Exemplo de configuração da autenticação da Web usando LDAP em controladores de LAN sem fio (WLCs)

Contents

Table Of Contents
Introdução
Pré-requisitos
<u>Requisitos</u>
Componentes Utilizados
Informações de Apoio
Conventions
Processo de autenticação da Web
<u>Configurar</u>
Diagrama de Rede
<u>Configurações</u>
Configurar o servidor LDAP
Criar usuários no controlador de domínio
Criar um banco de dados de usuário em uma UO
Configurar o usuário para acesso ao LDAP
Vinculação anônima
Habilitar recurso de vinculação anônima no servidor Windows 2012 Essentials
Concessão de acesso de LOGON ANÔNIMO ao usuário
Conceder permissão de conteúdo da lista na UO
Vinculação autenticada
Concessão de privilégios de administrador ao WLC-admin
Usar LDP para identificar os atributos do usuário
Configurar WLC para servidor LDAP
Configurar a WLAN para autenticação da Web
Verificar
Troubleshooting

Introdução

Este documento descreve como configurar um controlador de LAN sem fio (WLC) para autenticação da Web. Explica como configurar um servidor Lightweight Directory Access Protocol (LDAP) como o banco de dados de back-end para autenticação da Web, para recuperar as credenciais de usuário e autenticar o usuário.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da configuração de access points Lightweight (LAPs) e WLCs da Cisco
- Conhecimento do protocolo Control and Provisioning of Wireless Access Points (CAPWAP)
- Conhecimento de como instalar e configurar o Lightweight Directory Access Protocol (LDAP), o Active Directory e os controladores de domínio

Componentes Utilizados

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

- WLC Cisco 5508 com firmware versão 8.2.100.0
- LAP Cisco 1142 Series
- Adaptador de cliente sem fio Cisco 802.11a/b/g.
- Servidor Microsoft Windows 2012 Essentials que realiza a função do servidor LDAP

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.

Informações de Apoio

Conventions

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

Processo de autenticação da Web

A autenticação da Web é um recurso de segurança da camada 3 que faz com que o controlador não permita o tráfego IP (exceto pacotes relacionados a DHCP e DNS) de determinado cliente, até que o cliente forneça corretamente um nome de usuário e uma senha válidos. Quando você usar a autenticação da Web para autenticar clientes, defina um nome de usuário e uma senha para cada cliente. Em seguida, quando os clientes tentam ingressar na LAN sem fio, devem inserir o nome de usuário e a senha quando solicitados por uma página de login.

Quando a autenticação da Web está ativada (em Segurança da camada 3), ocasionalmente os

usuários recebem um alerta de segurança do navegador da Web, na primeira vez que tentam acessar um URL.

Dica: para remover este aviso de certificado, reverta para o seguinte guia sobre como instalar um certificado confiável de terceiros <u>http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lancontrollers/109597-csr-chained-certificates-wlc-00.html</u>

8	There is a problem with this website's security certificate.
	The security certificate presented by this website was not issued by a trusted certificate authority.
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
	We recommend that you close this webpage and do not continue to this website.
	Click here to close this webpage.
	 More information
•	III

Depois que você clicar em Sim para continuar (ou mais precisamente em Continuar neste site (não recomendado) no navegador Firefox, por exemplo) ou se o navegador do cliente não exibir um alerta de segurança, o sistema de autenticação da Web redirecionará o cliente para uma página de login, como mostrado na imagem:



A página de login padrão contém um logotipo da Cisco e um texto específico da Cisco. Você pode escolher que o sistema de autenticação da Web exiba um destes:

- A página de login padrão
- Uma versão modificada da página de login padrão
- Uma página de login personalizada que você configura em um servidor da Web externo
- Uma página de login personalizada que você baixa para o controlador

Quando você insere um nome de usuário e uma senha válidos na página de login de autenticação da Web e clica em Enviar, você é autenticado com base nas credenciais enviadas e em uma autenticação bem-sucedida do banco de dados de back-end (nesse caso, o LDAP). O sistema de autenticação da Web exibe uma página de login bem-sucedida e redireciona o cliente autenticado para o URL solicitado.



A página de login bem-sucedido padrão contém um ponteiro para uma URL de endereço de gateway virtual: <u>https://1.1.1.1/logout.html.</u> O endereço IP que você definiu para a interface virtual do controlador serve como endereço de redirecionamento da página de login.

Este documento explica como usar a página da Web interna no WLC para autenticação da Web. Este exemplo usa um servidor LDAP como banco de dados de back-end para autenticação da Web, para recuperar as credenciais de usuário e autenticar o usuário.

Configurar

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

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:



Configurações

Siga estas etapas para implementar essa configuração com sucesso:

- Configurar o servidor LDAP.
- Configurar WLC para servidor LDAP.
- Configurar a WLAN para autenticação da Web.

Configurar o servidor LDAP

A primeira etapa é configurar o servidor LDAP, que serve como banco de dados de back-end para armazenar as credenciais de usuário dos clientes sem fio. Neste exemplo, o servidor Microsoft Windows 2012 Essentials é usado como servidor LDAP.

A primeira etapa na configuração do servidor LDAP é criar um banco de dados do usuário no servidor LDAP para que o WLC possa consultar esse banco de dados para autenticar o usuário.

Criar usuários no controlador de domínio

Uma unidade organizacional (UO) contém vários grupos que levam as referências para as entradas pessoais em um PersonProfile. Uma pessoa pode ser membro de vários grupos. Todas as definições de classe e atributo de objeto são o padrão do esquema LDAP. Cada grupo contém as referências (dn) de cada pessoa que pertence a ele.

Neste exemplo, uma nova UO LDAP-USERS é criada, e o usuário User1 é criado nessa UO. Quando você configura esse usuário para acesso ao LDAP, o WLC pode consultar esse banco de dados LDAP para autenticação do usuário.

O domínio usado neste exemplo é CISCOSYSTEMS.local.

Criar um banco de dados de usuário em uma UO

Esta seção explica como criar uma nova UO no domínio e criar um novo usuário nessa UO.

- 1. Abra o Windows PowerShell e digite servermanager.exe
- 2. Na janela Gerenciador do servidor, clique em AD DS. Em seguida, clique com o botão direito do mouse no nome do servidor para selecionar Usuários e Computadores do Active Directory.
- 3. Clique com o botão direito do mouse no nome de domínio, que é CISCOSYSTEMS.local neste exemplo, e navegue para Novo> Unidade organizacional no menu de contexto para criar uma nova UO.

