ACS 5.2 مادختساب EAP-FAST و PEAP نيوكت WLC و

تايوتحملا

<u>ةمدقملا</u> <u>ةيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسماا تانوكماا</u> <u>تاحالطصالا</u> <u>نىوكتلا</u> <u>ةكبشلل ىطىطختاا مسراا</u> <u>تاضارتفا</u> <u>نىوكتلا تاوطخ</u> <u>RADIUS مداخ نیوکت</u> <u>ةكِتِشِلاً دراوم نيوكت</u> <u>نىمدختسملا نىوكت</u> <u>ةساىسلا رصانع فىرعت</u> <u>لوصولا تاسايس قيبطت</u> <u>(WLC) ةىكلساللا قىلحملا ةكبشلا ىف مكحتلا رصنع نىوكت</u> <u>ليصافت مادختساب (WLC) ةيكلساللا قيلحملا ةكبشلا يف مكحتلا رصنع نيوكتب مق</u> <u>ةقداصما مداخ</u> (VLANs) <u>قىكىمانىدلا تامجاولا نىوكت</u> <u>WLAN (SSID) تاكىش نىوكت</u> <u>ةدعاسملا Wireless Client ةادأ نىوكت</u> PEAP-MSCHAPv2 (user1) EAP-FAST (user2) <u>ةحصلا نم ققحتلا</u> (PEAP-MSCHAPv2) 1 مدختس مل ا نم ق ق حت ل <u>(EAP-FAST) 2 مدختسماا نم ققحتاا</u> <u>اهحالصاو ءاطخألا فاشكتسا</u> <u>اهحالصاو ءاطخاًلا فاشكتسا رماواً</u> <u>ةلص تاذ تامولعم</u>

ةمدقملا

(WLC) ةيكلساللاا ةيلحملاا ةكبشلاا يف مكحتلاا ةدحو نيوكت ةيفيك دنتسملاا اذه حرشي مداخ لثم يجراخ RADIUS مداخ مادختساب (EAP) عسوتملاا ةقداصملا لوكوتورب ةقداصمل .5.2 (ACS) لوصولاا يف مكحتلا

ةيساسألا تابلطتملا

تابلطتملا

نيوكتلا اذه ةلواحم لبق ةيلاتلا تابلطتملا ءافيتسا نم دكأت:

- (ينث) ةطقن ذفنم نزو فيفخو WLC لا نم ةيساسألاا ةفرعم ىقلتي
 - AAA مداخب ةيفيظو ةفرعم
 - يكلساللا نامألا تالكشمو ةيكلساللا تاكبشلاب قلماش قفرعم

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- 7.0.220.0 رادصإلا ،تباثلا جمانربلا لغشي يذلا Cisco 5508 WLC
- Cisco 3502 Series LAP ةلسلسلان نم Lightweight عضولاا يف لوصولاا ةطقن
- Intel ليغشتلا جمانرب عم Microsoft Windows 7 ليغشتلا ماظنل يلصألا جمانربلا 14.3 رادصإلا N-6300-N
 - 5.2 رادص إل الغشي يذل Cisco نم نم آل إيف اض إل يوت حمل ردص م
 - Lisco 3560 Series Switch ∙ لوحملا

.ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب .رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ةرشابم كتكبش

تاحالطصالا

<u>تاجالطصا لوج تامولعملا نم ديزم ىلع لوصحلل ةينقتلا Cisco تاجيملت تاجالطصا عجار</u> <u>.تادنتسملاا</u>

نيوكتلا

دنټسملا اذه يف ةحضوملا تازيملا نيوكټ ټامولعم كل مّدقُت ،مسقلا اذه يف.

نم ديزم ىلع لوصحلل (طقف <mark>نيلجسمل</mark>ا ءالمعلل) <u>رماوألا څحب ةاداً</u> مدختساً :ةظحالم .مسقلا اذه يف ةمدختسملا رماوألا لوح تامولعملا

ةكبشلل يطيطختلا مسرلا

يلاتال ةكبشلا دادعإ دنتسملا اذه مدختسي:



ططخملا اذه يف ةمدختسملا تانوكملا نيوكت ليصافت يه هذه:

- .192.168.150.24 وه ACS (RADIUS) مداخب صاخلا IP ناونع
- قيلحملا قكبشلا يف مكحتلا قدحوب قصاخل AP-Manager و قرادإلا قمجاو ناونع 192.168.75.44. وه (WLC) قيكلساللا
 - .DHCP 192.168.150.25 مداوخ ناونع
- سفنب نيمدختسملا الك لصتي .نيوكتلا اذه ربع VLAN 253 الاحتسامات متي -PEAP مادختساب المراحة مال المدختسمل اليوكت متي الماد عمو .SSID فرعمل "goa" و user2 و MSCHAPv2
 - 253 مقر VLAN ةكبش يف نيمدختسملا نييعت متيس
 - → VLAN 253: 192.168.153.x/24. اةباوبلا VLAN 253: 192.168.153.x/24. ا
 - → VLAN 75: 192.168.75.x/24. ةكبش VLAN 75: 192.168.75.1 ة

تاضارتفإ

- .3 VLANs ةقبط لك ل حاتفم تلكش
- .DHCP مداخل DHCP قاطن نييعت مت
- .ةكبشلا يف ةزهجألا عيمج نيب 3 ةقبطاا لاصتا دجوي
- ةيلحملا ةكبشلا يف مكحتلا ةدحوب لعفلاب ةلصتم (LAP) لوصولا ةطقن
 WLC) ةيكلساللا
 - .عانق 24/ ىلع VLAN ةكبش لك يوتحت
 - . ةتبثم ايتاذ ةعقوم ةداهش ىلع ACS 5.2 يوتحي

نيوكتلا تاوطخ

- .1. <u>RADIUS مداخ نيوكتب مق</u>
 - .<u>WLC.</u>2 <u>لا تلكش</u>
- <u>.يكلسالالا ليمعلال قدعاسماا قادألا نيوكتب مق.</u>

RADIUS مداخ نيوكت

:تاوطخ عبرأ ىلإ RADIUS مداخ نيوكت ميسقت متي

- .1<u>.ةكٻشلا دراوم نيوكتٻ مق</u>
- .<u>دنيمدختسملا نيوكتب مق</u>
- .3<u>.ةسايسلا رصانع فيرعت</u>
- .4<u>. لوصولا تاسايس قيبطت</u>

جذومن مدختسي ACS 5.x نأ يأ .ةسايسلا ىلع مئاق لوصولا يف مكحتلل ماظن وه ACS 5.x تارادصإ يف مدختسملا ةعومجم ىلإ دنتسملا جذومنلا نم الدب دعاوق ىلإ دنتسم ةسايس 4.x.

