sem fio zero de Microsoft (WZC), você deve aplicar o hotfix KB885453 de Microsoft. Isto impede diversas edições na autenticação relativa ao PEAP recomeça rapidamente.

Verificar e solucionar problemas

A fim verificar se a configuração trabalha como esperado, ative o perfil PEAP-MSCHAPv2 no cliente1 do cliente Wireless.

Uma vez que o perfil PEAP-MSCHAPv2 é ativado no ADU, o cliente executa a autenticação aberta do 802.11 e executa então a autenticação PEAP-MSCHAPv2. Está aqui um exemplo da autenticação PEAP-MSCHAPv2 bem sucedida.

Use os comandos debug compreender a sequência de evento que ocorrem.

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.

Estes comandos debug no controlador do Wireless LAN são úteis.

- **debugar eventos do dot1x permitem** — A fim configurar a eliminação de erros de eventos do 802.1x
- **debugar eventos aaa permite** — A fim configurar a eliminação de erros de eventos AAA
- **debugar o ADDR < MAC address > do Mac** — A fim configurar a eliminação de erros MAC, use o comando mac debugar
- **debugar o mensagem DHCP permitem** — A fim configurar debugar dos Mensagens de Erro DHCP

Estas são as saídas de exemplo do **comando enable dos eventos do dot1x debugar** e **debugam o** comando **< do MAC address > do cliente**.

debugar eventos do dot1x permitem:

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to mobile
00:40:96:ac:e6:57 (EAP Id 2) Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity
Response (count=2) from mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007:
00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3) Tue Dec 18
06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3,
EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile
00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
mobile 00:40:96:ac:e6:57 (EAP Id 4) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP
Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25) Tue Dec 18 06:58:51 2007:
00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51
2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5) Tue
Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP
Id 5, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from
AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received
EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 6, EAP Type 25) Tue Dec 18 06:58:51 2007:
00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51
2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 7) Tue
Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP
Id 7, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from
AAA to mobile 00:40:96:ac:e6:57 (EAP Id 8) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received
EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 8, EAP Type 25) Tue Dec 18 06:58:51 2007:
00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51
2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 9) Tue
Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP
Id 9, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from
AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received
EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25) Tue Dec 18 06:58:52 2007:
00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52
2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11) Tue
Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP
Id 11, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from
AAA to mobile 00:40:96:ac:e6:57 (EAP Id 12) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received
EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 12, EAP Type 25) Tue Dec 18 06:58:52 2007:
00:40:96:ac:e6:57 Processing Access-Accept for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52
2007: 00:40:96:ac:e6:57 Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0) Tue
Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id
```

13) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to mobile 00:40:96:ac:e6:57** Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57** Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received Auth Success while in Authenticating state for mobile 00:40:96:ac:e6:57**

debugar o ADDR < MAC address > do Mac:

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Association received from mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 - rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0 0 0 Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 RUN (20) Change state to START (0)** Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0) Initializing policy** Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0) Change state to AUTHCHECK (2)** Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2) Change state to 8021X_REQD (3)** Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3)** Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of Mobile Station: 00:40:96:ac:e6:57 (callerId: 48) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry. Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Connecting state Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP- Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAPOL START from mobile 00:40:96:ac:e6:57** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **EAP State update from Connecting to Authenticating for mobile 00:40:96:ac:e6:57** Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Authenticating state** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6) Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25) Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10) Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25) Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)** Wed Dec 19 02:31:56 2007:

00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Processing Access-Accept for mobile 00:40:96:ac:e6:57** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to mobile 00:40:96:ac:e6:57** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3) **Change state to L2AUTHCOMPLETE (4)** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 L2AUTHCOMPLETE (4) Change state to RUN (20) Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20) Reached PLUMBFASTPATH: from line 4041 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20) Replacing Fast Path rule type = Airespace AP Client on AP 00:0b:85:51:5a:e0, slot 0, interface = 2 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20) Card = 0 (slot 0), InHandle = 0x00000000, OutHandle = 0x00000000, npuCryptoFlag = 0x0000 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20) Successfully plumbed mobile rule (ACL ID 255) Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20) Reached RETURN: from line 4041 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend Auth Success state (id=12) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Received Auth Success** while in Authenticating state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x - moving mobile **00:40:96:ac:e6:57 into Authenticated state**

Nota: Se você usa o suplicante do Microsoft para autenticar com um Cisco Secure ACS para a autenticação de PEAP, o cliente potencialmente não autentica com sucesso. Às vezes a conexão inicial pode autenticar com sucesso, mas subsequente rápido-conecte tentativas de autenticação não conectam com sucesso. Este é um problema conhecido. Os detalhes desta edição e do reparo para o mesmos estão disponíveis aqui .

Informações Relacionadas

- PEAP sob redes Wireless unificadas com ACS 4.0 e Windows 2003
- Autenticação de EAP com exemplo de configuração dos controladores de WLAN (WLC)
- Upgrade de software do controlador do Wireless LAN (WLC) às versões 3.2, a 4.0, e a 4.1
- Manuais de configuração do Controladores de LAN sem fio Cisco série 4400
- Suporte Técnico e Documentação - Cisco Systems