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

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Conventions Visão geral do PEAP Configurar Diagrama de Rede Configurações Configurar o Microsoft Windows 2003 Server Configurar o Microsoft Windows 2003 Server Instalar e configurar os serviços DHCP no Microsoft Windows 2003 Server Instalar e Configurar o Microsoft Windows 2003 Server como um Servidor de Autoridade de Certificação (CA) Conectar clientes ao domínio Instale o Internet Authentication Service no Microsoft Windows 2003 Server e Solicite um Certificado Configurar o serviço de autenticação da Internet para a autenticação PEAP-MS-CHAP v2 Adicionar usuários ao Ative Diretory Permitir acesso sem fio aos usuários Configurar a controladora Wireless LAN e APs leves Configurar a WLC para autenticação RADIUS através do servidor RADIUS MS IAS Configurar uma WLAN para os clientes Configurar os clientes sem fio Configurar os clientes sem fio para a autenticação PEAP-MS CHAPv2 Verificar e solucionar problemas Informações Relacionadas

Introduction

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.

Prerequisites

Requirements

Há uma suposição de que o leitor tenha conhecimento da instalação básica do Windows 2003 e da instalação do controlador Cisco, uma vez que este documento abrange apenas as configurações específicas para facilitar os testes.

Observação: este documento tem como objetivo dar aos leitores um exemplo da configuração necessária no servidor MS para a autenticação PEAP - MS CHAP. A configuração do servidor Microsoft apresentada nesta seção foi testada no laboratório e descobriu-se que estava funcionando conforme esperado. Se você tiver problemas para configurar o servidor Microsoft, entre em contato com a Microsoft para obter ajuda. O Cisco TAC não suporta a configuração do servidor servidor Microsoft Windows.

Para obter informações sobre a instalação e a configuração iniciais dos Cisco 4400 Series Controllers, consulte o <u>Guia de Introdução: Cisco 4400 Series Wireless LAN Controllers</u>.

Os guias de instalação e configuração do Microsoft Windows 2003 podem ser encontrados em Instalando o Windows Server 2003 R2.

Antes de começar, instale o sistema operacional Microsoft Windows Server 2003 com SP1 em cada um dos servidores no laboratório de teste e atualize todos os Service Packs. Instale as controladoras e os pontos de acesso lightweight (LAPs) e verifique se as atualizações de software mais recentes estão configuradas.

Componentes Utilizados

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

- Controlador Cisco 4400 Series com firmware versão 4.0
- AP do protocolo LWAPP (Lightweight Access Point Protocol) do Cisco 1131
- Windows 2003 Enterprise Server (SP1) com serviços de Internet Authentication Service (IAS), Certificate Authority (CA), DHCP e Domain Name System (DNS) instalados
- Windows XP Professional com SP 2 (e Service Packs atualizados) e placa de interface de rede sem fio (NIC) Cisco Aironet 802.11a/b/g
- Aironet Desktop Utility Versão 4.0
- Switch Cisco 3560

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Visão geral do PEAP

O PEAP usa o Transport Level Security (TLS) para criar um canal criptografado entre um cliente PEAP de autenticação, como um laptop Wireless, e um autenticador PEAP, como o Microsoft Internet Authentication Service (IAS) ou qualquer servidor RADIUS. O PEAP não especifica um método de autenticação, mas fornece segurança adicional para outros protocolos de autenticação EAP, como EAP-MSCHAPv2, que podem operar através do canal criptografado TLS fornecido pelo PEAP. O processo de autenticação PEAP consiste em duas fases principais:

Fase um do PEAP: canal criptografado TLS

O cliente Wireless se associa ao AP. Uma associação baseada em IEEE 802.11 fornece uma autenticação de Sistema Aberto ou Chave Compartilhada antes de uma associação segura ser criada entre o cliente e o Ponto de Acesso (LAP). Depois que a associação baseada em IEEE 802.11 é estabelecida com êxito entre o cliente e o Ponto de acesso, a sessão TLS é negociada com o AP. Após a conclusão bem-sucedida da autenticação entre o cliente Wireless e o servidor IAS, a sessão TLS é negociada entre eles. A chave derivada nessa negociação é usada para criptografar todas as comunicações subsequentes.

Fase dois do PEAP: comunicação autenticada por EAP

A comunicação EAP, que inclui a negociação EAP, ocorre dentro do canal TLS criado pelo PEAP na primeira etapa do processo de autenticação PEAP. O servidor IAS autentica o cliente Wireless com EAP-MS-CHAP v2. O LAP e a controladora apenas encaminham mensagens entre o cliente Wireless e o servidor RADIUS. A WLC e o LAP não podem descriptografar essas mensagens porque não é o ponto final de TLS.

Depois que ocorre a etapa um do PEAP e o canal TLS é criado entre o servidor IAS e o cliente Wireless 802.1X, para uma tentativa de autenticação bem-sucedida em que o usuário forneceu credenciais válidas baseadas em senha com PEAP-MS-CHAP v2, a sequência de mensagens RADIUS é esta:

- 1. O servidor IAS envia uma mensagem de solicitação de identidade ao cliente: EAP-Solicitação/Identidade.
- 2. O cliente responde com uma mensagem de resposta de identidade: EAP-Resposta/Identidade.
- 3. O servidor IAS envia uma mensagem de desafio MS-CHAP v2: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge).
- 4. O cliente responde com um desafio e uma resposta MS-CHAP v2: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
- 5. O servidor IAS envia de volta um pacote de sucesso MS-CHAP v2 quando o servidor autentica com êxito o cliente: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Sucesso).
- 6. O cliente responde com um pacote de sucesso MS-CHAP v2 quando o cliente autentica com êxito o servidor: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Êxito).
- 7. O servidor IAS envia um EAP-TLV que indica uma autenticação bem-sucedida.
- 8. O cliente responde com uma mensagem de status de êxito EAP-TLV.
- O servidor conclui a autenticação e envia uma mensagem EAP-Success usando texto simples. Se as VLANs forem implantadas para isolamento do cliente, os atributos da VLAN serão incluídos nesta mensagem.

Configurar

Este documento fornece um exemplo para a configuração do 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:



Wireless Client C1 Wireless Client C2

Nesta configuração, um servidor Microsoft Windows 2003 executa estas funções:

- Controlador de domínio para o domínio Wireless.com
- servidor DHCP/DNS
- Servidor de Autoridade de Certificação (CA)
- Ative Diretory para manter o banco de dados do usuário
- Internet Authentication Service (IAS) para autenticar os usuários sem fio

Esse servidor se conecta à rede com fio por meio de um switch de Camada 2, como mostrado.

A controladora Wireless LAN (WLC) e o LAP registrado também se conectam à rede através do switch de Camada 2.

Os clientes sem fio C1 e C2 usarão a autenticação WPA2 (Wi-Fi Protected Access 2) - PEAP MSCHAP v2 para se conectar à rede sem fio.

O objetivo é configurar o servidor Microsoft 2003, o Wireless LAN Controller e o Light Weight AP para autenticar os clientes Wireless com a autenticação PEAP MSCHAP v2.

A próxima seção explica como configurar os dispositivos para essa configuração.

Configurações

Esta seção examina a configuração necessária para configurar a Autenticação PEAP MS-CHAP v2 nesta WLAN:

- Configurar o Microsoft Windows 2003 Server
- Configurar a controladora Wireless LAN (WLC) e os APs leves
- Configurar os clientes sem fio

Comece com a configuração do servidor Microsoft Windows 2003.

Configurar o Microsoft Windows 2003 Server

Configurar o Microsoft Windows 2003 Server

Como mencionado na seção Configuração de rede, use o servidor Microsoft Windows 2003 na rede para executar essas funções.

- Controlador de domínio para o domínio Wireless
- servidor DHCP/DNS
- Servidor de Autoridade de Certificação (CA)
- Internet Authentication Service (IAS) para autenticar os usuários sem fio
- Ative Diretory para manter o banco de dados do usuário

Configure o servidor Microsoft Windows 2003 para esses serviços. Comece com a configuração do servidor Microsoft Windows 2003 como um controlador de domínio.

Configurar o servidor Microsoft Windows 2003 como um controlador de domínio

Para configurar o servidor Microsoft Windows 2003 como um controlador de domínio, siga estas etapas:

 Clique em Iniciar, clique em Executar, digite dcpromo.exe e clique em OK para iniciar o Assistente de instalação do Ative Diretory.