نم ديزمب مستت لوصولاا ىلع ةرطيس ACS 5.x دعاوق ىلع ةمئاقلا تاسايسلا جذومن رفويو .تاعومجملا ىلع مئاقلا ميدقلا جەنلاب ةنراقم ةنورملاو ةوقلا

عاونأ ةثالث ىلع يوتحت اەنأل جەنلا ةعومجم ددحت ،ةعومجم ىلإ دنتسملا مدقألا جذومنلا يف :اەنيب طبرتو تامولعملا نم

 وأ AD تاعومجم يف ةيوضعلا ىلإ تامولعملا هذه دنتست نأ نكمي - ةيوهلا تامولعم نييلخادلا ACS يمدختسمل تباث نييعت وأ LDAP

- . كلذ ىلإ امو ةزهجألا دويقو تقول دويق ىرخأ طورش وأ دويق
 - .Cisco IOS[®] تازايتما تايوتسم وأ VLAN تاكبش تانوذألا

:جذومنلا دعاوق ىل ACS 5.x ةسايس جذومن دنتسي

ةجيتن ةلاحلا تناك اذإ

ةعومجم ىلإ دنتسملا جذومنلل ةفوصوملا تامولعملا مدختسن ،لاثملا ليبس ىلع:

ليوختال فيرعت فالم مث دييقت طرش وأ ةيوه قالح دوجو قالح يف

ىلإ لوصولاب مدختسملل حمسي يتلا طورشلا ديدحتل ةنورم اذه انل رفوي ،كلذل ةجيتنو .ةنيعم طورش ءافيتسا دنع هب حومسملا ليوختلا ىوتسم ىلإ ةفاضإلاب ةكبشلا

ةكبشلا دراوم نيوكت

.RADIUS مداخ ىلع WLC ل AAA ليمع نيوكتب موقن ،مسقلاا اذه يف

(WLC) ةيكلساللاا ةيلحملاا ةكبشلاا يف مكحتلاا رصنع ةفاضإ ةيفيك ءارجإلاا اذه حرشي ةيلحملا ةكبشلا يف مكحتلا رصنع ررمت نأ نكمي ىتح RADIUS مداخ ىلع AAA ليمعك .RADIUS مداخ ىلإ مدختسملا دامتعا تانايب (WLC) ةيكلساللاا

ةيلاتلا تاوطخلا لمكأ:

اتةزهجأ تاعومجم<ةكبشلا دراوم ىلإ لقتنا ،(ACS) ةيموسرلا مدختسملا ةهجاو نم. لفسألا يف) ءاشنإ قوف رقناو ،عقوملا<ةكبشلا.

cisco Cisco Secure A	CS
► 🛞 My Workspace	Network Resources > Network Device Groups > Location
👻 🧤 Network Resources	Network Device Groups
 Network Device Groups Location 	Filter: 💽 Match if: 🗨 Go 🔻
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name Description All Locations All Locations
Users and Identity Stores	
► 🎭 Policy Elements	
► 🔂 Access Policies	
Monitoring and Reports	
🕞 🍓 System Administration	

.2.لاسرا قوف رقناو ،ةبولطملا لوقحلا ةفاضإب مق

Name		
o Humo.	LAB	
Description	LAB Devices	
Parent:	All Locations	Select
• = Required fi	elds	

:ةشاشلا ەذە نآلا ىرتس

Cisco Secure ACS						
🕨 💮 My Workspace	Network Resources > Network Device Groups > Location					
👻 💵 Network Resources	Network Device Groups					
 Network Device Groups Location 	Filter: Match if:					
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Image: Name ▲ Description Image: The second secon					
Users and Identity Stores	LAB LAB Devices					
Policy Elements						
Access Policies						
Monitoring and Reports						
🖌 🍓 System Administration						

.3.ءاشنإ < زاهجلا عون قوف رقنا

cisco Cisco Secure ACS				
🕨 🚭 My Workspace	Network Resources > Network Device Groups > Device Type > Create			
Inetwork Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Device Group - General Image: State Image: State			
B Users and Identity Stores				
Policy Elements				
Access Policies				
 Monitoring and Reports 				
🔸 🍓 System Administration				

.4:ةشاشلا ەذە نآلا ىرتس .لاسرا ىلع رقنا

cisco Cisco Secure ACS					
My Workspace Network Resources > Network Device Groups > Device Type					
🔹 🦛 Network Resources	Network Device Groups				
 Network Device Groups Location Device Type 	Filter: Match if: Go 🗢				
Network Devices and AAA Clients	Name Description				
Default Network Device External RADIUS Servers	All Device Types All Device Types				
Users and Identity Stores	5508 Wireless LAN Controller				
Policy Elements					
Access Policies					
Monitoring and Reports					
System Administration					

.AAA.5 ءالمعو ةكبشلا ةزهجأ < ةكبشلا دراوم ىلإ لقتنا

.6:انه حضوم وه امك ليصافتلا ةئبعتب مقو ،ءاشنإ قوف رقنا

► 🚳 My Workspace	Network Resources > Net	work Devices and AAA Clerks > Create		
La Hatwork Resources Network Device Groups Location Device Type Network Devices and AAACtionts Default Network Device External RACIUS Service	Name. WL Description: Wr Network Device Gr Location Device Type	C-5508 eless LAN Controller paps [All Locations:LAB [All Device Types:5508	Select	
Buses and Identity Stores Q. Policy Elements C. Access Policies Monitoring and Reports Deduce Administration	IP Address G Single IP A 9 IP: 192 168 75	IP Address C Single IP Address C IP Range(s) 9 IP: 192.168.75.44		sation Options 39+ F S F ared Secret. cisco
• System Administration	Ø – Required fields		Co F Ka Me Ka	A port (170) Enable KeyWrap y Encryption Key: ssage Authenticator Code Key: y Input Format C ASCI @ HEXADECIMAL

.7:ةشاشلا ەذە نآلا ىرتس .لاسرا ىلع رقنا

Netw	etwork Resources > Network Devices and AAA Clents					
Filter	r. 🗌		Match It.	•	G0 🔻	
	Name		IP / Mask	NDG:Location	NDG:Device Type	Description
	WLC-5508		192.168.75.44/32	All Locations:LAB	All Device Types:5508	Wireless LAN Controller

نيمدختسملا نيوكت

نيمدختسملا الك نييعت مت .ACS ىلع نييلحم نيمدختسم ئشننس ،مسقلا اذه يف ."نويكلساللا نومدختسملا" ىمست ةعومجم يف (user2 و user1)

.1.ءاشنإ < ةيوەلا تاعومجم < ةيوەلا نزاخمو نيمدختسملا ىلإ لقتنا

cisco Cisco Secure ACS			
→ 😚 My Workspace	Users and identity Stores > Identity Groups > Create		
Network Resources			
B Users and Identify Stores Identity Groups	General s Name: Wireless Users		
 Internal identity Stores Users 	o Parent All Groups Select		
Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authonication Profile Identity Store Sequences	• = Required helds		
Policy Elements			

.2:يلي امك ةحفصلا ودبتس ،لاسرا قوف رقنلا درجمب

cisco Cisco Secure Ad	cs
▶ 🖓 My Workspace	Users and identity Stores > identity Groups
Network Resources	Identity Groups
Users and Identity Stores	Filler: Viatch it: Go V
Identity Groups Internal Identity Stores Users	□ Name ▲ Description
Hosts External Identity Stores ID4P	All Groups Identity Group Root Wireless Users Wireless Users authenticating over wireless
Active Directory RSASecurID Token Servers	
RADIUS Identity Servers Certificate Authorities Certificate Authentication Profile	
Gentity Store Sequences Solicy Elements	