3	Active Directory Users and Computers	_ D X
File Action View Help		
🗢 🔿 🙍 🖬 🗎 🖾 🍳 🔤 🍸	\$ <u>8</u>	
 Active Directory Users and Computers [WIN-A0) Saved Queries CSCOSVSTEMS.local Builtin Builtin Computer ForeignSe TPRS CostAndF Managed Program System System System TPM Dev All Tasks TPM Dev 	Type Description builtinDomain Container Container Default container for up Container Default container for sec Container Default container for stor Container Default location for stor Container Default container for up Container Default container for up Container Default container for or up Container Default container for or up infrastructureU LostAdFound LostAdFound Default container for or Computer fications co Contact fications co Group tainer for do InetOrgPerson msImaging-PSPs MSMQ Queue Alias Organizational Unit Printer User Shared Folder Shared Folder	
< III >		
Create a new object		

4. Atribua um nome a essa UO e clique em OK, como mostrado na imagem:

New Object - Organizational Unit
Create in: CISCOSYSTEMS.local/
Name:
LDAP-USERS
OK Cancel Help

Agora que a nova UO LDAP-USERS foi criada no servidor LDAP, a próxima etapa é criar o usuário User1 nessa UO. Para isso, siga estas etapas:

 Clique com o botão direito do mouse na nova UO criada. Navegue para LDAP-USERS > Novo > Usuário nos menus de contexto resultantes para criar um novo usuário, como mostrado na imagem:



2. Na página Configuração do usuário, preencha os campos obrigatórios conforme mostrado neste exemplo. Neste exemplo, User1 foi preenchido no campo Nome de logon do usuário.

Este é o nome de usuário verificado no banco de dados LDAP para autenticar o cliente. Este exemplo usa User1 nos campos Nome e Nome completo. Clique em Next.

	New Object - User
Creat	e in: CISCOSYSTEMS.local/LDAP-USERS
First name:	User1 Initials:
Last name:	
Full name:	User1
User logon name	
Uşer1	@CISCOSYSTEMS.local V
User logon name	(pre-Windows 2000):
CISCOSYSTEM	S\ User1
	< Back Next > Cancel
	Concer Cancer

3. Digite uma senha e confirme-a. Selecione a opção A senha nunca expira e clique em Avançar.

	New Object - User	X
Create in: Cl	SCOSYSTEMS.local/LDAP-USERS	
Password:	•••••	
Confirm password:	••••••	
User must change pas	sword at next logon assword	
✓ Password never expire	s	
Account is disabled		
	< Back Next > Ca	incel

4. Clique em Finish.

Um novo usuário User1 é criado na UO LDAP-USERS. Estas são as credenciais do usuário:

- nome de usuário: User1
- senha: Laptop123

	New Object - User	
8	Create in: CISCOSYSTEMS.local/LDAP-USERS	
When y	ou click Finish, the following object will be created:	
Full nan	ne: User1	<u>^</u>
User log	gon name: User1@CISCOSYSTEMS.local	
The pa	ssword never expires.	
		Y
	< Back Finish	Cancel

Agora que o usuário foi criado em uma UO, a próxima etapa é configurar esse usuário para acesso ao LDAP.

Configurar o usuário para acesso ao LDAP

Você pode selecionar Anônimo ou Autenticado para especificar o método de vinculação de autenticação local do servidor LDAP. O método Anônimo permite o acesso anônimo ao servidor LDAP. O método Autenticado exige que um nome de usuário e uma senha sejam inseridos para proteger o acesso. O valor padrão é Anonymous (Anônimo).

Esta seção explica como configurar os métodos Anônimo e Autenticado.

Vinculação anônima

Observação: o uso de associação anônima não é recomendado. Um servidor LDAP que permite a vinculação anônima não requer nenhum tipo de autenticação credenciada. Um invasor pode aproveitar a entrada de vinculação anônima para visualizar arquivos no diretório LDAP.

Execute as etapas nesta seção para configurar o usuário anônimo para acesso ao LDAP.

Habilitar recurso de vinculação anônima no servidor Windows 2012 Essentials

Para que as aplicações de terceiros (no nosso caso, o WLC) acessem o Windows 2012 AD no LDAP, o recurso de vinculação anônima deve ser ativado no Windows 2012. Por padrão, operações anônimas LDAP não são permitidas nos controladores de domínio do Windows 2012. Execute estas etapas para ativar o recurso de vinculação anônima:

- 1. Inicie a ferramenta ADSI Edit digitando: ADSIEdit.msc no Windows PowerShell. Essa ferramenta faz parte das ferramentas de suporte do Windows 2012.
- 2. Na janela da ADSI Edit, expanda o domínio raiz (Configuração [WIN-A0V2BU68LR9.CISCOSYSTEMS.local]).

Navegue para CN=Serviços > CN=Windows NT > CN=Serviço de diretório. Clique com o botão direito do mouse no contêiner CN=Serviço de diretório e selecione Propriedades no menu de contexto, como mostrado na imagem:

2				ADSI Edit		- 0 ×
File Action View Help						
(= =) 🖄 📰 🖄 👘 🙆	🔒 🛛 📰					
Z ADSI Edit		Name Class		Distinguished Name	Actions	
Domain [WIN-A0V2BU68L	R9.CISCOSYSTEMS.local]	CN=Directory Service	nTDSService	CN=Directory Service, CN=Windows NT, CN=Services, CN=Configuration, DC=CIS	CN=Windows NT	
A Configuration (WIN-A0V2)	a Configuration [WIN-A0V2BU68LR9.CISCOSYSTEMS.local]				More Actions	
a CN=Configuration,DC	#CISCOSYSTEMS,DC#local ers				hite Actors	
CN=Extended-Righ	nts					
CN=ForestUpdates						
CN=LostAndPound	dConfig					
CN=Partitions						
CN=Physical Locat	tions					
A CN#Services	F					
CN=Ctaims Co	Distribution Service					
CN=Microsoft	SPP					
CN=Microsoft SPP CN=Microsoft SPP CN=MsmqServices CN=MetServices						
CN=RRAS	JUNUS					
a 🧾 CN= Windows N	NT					
CN=Dire***	CN= Windows NT					
CN=Sites	New Connection from Here					
	New					
	Delete					
	Rename					
-	Refresh					
	Properties					
	Help					
	C Ne-Configuration, D.C. L (SC 05YSTEMS, D.C. Iocal Ne. To Long Variable Science C Ne-Fortubates C Ne-Fortubates C Ne-Fortubates C Ne-Fortubates C Ne-Fortubates C Ne-Fortubates C Ne-Configuration C Ne-C					
Opens the properties dialog box fo	or the current selection.	2h			<i>b</i> .	T T
					- Re S	1:07 PM

 Na janela CN=Propriedades do serviço de diretório, em Atributos, clique no atributo dsHeuristics no campo Atributo e selecione Editar. Na janela Editor de atributos de string deste atributo, digite o valor 0000002; clique em Aplicar e OK, como mostrado na imagem. O recurso de vinculação anônima está ativado no servidor Windows 2012.

Observação: o último (sétimo) caractere é aquele que controla a maneira como você pode se vincular ao serviço LDAP. 0 (zero) ou sem sétimo caractere significa que as operações anônimas LDAP estão desativadas. Se você definir o sétimo caractere 💊 como 2, o recurso de vinculação anônima será ativado.