2. Clique em **Avançar** para executar o Assistente de Instalação do Ative Diretory.

ctive	e Directory Installation Wizard
01	perating System Compatibility Improved security settings in Windows Server 2003 affect older versions of Windows.
	Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.
	Some older versions of Windows, including Windows 95 and Windows NT 4.0 SP3 or earlier, do not meet these requirements. Similarly, some non-Windows systems, including Apple Mac OS X and SAMBA clients, might not meet these requirements.
	For more information, see <u>Compatibility Help</u> .
	< <u>B</u> ack <u>Next</u> > Cancel

3. Para criar um novo domínio, escolha a opção **Domain Controller** para um novo domínio.

omain C Specify	ontroller Type I the role you want this server to have.
Dio you additior	want this server to become a domain controller for a new domain or an nal domain controller for an existing domain?
• Do	main controller for a new domain
Sel Thi	ect this option to create a new child domain, new domain tree, or new forest. s server will become the first domain controller in the new domain.
O <u>A</u> de	ditional domain controller for an existing domain
⚠	Proceeding with this option will delete all local accounts on this server.
	All cryptographic keys will be deleted and should be exported before continuing.
	All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.
	(Pack Nouth Canool

4. Clique em **Avançar** para criar uma nova floresta de árvores de domínio.

Active Directory Installation Wizard	×
Create New Domain Select which type of domain to create.	$\mathbf{\hat{z}}$
Create a new:	
Domain in a new forest	
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.	
Child domain in an existing domain tree	
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.	
O Domain tree in an existing forest	
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.	
< <u>B</u> ack <u>N</u> ext > Cancel	

5. Se o DNS não estiver instalado no sistema, o assistente fornecerá opções com as quais configurar o DNS. Escolha **Não, Apenas Instalar e Configurar DNS** neste computador. Clique em

Next.

tive Directory Installation Wizard		2
Install or Configure DNS You can configure or install Domain Namin	ig Service (DNS) on this computer.	R
Domain Naming Service (DNS) is not confi running on this network?	gured on this computer. Is DNS already	
Yes, I will configure the DNS client		
No, just install and configure DNS on the second	nis computer	
	< Back Next > Cance	el i

 Digite o nome DNS completo do novo domínio. Neste exemplo, Wireless.com é usado e clique em Avançar.

ive Directory Installation Wizard		
New Domain Name Specify a name for the new domain.		
Type the full DNS name for the new of (for example: headquarters.example.r	lomain nicrosoft.com).	
Wireless.com		

7. Insira o nome NETBIOS para o domínio e clique em Avançar. Este exemplo usa WIRELESS.

Active Directory Installation W	izard	×
NetBIOS Domain Name Specify a NetBIOS name for	r the new domain.	X
This is the name that users o domain. Click Next to accep	of earlier versions of Windows will use to identify the new t the name shown, or type a new name.	V
Domain NetBIOS name:	WIRELESS	
	< <u>B</u> ack <u>N</u> ext> 0	Cancel

8. Escolha o banco de dados e os locais de log para o domínio. Clique em Next.

Pirectory database and	d log files.
tore the database and	d the log on separate
ectory database?	
	B <u>r</u> owse
ectory log?	
	Browse
	virectory database and tore the database and ectory database? ectory log?

9. Escolha um local para a pasta Sysvol. Clique em Next.

hared System Volume Specify the folder to be shared as the system volume. The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.
The SYSVUL folder must be located on an NTFS volume.
Enter a location for the SYSVOL folder.
Eolder location:
C:\WINDOWS\SYSVOL Browse

10. Escolha as permissões padrão para os usuários e grupos. Clique em Next.

ve Dir	ectory Installation Wizard
Permi Se	ssions elect default permissions for user and group objects.
Sc sto	ome server programs, such as Windows NT Remote Access Service, read information pred on domain controllers.
۲	Permissions compatible with pre-Windows 2000 server operating systems Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.
	🗴 Anonymous users can read information on this domain.
0	Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems
	Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.
	< <u>B</u> ack <u>N</u> ext > Cancel

11. Defina a Senha do administrador e clique em **Avançar**.

Active Directory Installation Wizard
Directory Services Restore Mode Administrator Password This password is used when you start the computer in Directory Services Restore Mode.
Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.
Restore Mode Password:
Confirm password:
For more information about Directory Services Restore Mode, see <u>Active Directory Help</u> .
< <u>B</u> ack <u>N</u> ext > Cancel

12. Clique em **Avançar** para aceitar as opções de domínio definidas anteriormente.

You chose to: Configure this server as the first domain controller in a new forest of domain trees. The new domain name is Wireless.com. This is also the name of the new forest. The NetBIOS name of the domain is WIRELESS Database folder: C:WINDOWS\NTDS Log file folder: C:WINDOWS\NTDS SYSVOL folder: C:WINDOWS\SYSVOL The password of the new domain administrator will be the same as the password of the administrator of this computer.	um F	mary Review and confirm the options you selected.	
Configure this server as the first domain controller in a new forest of domain trees. The new domain name is Wireless.com. This is also the name of the new forest. The NetBIOS name of the domain is WIRELESS Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The password of the new domain administrator will be the same as the password of the administrator of this computer. To change an option, click Back. To begin the operation, click Next.	5	You chose to:	
 The new domain name is Wireless.com. This is also the name of the new forest. The NetBIOS name of the domain is WIRELESS Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The password of the new domain administrator will be the same as the password of the administrator of this computer. To change an option, click Back. To begin the operation, click Next. 	Ī	- Configure this server as the first domain controller in a new forest of domain trees.	
The NetBIOS name of the domain is WIRELESS Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The password of the new domain administrator will be the same as the password of the administrator of this computer. To change an option, click Back. To begin the operation, click Next.	-	The new domain name is Wireless.com. This is also the name of the new forest.	
Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The password of the new domain administrator will be the same as the password of the administrator of this computer.	-	The NetBIOS name of the domain is WIRELESS	
The password of the new domain administrator will be the same as the password of the administrator of this computer.		Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL	
To change an option, click Back. To begin the operation, click Next.	- t	The password of the new domain administrator will be the same as the password of he administrator of this computer.	
To change an option, click Back. To begin the operation, click Next.		*	
		o change an option, click Back. To begin the operation, click Next.	
		< Back Next > Cance	əl

 Clique em Concluir para fechar o Assistente de Instalação do Ative Diretory.



14. Reinicie o servidor para que as alterações tenham

ALU	re Directory Installation w	Izaru	
Wir Dire	ndows must be restarted before ectory Installation wizard take eff	the changes made by the Active fect.	•

Com esta etapa, você configurou o servidor Microsoft Windows 2003 como um controlador de domínio e criou um novo domínio **Wireless.com**. Em seguida, configure os serviços DHCP no servidor.

Instalar e configurar os serviços DHCP no Microsoft Windows 2003 Server

O serviço DHCP no servidor Microsoft 2003 é usado para fornecer endereços IP aos clientes Wireless. Para instalar e configurar os serviços DHCP neste servidor, siga estas etapas:

- 1. Clique em Adicionar ou remover programas no Painel de controle.
- 2. Clique em Adicionar/remover componentes do Windows.
- 3. Escolha Networking Services e clique em Details.
- 4. Escolha Dynamic Host Configuration Protocol (DHCP) e clique em

Networking Services	
To add or remove a component, click the c of the component will be installed. To see w	heck box. A shaded box means that only par what's included in a component, click Details.
Sub <u>c</u> omponents of Networking Services:	
🗹 📇 Domain Name System (DNS)	1.7 MB 🔄
🔽 县 Dynamic Host Configuration Protoc	ol (DHCP) 0.0 MB
🗌 🔲 🌉 Internet Authentication Service	0.0 MB
🗌 🗔 🚚 Remote Access Quarantine Service	e 0.1 MB
🔲 🔜 RPC over HTTP Proxy	0.0 MB
🗌 🗐 Simple TCP/IP Services	0.0 MB
🔲 🗆 🚚 Windows Internet Name Service (W	VINS) 0.9 MB 📘
Description: Sets up a DHCP server that addresses to client computer	automatically assigns temporary IP rs on the same network.
Total disk space required: 3.4 ME	3 Details
Space available on disk: 7224.5 ME	B Contraction
	OK Cancel

5. Clique em **Avançar** para instalar o serviço DHCP.

Ĩ
nat only nt, click
) MB 🔼
3 МВ 📃
ив
) МВ
MB
protocols.
alls

6. Clique em **Concluir para concluir a** instalação.



- 7. Para configurar os serviços DHCP, clique em **Start > Programs > Administrative tools** e clique no snap-in **DHCP**.
- 8. Escolha o servidor DHCP tsweb-lapt.wireless.com (neste exemplo).
- 9. Clique em **Action** e, em seguida, clique em **Authorize** para autorizar o serviço DHCP.