.3نيمدختسملا" ةعومجمل مەنييعتب مقو ،user2و user1 نيمدختسم ءاشنإب مق ."نييكلساللا

.Create.a<نيمدختسملا<ةيوەلا تاعومجم < ةيوەلا نزاخمو نيمدختسملا قوف رقنا

cisco Cisco Secure Ad	cs
► S My Workspace	Users and identity Stores > Internal identity Stores > Users > Create
Network Resources	Constant
🖌 🏭 Users and Identity Stores	o Name: User1 Status: Enabled ▼ @
Identity Groups	Description: PEAP:mschapv2 users
USER AND ADDRESS OF A	Identity Group: All Groups: Wireless Users
Hosts External Identity Stores Certificate Authonities Certificate Authentication Profile Identity Store Sequences 	Password Information Password must • Contain 4 - 32 characters
Policy Elements	C Password:
Access Policies	Confirm Password
 Monitoring and Reports 	Change password on next login
 System Administration 	User Information There are no additional identity attributes defined for user records

.user2.b ءاشنإب مق ،لثملاب

cisco Cisco Secure AC	CS		
🕨 🥳 My Workspace	Users and Identity Stores > Internal Identity Stores > Users > Create		
An Network Resources	Connect		
👻 🏰 Users and Identity Stores	© Name: User2 Status: Enabled T @		
Identity Groups Internal Identity Stores	Description: EAPFAST user		
Users	o Identity Group: All Groups: Wireless Users Select		
External Identity Stores Certificate Authorities Certificate Authentication Profile Identity Store Sequences	Password Information Password must • Contain 4 - 32 characters		
Policy Elements	Password: eeeee		
▶ 🔂 Access Policies	Confirm Password:		
Monitoring and Reports	Change password on next login		
System Administration	User information There are no additional identity attributes defined for user records • - Required fields		

:يلي امك ةشاشلا ودبتس

cisco Cisco Secure ACS					
🕨 🚭 My Workspace	Users and Identity Store	s > Internal identity Store	s > Users		
► 1/3 Network Resources	Internal Users				
Gers and identity Stores Identity Groups	Filter: Match it: Go 🗸				
 ✓ Internal Identity Stores Users Hosts External Identity Stores 	Status	User Name	 Identity Group 	Description	
		user1	All Groups:Wireless Users	PEAP:mschapv2 users	
	F 9	user2	All Groups:Wireless Users	EAPFAST user	
Certificate Authorities Certificate Authentication Profile Identity Store Sequences					
Policy Elements					

ةسايسلا رصانع فيرعت

لوصولاب حامسلا نييعت نم ققحت.

cisco Cisco Secure ACS							
 My Workspace 	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles						
Network Resources	Authorization Profiles						
🕨 🎳 Users and identity Stores	Filter Match It Go V						
👻 🏟 Policy Elements							
Session Conditions Authorization and Permissions	Name Description Permit Access						
 Network Access Authorization Profiles 							
 Device Administration Named Permission Objects 							
Access Policies							
Monitoring and Reports							
🕨 🍓 System Administration							

لوصولا تاسايس قيبطت

ئشنننس .دعاوقلا نيوكت ةيفيكو اهمادختسإ دارملا ةقداصملا قرط ددحنس ،مسقلا اذه يف .ةقباسلا تاوطخلا ىلإ دنتست دعاوق

ةيلاتلا تاوطخلا لمكأ:

ا.كىلإ يضارتفالا لوصول<كوصولا تامدخ<لوصولا تاسايس ىلإ لقتنا. ةكبشلا ىلإ يضارتفالا لوصولا" :ريرحت<ةكبشلا.

cisco Cisco Secure A	CS
 My Workspace 	Access Policies > Access Services > Default Network Access > Edit "Default Network Access"
Network Resources	
B Users and Identity Stores	General Allowed Protocols
► Sp. Policy Elements	Name: Default Network Access
👻 🛼 Access Policies	Description: Default Network Access Service
Access Services Bervice Selection Rules O Default Device Admin	Service Type : Network Access
Default Network Access	Identity
▶ Ø deleteme	Group Mapping
Monitoring and Reports	Authorization
🖌 🍓 System Administration	

.2،لاثملا اذه يف .هيلع نييكلساللا ءالمعلا ةقداصم ديرت يذلا EAP بولسأ ددح و EAP-FAST مدختسن

cisco Cisco Secure A	CIS
🕨 🧭 My Workspace	Access Palicies > Access Services > Default Network Access > Edit: "Default Network Access"
Network Resources	
Big Users and Identity Stores	General Allowed Protocols
Policy Elements	Process Host Lookup
🖌 🌉 Access Policies	Authentication Protocols
Access Services El Service Selection Rules O Default Device Admin	Allow PAP/ASCI Allow CHAP
Default Network Access Identity	► IF Allow MS-CHAPv1
> Ø deleterne	► MIow MS-CHAPv2
Monitoring and Reports	► 🕅 Allow EAP-MD5
System Administration	► 🕅 Allow EAP-TLB
	►
	Allow PEAP
	► 🕅 Allow EAP-FAST
	Preferred EAP protocol LEAP

- 👗 Access Policies	► Allow LEAP
Access Services El Service Selection Rules O Default Device Admin O Default Network Access Idently Authorization Ø deleteme El Monitoring and Reports System Administration	 ✓ Allow PEAP PEAP Inner Methods ✓ Allow EAP-MS-CHAPv2 ✓ Allow Password Change Retries: 1 ✓ Allow EAP-GTC ✓ Allow Password Change Retries: 1
	 Allow EAP-FAST EAP-FAST Inner Methods Allow EAP-MS-CHAPV2 Allow Password Change Retries: 3 Allow EAP-GTC Allow FASSword Change Retries: 3 Allow TLS-Renegotiation Use PACs Don't Use PACs Tunnel PAC Time To Live: 90 Days v Proactive PAC update will occur after 10 % of PAC Time To Live has expired Allow Authenticated In-Band PAC Provisioning Berver Returns Access Accept After Authenticated Provisioning Berver Returns Access Accept After Authenticated Provisioning Allow Machine Authentication Machine PAC Time To Live: 1 Weeks v Enable Stateless Session Resume Authorization PAC Time To Live: 1 Hours v
	Submit Cancel

.3.لاسرإ يلع رقنا

4نيمدختسملا مدختسن ،لااثملا اذه يف .اهتددح يتلا ةيوهلا ةعومجم نم ققحت. تارييغتلا ظفحب مق .ACS ىلع هانأشنأ يذلا ،نييلخادلا.