Show mandatory attni Show cational attni	butes				
 Show only attributes t Mitibutes: 	tes that have <u>v</u> alues				
Attribute	Syntax	Value 🔺			
can createTimeStamp description directReports displayName displayNamePrintable displayNamePrintable displayNamePrintable displayName displ	Unicode String UTC Coded Ti Unicode String Distinguished Unicode String IA5-String Distinguished Octet String UTC Coded Ti Unicode String Unicode String Integer	Not Seb (Not Seb (Not Seb (Not Seb (Not Seb) (Not Seb	String Attribute: Editor Attribute: dSHeuristics Value: ICCOURE Elear	ΟΚ. C.	ancel

Concessão de acesso de LOGON ANÔNIMO ao usuário

A próxima etapa é conceder acesso de LOGON ANÔNIMO ao usuário User1. Siga estas etapas para realizar essa ação:

- 1. Abra Usuários e computadores do Active Directory.
- 2. Verifique se a opção Visualizar recursos avançados está marcada.
- 3. Navegue até o usuário User1 e clique nele com o botão direito do mouse. Selecione Propriedades no menu de contexto. Esse usuário foi identificado com o nome User1.



4. Clique na guia Segurança, conforme mostrado na imagem:

		User1	Propert	ties		? X	
Published Cer	tificates	Member Of	Passwo	rd Replica	tion	Dial-in Object	
Remote D	esktop Se	op Services Profile COM+		A	Attribute Editor		
General	Address	Account	Profile	Teleph	iones	Organization	
Security	En	vironment	Ses	sions	Re	emote control	
Group or use	er names:						
Adminis Accour Acour Accour Acour Acour Acour Acour Acour Accour Acou	Administrators (CISCOSYSTEMS\Administrators) Administrators (CISCOSYSTEMS\Administrators) Account Operators (CISCOSYSTEMS\Account Operators) Account Operators						
Permissions	for ANON	YMOUS LOGO	DN	Add	llow	Remove Deny	
Full contro	bl						
Read				•	-		
Write				L			
Ureate all	child obje	cts		L			
Allowed to	o authentik	us vate		L			
		Juto		L			
For special p Advanced.	For special permissions or advanced settings, click Advanced						
Learn about	access co	ontrol and perm	nissions				
	O	< C	ancel	Ар	ply	Help	

- 5. Clique em Adicionar na janela resultante.
- 6. Insira LOGON ANÔNIMO na caixa de diálogo Digitar os nomes de objetos a serem

selecionados e confirme a caixa de diálogo, como mostrado na imagem:

Select Users, Computers, Service Accounts, or Grou	aps	?	x
Select this object type:			
From this location:	Obje	ect Typ	Des
CISCOSYSTEMS.local	Lo	cation	IS
Enter the object names to select (<u>examples</u>): ANONYMOUS LOGON	Che	eck Na	ames
Advanced OK		Can	cel

 Na ACL, observe que o LOGON ANÔNIMO tem acesso a alguns conjuntos de propriedades do usuário. Click OK. O acesso ao LOGON ANÔNIMO foi concedido a esse usuário, como mostrado na imagem:

		User1	Propert	ies		?	X
Published Certi	ficates	Member Of	Password	d Replicat	ion [Dial-in	Object
Remote Desktop Services Pr				DM+	At	tribute E	ditor
General A	ddress	Account	Profile	Teleph	ones	Organ	nization
Security Environment Sessions Remote control							ntrol
Group or user	names:						
& ANONYI	MOUSL	DGON					
8 Everyone	9						
SELF							≡
🛛 🍇 Authentia	cated Us	ers					
SYSTEM	1						
Section 2010	Admins (CISCOSYSTE	MS\Domai	n Admins			
Kert Pub	lishers (C	SCOSYSTEM	IS\Cert Pu	ublishers)			~
				Add		Remo	ve
Permissions fo	r ANON	YMOUS LOGO	DN	A	ow	Den	У
Full control							_
Read					/		
Write							
Create all c	hild obje	cts					
Delete all c	hild obje	cts					
Allowed to a	authentic	ate					
					<u> </u>		
For special pe Advanced.	mission	s or advanced	settings, c	lick	1	Advance	ed
<u>Learn about a</u>	ccess ci	ontrol and pem	nissions				
	0	< C	ancel	Арр	oły		Help

Conceder permissão de conteúdo da lista na UO

A próxima etapa é conceder pelo menos a permissão de conteúdo da lista para o LOGON ANÔNIMO na UO em que está localizado o usuário. Neste exemplo, o User1 está localizado na UO LDAP-USERS. Siga estas etapas para realizar essa ação: 1. Em Usuários e computadores do Active Directory, clique com o botão direito do mouse na UO LDAP-USERS e selecione Propriedades, como mostrado na imagem:

			Active Direct	ory Users and Computers			- 0 X
File Action View Help							
**	3e						
Image: Anive Directory Users and Computers [WIN-A0/28U68L89.CISCOSYSTEMS.loc ▷ Saved Queries ▷ Builtin ▷ Computers ▷ Domputers ▷ Delegate Control ▷ Torn □ Delete Rename Refresh □ Delete Properties Help	Name	Type User	Description				
					Activ	ate Windows Action Center to activate Wind	lows
C III >					 ÷ 00 107	and a server to accord to Willing	
Opens the properties dialog box for the current selection.							

- 2. Clique em Segurança.
- 3. Clique em Add. Na caixa de diálogo exibida, insira LOGON ANÔNIMO e confirme a caixa de diálogo, como mostrado na imagem:

Select Users, Computers, Service Accounts, or Grou	aps	?	x
Select this object type:			
Users, Groups, or Built-in security principals	Obje	ect Typ	bes
From this location:			
CISCOSYSTEMS.local	Lo	cation	s
Enter the object names to select (examples):	-		
ANONYMOUS LOGON	Che	eck Na	imes
Advanced OK		Cano	cel

Vinculação autenticada

Execute as etapas nesta seção para configurar um usuário para autenticação local no servidor LDAP.

- 1. Abrir o Windows PowerShell e digitar servermanager.exe
- 2. Na janela Gerenciador do servidor, clique em AD DS. Em seguida, clique com o botão direito do mouse no nome do servidor para escolher Usuários e computadores do Ative Diretory.
- 3. Clique com o botão direito em Users. Navegue para Novo > Usuário nos menus de contexto resultantes para criar um novo usuário.

	Active Dir	rectory Users and Computers	 x
File Action View Help			
🗢 🔿 📶 🔏 🗂 🗙 🗔 😣 🚺	🖬 🗏 🔌 🛍 🍸 🚨 🍇		
Active Directory Users and Computers [WIN-A0V Saved Queries CISCOSYSTEMS.local Builtin Computers Difference Controllers Controll	Name Type Allowed RO Security Group Cert Publish Security Group Cert Publish Security Group Denied ROD Security Group ConsAdmins Security Group No. Security Group Computer Computer Computer Contact	Description Description Members in this group c Members of this group c Dimembers of this group t Dimembers of this group t	Ξ
View ▶ Refresh Export List Properties Help <	Group F InetOrgPerson F msImaging-PSPs F MSMQ Queue Alias F Printer F User F Shared Folder F	2 2 2 2 2 2 2 Members of this group	 >
Create a new object			

- 4. Na página Configuração do usuário, preencha os campos obrigatórios conforme mostrado neste exemplo. Neste exemplo, WLC-admin foi preenchido no campo Nome de logon do usuário. Este é o nome de usuário a ser usado para autenticação local no servidor LDAP. Clique em Next.
- 5. Digite uma senha e confirme-a. Selecione a opção A senha nunca expira e clique em Avançar.
- 6. Clique em Finish.