- Na árvore Console, clique com o botão direito do mouse em tsweb-lapt.wireless.com e, em seguida, clique em Novo escopo para definir um intervalo de endereços IP para os clientes Wireless.
- 11. Na página Bem-vindo ao Assistente de Novo Escopo do Assistente de Novo Escopo, clique em



12. Na página Nome do escopo, digite o nome do escopo DHCP. Neste exemplo, use DHCP-Clients como o nome do escopo. Clique em

N	ext
	ΟΛι.

New Scope Wizard	
Scope Name You have to pr providing a des	ovide an identifying scope name. You also have the option of cription.
Type a name a how the scope	nd description for this scope. This information helps you quickly identify is to be used on your network.
N <u>a</u> me:	DHCP-Clients
Description:	DHCP Server for Wireless Clients
	< <u>B</u> ack <u>N</u> ext > Cancel

13. Na página Intervalo de endereços IP, insira os endereços IP inicial e final do escopo e clique em

Avançar.

New Scope Wizard
IP Address Range You define the scope address range by identifying a set of consecutive IP addresses.
Enter the range of addresses that the scope distributes.
Start IP address: 10 . 77 . 244 . 218
End IP address: 10 . 77 . 244 . 219
A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.
Length: 8
S <u>u</u> bnet mask: 255 . 0 . 0 . 0
< <u>B</u> ack <u>N</u> ext > Cancel

 Na página Adicionar exclusões, mencione o endereço IP que você gostaria de reservar/excluir do escopo do DHCP. Clique em Next.

Type the IP address r address, type an add	ange that you want to exclu ress in Start IP address only	ide. If you want to exclude a single
<u>S</u> tart IP address:	End IP address:	
		Add
Excluded address ran	ige:	
		Remo <u>v</u> e

15. Mencione a duração da concessão na página Lease Duration e clique em **Next**.

New Scope	e Wizard
Lease Th sc	Duration le lease duration specifies how long a client can use an IP address from this ope.
Le coi poi Lik loc Se	ase durations should typically be equal to the average time the computer is nnected to the same physical network. For mobile networks that consist mainly of rtable computers or dial-up clients, shorter lease durations can be useful. ewise, for a stable network that consists mainly of desktop computers at fixed ations, longer lease durations are more appropriate. t the duration for scope leases when distributed by this server.
Lin	nited to:
<u>D</u> a 8	ys: H <u>o</u> urs: <u>M</u> inutes:
	< <u>B</u> ack <u>N</u> ext > Cancel

16. Na página Configure DHCP options (Configurar opções de DHCP), escolha Yes, I want to configure DHCP Option now (Sim, desejo configurar a opção de DHCP agora) e clique em Next

(Avançar).

Configure DHCP Options You have to configure the most common DHCP options before clients can use the scope. When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope. The settings you select here are for this scope and override settings configured in the Server Options folder for this server. Do you want to configure the DHCP options for this scope now? • Yes, I want to configure these options now! • Ng, I will configure these options later	w Scope Wizard	
 When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope. The settings you select here are for this scope and override settings configured in the Server Options folder for this server. Do you want to configure the DHCP options for this scope now? Yes, I want to configure these options now Ng, I will configure these options later 	Configure DHCP Options You have to configure the most common D scope.)HCP options before clients can use the
The settings you select here are for this scope and override settings configured in the Server Options folder for this server. Do you want to configure the DHCP options for this scope now? • Yes, I want to configure these options now? • No, I will configure these options later	When clients obtain an address, they are g addresses of routers (default gateways), D1 scope.	jiven DHCP options such as the IP NS servers, and WINS settings for that
Do you want to configure the DHCP options for this scope now? Yes, I want to configure these options now Ng, I will configure these options later	The settings you select here are for this sc Server Options folder for this server.	ope and override settings configured in the
 Yes, I want to configure these options now No, I will configure these options later 	Do you want to configure the DHCP option	is for this scope now?
No. I will configure these options later	Yes, I want to configure these options is	now
	O No, I will configure these options later	
< <u>B</u> ack <u>N</u> ext> Cancel		< <u>B</u> ack <u>N</u> ext > Cancel

17. Se houver um roteador de gateway padrão, mencione o endereço IP do roteador de gateway na página Roteador (gateway padrão) e clique em **Avançar**.

IP address:	or a router used by clients, enter the address belo	Ν.
	A <u>d</u> d	
10.77.244.220	<u>H</u> emove	
	Up	
	Down	

 Na página Nome do domínio e servidores DNS, digite o nome do domínio que foi configurado anteriormente. No exemplo, use Wireless.com. Insira o endereço IP do servidor. Clique em Add.

Domain Name and DNS Servers The Domain Name System (DNS) ma clients on your network.	aps and translates domain names	s used by
You can specify the parent domain you w DNS name resolution.	vant the client computers on your	network to use for
Parent do <u>m</u> ain: Wireless.com		
servers.		
<u>S</u> erver name:	I <u>P</u> address:	Add
<u>S</u> erver name: R <u>e</u> solve	IP address: · <td< td=""><td>A<u>d</u>d <u>H</u>emove</td></td<>	A <u>d</u> d <u>H</u> emove
<u>S</u> erver name: R <u>e</u> solve	P address:	A <u>d</u> d <u>R</u> emove
<u>S</u> erver name: Resolve	IP address: • <td< td=""><td>A<u>d</u>d <u>R</u>emove Up D<u>o</u>wn</td></td<>	A <u>d</u> d <u>R</u> emove Up D <u>o</u> wn

- 19. Clique em Next.
- 20. Na página Servidor WINS, clique em Avançar.
- 21. Na página Ativar escopo, escolha **Sim, desejo ativar o escopo agora** e clique em **Avançar**.

New Scope Wizard			
Activate Scope Clients can obtain address leases only if a s	cope is activated	ł.	₹ C
Do you want to activate this scope now?			
Yes, I want to activate this scope now			
C No, I will activate this scope later			
	< <u>B</u> ack	<u>N</u> ext >	Cancel

22. Ao concluir o Assistente de Novo Escopo, clique em **Concluir**.



23. Na janela Snap-in DHCP, verifique se o escopo DHCP que foi criado está

File Artiso View Linko				्राह्य २ (Dec
+ → <u>1</u> 1 × # 7 7 8 10 10 1	l op			
Фонор	towb-lapt.niceleos.com [10.77.244.2	17]		
B- Dissective interest control (10.77.244.217) (0.00) Second (127.16.0.0) [10.77.244.217]	Carteris al DHCP Server	2.8.15	Description	
Server Optione	Scape [172. 56.0.0] DHCP-Clients	** Artino **	DHCP Server for Wineless Clients	
🐮 Skart 🛛 🎉 Network Connections	Фонсь			

Agora que o DHCP/ DNS está habilitado no servidor, configure o servidor como um servidor de Autoridade de Certificação (CA) empresarial.

Instalar e Configurar o Microsoft Windows 2003 Server como um Servidor de

Autoridade de Certificação (CA)

O PEAP com EAP-MS-CHAPv2 valida o servidor RADIUS com base no certificado presente no servidor. Além disso, o certificado do servidor deve ser emitido por uma autoridade de certificação pública que seja confiável para o computador cliente (ou seja, o certificado público da autoridade de certificação pública já existe na pasta Autoridade de Certificação Raiz Confiável no repositório de certificados do computador cliente). Neste exemplo, configure o servidor Microsoft Windows 2003 como uma Autoridade de Certificação (CA) que emite o certificado para o Serviço de Autenticação da Internet (IAS).