Access Policies > Access Sen	C Rule based result	coess > identity selection
Identity Source: Internal Us	ers	Select
✓ Advance	ad Options	
If authentin	ation failed Reject	•
If user not	lound Reject	
If process	ailed Drop	•
Note: For a processing be rejected	uthentications using PE when authentication fa	AP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue ils or user is not found. If continue option is selected in these cases, requests will

.5تامدخ < لوصولا تاسايس ىلإ لقتنا ،ليوختلا فيرعت فلم نم ققحتلل

ليوختلاحةكبشلا ىلإ يضارتفالا لوصولا<لوصولا.

يأو ةكبشلا ىلإ لوصولا مدختسملل حيتتس طورش يأ تحت صيصختلا كنكمي ةيلباقلا هذه رفوتت الو .هيلع ةقداصملا درجمب هررمتس (تامس) ليوخت فيصوت ،زاهجلا عونو ،عقوملا ديدحتب انمق ،لاثملا اذه يف ACS 5.x يف الإ ليدعتلل .EAP ةقداصم بولسأو ،ةيوهلا ةعومجم ،لوكوتوربلا

Access Polices > Access Services > Default Network Access > Authorization Standard Policy Exception Policy
Network Access Authorization Palicy
Filter. Status Match it Equais Enabled Clear Filter Go
Status Name Coeditions Results NDQ:Lecation Time And Date Authorization Profiles Hit Count
No deta to display
Mails finets Import/192168150.24/accodmix/Policy/ppcAction.do Second Conditions Import/192168150.24/accodmix/Policy/ppcAction.do Compound Conditions Import Policy/ppcAction.do Device Filter Import Policy/ppcAction type Device Filter Import Policy/ppcAction.do Device Policy Filter Import Policy/ppcAction.do Was Nachtme Activenticated Import Policy/ppcAction.do
Default If no rules defined or no enabled rule matches. Permit Access
Create + Duplicate + Edit Delete A Move to Y

.6.تارييغتلا ظفحا مث ،قفاوم قوف رقنا

7حامسلا متي ،دعاوق ةيأ فيرعت متي مل اذإ .ةدعاق ءاشنإ يف ةيلاتلا ةوطخلا لثمتت. طورش ةيأ نود لوصولاب ليمعلل.

> ةعومجم يف نيمدختسملاب ةصاخ ةدعاقلا هذه .1-ةدعاقلا < ءاشنإ قوف رقنا ."نييكلساللا نيمدختسملا"

Access Pa	iloles > Access Services > De	fault Network Access > Authorization				
Standard	Policy Exception Policy					
Networ	k Access Authorization Pr	tions .				
Fiter.	Status	Cisco Secure ACS - Mosilla Firefox			×	
		192168150.24 https://192168	150.24/acsadmin/Policy	inputAction.do	合	
	Status Name NE			-		
	No data to display	General		-0		
		Name: Rule-1	Status: Enabled	- 0		
		The Customize b policy conditions	utton in the lower rigt and results are availa	It area of the policy rules screen con able here for use in policy rules.	trois which	
		NDG:Location:	in	All Locations LAB	Select	
		NDG:Device Type:	in	 All Device Types 5500 	Select	
		Protocol:	match	Radus	Select	
		Identity Group:	in	MI Groups Wireless Users	Select	
		Eap Authentication Method	-ANY-			
		Results Authorization Profiles: Permit Access Select Deselect OK Cancel		You may select multiple authorization pro defined in multiple profiles will use the va profile defined.	files. Attributes Aue from the first	
Onet	ul parter tal an		1			Lungard
Create	- I. Dobecter I. Equ				Custemas	HICount

.8:يلي امك ةشاشلا ودبتس .تارييغتلا ظفحب مق

COLUMN PROPERTY	Access As	thorization Policy						
Filter. St	atus	- Mate	ch it Equals 💽 Enat	bled - C	ear Filter Go 🔫			
Status	Name	NDG:Location	NDG Device Type	Conditi Protocol	identity Group	Eap Authentication Method	Resul	Profile
۲	Rule-1	in All Locations:LAB	in All Device Types 5508	match Radius	in All Groups:Wireless Users	-4117-	Permit Acces	s
Default		If no rules defined or r	no enabled rule matches.				Permit Acces	5

ريرحتب مقف ،طورشلا عم نوقباطتي ال نيذلا نيمدختسملا ضفر يف بغرت تنك اذإ ."لوصولا ضفر" لوقلل ةيضارتفالا ةدعاقلا

.9وأ طيسب جەن نيوكتل ةحفصلا ەذە مدختسأ .ةمدخلا رايتخإ دعاوق ديدحتب نآلا موقنس

اذه يف .ةدراولا تابلطلا ىلع اەقيبطت متيس يتلا ةمدخلا ديدحتل دعاوق ىلإ دنتسم .دعاوق ىلإ ةدنتسم ةسايس مادختسإ متي ،لاثملا

A	coess Policies > Access Services > Service Selection Rules									
L	0 Sin	gle res	ult select	ton 🤗 A	lule based resul	t selection				
	Servic	e Sele	ction Pol	cy						
	Filter	Statu	5 💌	Natch it	Equals 💌	Enabled	✓ Clea	ar Filter	Go 🔫	
			Status	Name	Protocol	Conditions			Results Service	Htt Count
	1		۲	Rule-1	match Radius				Detault Network Access	0
	2		8	Rule-2	match Tacacs				Default Device Admin	0

ةيكلساللاا ةيلحملا ةكبشلا يف مكحتلا رصنع نيوكت (WLC)

ةيلاتلا تاوطخلا نيوكتلا اذه بلطتي:

- 1<u>مادختساب (WLC) ةيكلساللا قيلحملا ةكبشلا يف مكحتلا رصنع نيوكتب مق.</u> <u>ةقداصملا مداخ ليصافت</u>
 - .(VLANs).2 <u>قېكېمانېدلا تامجاولا نېوكتب مق</u>
 - <u>WLAN (SSID).</u>3. ت<u>اكبش نيوكت</u>

(WLC) ةيكلساللاا ةيلحملا ةكبشلا يف مكحتلا رصنع نيوكتب مق ةقداصملا مداخ ليصافت مادختساب

ەنكمي ىتح (WLC) ةيكلساللاا ةيلحملا ةكبشلا يف مكحتلا رصنع نيوكت يرورضلا نم .ىرخأ تاكرح يأل كلذكو ،ءالمعلا ةقداصمل RADIUS مداخب لاصتالا

:ةيلاتلا تاوطخلا لمكأ

- .1.نامألا قوف رقنا ،مكحتلا ةدحول (GUI) ةيموسرلا مدختسملا ةهجاو نم
- .2مداخ نيب مدختسملا كرتشملا يرسلا حاتفملاو RADIUS مداخب صاخلا IP ناونع لخدأ RADIUS و WLC.