Um novo usuário WLC-admin foi criado no contêiner Usuários. Estas são as credenciais do usuário:

- nome de usuário: WLC-admin
- senha: Admin123

Concessão de privilégios de administrador ao WLC-admin

Agora que o usuário de autenticação local foi criado, precisamos conceder a ele privilégios de administrador. Siga estas etapas para realizar essa ação:

- 1. Abra Usuários e computadores do Active Directory.
- 2. Verifique se a opção Visualizar recursos avançados está marcada.
- 3. Navegue até o usuário WLC-admin e clique nele com o botão direito do mouse. Selecione Propriedades no menu de contexto, como mostrado na imagem. Esse usuário foi identificado com o nome WLC-admin.



4. Clique na guia Membro de, conforme mostrado na imagem:

WLC-admin Properties

	2

?

Security	Er	vironment	Sess	ions	Re	emote co	ontrol	
Remote	Desktop Se	ervices Profile	C	COM+		Attribute Editor		
General	Address	Account	Profile	Teleph	ones	Orga	nization	
Published C	Certificates	Member Of	Password	d Replica	tion	Dial-in	Object	
Member o	f:							
Name		Active Directo	ry Domain	Services	s Folde	r		
Domain	Users	CISCOSYSTE	MS.local/	Users				
Add Remove								
Primary group: Domain Users Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.								
	0	к с	ancel	Ар	ply		Help	

5. Clique em Add. Na caixa de diálogo exibida, digite Administradores e clique em OK, como mostrado na imagem:

Select Groups	? X
Select this object type:	
Groups or Built-in security principals	Object Types
From this location:	
CISCOSYSTEMS.local	Locations
Enter the object names to select (examples):	
Administrators	Check Names
Advanced OK	Cancel

Usar LDP para identificar os atributos do usuário

Essa ferramenta da GUI é um cliente LDAP que permite que os usuários realizem operações, como conectar, vincular, pesquisar, modificar, adicionar ou excluir, em qualquer diretório compatível com o LDAP, como o Active Directory. O LDP é usado para visualizar os objetos armazenados no Active Directory, juntamente com seus metadados, como descritores de segurança e metadados de replicação.

A ferramenta LDP GUI é incluída quando você instala as ferramentas de suporte do Windows Server 2003 do CD do produto. Esta seção explica como usar o utilitário LDP para identificar os atributos específicos associados ao usuário User1. Alguns desses atributos são usados para preencher os parâmetros de configuração do servidor LDAP no WLC, como tipo de atributo de usuário e tipo de objeto de usuário.

- 1. No servidor Windows 2012 (mesmo no mesmo servidor LDAP), abra o Windows PowerShell e insira LDP para acessar o navegador LDP.
- 2. Na janela principal LDP, navegue para Conexão > Conectar e conecte-se ao servidor LDAP ao digitar o endereço IP do servidor LDAP, como mostrado na imagem.

				Ldp	
onnection Browse	View	Options	Utilities	Help	
Connect					
Bind Disconnect	Ctrl+B				
New of Save	Ctrl+N				
Save As Exit		_			
onnect to specified ser	ver				ł

3. Uma vez conectado ao servidor LDAP, selecione Visualizar no menu principal e clique em Árvore, como mostrado na imagem:

\$						ldap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local	-		x
Connection	Browse	View	Options	Utilities	Help				
Ready						<pre>defaultNamingContext: DC-CISCOSYSTEMS.DC-local; domainControllerFunctionality: 5; domainControllerFunctionality: 5; domainControllerFunctionality: 5; domainControllerFunctionality: 5; domainControllerFunctionality: 5; highestCommtButUSN: 16580; isGlobalCatalogReady: TRUE; isSynchronized: TRUE; dbgServiceName: CISCOSYSTEMS.DC-local; DC-CISCOSYSTEMS.DCC-local; CN-Schema,CN=Configuration,DC=CISCOSYSTEMS.DC-local; siglobalCatalogReady: TRUE; isSynchronized: TRUE; dbgServiceName: CISCOSYSTEMS.DC-local; DC-ForestDnaZones.DC=CISCOSYSTEMS.DC-local; CODomainNamingContext: DC=CISCOSYSTEMS.DC-local; DC=ForestDnaZones.DC=CISCOSYSTEMS.DC=local; rootDomainNamingContext: DC=CISCOSYSTEMS.DC=local; serverName: CN=WIN-A0V2BU68L89,CN=Servers.CN=Default-First-Site-Name,CN=Stes.CN=Configuration,DC=CISCOSYSTEMS,DC=local; supportedCoapabilities (6): 12.840.113556.1.4.800 = (ACTIVE_DRECTORY_V1): 12.840.113556.1.4.1670 = (ACTIVE_DRECTORY_V51): 12.840.113556.1.4.8179 ACTIVE_DRECTORY_LDAP_NTE0; 1: 12.440.113556.1.4.1935 = (ACTIVE_DRECTORY_V61): 12.840.113556.1.4.8179 = (ACTIVE_DRECTORY_V61):</pre>	cal; i = (); 556.1. 822 = (k22 = (k22 = (k22 = (k22 = (k22 = k2); k2 = k2 k2 = k2 k2 k2 = k2 k2 k2 = k2 k2 k2 = k2 k2 k2 = k2 k2 k2 k2 = k2 k2 k2 k2 k2 k2 k2 k2 k2 k2 k2 k2 k2 k	4.528 = EST); X); 1.4.221 ange;	

4. Na janela resultante Visualização em árvore, insira o BaseDN do usuário. Neste exemplo, o User1 está localizado na UO "LDAP-USERS" no domínio CISCOSYSTEMS.local. Clique em OK, como mostrado na imagem:

@	Idap://WIN-A0V2BU68LR9.CISCOSYSTEMS.local/DC=CISCOSYSTEMS,DC=local	-		x	
Connection Browse View Options Utilities	Help				
	defaultNamingContext: DC-CISCOSYSTEMS, DC-local; domainContoilerFunctionalty: 5; domainFunctionalty: 5; highestCommittedUSN: 16855; isGlobalCatalogReady: TRUE; isSynchronized: TRUE; isSynchrefa; isSynchronized: TRUE; isSynchronized: TRUE; isSynchronized:	; ; ;; ;; ;; ; ; ; ; ; ; ; ; ; ; ; ; ;	4.528 EST); X); 1.4.22 ange;	= (
ready		_	_	_	4

5. O lado esquerdo do navegador LDP mostra a árvore inteira que é exibida no BaseDN especificado (UO=LDAP-USERS, dc=CISCOSYSTEMS, dc=local). Expanda a árvore para localizar o usuário User1. Esse usuário pode ser identificado com o valor de CN que representa o nome do usuário. Neste exemplo, é CN=User1. Clique duas vezes em CN=User1. No painel do lado direito do navegador LDP, o LDP exibe todos os atributos associados ao User1, como mostrado na imagem:

Connection Browse View Options Utilities Help	
 ○ OULLDAP-USERS_DC=CISCOSYSTEMS_DC=local ○ CNELDAP-USERS_DC=CISCOSYSTEMS_DC=CISCOSYSTEMS_DC=CISCOSYSTEMS_DC=local ○ CNELDAP-USERS_DC=CISCOSYSTEMS_DC=CISCOSYSTEMS_DC=local ○ CNELDAP-USERS_DC=CISCOSYSTEMS_DC=CISCOSYSTEMS_DC=local ○ CNELDAP-USERS_DC=CISCOSYSTEMS_DC=CISCOSYSTEMS_DC=local ○ CNELDAP-USERS_DC=CISCOSYSTEMS_DC=CISCOSYSTEMS_DC=local ○ CNELDAP-USERS_DC=CISCOSYSTEMS_DC=local ○ CNEDTS ○ CNEDTS	ш >
C III >	~

6. Ao configurar o WLC para o servidor LDAP, no campo Atributo do usuário, digite o nome do atributo no registro do usuário que contém o nome de usuário. Nessa saída do LDP, você pode ver que sAMAccountName é um atributo que contém o nome de usuário "User1"; portanto, insira o atributo sAMAccountName que corresponde ao campo Atributo do usuário no WLC.

7. Ao configurar o WLC para o servidor LDAP, no campo Tipo de objeto do usuário, insira o valor do atributo LDAP objectType que identifica o registro como usuário. Frequentemente, os registros de usuário têm diversos valores para o atributo objectType, sendo que alguns são exclusivos e outros são compartilhados com diversos tipos de objeto. Na saída do LDP, CN=Pessoa é um valor que identifica o registro como usuário; portanto, especifique Pessoa como o atributo Tipo de objeto do usuário no WLC.

A próxima etapa é configurar o WLC do servidor LDAP.

Configurar WLC para servidor LDAP

Agora que o servidor LDAP está configurado, a próxima etapa é configurar o WLC com os detalhes do servidor LDAP. Siga estas etapas na GUI do WLC:

Nota:Este documento supõe que a WLC esteja configurada para operação básica e que os LAPs estejam registrados na WLC. Se você for um novo usuário que deseja configurar o WLC para operação básica com LAPs, consulte <u>Registro de AP Lightweight (LAP) em um</u> <u>controlador de LAN sem fio (WLC)</u>.

1. Na página Segurança do WLC, selecione AAA > LDAP no painel de tarefas do lado esquerdo para migrar para a página de configuração do servidor LDAP.

cisco	MONITOR	WLANS CONTROLL	ER WIRELESS SECURIT	MANAGEMENT COM	MANDS HELP FEEDB	ACK	Sa <u>v</u> e Cor	nfiguration P	ing Logout <u>R</u> efresh A <u>H</u> ome
Security	LDAP Ser	rvers							New
▼ AAA General ▼ RADIUS	Server Index	Server Address(Ip	v4/1pv6)	Port	Server State	Secure Mode(via TLS)	Bind		
Authentication Accounting	1	172.16.16.200		389	Enabled	Disabled	Authenticated		
Accounting Fallback DNS Downloaded AVP • TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies									
▶ Local EAP									
Advanced EAP									
Certificate									

Para adicionar um servidor LDAP, clique em Novo. A página LDAP Servers (Servidores LDAP) > New (Novo) é exibida.

- Na página Editar servidores LDAP, especifique os detalhes do servidor LDAP, como o endereço IP do servidor LDAP, o número da porta, o status Ativar servidor e assim por diante.
 - Selecione um número na caixa suspensa Índice do servidor (prioridade) para especificar a ordem de prioridade deste servidor em relação a qualquer outro servidor LDAP configurado. É possível configurar até dezessete servidores. Se o controlador não puder acessar o primeiro servidor, ele tentará o segundo da lista e assim por diante.

- Digite o endereço IP do servidor LDAP no campo Endereço IP do servidor.
- Digite o número da porta TCP do servidor LDAP no campo Número da porta. O intervalo válido é de 1 a 65535, e o valor padrão é 389.
- Para a vinculação simples, usamos Autenticado, para o nome de usuário da vinculação que é a localização do usuário admin do WLC que será usado para acessar o servidor LDAP e sua senha.
- No campo User Base DN (Nome diferenciado da base de usuários), digite o nome diferenciado (DN) da subárvore do servidor LDAP que contém uma lista de todos os usuários. Por exemplo, ou=organizational unit, .ou=next organizational unit e o=corporation.com. Se a árvore que contém os usuários for o DN base, digite o=corporation.com ou dc=corporation, dc=com.

Neste exemplo, o usuário está localizado na UO LDAP-USERS, que, por sua vez, foi criada como parte do domínio lab.wireless.

O DN base do usuário deve indicar o caminho completo onde estão localizadas as informações do usuário (credenciais de usuário de acordo com o método de autenticação EAP-FAST). Neste exemplo, o usuário está localizado no DN base UO=LDAP-USERS, DC=CISCOSYSTEMS, DC=local.

• No campo User Attribute (Atributo de usuário), digite o nome do atributo no registro do usuário que contém o nome de usuário.

No campo User Object Type (Tipo de objeto de usuário), insira o valor do atributo objectType do LDAP que identifica o registro como um usuário. Muitas vezes, os registros de usuário têm vários valores para o atributo objectType, alguns dos quais são exclusivos para o usuário e são compartilhados com outros tipos de objeto.

Você pode obter o valor desses dois campos no servidor de diretório com o utilitário de navegador LDAP, que faz parte das ferramentas de suporte do Windows 2012. Essa ferramenta do navegador LDAP da Microsoft denomina-se LDP. Com a ajuda dessa ferramenta, você pode conhecer os campos DN base do usuário, Atributo do usuário e Tipo de objeto do usuário desse usuário específico. As informações detalhadas sobre como usar o LDP para conhecer esses atributos específicos do usuário são discutidas na seção Uso do LDP para identificar os atributos do usuário neste documento.

- No campo Limite de tempo do servidor, digite o número de segundos entre as retransmissões. O intervalo válido é de 2 a 30 segundos, e o valor padrão é de 2 segundos.
- Marque a caixa de seleção Enable Server Status (Status de servidor ativo) para ativar o servidor LDAP ou desmarque a caixa para desativá-lo. O valor padrão é desativado.
- Clique em Apply (Aplicar) para confirmar as alterações. Este é um exemplo já configurado com essas informações:

cisco	MONITOR WLANS CONTROLL	er wireless <mark>security management commands help eeedback</mark>	Sa <u>v</u> e Configuration Ping Logout Refresh nternet
Security	LDAP Servers > Edit		< Back Apply
AAA General Caneral Authentication Acounting Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC filtering Disabled Clients User Login Policies Password Policies Password Policies Local EAP Advanced EAP Priority Order Certificate	Server Index Server Address(Ipv4/Ipv6) Port Number Simple Bind Bind Username Bind Password Confirm Bind Password User Base ON User Attribute User Object Type Secure Mode(via TLS) Server Timeout Enable Server Status	1 172.16.16.200 389 Authenticated CN=WLC-ADMIN,CN=Users,DC=CISCOSYSTEMS,E CN=Users,DC=CISCOSYSTEMS,DC=LOCAL SAMAccountName Person Disabled 2 seconds Enabled	

3. Agora que os detalhes sobre o servidor LDAP foram configurados no WLC, a próxima etapa é configurar uma WLAN para autenticação da Web.