Para instalar e configurar os serviços de certificado no servidor, siga estas etapas:

- 1. Clique em Adicionar ou remover programas no Painel de controle.
- 2. Clique em Adicionar/Remover componentes do Windows.
- 3. Clique em Certificate Services.

ows Components Wizard	
Vindows Components You can add or remove components of Windows.	
To add or remove a component, click the checkbox. A shade part of the component will be installed. To see what's included Details.	d box means that only I in a component, click
Components:	
🖉 📻 Accessories and Utilities	4.9 MB 🔺
🗹 🧃 Application Server	34.4 MB 💻
🗹 📴 Certificate Services	1.8 MB
🔲 🛄 E-mail Services	1.1 MB
Eax Services	7.9 MR 🔟
Description: Installs a certification authority (CA) to issue certif public key security programs.	icates for use with
Total disk space required: 13.8 MB	Detaile
Space available on disk: 7310.6 MB	
< <u>B</u> ack <u>N</u> ext>	Cancel Hel

4. Clique em Sim para a mensagem de aviso, Depois de instalar os serviços de certificado, o computador não poderá ser renomeado e não poderá ingressar nem ser removido de um domínio. Deseja continuar?

Microsof	t Certificate Services		
⚠	After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to C information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issued from the C Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?		
	Yes No		

5. Em Tipo de autoridade de certificação, escolha **CA raiz empresarial** e clique em **Avançar**.

dows Components Wizaı	۰d			
CA Type Select the type of CA yo	u want to set up).		Ē
Enterprise root CA				
C Enterprise subordinat	e CA			
C Stand-alone root CA				
C Stand-alone subordin	iate CA			
The most trusted CA in	an enterprise. S	ihould be installe	d before any other C	A.
Use custom settings	to generate the	key pair and CA	certificate	

 Insira um nome para identificar a autoridade de certificação. Este exemplo usa Wireless-CA. Clique em Next.

Common name for this C	A:		
Wireless-CA			
_ Distinguished name suff	ïx:		
DC=Wireless,DC=com			
Preview of distinguished	i name:		
CN=Wireless-CA,DC=V	/ireless,DC=com		
personal and a second sec			
 ⊻alidity period:		Expiration date:	

 Um diretório de "Log de Certificados" é criado para o armazenamento do banco de dados de certificados. Clique em Next.

idows components wizard	
Certificate Database Settings Enter locations for the certificate database, database log, and o information.	configuration
<u>C</u> ertificate database:	
C:\WINDOWS\system32\CertLog	Br <u>o</u> wse
Certificate <u>d</u> atabase log:	
C:\WINDOWS\system32\CertLog	Browse
Shared folder:	
	Province
	Biowse
	Browse
Preserve existing certificate database	Biowse
Preserve existing certificate database	Blowse
Preserve existing certificate database	Browse

8. Se o IIS estiver habilitado, ele deverá ser interrompido antes que você continue. Clique em OK para exibir a mensagem de aviso de que o IIS deve ser interrompido. Ele é reiniciado automaticamente após a instalação do



9. Clique em **Concluir** para concluir a instalação dos serviços da Autoridade de certificação (CA).



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

Conectar clientes ao domínio

A próxima etapa é conectar os clientes à rede com fio e baixar as informações específicas do domínio do novo domínio. Em outras palavras, conecte os clientes ao domínio. Para isso, conclua essas etapas:

- 1. Conecte os clientes à rede com fio com um cabo Ethernet direto.
- 2. Inicialize o cliente e faça login com o nome de usuário/senha do cliente.
- 3. Clique em Iniciar; clique em Executar; digite cmd; e clique em OK.
- 4. No prompt de comando, digite **ipconfig** e clique em **Enter** para verificar se o DHCP funciona corretamente e se o cliente recebeu um endereço IP do servidor DHCP.
- 5. Para unir o cliente ao domínio, clique com o botão direito do mouse em **Meu computador** e escolha **Propriedades**.
- 6. Clique na guia Nome do computador.
- 7. Clique em Alterar.
- 8. Clique em Domain; digite wireless.com; e clique em
| | | | ? |
|---|----------------------------------|---------------------------|------------------------|
| You can change the
computer. Changes n | name and the r
ay affect acce | nembership
ss to netwo | of this
rk resource |
| Computer name: | | | |
| Client1 | | | |
| Member of
Omain: | | | More |
| Wireless | | | |
| | | | |
| 🔘 Workgroup: | | | |

9. Digite **Username Administrator** e a senha específica do domínio ao qual o cliente ingressa. (Esta é a conta de administrador no Ative Diretory no





- 10. Click **OK**.
- 11. Clique em Sim para reiniciar o computador.
- Quando o computador for reiniciado, faça login com estas informações: Nome de usuário = Administrador; Senha = <senha do domínio>; Domínio = Sem fio.
- 13. Clique com o botão direito do mouse em Meu computador e clique em Propriedades.
- 14. Clique na guia Nome do computador para verificar se você está no domínio

Wireless.com.

System Properties			? 🔀
System Restore	Autom	atic Updates	Remote
General Com	puter Name	Hardware	Advanced
Windows uses on the network	s the following in K.	nformation to identify ;	your computer
Computer <u>d</u> escription:			
	For example: Computer''.	"Kitchen Computer" o	or ''Mary's
Full computer name:	Client1.Wirele	ss.com	
Domain:	Wireless.com		
To use the Network Ider domain and create a loc ID.	ntification Wizar al user account	d to join a , click Network	<u>N</u> etwork ID
To rename this compute	r or join a domai	n, click Change. 🛛	<u>C</u> hange
🔥 Changes will take (effect after you	restart this computer. K Cancel	Apply

- 15. A próxima etapa é verificar se o cliente recebeu o certificado CA (confiança) do servidor.
- 16. Clique em Iniciar; clique em Executar; digite mmc e clique em OK.
- 17. Clique em File e clique em Add/Remove snap-

Use this pag	ge to add	d or remove a standalone Snap-in from the console.	
Snap-ins ad	ded to:	🔁 Console Root 💌	
- Descriptio	n		
- Descriptio	n		

- 18. Clique em Add.
- 19. Escolha **Certificate** e clique em

Snap-in	Vendor
🌉 .NET Framework 1.1 Configuration	Microsoft Corporation
🗯 ActiveX Control	Microsoft Corporation
🐻 Certificates	Microsoft Corporation
🙆 Component Services	Microsoft Corporation
📕 Computer Management	Microsoft Corporation
颶 Device Manager	Microsoft Corporation
💕 Disk Defragmenter	Microsoft Corp, Executi
👑 Disk Management	Microsoft and VERITAS
🔟 Event Viewer	Microsoft Corporation
🛄 Folder	Microsoft Corporation
Description The Certificates snap-in allows you to bro certificate stores for yourself, a service, o	wse the contents of the r a computer.

20. Escolha Computer Account e clique em Next.

Certificates snap-in		×
This snap-in will always manage certificates for:		
O My user account		
 Service account 		
 Computer account 		
	< Back Next > Cancel]

21. Clique em **Concluir** para aceitar o computador local padrão.

this console is running	on)	
		Browse
isole.	-	
r r	r this console is running be changed when lau nsole.	r this console is running on) be changed when launching from the comman nsole.

22. Clique em **Fechar** e em **OK**.

23. Expanda Certificados (Computador Local); expanda Autoridades de Certificação Raiz Confiáveis; e clique em Certificados. Localize Wireless na

Console1 - [Console Root/Certific	ates (Local Computer)\Trusted R	oot Certification Authorities/Cer	tificates]			1 🛛 🔀
E File Action View Favorites Wind	low Help					_ Cose
⇔→ 🖻 🖭 🎗 🗞 🗙 🗗 🖫	l 🕼					
Console Root	Issued To /	Issued By	Espiration Date	Intended Purposes	Friendly Name	Stats A
🖻 🗐 Certificates (Local Computer)	SERVICIOS DE CERTIFICACION	SERVICIOS DE CERTIFICACION - A	3/10/2009	Secure Email, Server	SERVICIOS DE CERT	
🗄 🔤 Personal	SIA Secure Client CA	51A Secure Client CA	7/9/2019	Secure Email, Server	Societa Interbancari	
E - M Trusted Root Certification Author	SIA Secure Server CA	SIA Secure Server CA	7/9/2019	Secure Email, Server	Societa Interbancari	
Certificates	Seetsskey Root CA	Swisskey Root CA	1/1/2016	Secure Email, Server	Swisskey Root CA	
H Enterprise Trust	Symantec Root CA	Symantec Root CA	5/1/2011	<al></al>	<none></none>	
Intermediate Certification Author	TC TrustCenter Class I CA	TC TrustCenter Class 1 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
R. M Linksustad Castificatae	TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
H-100 Third-Party Root Certification Au	TC TrustCenter Class 3 CA	TC TrustCenter Class 3 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
H- Insted People	TC TrustCenter Class 4 CA	TC TrustCenter Class 4 CA	1/1/2011	Secure Email, Server	TC TrustCenter Clas	
H-M SPC	TC TrustCenter Time Stamping CA	TC TrustCenter Time Stamping CA	1/1/2011	Time Stamping	TC TrustCenter Time	
	Thavte Personal Basic CA	Thavite Personal Basic CA	1/1/2021	Client Authentication	Thawte Personal Bas	
	Thavte Personal Freemail CA	Thavite Personal Freemail CA	1/1/2021	Client Authentication	Thawte Personal Pre	
	Thavte Personal Premium CA	Thavite Personal Premium CA	1/1/2021	Client Authentication	Thavke Personal Pre	
	Thavte Premium Server CA	Thavite Premium Server CA	1/1/2021	Server Authenticatio	Thawte Premium Ser	
	Thavte Server CA	Thavite Server CA	1/1/2021	Server Authenticatio	Thanke Server CA	
	Thavte Timestamping CA	Thavte Timestamping CA	1/1/2021	Time Stamping	Thavke Timestampin	
	UTN - DATACorp 5GC	UTN - DATACorp SGC	6/25/2019	Server Authentication	UTN - DATACorp SGC	
	UTN-USERFirst-Client Authenticati	UTN-USERFirst-Client Authentication	7/9/2019	Secure Email	UTN - USERFirst-Clie	
	UTN-USERFirst-Hardware	UTN-USER/First-Hardware	7/9/2019	Server Authentication	UTN - USER Pirst-Har	
	UTN-USERFirst-Network Applications	UTN-USERFirst-Network Applications	7/10/2019	Secure Email, Server	UTN - USERFirst-Net	
	UTN-USERFirst-Object	UTN-USER/First-Object	7/10/2019	Time Stamping, Code	UTN - USERFirst-Object	
	WeriSign Commercial Software Publ	VeriSign Commercial Software Publis	12/31/1999	Secure Email, Code S	VeriSign Commercial	
	WeriSign Commercial Software Publ	VeriSign Commercial Software Publis	1/8/2004	Secure Email, Code S	VeriSign Commercial	
	WeriSign Individual Software Publis	VeriSign Individual Software Publishe	12/31/1999	Secure Email, Code S	VeriSign Individual 5	
	WeriSign Individual Software Publis	VeriSign Individual Software Publishe	1/8/2004	Secure Email, Code S	VeriSign Individual S	
	VeriSign Trust Network	Vertigen Trust Network	5/19/2018	Secure Enail, Clent	Veri5ign Class 2 Prim	
	WeriSign Trust Network	VeriSign Trust Network	8/2/2028	Secure Email, Client	VeriSign Class 2 Prim	
	WeriSign Trust Network	Verbign Trust Network	5/19/2018	Secure Enal, Clent	Veri5ign Class 3 Prim	
	VeriSign Trust Network	VeriSion Trust Network	8/2/2028	Secure Email, Client	VeriSign Class 3 Prim	
	VeriSign Trust Network	VeriSign Trust Network	5/19/2018	Secure Enail, Clent	VeriSign Class 4 Prim	
	VeriSign Trust Network	VeriSion Trust Network	8/2/2028	Secure Email, Client	VeriSign Class 1 Prim	
	VeriSign Trust Network	VeriSion Trust Network	8/2/2028	Secure Email, Clent	VeriSign Class 4 Prim	
	VeriSign Trust Network	VeriSion Trust Network	5/19/2018	Secure Email, Client	VeriSign Class 1 Prim	
	Wreless-CA	Wireless-CA	12/17/2012	<al></al>	<hkne></hkne>	
	Excert EZ by DST	Xcert EZ by DST	7/11/2009	Secure Email, Server	Xcert EZ by DST	~
<i></i>	<					>
rusted Root Certification Authorities store cor	ntains 109 certificates.					
Start Te Constiet - [Const				0.1	400000	2:42 PM

24. Repita este procedimento para adicionar mais clientes ao domínio.

Instale o Internet Authentication Service no Microsoft Windows 2003 Server e Solicite um Certificado

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

Conclua estas etapas para instalar e configurar o IAS no servidor.

- 1. Clique em Adicionar ou remover programas no Painel de controle.
- 2. Clique em Adicionar/remover componentes do Windows.
- 3. Escolha Networking Services e clique em Details.
- 4. Selecione Internet Authentication Service; clique em OK; e clique em

or the compt	onent will be inst	alled. To see what's	included in a compon	ient, click D
Sub <u>c</u> ompone	ents of Networki	ng Services:		
🗹 🚚 Dom	ain Name Syster	m (DNS)		1.7 M
🗹 🚚 Dyn	amic Host Config	juration Protocol (DH	ICP)	0.0 M
🗹 畏 Inter	net Authenticatio	on Service		0.0 M
🗆 🚚 Rem	ote Access Qua	rantine Service		0.1 M
🗆 🚚 RPC	over HTTP Pro	ху		0.0 M
🗆 🚚 Simp	le TCP/IP Servi	ces		0.0 M
🗆 🚚 Win	dows Internet Na	ame Service (WINS)		0.9 N
Description:	Enables authe users, IAS sup	entication, authorizat oports the RADIUS p	ion and accounting of rotocol.	f dial-up and
Total disk sp	ace required:	3.4 MB		Deta
C 1	able on disk:	7208 2 MB		

5. Clique em **Concluir** para concluir a instalação do IAS.

Windows Components Wizard		×
	Completing the Windows Components Wizard You have successfully completed the Windows Components Wizard.	
	To close this wizard, click Finish.	
	K Back Finish He	alp

- 6. A próxima etapa é instalar o certificado do computador para o IAS (Internet Authentication Service).
- 7. Clique em **Iniciar**; clique em **Executar**; digite **mmc**; e clique em **OK**

UK.						
Tonsole1 - [Conso	ée Root j					
Si Gle Action Se	w Favgites Window Help					-@×
* + I B						
Canacle Roak	Norez					
				There are no items to sh	ove in this view.	
2 Start 6	Network Connections	Dava .	A dramant - 10462.15	WED	in Presslet - fresslet	
	1-2	and also		and all and a second se	Construct	a second to construct the

- 8. Clique em **Console** no menu Arquivo e escolha o snap-in **Adicionar/Remover**.
- 9. Clique em Adicionar para adicionar um snap-

d/Remove Snap-i	n	?
Standalone Extensi	ons	
Use this page to ad	d or remove a stand-alone sna	p-in from the console.
Snap-ins added to:	Console Root	
		1
Description		
Description		
Description	numera de atract	
A <u>d</u> d	<u>R</u> emove A <u>b</u> out]

10. Escolha **Certificados** na lista de snap-ins e clique em

Snap-in	Vendor
🍇 .NET Framework 1.1 Configuration	Microsoft Corporation
Bactive Directory Domains and Trusts	Microsoft Corporatio
📓 Active Directory Sites and Services 🛛	Microsoft Corporatio
Active Directory Users and Compu	Microsoft Corporatio
📺 ActiveX Control	Microsoft Corporatio
🚭 ADSI Edit	Microsoft Corporatio
🚰 Authorization Manager	Microsoft Corporatio
Certificate Templates	Microsoft Corporatio
Certificates	Microsoft Corporatio
Certification Authority	Microsoft Corporatio
Description The Certificates snap-in allows you to br certificate stores for yourself, a service,	owse the contents of t or a computer.

11. Escolha **Conta do computador** e clique em **Avançar**.

ertificates snap-in			×
This snap-in will always manage certificates for:			
C My user account			
C Service account			
Computer account			
	< <u>B</u> ack	<u>N</u> ext>	Cancel

12. Escolha Computador local e clique em

Concluir.		
Select Computer		×
Select the computer you want This snap-in will always man	: this snap-in to manage. lage:	1
Local computer: (the c	omputer this console is running on)	
Allo <u>w</u> the selected corr only applies if you save	puter to be changed when launching from the command line. This the console.	
]
	< <u>B</u> ack Finish Cancel	

13. Clique em **Fechar** e em **OK**.

14. Expanda Certificados (Computador Local); clique com o botão direito do mouse em Pasta Pessoal; escolha Todas as tarefas e, em seguida, Solicitar Novo

15. Clique em Avançar em *Bem-vindo ao Assistente de Solicitação de Certificado*.



16. Escolha o modelo de certificado do Controlador de Domínio (se você solicitar um certificado

de computador em um servidor que não seja o DC, escolha um modelo de certificado do **Computador**) e clique em

Avançar.

Certificate Request Wizard	×
Certificate Types	
A certificate type contains preset properties for certificates.	
Select a certificate type for your request. You can access only certificate types that you have permissions for and that are available from a trusted CA.	
<u>C</u> ertificate types:	
Directory Email Replication Domain Controller Domain Controller Authentication	
To select a cryptographic service provider and a CA, select Advanced.	
< <u>B</u> ack <u>N</u> ext > Cancel	

17. Digite um nome e uma descrição para o certificado.

ertificate Friendly Name and Desc	ription	
You can provide a name and des certificate.	scription that help you quickly identify a spe	ecific
Type a friendly name and descrip	ption for the new certificate.	
Friendly name:		
PEAP-Wireless		
) Description:		
IAS Server Certificate - 802.1x	Authentication	
9		

 18. Clique em Concluir para concluir o assistente de solicitação de certificação.



Configurar o serviço de autenticação da Internet para a autenticação PEAP-MS-CHAP v2

Agora que você instalou e solicitou um certificado para o IAS, configure o IAS para autenticação.

Conclua estes passos:

- 1. Clique em Iniciar > Programas > Ferramentas Administrativas e clique em Internet Authentication Service snap-in.
- Clique com o botão direito do mouse em Internet Authentication Service (IAS) e clique em Register Service in Ative Diretory.

Event Advertised of the server of the s	
Kiterret Autoecologion Service and it By Piter Access Degine Connection Request Process Year Y	
	rea to Inferrent Authentication Envice reaction Service (IAS) to authentication survive, authorized, authentication Diakin User Service (IAZOLIS). to read the remote access properties of user accounts in Addre Directory, and the Addre Service (IAZOLIS). to read the remote access properties of user accounts in Addre Directory, and the Addre Service (IAZOLIS). to read the remote access properties of user accounts in Addre Directory, and the Addre Service (IAZOLIS). to read the remote access properties of user accounts in Addre Directory, and the Addre Directory, and the Addre Directory. this addres setting up 1455, deployment scenarios, and troubleshapting, see Help.
Register Server in Active Devictory Register Server in Active Devictory Register Server in Active Devictory Register Server in Active Devictory Register Server in Active Devictory Register Server in Active Devictory Register Server in Active Devictory Register Server in Active Devictory Register Server in Active Devictory Register Server in Active Devictory Register Server in Active Devictory Register Server in Active Device in Active Devictory Register Server in Active Device in	Disco Anargat - Dis2/15/05 Statement Asthewitkette

3. A caixa de diálogo Registrar Internet Authentication Service no Ative Diretory é exibida; clique em OK. Isso permite que o IAS autentique usuários no Ative Diretory.

Register Internet Authentication Server in Active Directory:	×
To enable IAS to authenticate users in the Active Directory, the computers running	g IAS must be authorized to read users' dial-in properties from the domain.
Do you wish to authorize this computer to read users' dial-in-properties from the V	Mreless.com domain?
ОК	Cancel

4. Clique em \mathbf{OK} na próxima caixa de

diálog Server r	0. egistered:
4	This computer is now authorized to read users' dial-in properties from domain Wireless.com. To authorize this computer to read users' dial-in properties from other domains, you must register this computer to be a member of the RAS/IAS Servers Group in that domain.
	OK

- 5. Adicione o Wireless LAN Controller como um cliente AAA no servidor MS IAS.
- 6. Clique com o botão direito do mouse em RADIUS Clients e escolha New RADIUS Client.

🖗 Internet Authentication Service			18X
Elle Action View Linkp			
◆ → 🖪 🗄 🕄 😫 🖪			
Internet Authentication Service (Local) Internet Authentication Service (Local) <t< th=""><th>Maree Connections to Microsoft Routing and Resolute 1</th><th></th><th></th></t<>	Maree Connections to Microsoft Routing and Resolute 1		
New Clerk	Divers (there is a second		
Rentwork Contractions	A grander - [new town	The second without any second	

7. Digite o nome do cliente (WLC nesse caso) e insira o endereço IP da WLC. Clique em Next.

	Deknerarni Address or Ding na	ame for the client.
Eriendly name:	WLC	
Client a <u>d</u> dress (IP or DNS	6):	
10.77.244.210		⊻erify

- 8. Na próxima página, em Client-Vendor, escolha **RADIUS Standard**; insira o segredo compartilhado e clique em **Finish**.
- 9. Observe que a WLC é adicionada como um cliente AAA no

CH Lot Lo
 In the rel Aufletitation Service (Lack) Interde Access Logger) Encode Access Degres Correction Regast Phonesing
Prends Huffertication Service (Local) Prends Harer / Kabreso Prends Horeso Local) Prends Horeso Local Prends Horeso Horeso Prends Horeso Local Prends Horeso Horeso Prends Horeso Local P

- 10. Crie uma política de acesso remoto para os clientes.
- 11. Para fazer isso, clique com o botão direito do mouse em **Remote Access Policies** e escolha **New Remote Access**

Policy.				
🐓 Internet Authentie	ation Service			
Ele Action Yern	ump			
* > 1 1				
Ein Artism View	Helpo 1 12 199 191 ion Service (Local) Opping Mark Permote Access Bolicy Mark Per	Mane Connections to Microsoft Routing and Peerute Connections to other access servers	Order 2	
🧶 Start 🛛 🏉	Network Connections	Dava Adaran	t-[DH2]12WID Platemet Authenticati	🔍 🕈 💽 💓 👯 🔽 INTERM

 Digite um nome para a política de acesso remoto. Neste exemplo, use o nome PEAP. Em seguida, clique em Avançar.

ew Remote Acce	ss Policy Wizard
Policy Configu The wizard o	ration Method an create a typical policy, or you can create a custom policy.
How do you v	vant to set up this policy?
Use the	e wizard to set up a typical policy for a common scenario
C Set up	a custom policy
Policy name:	PEAP-Wireless
	Example: Authenticate all VPN connections.
	≺ <u>B</u> ack <u>N</u> ext> Cancel

13. Escolha os atributos da política com base em seus requisitos. Neste exemplo, escolha **Wireless**.

		×
Access Method Policy conditions are based on the metho	d used to gain access to the network.	ŷ
Select the method of access for which you	want to create a policy.	
Use for all VPN connections. To creat previous page, and select Set up a c	ate a policy for a specific VPN type, go ba sustom policy.	ack to the
◯ <u>D</u> ial-up		
Use for dial-up connections that use Digital Network (ISDN) line.	a traditional phone line or an Integrated 9	Services
Use for wireless LAN connections on	ıly.	
C Ethernet		
Use for Ethernet connections, such a	as connections that use a switch.	

14. Na próxima página, escolha **Usuário** para aplicar esta política de acesso remoto à lista de usuários.

w Remote Access Policy Wizard	
User or Group Access You can grant access to individual users, or you can grant access to select groups.	ed 🕅
Grant access based on the following: User User access permissions are specified in the user account.	
 <u>Group</u> Individual user permissions override group permissions. Group name: 	
	A <u>d</u> d
	<u>R</u> emove
< <u>B</u> ack <u>N</u> ext >	Cancel

15. Em Authentication Methods, escolha **Protected EAP (PEAP)** e clique em **Configure**.

New Remote Access Policy Wizard		×
Authentication Methods EAP uses different types of security device	es to authenticate users.	ŷ
Select the EAP type for this policy.		
<u>T</u> ype:		
Protected EAP (PEAP)	•	Configure
	< <u>B</u> ack <u>N</u> ext	> Cancel

16. Na página **Protected EAP Properties**, escolha o certificado apropriado no menu suspenso Certificate Issued e clique em

Protected EAP Prop	erties			2		
This server identifies Select the certificate	itself to ca that you v	allers before the conr want it to use as proc	nection is comp of of identity.	leted.		
Certificate issued	ts	web-lapt.Wireless.co	m			
Friendly name:	PE/	PEAP-Wireless				
Issuer:	Wir	Wireless-CA				
Expiration date:	12/	12/16/2008 5:53:02 PM				
🔲 Enable Fast Reco	onnect					
Eap Types						
Secured password (EAP-MSCH	AP v2)		Move Up		
				Move <u>D</u> ow		
Add	<u>E</u> dit	Remove	ОК	Cancel		

17. Verifique os detalhes da política de acesso remoto e clique em **Finish**.

New Remote Access Policy Wizard



X

18. A política de acesso remoto foi adicionada à



 Clique com o botão direito do mouse na diretiva e clique em Propriedades. Escolha "Conceder permissão de acesso remoto" em "Se uma solicitação de conexão corresponder às condições

PEAP Properties	<u>?</u> ×
Settings	
Specify the conditions that c	connection requests must match.
Policy <u>c</u> onditions:	
NAS-Port-Type matches "W	Vireless - Other OR Wireless - IEEE 802.11''
Add Fdit	
If connection requests match	h the conditions specified in this policy, the
associated profile will be app	plied to the connection.
Edit Profile	
Unless individual access per policy controls access to the	rmissions are specified in the user profile, this entry of the second second second second second second second
If a connection request mate	ches the specified conditions:
C Deny remote access per	rmission
• <u>G</u> rant remote access per	rmission

Adicionar usuários ao Ative Diretory

Nessa configuração, o banco de dados do usuário é mantido no Ative Diretory.

Para adicionar usuários ao banco de dados do Ative Diretory, siga estas etapas:

 Na árvore do console Ative Diretory Users and Computers, clique com o botão direito do mouse em Users, clique em New e clique em User.



 Na caixa de diálogo New Object - User (Novo objeto - Usuário), digite o nome do usuário sem fio. Este exemplo usa o nome WirelessUser no campo Nome e WirelessUser no campo Nome de logon do usuário. Clique em

Eirst name:	Client 1		Initials:	
Last name:				
Full name:	Client 1	Client 1		
User logon name	e:			
Client1		@Wireless	.com	-
User logon name	e (pre- <u>W</u> indows)	2000):		
WIBELESS\		Client1		

3. Na caixa de diálogo Novo objeto - usuário, digite uma senha de sua escolha nos campos Senha e Confirmar senha. Desmarque a caixa de seleção O usuário deve alterar a senha no próximo logon e clique em

Password:	•••••	-
<u>C</u> onfirm password:	•••••	
User must chang	ge password at next logon	
User cannot cha	ange password	
Pass <u>w</u> ord never	expires	
Account is disab	oled	

Avançar

4. Na caixa de diálogo Novo objeto - usuário, clique em



5. Repita as etapas de 2 a 4 para criar contas de usuário adicionais.

Permitir acesso sem fio aos usuários

Conclua estes passos:

- Na árvore do console Usuários e computadores do Ative Diretory, clique na pasta Usuários; clique com o botão direito do mouse em WirelessUser; clique em Propriedades; e vá para a guia Discar.
- 2. Escolha Permitir acesso e clique em

eneral Address Account	Profile Telephones Organizati
Member Ut Diami	Environment Sessions
Remote Access Permission (Dial-ir	n or VPNJ
Allow access	
Deny access	
C Control access through Remot	e Access <u>P</u> olicy
Verify Caller-ID:	
Callback Options	1
No Callback	
Set by Caller (Routing and Rer	note Access Service only)
C Always Callback to:	
Assign a Static IP Address	
Apply Static <u>R</u> outes)
Define routes to enable for this D connection.	ial-in Static Ro <u>u</u> tes

Configurar a controladora Wireless LAN e APs leves

Agora, configure os dispositivos Wireless para essa configuração. Isso inclui a configuração de controladores de LAN sem fio, APs leves e clientes sem fio.

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

Primeiro configure o WLC para usar o MS IAS como o servidor de autenticação. A WLC precisa ser configurada para encaminhar as credenciais do usuário a um servidor RADIUS externo. O servidor RADIUS externo valida as credenciais do usuário e fornece acesso aos clientes Wireless. Para fazer isso, adicione o servidor MS IAS como um servidor RADIUS na página **Segurança > Autenticação RADIUS**.

Conclua estes passos:

 Escolha Security e RADIUS Authentication na GUI da controladora para exibir a página RADIUS Authentication Servers. Em seguida, clique em New para definir um servidor RADIUS.

3 · 🛇 · 🖻 🖻	🚯 🔎 🛠 🛛 🙆 🛬	· 🖂 🚳					ar
C. STETENS	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	Save C COMMANDS	onfiguration Fing HELP	Logout Ref
ecurity	RADIUS Authentication Se	rvers > New				< Back	Apply
AA General	Server Index (Priority)	1 💌					
RADIUS Authentication RADIUS Accounting Local Net Users	Server IPAddress	10.77.244.198					
MAC Filtering Disabled Clients User Login Policies	Shared Secret Format	ASCII 💌					
AP Policies	Shared Secret	•••••					
ccess Control Lists PSec Certificates	Confirm Shared Secret	•••••					
ID Certificate	Key Wrap						
Vireless Protection Policies	Port Number	1812					
Trusted AP Policies Rogue Policies Standard Signatures	Server Status	Enabled 💌					
Custom Signatures Client Exclusion Policies	Support for RFC 3576	Enabled 💌					
AP ROCIENCEDURI	Retransmit Timeout	2 seconds					
	Network User	Enable					
	Management	Enable Enable					
	IPSec	🔄 Enable					

2. Defina os parâmetros do servidor RADIUS na página Servidores de autenticação RADIUS > Novo. Esses parâmetros incluem o endereço IP do servidor RADIUS, o segredo compartilhado, o número da porta e o status do servidor. As caixas de seleção Network User and Management determinam se a autenticação baseada em RADIUS se aplica a usuários de gerenciamento e de rede. Este exemplo usa o MS IAS como o servidor RADIUS com o endereço IP

10.77.244.198.

3 · 0 🖻	6 P 📩	<i>€</i> ⊜.	200	8				1	1 - 8
ince Speccus	MONITOR	WLANS CO	ONTROLLER	WIRELESS 5	ECURITY	MANAGEMENT C	Save Configuratio OMMANDS HELP	n Ping Loga	out Refre
Security	RADIUS AU	thentication	n Servers				A	oply New	P
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies	Call Station Credential Use AES Ke	n ID Type s Caching ey Wrap	IP Address	×					
Access Control Lists	Network Nuser	fanagement	Server Index	Server Address	Port	IPSec	Admin Status		
IPSec Certificates CA Certificate ID Certificate Web Auth Certificate	2	V	1	10.77.244.198	1812	Disabled	Enabled	Edit Remov	e Eina
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Client Exclusion Policies AP Authentication									

- 3. Clique em Apply.
- 4. O servidor MS IAS foi adicionado à WLC como um servidor Radius e pode ser usado para autenticar clientes Wireless.

Configurar uma WLAN para os clientes

Configure o SSID (WLAN) ao qual os clientes Wireless se conectam. Neste exemplo, crie o SSID e nomeie-o como **PEAP**.

Defina a Autenticação da Camada 2 como WPA2 para que os clientes executem a autenticação baseada em EAP (PEAP-MSCHAPv2 neste caso) e usem AES como o mecanismo de criptografia. Deixe todos os outros valores em seus padrões.

Observação: este documento vincula a WLAN às interfaces de gerenciamento. Quando há várias VLANs na rede, você pode criar uma VLAN separada e vinculá-la ao SSID. Para obter informações sobre como configurar VLANs em WLCs, consulte <u>Exemplo de Configuração de</u> <u>VLANs em Wireless LAN Controllers</u>.

Para configurar uma WLAN na WLC, siga estes passos:

- 1. Clique em **WLANs** na GUI do controlador para exibir a página WLANs. Esta página lista as WLANs que existem na controladora.
- Escolha New para criar uma nova WLAN. Insira o ID da WLAN e o SSID da WLAN para a WLAN e clique em Apply.

3 · 0 · 🖹 🖻	0 0 2 2 0 6)• 🍓 🖂 🚳					🦓 – 8 ×
Disca Sestems	MONITOR WEANS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT	Save C	nfiguration (Ping) HELP	Logout Retresh
WLANs	WLANs > New					< Back	Apply
WLANS WLANS AP Groups VLAN	WLAN ID WLAN SSID	1 M					

 Quando você criar uma nova WLAN, a página WLAN > Edit da nova WLAN será exibida. Nesta página você pode definir vários parâmetros específicos para esta WLAN que incluem Políticas Gerais, Servidores RADIUS, Políticas de Segurança e Parâmetros 802.1x.

002.17.								
Luce Status					Save Co	nfiguration Ping	Logout Refr	
official designs	MONITOR WLANS CO	ONTROLLER WIRELESS	SECURITY I	MANAGEMENT	COMMANDS	HELP		
WLANs	WLANs > Edit					< Back	Apply	
WLANS WLANS AP Groups VLAN	WLAN ID	1						
	Profile Name	PEAP						
	WLAN SSID	PEAP						
	General Policies				Security Polici	es		
	Radio Policy	All			1Pv6 Enable			
	Admin Status	✓ Enabled						
	Session Timeout (secs)	0			Layer 2 Securit	WPA1+W	PA2 💌	
	Quality of Service (QoS)	Silver (best effort)				MAC Fik	ering	
	WMM Policy	Disabled 💌			Laver 3 Securit	v None		
	7920 Phone Support	Client CAC Limit CAP	CAC Limit			E Web Bol	ing •	
	Broadcast SSID	T Enabled					(a)	
	Aironet IE	✓ Enabled						
	Allow AAA Override	Enabled			* Web Policy of	annot be used in co	mbination with	
	Client Exclusion	Enabled ** 60			## When client	austurian is anable	d a time of	
	DHCP Server	Timeout Value (secs)		value of zero means infinity(will require administrative override to reset excluded clients				
	DHCP Addr. Assignment	Required			*** CKIP is not	t supported by 10x	x APs	
	Interface Name	management 💌						
	MFP Version Required	1						
	MFP Signature Generation	Global MPP Disabled)						
	H-REAP Local Switching							
	* H-REAP Local Switching authentications.	g not supported with IPSEC, (CRANITE and PO	RTRESS				

- 4. Verifique **Admin Status** em General Policies para habilitar a WLAN. Se você quiser que o AP transmita o SSID em seus quadros beacon, marque **Broadcast SSID**.
- 5. Em Layer 2 Security, selecione WPA1+WPA2. Isso ativa a WPA na WLAN. Role para baixo na página e escolha a política WPA. Este exemplo usa a criptografia WPA2 e AES. Escolha o servidor RADIUS apropriado no menu suspenso em Servidores RADIUS. Neste exemplo, use 10.77.244.198 (endereço IP do servidor MS IAS). Os outros parâmetros podem ser modificados com base no requisito da rede

	WLAN.									
	Cinco Station						Save O	onfiguration Ping	Logout R	efresh
	As As	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
	WLANS	WPA1+WPA2 Parameters			-					*
	WLANS WLANS AP Groups VLAN	WPA1 Policy WPA2 Policy WPA2 Encryption	⊡ IZ IZ AES	Пткір						
		Auth Key Mgmt	802.1x	¥.						
		ID D								
6.	Clique em									
	Apply.									
	Cince Stations						Save C	onfiguration Ping	Logout R	efresh
	.A. A.	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
	WLANs	WLANS								1
	WLANS WLANS	Profile Name	W 10	LAN WLANS	SID	A.c St	lmin Secur	rity Policies		
	AP Groups VLAN	PEAP	1	PEAP		En	abled [WPA	2][Auth(802.1x)]	Es	8 Rem

Configurar os clientes sem fio

Configurar os clientes sem fio para a autenticação PEAP-MS CHAPv2

Este exemplo fornece informações sobre como configurar o cliente Wireless com o Cisco Aironet Desktop Utility. Antes de configurar o adaptador cliente, certifique-se de que a versão mais recente do firmware e do utilitário seja usada. Encontre a versão mais recente do firmware e dos utilitários na página Wireless downloads (Downloads sem fio) em Cisco.com.

Para configurar o adaptador cliente Wireless Cisco Aironet 802.11 a/b/g com o ADU, siga estas etapas:

- 1. Abra o Aironet Desktop Utility.
- 2. Clique em Gerenciamento de perfil e clique em Novo para definir um perfil.
- Na guia General (Geral), insira o Profile name (Nome do perfil) e o SSID (SSID). Neste exemplo, use o SSID que você configurou no WLC (PEAP).

Profile Management		? 🔀
General Security Advanc	ed	
Profile Settings Profile Name: Client Name:	PEAP-MSCHAPv2 CLIENT1	
Network Names	fact ind	
SSID1:	PEAP	
SSID2:		
SSID3:		
		Cancel

4. Escolha a guia Security; escolha **WPA/WPA2/CCKM**; em WPA/WPA2/CCKM EAP, digite **PEAP [EAP-MSCHAPv2]** e clique em **Configure**.

Profile Management	n a han an a	? 🗙
General Security Advanced		
- Set Security Options		
⊙ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type: FEAP (EAP-MSCHAP V2)	
○ WPA/WPA2 Passphrase		
Ø 802.1x	802.1x EAP Type: EAP-FAST	
O Pre-Shared Key (Static WEP)		
O None		
Configure	Allow Association to Mixed Cells	
	Limit Time for Finding Domain Controller To: 0 0 sec	
Group Policy Delay:	60 🗘 sec	
	ОК С	ancel

5. Escolha Validate Server Certificate e Wireless-CA no menu suspenso Trusted Root Certificate

Co	nfigure PEAP (EAP-MSCHAP V2)
	Use Machine Information for Domain Logon
[✓ Validate Server Identity
	Trusted Root Certification Authorities
	Wireless-CA 🛛 👻
ľ	When connecting, use:
	O Certificate
	 User Name and Password
	Select a Certificate
	<u> </u>
	VII se Windows User Name and Password
	User Information for PEAP (EAP-MSCHAP V2) Authentication
	User Name: Administrator
	Password.
	Confirm Password:
	Advanced OK Cancel

6. Clique em OK e ative o perfil.Observação: quando você usa o EAP Protegido-Microsoft Challenge Handshake Authentication Protocol Versão 2 (PEAP-MSCHAPv2) com o Microsoft XP SP2 e a placa Wireless é gerenciada pelo Microsoft Wireless Zero Configuration (WZC), você deve aplicar o hotfix KB885453 da Microsoft. Isso evita vários problemas de autenticação relacionados ao PEAP Fast Resume.

Verificar e solucionar problemas

Para verificar se a configuração funciona como esperado, ative o perfil PEAP-MSCHAPv2 no Wireless client Client1.

🖻 Cisco Aironet Desktop Utility - Current Profile: PEAP-MSCHAPv2 🛛 😨 🔀				
Action Options Help				
Current Status Profile Management	Diagnostics			
CISCO SYSTEMS				
Profile Name:	PEAP-MSCHAPv2			
Link Status:	Authenticated	Network Type: Infrastructure		
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 64		
Server Based Authentication:	PEAP (EAP-MSCHAP V2)	Data Encryption: AES		
IP Address:	10.77.244.218			
Signal Strength:				
		Advanced		

Quando o perfil PEAP-MSCHAPv2 é ativado no ADU, o cliente executa a autenticação aberta 802.11 e, em seguida, executa a autenticação PEAP-MSCHAPv2. Este é um exemplo de autenticação PEAP-MSCHAPv2 bem-sucedida.

Use os comandos debug para entender a sequência de eventos que ocorrem.

A <u>Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados</u> <u>comandos show.</u> Use a OIT para exibir uma análise da saída do comando show.

Esses comandos debug no Controller de LAN Wireless são úteis.

- debug dot1x events enable Para configurar a depuração de eventos 802.1x
- debug aaa events enable Para configurar a depuração de eventos AAA
- debug mac addr <mac address> Para configurar a depuração MAC, use o comando debug mac
- debug dhcp message enable Para configurar a depuração de mensagens de erro DHCP

Estas são as saídas de exemplo dos comandos **debug dot1x events enable** e **debug client <mac address>**.

debug dot1x events enable:

```
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

debug mac addr <MAC Address>:

```
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 Reg 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 = 0x0000000,
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
```

Observação: se você usar o Microsoft Supplicant para autenticar com um Cisco Secure ACS para autenticação PEAP, o cliente possivelmente não será autenticado com êxito. Às vezes, a conexão inicial pode ser autenticada com êxito, mas as tentativas subsequentes de autenticação de conexão rápida não se conectam com êxito. Esse é um problema conhecido. Os detalhes desse problema e a correção para o mesmo estão disponíveis <u>aqui</u>.

Informações Relacionadas

- PEAP em redes sem fio unificadas com ACS 4.0 e Windows 2003
- Exemplo de Configuração de Autenticação EAP com WLAN Controllers (WLC)
- <u>Atualização do software da controladora Wireless LAN (WLC) para as versões 3.2, 4.0 e 4.1</u>
- Guias de configuração de Cisco 4400 Series Wireless LAN Controllers
- <u>Suporte Técnico e Documentação Cisco Systems</u>

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.