مداخ يف ەنيوكت مت يذلا ەسفن وە كرتشملا يرسلا حاتفملا اذە نوكي نأ بجي .RADIUS

cisco			WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	RADIUS Authenti	cation Servers	s > New					
 AAA General RADIUS Authentication Accounting Folbeck TACACS+ LDAP Local Net Users MAC Filtering Disabled Clienta User Login Policies AP Policies Password Policies Local EAP Priority Order Certificate Access Control Lists Wireless Protection Policies 	Server Index (Priori Server IP Address Shared Secret Form Shared Secret Confirm Shared Sec Key Wrap Port Number Server Status Support for RFC 357 Server Timeout Network User Management IPSec	ty) at ret	1 x 192.168.150.2 ASCII • •••••• (Designed for 1812 Enabled • Enabled • Enable Fable Enable Enable Enable	FIPS custome	ers and requires a	key wrap compl	ant RADI	US server)
k Web Auth								

Advanced

(VLANs) ةيكيمانيدلا تاهجاولا نيوكت

.WLC لا ىلع يكرح نراق لكشي نأ فيك ءارجإ اذه فصي

ةيلاتلا تاوطخلا لمكأ:

اةدحوب ةصاخلا (GUI) ةيموسرلا مدختسملا ةهجاو نم ةيكيمانيدلا ةهجاولا نيوكت مت. تاهجاولا < مكحتلا ةذفان يف ،مكحتلا.

cisco	MONITOR WLAN	s <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Controller	Interfaces > Nev	w			
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management POrts NTP CDP	Interface Name VLAN Id	vlan253 253			

.2.قيبطت قوف رقنا

انه VLAN 253) يكرح نراق اذه نم ةذفان ريرحتلا ىلإ كلقني اذه.

.3.ةيكيمانيدلا ةەجاولا ەذەل ةيضارتڧالا ةباوبلاو IP ناونع لخدأ

cisco	MONITOR WLANS		WIRELESS	<u>s</u> ecurity	MANAGEMENT
Controller Ceneral Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server	MONITOR WLANS OF Interfaces > Edit General Information Interface Name NAC Address Configuration Guest Lan	CONTROLLER Vlan253 00;24;97	WIRELESS :09:63:cf	SECURITY	MANAGEMENT
 Ports NTP CDP Advanced 	Quarantine Quarantine Vian Id Physical Information The interface is attache Enable Dynamic AP Management Interface Address	n ed to a LAG.			
	VLAN Identifier IP Address Netmask Gateway DHCP Information Primary DHCP Server Secondary DHCP Server Secondary DHCP Server Access Control List ACL Name Note: Changing the Interf	253 192.168.153 255.255.255 192.168.153 192.168.153 192 er	.81 .0 .1 2.100.130.23	Alls to be ectivity for	

.4.قيبطت قوف رقنا

.5:يلي امك اەنيوكت مت يتلا تاەجاولا ودبتس

ululu cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>s</u> ecurity	MANAGEMENT		5 HELP	FEEDBACK	
Controller	Interfaces	\$								
Inventory	Interface	Name	1	/LAN Identifier	IP Address	s Interfac	e Type Dy	mamic AP I	Management	
Interfaces	manageme	nt	;	75	192.168.75	.44 Static	En	abled		
Interface Groups	service-por	±	,	4/A.	0.0.0.0	Static	No	t Supported		
Multicast	virtual		,	¢∕A.	1.1.1.1	Static	No	x Supported		
Network Routes	<u>vlan253</u>		;	253	192,168,15	3.81 Dynamic	Di	sabled		
Internal DHCP Server										
Mobility Management										
Ports										
▶ NTP										
CDP										
Advanced										
Advanced										

WLAN (SSID) تاكبش نيوكت

ةيلحملا ةكبشلا يف مكحتلا رصنع يف WLAN تاكبش نيوكت ةيفيك ءارجإلا اذه حرشي .(WLC) ةيكلساللا

ةيلاتلا تاوطخلا لمكأ:

تاكبش ىلإ لقتنا ،مكحتلا ةدحوب ةصاخلا (GUI) ةيموسرلا مدختسملا ةهجاو نم WLAN1 تاكبش ىلإ لقتنا ،مكحتلا ةدحوب ةصاخل ةديدجلا WLAN تاكبش ةذفان ضرع متي .ةديدج WLAN قكبش ءاشنإل ديدج ءاشنإ <

.WLAN SSID.2 تامولعمو WLAN فرعم لخدأ

ةكبشل SSID فرعمك GOA لاثملا اذه مدختسي .WLAN SSID مساب مسا يأ لاخدإ كنكمي WLAN SSID فرعمك WLAN.

cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMAND5
WLANs	WLANs >	New					
 WLANS WLANS ▶ Advanced 	Type Profile Ne SSID ID	erne	gos gos 1				

.WLAN goa.3 لا نم ةذفان edit لا ىل تبهذ wLAN goa.3 قربطي ةقطقط WLAN goa.3.

،، ،،، ı، cısco	MONITOR MLANS	ONTROLLER WIRELESS	SECURITY MANAGEM	MENT COMMANDS HELP
WLANs	WLANs > Edit 'goa	1		
WLANS WLANS	General Security	QoS Advanced		
Advanced AP Groups	Profile Name Type SSID Status Security Policies Radio Policy Interface/Interface Group(G) Nulticast Vian Featur Broadcast SSID	gos WLAN cos Enabled [WPA2][Auth(802.1X (Modifications done unde All vlan253 • Enabled Enabled Enabled	+ CCKM)] r security tab will appear a	after applying the changes.)

uluilu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY
WLANs	WLANs > Edit 'goa'
WLANs WLANs Advanced	General Security QoS Advanced Laver 2 Laver 3 AAA Servers
	Layer 2 Security [®] WPA+WPA2 - <i>B</i> MAC Filtering WPA+WPA2 Parameters
	WPA Policy WPA2 Policy WPA2 Encryption Auth Key Mont 802.1X+CCKN

WLANs > Edit 'goa'

General Security QoS /	dvanced	
Layer 2 Layer 3 AAA Ser	vers	
Select AAA servers below to over	ide use of default servers on this WLAN	
Radius Servers		LDAP Servers
Radius Server Overwrite interface	Enabled	Server 1 None -
	Authentication Servers Accounting Servers	Server 2 None 💌
	Totabled Totabled	Server 3 None •
Server 1	IP:192.168.150.24, Port:1812 V None V	
Server 2	None Vione V	
Server 3	None v None v	
Local EAP Authentication		
Local EAP Authentication Enabl	ed	
Authentication priority order fo web-auth user	я	
Not Used	Order Used For Authentication	

WLANs > Edit 'goa'

General Security QoS Advanc	red
Allow AAA Override 🛛 Enabled	DHCP
Coverage Hole Detection Coverage Hole Detection Coverage Hole Detection	DHCP Server Override
Aironet IE 🛛 🖓 Enabled	DHCP Addr. Assignment 🕅 Required
Diagnostic Channel TEnabled	Management Frame Protection (MFP)
1Pv6 Enable 2	MPP Client Protection # Disabled -
P2P Blocking Action Disabled	DTIM Period (in beacon intervals)
Client Exclusion 2 Enabled	802.11a/n (1 - 255) 1
Maximum Allowed 0	802.11b/g/n (1 - 255) 1
Static IP Tunneling 😰 🗌 Enabled	NAC State None •
ff Channel Scanning Defer	Load Balancing and Band Select
Scan Defer Priority 0 1 2 3 4	S 6 7 Client Load Balancing
Scan Defer Time(msecs) 100	Client Band Select #