A primeira etapa é criar uma WLAN para os usuários. Conclua estes passos:

1. Clique em WLANs na GUI do controlador para criar uma WLAN.

A janela WLANs será exibida. Essa janela lista as WLANs configuradas no controlador.

2. Clique em Novo para configurar uma nova WLAN.

Neste exemplo, a WLAN foi nomeada como Web-Auth.

cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs >	New							
 WLANs WLANs Advanced 	Type Profile Na SSID ID	ame	WLAN LDAP- LDAP- 11	TEST					

- 3. Clique em Apply.
- 4. Na janela WLAN > Editar, defina os parâmetros específicos para a WLAN.

cisco	MONITOR WLANS CO	VTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	Sa <u>v</u> e Configuration Ping Logout <u>R</u> efresh <
WLANs	WLANs > Edit 'LDAP-T	EST' QoS Policy-Mapping Advanced	< Back Apply
WLAWS Advanced	Profile Name Type SSID Status Security Policies Radio Policy Interface/Interface Group(G) Multicast Vian Feature Broadcost SSID NAS-ID	LDAP-TEST WLAN LDAP-TEST Carbon content of the security tab will appear after applying the changes.) All Tenabled Enabled Tenabled Tenabled	

- Marque a caixa de seleção Status para ativar a WLAN.
- Na WLAN, selecione a interface apropriada no campo Nome da interface.

Este exemplo mapeia a interface de gerenciamento conectada à WLAN Web-Auth.

5. Clique na guia Security. No campo Segurança da camada 3, marque a caixa de seleção Política da Web e selecione a opção Autenticação.

cisco	Monitor Wlans Controller Wireless Security Management Commands Help Eeedback	Save Configuration Bing Logout Befresh n Home
WLANS WLANS WLANS Advanced	WLANs > Edit 'LDAP-TEST' General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers Layer 3 Security 1 Web Policy AAA Servers Security 1 Web Policy AAA Servers Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure ¹² Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None Sleeping Client Enable Over-ride Global Config ¹² Enable	< Back Apply

Essa opção é selecionada porque a autenticação da Web é usada para autenticar os clientes sem fio. Marque a caixa de seleção Substituir configuração global para ativar a configuração de autenticação da Web de acordo com a WLAN. Selecione o tipo de autenticação da Web apropriado no menu suspenso Tipo de autenticação da Web. Este exemplo usa a Autenticação da Web interna.

Observação: a autenticação da Web não tem suporte na autenticação 802.1x. Isso significa que não é possível selecionar 802.1x ou um WPA/WPA2 com 802.1x como a segurança da camada 2 ao usar a autenticação da Web. A autenticação da Web é compatível com todos os outros parâmetros de segurança da camada 2.

6. Clique na guia Servidores AAA. Selecione o servidor LDAP configurado no menu suspenso Servidor LDAP. Se você usar um banco de dados local ou um servidor RADIUS, poderá definir a prioridade de autenticação na ordem de prioridade de autenticação para web-auth userfield.

cisco	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh <mark>A</mark> Home
WLANs	WLANs > Edit 'LDAP-TEST'		< Back Apply
* WLANS	General Security QoS Policy-Mappin	g Advanced	
▶ Advanced	Layer 2 Layer 3 AAA Servers		
	Interim Update		^
	Server 1 IP:172.16.16.200, Port:389 ▼ Server 2 None ▼ Server 3 None ▼		Ħ
	Local EAP Authentication Local EAP Authentication Enabled	_	
	Authentication priority order for web-auth	user	E.
	Not Used	Order Used For Authentication	
	LOCAL RADIUS	> LDAP A Up < Down	
	•	Ш	*

7. Clique em Apply.

Observação: neste exemplo, os métodos de segurança da camada 2 para autenticar usuários não são usados, portanto escolha Nenhum no campo Segurança da camada 2.

Verificar

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

Para verificar essa configuração, conecte um cliente sem fio e verifique se a configuração funciona conforme o esperado.

O cliente sem fio fica ativo e o usuário digita o URL, como <u>www.yahoo.com, no navegador da</u> <u>Web.</u> Como o usuário não foi autenticado, o WLC o redireciona para o URL de login da Web interna.

O usuário é solicitado a fornecer as credenciais de usuário. Depois que o usuário envia o nome de usuário e a senha, a página de login recebe as credenciais de usuário e, após o envio, devolve a solicitação para o exemplo action_URL, <u>http://1.1.1.1/login.html</u>, do servidor Web do WLC. Isso é fornecido como um parâmetro de entrada para o URL de redirecionamento do cliente, onde 1.1.1.1 é o endereço de interface virtual no switch.

O WLC autentica o usuário no banco de dados do usuário LDAP. Após a autenticação bemsucedida, o servidor Web da WLC encaminha o usuário para a URL de redirecionamento configurada ou para a URL com a qual o cliente foi iniciado, como <u>www.yahoo.com</u>.

	More information	
	Click here to close this webpage.	
	We recommend that you close this webpage and do not continue to this website.	
	Security certificate problems may indicate an attempt to fool you or intercept any data you send server.	to the
	The security certificate presented by this website was not issued by a trusted certificate authority.	
8	There is a problem with this website's security certificate.	

O Image: Contract of the second second

Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and putyour air space to work.

Oper Harpe	User1	
Password		
	Submit	



Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua

configuração.

Use estes comandos para solucionar problemas na configuração:

- debug mac addr <client-MAC-address xx:xx:xx:xx:xx:xx:xx:xx:xx
- · debug aaa all enable
- · debug pem state enable
- · debug pem events enable
- · debug dhcp message enable
- · debug dhcp packet enable

Este é um exemplo de saída dos comandos debug mac addr cc:fa:00:f7:32:35

debug aaa ldap enable

(Cisco_Controller) >*pemReceiveTask: Dec 24 03:45:23.089: cc:fa:00:f7:32:35 Sent an XID frame *apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Processing assoc-req station:cc:fa:00:f7:32:35 *apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Association received from mobile on BSSID 00:2 *apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Global 200 Clients are allowed to AP radio *apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Max Client Trap Threshold: 0 cur: 1 *apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Rf profile 600 Clients are allowed to AP wlan *apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 override for default ap group, marking intgrp *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Interface policy on Mobile, role Loca *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Re-applying interface policy for client *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing IPv4 A *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing IPv6 A *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfApplyWlanPolicy: Apply WLAN Policy over PMI *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6246 setting Central switched *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6249 apVapId = 1 and Split Ac *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying site-specific Local Bridging override *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Local Bridging Interface Policy for s *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE statusCode is 0 and status is 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE ssid_done_flag is 0 finish_flag *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 STA - rates (3): 24 164 48 0 0 0 0 0 0 0 0 0 0 *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 suppRates statusCode is 0 and gotSuppRatesEle *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 AID 2 in Assoc Req from flex AP 00:23:eb:e5:04 *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfMs1xStateDec *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change state to *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 pemApfAddMobileStation2: APF_MS_PEM_WAIT_L2_AU *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Initializing policy *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Change state to AUTHCH *apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 AUTHCHECK (2) Change state to L2 *pemReceiveTask: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 Removed NPU entry.

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Not Using WMM Compliance code qosCap 00

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Plumbed mobil *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Change state *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) pemApfAddMobile *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Adding Fast Pat type = Airespace AP Client - ACL passthru on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0 IPv4 ACL I *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Successfully pl *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) pemApfAddMobile *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Replacing Fast type = Airespace AP Client - ACL passthru on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0 IPv4 AC *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast Path rule *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Successfully pl *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2 (apf_policy.c:359) Changing sta *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2:session timeout forstation cc:f *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Scheduling deletion of Mobile Station: (calle *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Func: apfPemAddUser2, Ms Timeout = 1800, Sessi *apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Sending assoc-resp with status 0 station:cc:fa *apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sending Assoc Response to station on BSSID 00: *apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 apfProcessAssocReq (apf_80211.c:10187) Changin *pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2, dtlFla *pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sent an XID frame *pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2, dtlFla *pemReceiveTask: Dec 24 03:45:43.558: cc:fa:00:f7:32:35 Sent an XID frame *DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len 322,vla *DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype Off:ff:ff:ff: *DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settin dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0, dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25 VLAN: 16 *DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLoc *DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settin dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0, dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25 VLAN: 16 *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settin dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16 *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLoc *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP transmitting DHCP DISCOVER (1) *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP op: BOOTREQUEST, htype: Ethernet, hlen *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0,

*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35 *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0 *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 172.16.16.25 *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settin dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16 *DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE *DHCP Proxy Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len 572,vlan 0 *DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418, port 1, vl *DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP transmitting DHCP OFFER (2) *DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6 *DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0, *DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35 *DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 172.16.16.122 *DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0 *DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP server id: 1.1.1.1 rcvd server id: 172 *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len 334,vla *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype Off:ff:ff:ff: *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block settin dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16 *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25 mscbVapLoc *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25 (local a *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP transmitting DHCP REQUEST (3) *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP op: BOOTREQUEST, htype: Ethernet, hlen xid: 0x62743488 (1651782792), secs: 0, *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP *DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35 *DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0 *DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 172.16.16.25 *DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP requested ip: 172.16.16.122 *DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP server id: 172.16.16.25 rcvd server i *DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block settin dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25 VLAN: 16 *DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len 572,vlan 0 *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP setting server from ACK (mscb=0x40e64b88 *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418, port 1, vl *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP transmitting DHCP ACK (5) *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6 *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP xid: 0x62743488 (1651782792), secs: 0, *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP chaddr: cc:fa:00:f7:32:35 *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP ciaddr: 0.0.0.0, yiaddr: 172.16.16.122 *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0 *DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP server id: 1.1.1.1 rcvd server id: 172 *ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created for mobile, leng *ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created in mscb for mobi *aaaQueueReader: Dec 24 03:46:01.222: AuthenticationRequest: 0x2b6bdc3c *aaaQueueReader: Dec 24 03:46:01.222: Callback.....0x12088c50 *aaaQueueReader: Dec 24 03:46:01.222: protocolType.....0x0000002 *aaaQueueReader: Dec 24 03:46:01.222: proxyState.....CC:FA:00:F7:32:35-

*aaaQueueReader: Dec 24 03:46:01.222: Packet contains 15 AVPs (not shown)

*LDAP DB Task 1: Dec 24 03:46:01.222: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)
*LDAP DB Task 1: Dec 24 03:46:01.222: LDAP server 1 changed state to INIT
*LDAP DB Task 1: Dec 24 03:46:01.223: LDAP_OPT_REFERRALS = -1

*LDAP DB Task 1: Dec 24 03:46:01.223: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success) *LDAP DB Task 1: Dec 24 03:46:01.225: ldapInitAndBind [1] configured Method Authenticated lcapi_bind (r *LDAP DB Task 1: Dec 24 03:46:01.225: LDAP server 1 changed state to CONNECTED *LDAP DB Task 1: Dec 24 03:46:01.225: disabled LDAP_OPT_REFERRALS *LDAP DB Task 1: Dec 24 03:46:01.225: LDAP_CLIENT: UID Search (base=CN=Users,DC=CISCOSYSTEMS,DC=local, *LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: ldap_search_ext_s returns 0 -5 *LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned 2 msgs including 0 references *LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned msg 1 type 0x64 *LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Received 1 attributes in search entry msg *LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned msg 2 type 0x65 *LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT : No matched DN *LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT : Check result error 0 rc 1013 *LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Received no referrals in search result msg *LDAP DB Task 1: Dec 24 03:46:01.226: ldapAuthRequest [1] 172.16.16.200 - 389 called lcapi_query base=" *LDAP DB Task 1: Dec 24 03:46:01.226: Attempting user bind with username CN=User1,CN=Users,DC=CISCOSYST *LDAP DB Task 1: Dec 24 03:46:01.228: LDAP ATTR> dn = CN=User1,CN=Users,DC=CISCOSYSTEMS,DC=local (size *LDAP DB Task 1: Dec 24 03:46:01.228: Handling LDAP response Success *LDAP DB Task 1: Dec 24 03:46:01.228: Authenticated bind : Closing the binded session *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change state to *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 apfMsRunStateInc *LDAP DB Task 1: Dec 24 03:46:01.228: ldapClose [1] called lcapi_close (rc = 0 - Success) *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_NOL3SEC (14) Change state *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Stopping deletion of Mobile Station: (callerId: *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Setting Session Timeout to 1800 sec - starting *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Reached PLUMBFASTPATH: f *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Replacing Fast Path rule type = Airespace AP Client on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0 IPv4 ACL ID = 255, IPv6 ACL ID*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd... *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd... *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd... *ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule (contd... *ewmwebWebauth1: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Successfully plumbed mob *pemReceiveTask: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 1, dtlFla

(Cisco_Controller) > show client detail cc:fa:00:f7:32:35 Client MAC Address..... cc:fa:00:f7:32:35 Client Username User1 AP Name..... AP1142-1 AP radio slot Id..... 1 Client State..... Associated Client User Group..... User1 Client NAC OOB State..... Access Wireless LAN Id..... 1 Wireless LAN Network Name (SSID)..... LDAP-TEST Wireless LAN Profile Name..... LDAP-TEST Hotspot (802.11u)..... Not Supported BSSID......00:23:eb:e5:04:1f Connected For 37 secs IP Address..... 172.16.16.122 Gateway Address..... 172.16.16.1

Netmask	255.255.254.0
Association Id	2
Authentication Algorithm	Open System
Reason Code	1
Status Code	0
Mana an (a) wit average modula an intelle	
More or (q)uit current module or <ctri-2> to abo</ctri-2>	1800
Client CCX version	No CCX support
	Silver
Avg data Rate	0
Burst data Rate	0
Avg Real time data Rate	0
Burst Real Time data Rate	0
802.1P Priority Tag	disabled
CTS Security Group Tag	Not Applicable
KTS CAC Capability	No
Qos Map Capability	No
WMM Support	Enabled
APSD ACS	BK BE VI VO
Current Rate	m/
Supported Rates	12.0,18.0,24.0
Mobility Move Count	0
Security Policy Completed	Yes
Policy Manager State	RUN
Audit Session ID	ac1010190000005567b69f8
AAA Role Type	none
Local Policy Applied	none
IPv4 ACL Name	none
More or (q)uit current module or <ctrl-z> to abo</ctrl-z>	ort
More or (q)uit current module or <ctrl-z> to about the status</ctrl-z>	ort Unavailable
More or (q)uit current module or <ctrl-z> to about the status s</ctrl-z>	ort Unavailable Unavailable
More or (q)uit current module or <ctrl-z> to about the second state of the second st</ctrl-z>	ort Unavailable Unavailable none
More or (q)uit current module or <ctrl-z> to about the second state of the second st</ctrl-z>	ort Unavailable Unavailable none Unavailable none
More or (q)uit current module or <ctrl-z> to about the second status</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable
More or (q)uit current module or <ctrl-z> to about the second state of the second st</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP
More or (q)uit current module or <ctrl-z> to about the second state of the second st</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled
More or (q)uit current module or <ctrl-z> to about the second state of the second st</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile
More or (q)uit current module or <ctrl-z> to about the status s</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile 0
More or (q)uit current module or <ctrl-z> to about the status s</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile 0 N/A
More or (q)uit current module or <ctrl-z> to about the second state of the second st</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile O N/A None
More or (q)uit current module or <ctrl-z> to about the status s</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile O N/A None
More or (q)uit current module or <ctrl-z> to about the status s</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile O N/A None No
More or (q)uit current module or <ctrl-z> to about the second status s</ctrl-z>	Ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile O N/A None No Unknown
More or (q)uit current module or <ctrl-z> to about the status s</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile 0 N/A None No No Unknown Central
More or (q)uit current module or <ctrl-z> to about the status s</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile O N/A None No No Unknown Central Central
More or (q)uit current module or <ctrl-z> to about the status s</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile O N/A None No No Unknown Central Central No
More or (q)uit current module or <ctrl-z> to about the status s</ctrl-z>	Ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile O N/A None No Unknown Central Central No Central No
More or (q)uit current module or <ctrl-z> to about the status s</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile O N/A None No No Unknown Central Central No Central No Central No management
<pre>More or (q)uit current module or <ctrl-z> to abd FlexConnect ACL Applied Status</ctrl-z></pre>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile O N/A None No No Unknown Central Central No Central No management 16
More or (q)uit current module or <ctrl-z> to about the status of the</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile O N/A None No No Unknown Central Central Central No Central No management 16 O
More or (q)uit current module or <ctrl-z> to abd FlexConnect ACL Applied Status</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile 0 N/A None No Unknown Central Central No Central No management 16 0
More or (q)uit current module or <ctrl-z> to about the status of the s</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile 0 N/A None No No Unknown Central Central Central No Central No Central No Central No
More or (q)uit current module or <ctrl-z> to abo FlexConnect ACL Applied Status</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile O N/A None No No Unknown Central Central Central No Central No Central No Central No Central No Central No Central No
More or (q)uit current module or <ctrl-z> to abo FlexConnect ACL Applied Status</ctrl-z>	ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile O N/A None No No Unknown Central Central Central No Central No Central No Tort 16 16
More or (q)uit current module or <ctrl-z> to abo FlexConnect ACL Applied Status</ctrl-z>	Ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile 0 N/A None No Unknown Central Central No Central No Central No Central No Central No Central No Central No Central No Central No Central No No Central No Central No No Central No Central No Central No Central No No Central No Central No No Central No No No No No No No No No No No No No
More or (q)uit current module or <ctrl-z> to abo FlexConnect ACL Applied Status</ctrl-z>	Ort Unavailable Unavailable none Unavailable none Unavailable SimpleIP Enabled default-mdns-profile 0 N/A None No No Unknown Central Central Central No Central Central No Central Central No Central No Central No Central No Central Central No Central Central No Central No Central No Central No Central No Central No Central Central No Central Central No Central So Central So Central So Central So Central So Central So Central So Central So Central So Central So Central So Central So Central So So Central So So Central So So Central So So So Central So So So So So So So So So So So So So

Short Preamble..... Not implemented PBCC..... Not implemented Channel Agility..... Not implemented Listen Interval..... 10 Fast BSS Transition..... Not implemented 11v BSS Transition..... Not implemented Client Wifi Direct Capabilities: WFD capable..... No Manged WFD capable..... No Cross Connection Capable..... No Support Concurrent Operation..... No Fast BSS Transition Details: Client Statistics: Number of Bytes Received..... 16853 Number of Bytes Sent..... 31839 Total Number of Bytes Sent...... 31839 Total Number of Bytes Recv..... 16853 Number of Bytes Sent (last 90s)..... 31839 --More or (q)uit current module or <ctrl-z> to abort Number of Bytes Recv (last 90s)..... 16853 Number of Packets Received..... 146 Number of Interim-Update Sent..... 0 Number of EAP Id Request Msg Timeouts..... 0 Number of EAP Id Request Msg Failures..... 0 Number of EAP Request Msg Timeouts..... 0 Number of EAP Request Msg Failures..... 0 Number of EAP Key Msg Timeouts..... 0 Number of EAP Key Msg Failures..... 0 Number of Data Retries..... 2 Number of RTS Retries..... 0 Number of Duplicate Received Packets..... 0 Number of Decrypt Failed Packets...... 0 Number of Mic Failured Packets..... 0 Number of Mic Missing Packets..... 0 Number of RA Packets Dropped...... 0 Number of Policy Errors..... 0 Radio Signal Strength Indicator..... -48 dBm Signal to Noise Ratio..... 41 dB Client Rate Limiting Statistics: Number of Data Packets Received...... 0 Number of Data Rx Packets Dropped..... 0 --More or (q)uit current module or <ctrl-z> to abort Number of Data Bytes Received...... 0 Number of Data Rx Bytes Dropped...... 0 Number of Realtime Packets Received...... 0 Number of Realtime Rx Packets Dropped..... 0 Number of Realtime Bytes Received...... 0 Number of Realtime Rx Bytes Dropped..... 0 Number of Data Packets Sent...... 0 Number of Data Tx Packets Dropped..... 0 Number of Data Bytes Sent..... 0 Number of Data Tx Bytes Dropped...... 0 Number of Realtime Packets Sent...... 0 Number of Realtime Tx Packets Dropped..... 0 Number of Realtime Bytes Sent...... 0 Number of Realtime Tx Bytes Dropped..... 0 Nearby AP Statistics: AP1142-1(slot 0)

antenna1: 25 secs ago..... -37 dBm AP1142-1(slot 1) antenna0: 25 secs ago.... -44 dBm antenna1: 25 secs ago.... -57 dBm DNS Server details: DNS server IP 0.0.0.0 --More or (q)uit current module or <ctrl-z> to abort DNS server IP 0.0.0.0

Assisted Roaming Prediction List details:

Client Dhcp Required: False

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.