ةدعاسملا Wireless Client ةادأ نيوكت

PEAP-MSCHAPv2 (user1)

ماظنب ةيلصألا مكحتلا ةدحو مدختسن اننإف ،ەكلمن يذلا ليمعلا رابتخالا زاەج يف .14.3 ليغشت جمانرب رادصإ لغشت Intel نم N-6300 زارط ةقاطب عم Windows 7 ليغشتلا .نيدروملا نم ليغشتلا جمارب ثدحأ مادختساب رابتخإ ءارجإب ىصوي

:Windows Zero Config (WZC) يف فيرعت فلم ءاشنإل ةيلاتا تاوطخلا لمكأ

- .1.ةيكلساللا تاكبشلا ةرادإ < تنرتنإلاو ةكبشلا < مكحتلا ةحول ىلإ لقتنا
 - .2.ةفاضإ بيوبتلا ةمالع قوف رقنا
 - .3.ايودي ةكبش فيصوت ءاشنإ ىلع رقنا



- ةيلحملا ةكبشلا يف مكحتلا رصنع ىلع اەنيوكت مت امك ليصافتلا فضأ. (WLC) ةيكلساللا
 - .فرحألا ةلاحل اساسح SSID دعي :ةظحالم
 - .5.(يلاتالا) Next قوف رقنا

9	㎡ Manually connect to a wi	reless network	
	Enter information for	the wireless network you want to add	_
	Network name:	goa	
	Security type:	WPA2-Enterprise	
	Encryption type:	AES 🔹	
	Security Key:	Hide characters	
	Start this connection a	automatically	
	Connect even if the new Warning: If you select	etwork is not broadcasting this option, your computer's privacy might be at risk.	
1			-
		Ne	d Cancel

.6.دادعا ةيلمعلا تققد in order to دادعا ةيلمع ليصوت ريغي ةقطقط.

Manually connect to a wireless network	
Successfully added goa	
Change connection settings Open the connection properties so that I can change the settings.	
	Close

.PEAP.7 نيكمت نم دكأت

goa Wireless Network P	roperties	23
Connection Security		
Security type: Encryption type:	WPA2-Enterprise AES	
Choose a network aut Microsoft: Protected	hentication method: EAP (PEAP) Settings dentials for this connection each	
Advanced settings		
	OK	ncel

goa Wireless Network Properties	×
Connection	
Security type: WPA2-Enterprise	
Encryption type: AES -	
Choose a network authentication method:	
Microsoft: Protected EAP (PEAP) Settings	
Remember my credentials for this connection each time I'm logged on Advanced settings	
OK Cancel	

.8نكمتت ملو عبرملا اذه تددح اذإ .مداخلا ةداهش ةحص نم ققحتلاب موقن ال ،لاثملا اذه يف .ىرخأ ةرم رابتخالاا مث ةزيملا ليطعت لواحف ،لاصتالاا نم

Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
AAA Certificate Services
AddTrust External CA Root
Class 3 Public Primary Certification Authority
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
DigiCert High Assurance EV Root CA
DST Root CA X3 👻
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Enable Fast Reconnect
Enforce Network Access Protection Disconnect if convex does not access to watching in a Trive
Enable Identity Privacy
Enable Identity Privacy
OK Cancel

.9،لاح يأ ىلع .لوخدلا ليجستل Windows دامتعا تانايب مادختسإ كنكمي ،كلذ نم الدب

OK. قوف رقناو .كلذ مدختسن نل لاثملا اذه يف



.10.ةملكو username تلكش in order to دادعإ ةيلمع مدقتم تقطقط.

goa Wireless Network P	roperties	x
Connection Security		
Security type:	WPA2-Enterprise	
Encryption type:	AES 👻	
Choose a network aut	thentication method:	
Microsoft: Protected	EAP (PEAP) Settings	
Remember my cree time I'm logged on	dentials for this connection each	
Advanced settings		
	OK	ncel

Advanced settings		
802.1X settings 802.11 settings		
Specify authentication mode:		
User authentication Save credentials		
Delete credentials for all users		
Enable single sign on for this network		
Perform immediately before user logon		
Perform immediately after user logon		
Maximum delay (seconds): 10		
Allow additional dialogs to be displayed during single sign on		
This network uses separate virtual LANs for machine and user authentication		
OK Cancel		

Windows Security	
Save crede Saving your cre when you're ne	ntials edentials allows your computer to connect to the network ot logged on (for example, to download updates).
	user1
	•••••
	OK Cancel

لاصتالل نآلا ةزهاج ليمعلل ةدعاسملا ةادألا.

EAP-FAST (user2)

ماظنب ةيلصألاا مكحتلا ةدحو مدختسن اننإف ،ەكلمن يذلا ليمعلا رابتخالا زاهج يف .14.3 ليغشت جمانرب رادصإ لغشت Intel نم N-6300 زارط ةقاطب عم Windows 7 ليغشتلا .نيدروملا نم ليغشتلا جمارب ثدحأ مادختساب رابتخإ ءارجإب ىصوي

:WZC يف فيصوت ءاشنإل ةيلاتلا تاوطخلا لمكأ

.1.ةيكلساللا تاكبشلا ةرادإ < تنرتنإلاو ةكبشلا < مكحتلا ةحول ىلإ لقتنا

.2.ةفاضإ بيوبتلا ةمالع قوف رقنا

.3.ايودي ةكبش فيصوت ءاشنإ ىلع رقنا



.4ةيلحملا ةكبشلا يف مكحتلا رصنع ىلع اەنيوكت مت امك ليصافتلا فضأ (WLC) ةيكلساللا

.فرحألا ةلاحل اساسح SSID دعي :ةظحالم

.5.(يلاتلا) Next قوف رقنا.5.

0	Manually connect to a wi	reless network	
	Enter information for	the wireless network you want to add	
	Network name:	goa	
	Security type:	WPA2-Enterprise	
	Encryption type:	AES 🔹	
	Security Key:	Hide characters	
	Start this connection a	automatically	
	Connect even if the n Warning: If you select	etwork is not broadcasting this option, your computer's privacy might be at risk.	
		Next	Cancel

.6.دادعا ةيلمعلا تققد in order to دادعا ةيلمع ليصوت ريغي ةقطقط.

Manually connect to a wireless network	
Successfully added goa	
 Change connection settings Open the connection properties so that I can change the setter 	ings.
	Close

.EAP-FAST.7 نيكمت نم دكأت

بجي .ةقداصم ةقيرطك EAP-FAST ىلع يضارتفا لكشب WZC يوتحي ال :ةظحالم ،Intel ةقاطب اهنأ امب ،لاثملا اذه يف .ةيجراخ ةهجل عبات دروم نم ةدعاسملا ةادألا ليزنت .ماظنلا ىلع ةتبثم Intel PROSet انيدلف

goa Wireless Network Pr	operties
Connection Security	
Security type: Encryption type:	WPA2-Enterprise AES
Choose a network aut Cisco: EAP-FAST Microsoft: Smart Card Microsoft: Protected B Cisco: LEAP Cisco: PEAP Cisco: EAP-FAST Intel: EAP-SIM Intel: EAP-TTLS Intel: EAP-AKA Advanced settings	entication method: or other certificate AP (PEAP) in each
	OK Cancel

goa Wireless Network Properties			
Connection			
Security type: WPA2-Enterprise			
Encryption type: AES			
Choose a network authentication method:			
Cisco: EAP-FAST			
Remember my credentials for this connection each time I'm logged on			
Advanced settings			
OK Car	ncel		

.8.مداخلا ةداەش نم ققحتلا ديدحت مدع نم دكأتو يئاقلتلا PAC دادمإب حامسلا نكم

EAP-FAST Properties
Connection User Credentials Authentication About
Use anonymous outer identity anonymous Use Protected Access Credentials (PAC) Allow automatic PAC provisioning
PAC Authority: None Import
Validate server certificate Connect to only these servers:
AAA Certificate Services AddTrust External CA Root Class 3 Public Primary Certification Authority Class 3 Public Primary Certification Authority Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA DigiCert High Assurance EV Root CA DST Root CA X3 Do not prompt user to authorize new servers or trusted certification authorities.
OK Cancel Help

9نم الدب .2 مدختسملا تاغوسم لخدأو ،مدختسملا تاغوسم بيوبتلا ةمالع قوف رقنا. اذه يف ،لاح يأ ىلع .لوخدلا ليجستل Windows دامتعا تانايب مادختسإ كنكمي ،كلذ .كلذ مدختسن نل لاثملا

EAP-FAST Properties	? ×	
Connection User Credentia	Is Authentication About	
Use certificate on th	is computer	
Use one-time passw	ord	
Use Windows userna	ame and password	
Prompt automatically	/ for username and password	
O Use saved username	and password	
Username:	user2	
Password:	•••••	
Confirm password:	•••••	
₽		
	OK Cancel Help	

.0K.10 قوف رقناو

EAP-FAST Properties	? <mark>×</mark>
Connection User Credentials Authentication About	
Colort authorities institude	
Select authentication method:	
Any method Configure .	
Enable Fast Reconnect	
Enable Posture validation	
OK Cancel	Help

2. مدختسملل لاصتالل نآلا ةزهاج ليمعلل ةدعاسملا ةادألا

.PAC يمحم لوصو غوسم RADIUS مداخ لسري ،ةقداصملا 2مدختسملا ةلواحم دنع :ةظحالم .ةقداصملا لامكتسال (PAC) يمحملا لوصولا تاغوسم لوبق



ةحصلا نم ققحتلا

جيحص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا.

مجرتم ةادأ مدختسا. show <u>رماوأ ضعب (طقف نيلجسملاءالمعلل) جارخالا مجرتم ةادأ</u> معدت . show رمألا جَرخُم ليلحت ضرعل (OIT) جارخإلا

(PEAP-MSCHAPv2) 1 مدختسملا نم ققحتلا

ةيلحملا ةكبشلا يف مكحتلا ةدحوب ةصاخلا (GUI) ةيموسرلا مدختسملا ةهجاو نم .MAC ناونع ددحو ،ءالمعلا < ةشاشلا ىل لقتنا ،(WLC) ةيكلساللا

Clients > Detail

Client Properties		AP Properties	
MAC Address	00:24:d7:ae:f1:98	AP Address	2c:3f:38:c1:3c:f0
IP Address	192,168,153,107	AP Name	3502e
Client Type	Regular	AP Type	802.iian
User Neme	user1	WLAN Profile	9018
Port Number	13	Status	Associated
Interface	vian253	Association ID	1
VLAN ID	253	802.11 Authentication	Open System
CCX Version	CCXv4	Reason Code	1
E2E Version	E2Ev1	Status Code	0
Mobility Role	Local	CF Pollable	Not Implemented
Mobility Peer IP Address	N/A	CF Pol Request	Not Implemented
Policy Manager State	RUN	Short Preamble	Not Implemented
Management Frame Protection	No	PBCC	Not Implemented
UpTime (Sec)	12	Channel Agility	Nat Implemented
Power Save Node	OFF	Re-authentication timeout	86365
Current TxRateSet	6.0.9.0.12.0.15.0.24.0.36.0	Remaining Re-authentication 1.54. timeout	0
Data RateSet	0	WEP State	WEP Enable

Security Information

Security Policy Completed	Yes
Policy Type	REN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Rediue NAC State	RLIN

تالاح WLC RADIUS:

<#root>

(Cisco Controller) >

show radius auth statistics

	Authentication Servers:
Server Index	
Server Address	192.168.150.24
Msg Round Trip Time	1 (msec)
First Requests	
Retry Requests	

Accept Responses1Reject Responses0Challenge Responses7Malformed Msgs0Bad Authenticator Msgs0

Pending Requests	0
Timeout Requests	0
Unknowntype Msgs	0
Other Drops	0

ACS: تالجس

- .1:ددع برض لI تدهاش steps in order to اذه تمتأ
- اتارم ددع ثيدحت نم دكأتف ،ةقداصملا نم ةقيقد 15 لالخ تالجسلا صحفب تمق اذا. لوصولا

A00	ess F Sir Servik	Policies » ngle rea ce Sele	Access a	Services > 1on 🔍 R Icv	Service Selection Rules ule based result selec	dion						
	Filter: Status Match it: Equals Enabled Clear Filter Go											
			Statue	Name	Co Protocol	nditions		Results Service	Hit Count			
	1		0	Rule-1	match Radius			Default Network Access	1			
	2		0	Rule-2	match Tacaca			Default Device Admin	0			

.b.ةحفصلا سفن لفسأ يف لوصولا تارم ددع ل بيوبت ةمالع كيدل.

Access Palo	ies > Access Services > I	Default Network Access > Ast	orization				
Standard P	Policy Exception Policy						
Network	Access Authorization	Policy					
Filter: 9	talus	Match if: Equals	Enabled	💌 Clear Fitter 🛛 Go 💌			
Name	NDG:Location	NDG:Device Type	Conditi Protacol	ons Identity Group	Eap Authentication Method	Results Authorization Profiles	Hit Count
Rule-1	in All Locations LAB	in All Device Types:5508	match Radius	in All Groups:Wireless Users	-ANY-	Permit Access	1
							п
4							{}
faut	If no rules define	d or no enabled rule matche	8.			Permit Access	V
Create	- Duplicate - E	dit Delete \Lambda Mov	e to V			Customize	HitCount

قوطقط monitore and Reporting تقطقط عالي القتنا. تاقداصمل الن القتنا القامي القام التقامي التقامي التقامي التقا التا التي التا تم التقام التقامي التقامي التقامي التقامي التقامي التقامين التقامين التقامين التقامين التقامين التقامي التقام التقامين التقام

그 5 1											Launch Inter	active Vever
Showing Page 1	of 1					6	loto Paga: Ge					
AAA Protocol > RADIU	S Auther	tication	•									
Authentication Status : Pa Dote : Je	nuary 29, 3	2012 05:4	la PM - J	muory 29,	2012 06:10 PM (1	.ost 30 Minufes (Lost Hour	I Loot 12 Hours Tedar Yeat	erder i Last 7 Dov	a I Lost 30 Dava)			
Generated on January 29,	2012 6 10	42 PM E	8T									
Rebai V-Fast X-Fail %-	Click for de	state	Q -Mause	e over then	n flor additional info	mater						
Logged At	RADIUS	NAS Falure	Details U	Isomanie	MAC/IP Address	Access Service	Authentication Method	Natwork Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Instanc
Jan 29,12 6:07:37.943 PM			e.,	iser1	00-24-d7-as-f1-98	Default Netesrk Access	PEAP (EAP MISCHAPV2)	WLC:5508	192.168.75.44			SALL-ACSS

(EAP-FAST) 2 مدختسملا نم ققحتلا

ةيلحملا ةكبشلا يف مكحتلا ةدحوب ةصاخلا (GUI) ةيموسرلا مدختسملا ةهجاو نم .MAC ناونع ددحو ،ءالمعلا < ةشاشلا ىلإ لقتنا ،(WLC) ةيكلساللا

Clients > Detail

Client Properties	Client	Properties
-------------------	--------	------------

MAC Address	00r24rd7raerf1r98	
1P Address	192.168.153.111	
Client Type	Regular	
User Name	user2	
Port Number	13	
Interface	vlan253	
VLAN ID	253	
CCX Version	CCXV4	•
EZE Version	E2Ev1	
Mobility Role	Local	
Mobility Role Mobility Peer IP Address	Local N/A	
Mobility Role Mobility Peer IP Address Policy Manager State	Local N/A RUN	
Mobility Role Mobility Peer IP Address Policy Manager State Management Frame Protection	Local N/A RUN No	
Mobility Role Mobility Peer IP Address Policy Manager State Management Frame Protection UpTime (Sec)	Local N/A RUN No 29	
Mobility Role Mobility Peer IP Address Policy Manager State Management Frame Protection UpTime (Sec) Power Save Mode	Local N/A RUN No 29 OFF	
Mobility Role Mobility Peer IP Address Policy Manager State Management Frame Protection UpTime (Sec) Power Save Mode Current TxRateSet	Local N/A RUN No 29 OFF m15	

AP Properties

AP Address	2cr3fr38rc1r3crf0
AP Name	3502e
AP Type	802.11an
WLAN Profile	goa
Statue	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication	86392
Remaining	
Re-authentication timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
ЕАР Туре	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

:ACS تالجس

.1:ددع برض لا تدهاش steps in order to اذه تمتأ

عتارم ددع ثيدحت نم دكأتف ،ةقداصملا نم ةقيقد 15 لالخ تالجسلا صحفب تمق اذاٍ. ماظنلا ىلإ لوصولا

Servi	ce Sele	ection Po	licy					
Filter	Statu	IS –	Match It.	Equals 💌	Enabled	Clear Filte	Go 🗢	
	Г	Status	Name	Protocol	Conditions		Results Service	Hit Cour
1		0	Rule-1	match Radius			Default Network Access	3
2	Г	0	Rule-2	match Tacacs			Default Device Admin	0

b.ةحفصلا سفن لفسأ يف لوصولا تارم ددع ل بيوبت ةمالع كيدل.

letwork	Access Authorization I	Policy					
Filter: S	tatus	Match if: Equals	 Enabled 	▼ Clear Fitter Go 🗢			
Name	NDG:Location	NDG:Device Type	Condition Protocol	ons Identity Group	Eap Authentication Method	Results Authorization Profiles	Hit Cou
Rule-1	in All Locations:LAB	in All Device Types:5508	match Radius	in All Groups: Wireless Users	-ANY-	Permit Access	2
							п
							л
đ	if no rules define	d or no enabled rule matche	15.			Permit Access	₽

قوطقط monitore and Reporting اىل لقتنا .ةديدج ةقثبنم ةذفان رەظيو monitore and Reporting ققطقط يتلا ةمدخلا ديدحت ةدعاق نم ققحتلل Details قوف رقنلا اضيأ كنكمي .مويلا- RADIUS اەقىبطت مت

28) 🖻											La	anch Interactive	Vewer 5
1991233	Showing Pa	çe 1	of 1		1111	int they	most Lost	Get	to Page: Ge					
AAA Pro	otocol > RA	DIUS	Auther	ticatio	n									
Authenti Data :	cation Status	: Pas Jan	s or Fail many 29, 3	2012 06:	SD PM -	January 29,	2012 06:23 PM (La	st 30 Nitrutes Last Hour L	ast 12 Hours Today Yesterday	Last7 Days Las	120 Days)			
Generate	ed on January	29, 2	12 6 23	17 PM E	ST									
Reica	d N-Fail	A-c	lich far di	dala	Q -Hee	aa siyar ilare	for additional inform	nation						
	Logged At		RACIUS Status	NAS Failure	Details	Usemane	MAC/IP Address	Access Service	Authentication Method	Natwork Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS INS
Jan 29,1	12 6 19 27 27	I PM	*		94	upor2	90-24-d7-ap-f1-98	Default Network Access	EAP-FAST (EAP-MSCH4P42)	WLC-5508	192.168.75.44			SALL-A
Jan 29	12 6 07 37 94	3 PM	*		4	user1	00-24-d7-ap-f1-98	Default Network Access	PEAP (EAP-MSCHAPV2)	WLC-5588	192 168 75 44			SALL-A

اهحالصإو ءاطخألا فاشكتسا

.امحالصإو نيوكتلا ءاطخأ فاشكتسال اهمادختسا كنكمي تامولعم مسقلا اذه رفوي

اهحالصإو ءاطخألا فاشكتسا رماوأ

مجرتم ةادأ مدختسا. show <u>رماوأ ضعب (طقف نيلجسملاءالمعلل) جارخالا مجرتم ةادأ</u> معدت . show رمألا جَرخُم لـيلحت ضرعل (OIT) جارخإلاا

.debug رماوأ مادختسإ لبق <u>حيحصتا رماواً لوح ةمهم تامولعم</u> ىلإ عجرا :ةظحالم

.WLC:1 لا ىلع رمأ اذه تردصأ ،ةلكشم يأ تنأ هجاوي نإ

- <mac add of client> ليمعلاا ءاطخأ حيحصت
 - debug aaa all enable •
- .جەنلا ريدم ةلاح نم ققحتلا <mac addr> ليمعلا ليصافت راەظإ
 - .ببس لشفلا تققد show radius auth statistics
 - .ءاطخألا حيحصت ليغشت فاقياٍ debug disable-all
- رصنع ىلع رطقلا فصن تايئاصحإ حسم لكلا رطقلا فصن ةقداصم تالاح حسم (WLC) ةيكلساللا ةيلحملا ةكبشلا يف مكحتلا

.2.لشفلا ببس ظحالو ACS يف ةدوجوملا تالجسلا نم ققحت

ةلص تاذ تامولعم

• <u>Cisco Systems - تادنټسملاو ينقټلا معدلا</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما