Cours 58 : Configuration Sans Fil

Dans ce cours nous verrons la configuration sans fil.

Nous ferons d'abord une introduction sur les topologies réseaux que nous utiliserons.

Nous ferons aussi une introduction sur la configuration nécessaire sur un Switch avant d'y connecter tous les appareils à ce Switch central.

Nous verrons la mise en place de base des contrôleurs sans fil LAN nous pourrons accéder au GUI (Graphical User Interface) et faire la configuration. Nous verrons ensuite comment configurer les interfaces WLC, et nous configurerons quelques WLAN. En dernier temps nous verrons quelques fonctionnalités additionnels de WLC.

La topologie du réseau que nous utiliserons sera la suivante :



Sur cette topologie on peut voir 1 Switch, UN WLC controler et 2 point d'accès (AP pou access Point). On peut voir que les points d'accès ne sont pas alimentés par des alimentations, elles sont alimentés par les câbles Ethernet qui fournissent l'énergie en PoE.

Comme on peut le voir sur l'image suivante le Switch supporte le PoE, tout comme le WLC (en haut)



La topologie du réseau en le suivant :



Le WLC est connecté au Switch par un LAG (Link Aggregation Group) ou EtherChannel. Les WLC supportent uniquement le LAG Statique et non pas PagP ou LACP. Nous utiliserons dans ce réseau 3 VLAN : VLAN 10 : Management, 192.168.1.0/24 VLAN 100 : Internal, SSID : Internal, 10.0.0.0/24 VLAN 200 : Guest, SSID : Guest, 10.1.0.0/24

Le Vlan 10 est utile seulement dans la gestion des appareils, modifier leurs configurations etc.. Les VLAN 100 et 200 seront utile dans l'usage des utilisateurs.

Le switch aura un SVI pour chaque VLAN à chaque fois l'adresse finissant par .1 de chaque sous réseau. Le WLC aura lui aussi une adresse IP de chaque VLAN aussi avec pour adresse finissant par .100 dans chaque sous réseau.

Le Switch a été configuré pour être à la fois le serveur DHCP et le serveur NTP. Seulement le lien avec le WLC doit être configuré avec le Switch pour être un port Trunk. Par exemple lorsqu'un client se connecte à l'un des points d'accès, les données sont transmises avec CAPWAP vers le WLC qui lui même fais le transfert vers le Switch. Le Switch transfère ensuite ses données au client en passant par le même chemin, c'est à dire le WLC puis le point d'accès. Maintenant que se passe t-il si le client du VLAN 100 (Interne) veut communiquer avec un autre client du VLAN 200 (Guest) ? Le client enverra le trafique vers son Gateway, qui transmettra au WLC puis au Switch. Le Switch va redistribuer le trafique vers le WLC qui le transmettra au Switch puis au point d'accès afin de le faire passer vers le client de l'autre VLAN. Comme sur le schéma suivant :



Commençons par faire la configuration du Switch, con utilise les commandes suivantes :

SW1(config)#vlan 10 SW1(config-vlan)#name Management SW1(config-vlan)#vlan 100 SW1(config-vlan)#name Internal SW1(config-vlan)#vlan 200 SW1(config-vlan)#name Guest
SW1(config)#int range f0/6 - 8 SW1(config-if-range)#switchport mode access SW1(config-if-range)#switchport access vlan 10 SW1(config-if-range)#spanning-tree portfast
SW1(config-if-range)#interface range f0/1 - 2 SW1(config-if-range)#channel-group 1 mode on
SW1(config-if-range)#interface port-channel 1 SW1(config-if)#switchport mode trunk SW1(config-if)#switchport trunk allowed vlan 10,100,200

On commence par créer les 3 VLAN, et leur donner un nom avec les commandes suivantes SW1 (config) #vlan_10

SW1(config-vlan)#name	Management
SW1(config-vlan)#vlan	<mark>100</mark>
SW1(config-vlan)#name	Internal
SW1(config-vlan)#vlan	<mark>200</mark>
SW1(config-vlan)#name	Guest

On configure ensuite les interface pour spécifier le « mode access » : SW1 (config) #int range f0/6 – 8

```
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#spanning-tree portfast
```

On configure les interfaces vers le WLC en Etherchannel (LAG) avec les commandes suivantes : WLC supporte uniquement le LAG statique et non pas PagP ou LACP. SW1 (config-if-range) #interface range f0/1 - 2 SW1 (config-if-range) #channel-group 1 mode on

On configure les interface port channel en mode Trunk avec les commandes : SW1 (config-if-range) #interface port-channel 1 SW1 (config-if) #switchport mode trunk SW1 (config-if) #switchport trunk allowed vlan 10,100,200

Une fois ces cela configuré on lance ensuite les commandes suivantes pour la configuration des SVI (Switch Virtual Interface) des VLAN, du serveur DHCP et de NTP :

SWI(config)#interface vian 10
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
SW1(config-if)#in address 10.0.0.1 255.255.255.0
SW1(config-if)#interface vlan 200
SW1(config-if)#ip address 10.1.0.1 255.255.255.0
SW1(config)#ip dhcp pool VLAN10
SW1(dhcp-config)#network 192.168.1.0 255.255.255.0
SW1(dhcp-config)#default-router 192.168.1.1
Swi(uncp-config)#opcion 45 ip 192.108.1.100
SW1(config)#ip dhcp pool VLAN100
SW1(dhcp-config)#network 10.0.00 255.255.255.0
Swi(dncp-config)#default-router 10.0.0.1
SW1(config)#ip dhcp pool VLAN200
SW1(dhcp-config)#network 10.1.0.0 255.255.255.0
Swi(ancp-config)#default-router 10.1.0.1
SW1(config)#ntp master

On configure les SVI (Switch Virtual Interface) des Vlan, ces adresses sont utilisés comme passerelle par défaut de leur sous réseau, on lance les commandes suivantes :

```
SW1 (config) #interface vlan 10
SW1 (config-if) #ip address 192.168.1.1 255.255.255.0
SW1 (config-if) #interface vlan 100
SW1 (config-if) #ip address 10.0.0.1 255.255.255.0
SW1 (config-if) #interface vlan 200
SW1 (config-if) #ip address 10.1.0.1 255.255.255.0
```

On configure ensuite les pool DHCP avec les commandes suivantes :

Le VLAN 10 a la commande option 43 lancé, cette commande permet de dire aux points d'accès l'adresse IP de leur WLC (ici l'adresse du WLC est 192.168.1.100).

```
SW1(config)#ip dhcp pool VLAN 10
SW1(dhcp-config)#network 192.168.1.0 255.255.255.0
SW1(dhcp-config)#default-router 192.168.1.1
SW1(dhcp-config)#option 43 ip 192.168.1.100
```

```
SW1(config)#ip dhcp pool VLAN100
SW1(dhcp-config)#network 10.0.0.0 255.255.255.0
SW1(dhcp-config)#default-router 10.0.0.1
```

```
SW1(dhcp-config)#dhcp pool VLAN200
SW1(dhcp-config)#network 10.1.0.0 255.255.255.0
SW1(dhcp-config)#default-router 10.1.0.1
```

On lance en dernier temps la commande suivante pour activer le serveur NTP : SW1 (config) #ntp_master

Voyons à présent comment le WLC :



Lorsque l'on se connecte au WLC on utilise un câble console, le premier message que l'on peut voir apparaître est qu'il demande s'il est nécessaire de faire la terminer la configuration avec « autoinstall » qui va récupérer la configuration à partir d'un serveur TFTP. On configure ensuite le nom de système, le nom d'utilisateur et le mot de passe. On spécifie si l'on veut activer LAG (Link Aggregation), on indique « yes » car la réponse par défaut est ici « NO ». On indique les adresses voulue à configurer.

On continue la configuration basique du WLC en répondant aux question au lieu de lancer les commandes de configuration directement sur une ligne de commande :



Les trois première options sont utile, le Virtual Gateway IP est une adresse utilisé lorsque le WLC pour communiquer directement avec ses clients sans fil.

L'adresse Multicast est l'adresse utilisé pour transmettre le trafique vers ces IP.

Le Mobility/RF Group Name est utilisé lorsque l'on a par exemple plusieurs WLC et que l'on veut qu'ils fonctionnent ensemble.

A la suite de la configuration est demandé de configurer le SSID, on en configure pour l'instant 1 et on laisse le reste de la configuration avec les réponses par défaut.

On ne configure pas pour l'instant de serveur RADIUS nous changerons la politique de sécurité WLAN vers PSK donc il ne sera plus nécessaire de configurer de serveur RADIUS.

On entre le code du pays « FR » pour « France », ici on configure la France comme pays car le modèle est compatible avec l'Europe, le nom du modèle du point d'accès est avec un « E » pour Europe. (Modèle : AIR-CAP3502I-E-K9)



On continue la configuration du WLC :

Enable 802.11b Network [YES][no]: Enable 802.11a Network [YES][no]: Enable 802.11g Network [YES][no]: Enable Auto-RF [YES][no]:
Configure a NTP server now? [YES][no]: yes Enter the NTP server's IP address: 192.168.1.1 Enter a polling interval between 3600 and 604800 secs: 3600
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
Configuration saved! Resetting system with new configuration

On choisie ici d'activer les mode 802.11b, 802.11a, 802.11g. On configure ensuite le serveur NTP pour que le WLC ait le temps correct. On sauvegarde les paramètre et l'appareil se réinitialise.

Une fois tout cela configuré il est possible de se connecter au WLC par le moyen d'un navigateur web. On lance donc l'adresse du WLC (192.168.1.100) depuis le navigateur.



Il faut cliquer sur Advanced et « accéder à 192.168.1.100 »

On peut à présent accéder à l'interface de gestion du WLC, on clique sur « Login » puis on entre les identifiant et mot de passe configuré au départ :



© 2005 - 2014 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

Sign in		
https://192.1	68.1.100	
Username	admin	
Password		
		Sign in Cancel

Voici le panel de gestion du WLC :

ð wici	× +									0 -	-
a D C A A	A Not secure 4	44psk//192.1	68.1,100/	screens/fr	ameset.html					0	Δ :
uludu. cisco	MONITOR WLA	NS CONT	ROLLER	witerurs	s securi	Y MANAGEMENT O	OMMANDS HELP	FEEDBACK	Seve Cor	inguration Brog	Logout
Aonitor Summary • Access Points • Clsco CleanAir • Statistics • CDP • Rogues	Summary 3 Ansee Paris Supported -the de- rise de- -the de- -t					500 Series Wireless Cont	rollar IIII H 2004				
Clients	Controller Sur	mary				Rogue Summary	,				
Sleeping Clients	Hanagement IP Ar	dress 193	2.168.1.100								
Multicast	Software Version	7.6	120.0			Active Rogie APS		22	Datal		
Applications	Field Recovery Im	age 7.6	101.1			Address Register Calence		25	Dates		
Local Profiling	System Name	WL.	c1			Passar an Wood No.	the second s	2.1	LINGUE		
	Up Time	o d	days, 0 hours, 3 minutes			Rogues on miles in	6 mil 5				
	System Time	Fri	Oct 10 05:	12:30 2014							
	Redundancy Node	14/4				Top WLANS					
	Internal Temperat	ure +3	4 C			Profile Name		# of Clients			
	802.11e Network	State Em	Enabled group								
	802.11b/g Networ	k State End				Most Recent Tra	ins				
	Local Mobility Gro	io pro				Host Recent Traps					
	CPU(s) Usage	0%				Adhoc Rogue 1 1818	e914e1db14c1c3 detect	ed on Base Radio MAC 1 0810	d0:9fiedieci70 Interface n	0(802.11n(2.4 GH	Hz)) on Ch
	Individual CPU Us	10t 01W	0%. 1%/1	15		Link Up: Slot: 0 Po	rt: 2 Admin Status: E	nable Oper Status: Link Up r	retry-2		
	Hemory Usege	431	5			Link Up: Slot: 0 Po	rt: 1 Admin Stehus: E	nable Oper Status: Unic Up a	retry-2		
						Adhoc Reque : 98:	60ccaceb:91cb0 detect	ted on Base Radio MAC : 08:	d0:9f:ed:ec:70 Interface r	a: 0(802.11m(2.4 G	H(z)) on Ch
	Access Point 5	ummary				Adhoc Rogue : D4:	72:95:1c:87:e8 detec	ted on Base Radio NAC : 08:	:d0:9fted:ec:70 Interface r	10: 0(802.11=(2.4 G	ittz]) on Ci
						Man All					
	Tubi	i U	p	Dawn		Top Applications					
	Radios 2			0	Detail						
	ORD addresses			0	Datal	Apprication Name		racant count byte	Contractor		
	Bathon 2										
	Radice 0 Radice 0	•		• •	Detail						

On peut voir quelle interface sont active et des informations divers sur le WLC avec les points d'accès connectés etc..

Sur la page « Controller » on clique sur « Interfaces », on peut voir la VLAN que l'on configuré au départ, il n'y a pour le moment que le VLAN 10. On clique sur « New » pour en ajouter une nouvelle.

me	VLAN Identifier 10 N/A	IP Address 192.165.1.100 172.16.1.1	Interface Type Static Static	Dynamic AP Management Enabled Not Supported	Entries 1 - 3 of 3	iew
me	VLAN Identifier 10 N/A	IP Address 192.168.1.100 172.16.1.1	Interface Type Static Static	Dynamic AP Management Enabled Not Supported		
	10 N/A	192.165.1.100 172.16.1.1	Static Static	Enabled Not Supported		
	N/A	172.16.1.1	Static	Not Supported		

Les ports de WLC sont des ports physique sur lesquelles des câbles se connectent. Les interfaces WLC sont des interfaces logique inclus dans le WLC (Par exemple le SVI sur un Switch), WLC a plusieurs sorte de ports :

- Service port : Un port de gestion dédié utilisé pour la gestion. Il doit être connecté à un port access du Switch car il ne supporte qu'une seule VLAN. Ce port peut être utilisé pour se connecter à l'appareil tant que celui ci démarre, récupère le système, etc...

- Distribution system port : Ce sont les ports standard du réseau qui connectent au système de distribution (réseau câblé) et qui est utilisé pour le trafique de donnée. Ces ports se connectent aux ports Switch Trunk, et si plusieurs ports de distribution sont utilisé ils peuvent former un LAG.

- Port console : C'est le port console standard, avec un port RJ45 ou USB.

- Port de redondance : Ce port est utilisé pour se connecter à un autre WLC pour former une pair de haute disponibilité (High Availability en Anglais).

On peut voir ici 4 ports de distribution, et un port Console.





Voici un réseau avec une pair de 2 WLC, voyons chacun des numéro de 1 à 9 :

- 1) Le Service Port
- 2) Port Console (RJ45)
- 3) Port Console (USB)
- 4) USB (Pour mis à jour logicielle)
- 5) Port système de Distribution (Multi-gigabit)
- 6) Port système de Distribution (1-gig)
- 7) Bouton Reset
- 8) LED de Statut
- 9) Port de Redondance

Les WLC ont différents type d'interfaces :

- Interface de gestion : utilisé pour gérer le trafique comme Telnet, SSH, HTTP, HTTPS, Authentification RADIUS, NTP, Syslog, etc... Tunnels CAPWAP sont aussi formés vers/depuis l'interface de gestion du WLC.

- Interface de gestion de redondance : Lorsque deux WLC sont connectés par leurs ports de redondance, un WLC est « active » et l'autre est en « standby ». Cette interface est utilisé pour connecter et gérer le WLC « standby ».

- Interface Virtuel : Cette interface est utilisé lorsque l'on communique avec les clients sans fil vers le relai de requête DHCP, que l'on fait fonctionner une authentification web client, etc...

- Interface de port de Service : Si le port de service est utilisé, cette interface est lié vers celle ci et utilisé pour la gestion externe.

- Dynamic interface : Ce sont les interfaces utilisé pour cartographier un WLAN vers un VLAN. Par exemple, le trafique depuis le WLAN « internal » sera envoyé vers le réseau câblé depuis l'interface dynamic du WLC « internal »

Retournons à présent sur l'interface GUI pour configurer des interfaces Dynamique :



L'écran affiche la page suivante :

On indique l'adresse IP du vlan et son masque de sous réseau puis on applique les modifications en cliquant sur « Apply »

aludu		Sage Configuration ging Logout Befresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT OF	AMMANDS HELP ELEDBACK
Controller General Inventory	Interfaces > Edit General Information	< Back Apply
Interfaces Interface Groups Multicast Internal DHCP Server	Interface Name Internal M4C Addreas 00:08:2/f10:45:4f Configuration	
Hobility Management Ports NTP CDP Dot	Quarantine Quarantine Vian Ed WLC1	
mDNS Advanced	The interface is attached to a UAG. Exologramic AP	
	VLAN Identifier [100] IP Adress [10.0.0.100 Reference [253,255.55.5] Galeway [10.0.0.1	
	DHCP Information Preventy DHCP Server Exceedary DHCP Server DHCP Pray Hole Code DHCP Option 12	
	Access Control List	
	mDNS	
	mDNS ProBis none V	

Depuis le menu Dynamic on peut à présent voir les 3 interfaces, dont celle venant d'être crée qui est « Internal »

cisco	MONITOR WLANS CONTROLLER	WIRELESS SECU	RITY MANAGEMENT	COMMANDS	HELP FEEDBACK	Save Configuration Ping Log	aut Refresh
Controller General Inventory Interfaces Interface Groups Multicast > Internal DICP Server > Mobility Management Ports > NTP > ODP > IPv6 > mDNS > Advanced	Interface Name internal massement vrtual	VLAN Identifier 100 10 N/A	IP Address 10.0.0100 192.168.100 172.16.1.1	Interface Type Dynamic Static Static	Dynamic AP Hanagemen Disabled Enabled Not Supported	Entries 1 - 4 of 4	New

Il reste à créer l'interface « Guest », pour cela on procède comme auparavant en spécifiant les paramètre voulant être appliqué pour l'interface « Guest » :

	alla	di.		Sage Configuration Bing Logout Befresh
	CIS		MUANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	
	Controller	Interface	> New	< flack Apply
	General Inventory Interfaces Interface Multicast Internal D	Interface VLAN Id Groups HCP Server anagement	Guest 200	
	Ports	alala	MONITOR WILNER CONTROLLED INTRELESS SECTIOTY MANAGEMENT COMMANDS LIELD SEEDBA	Sage Configuration Bing Logout Befreak
	F CDP	Controller	Interfaces > Edit	e Rich Analysis
	 IPv6 mDNS Advanced 	General Inventory	General Information	Conv what
	P MOVANCEO	Interfaces Interface Groups	Interface Name Guest	
Sur cette	nage	Multicast	MAC Address 00:00:2f:10:65:6f	
an indiau		Internal DHCP Server Mobility Management	Configuration	
on maiqu	le les	Ports	Quarantine Ousrantine Vian Id 0	
adresse I	P	NTP CDP	NAS-ID WIC1	
nócossair	-o	▶ IPv6	Physical Information	
necessan	с <u>,</u>	mDN5	The interface is attached to a LAG. Enable Dynamic AP	
correspon	ndant	- Autonceu	Narapement LJ	
au VLAN	1 · 1		VLAN Identifier 200	
uu v Li li	••		1P Address 10.1.0.100	
			Netmask 255-255-0	
			DHCP Information	
			Primary DHCP Server 10.1.0.1	
			Secondary DHCP Server	
			DHCP Proxy Node Global V	
			Access Control List	
			ACL Name none V	
			mDNS	
			mDNS Profile name V	
	l		Note: Changing the Interface parameters causes the WLANs to be	

Toutes les interfaces sont à présent bien configurés :

cisco	MONITOR WLANS CONTROLLER	WIRELESS SECUR	RITY MANAGEMENT	COMMANDS	HELP EEEDBACK	Sage Configuration Bing	Logout Bchrish
Controller General Inventory	Interfaces Interface Name	VLAN Identifier	IP Address 10.1.0.100	Interface Type	Dynamic AP Management Disabled	Entries 1 - 5 of 5	New
Interface Groups Multicast Internal DHCP Server Mobility Management Ports NTP COP IPV6 IPV6 Advanced	internal manapatments victual	100 10 N/A	10.0.0.100 192.195.1.100 172.16.1.1	Dynamic Static Static	Disabled Enabled Not Supported		

Faisons la configuration des WLAN :

WLANS WLANS Entries 1 * WLANS Current Filter: None (Charse Filter) Creats Rew Ce * Advanced Image: Provide Rame WLANS SSID Admini Status Security Policies		ALER WIRELESS SECURITY	MANAGEMENT COMMANDS HE	Save Configure	ition <u>P</u> ing Logout <u>Befree</u>
WLANS VLANS Current Filter: Hone (Charge Filter) Create New Con > Advanced WLAN 1D Type Prefile Name WLAN SSID Admini Status Security Policies	WLANs				Entries 1 - 1 of 1
Advanced WLAN 1D Type Profile Name WLAN SSID Admin Status Security Policies Transition Transition Transition Transition	Current Filter: None	[Change Filter] [Clear Filter]		Create New V Go	
C . Black belowed belowed Beneficial Resulted States and	WLAN ID Type	Profile Name	WLAN SSID	Admin Status Security Policies	
T ALTAN THREAM T	C 1 WLAN	Internal	Internal	Enabled [WPA2][Auth(802.1X)]	
		MONITOR WLANS CONTRO WLANS Current Filter: None WLAN 10 Type 3 WLAN	MONITOR WLANS CONTROLLER WIPELLESS SECURITY WLANS Current Filter: None <u>Charge Filter</u>] ULAN ID Type Profile Name 2 WLAN Internal	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS IN WLANS Current Filter: None [Chanse Filter] ULAN ID Type Profile Name WLAN SSID 3 WLAN Internal Internal	BONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT CONTRACLE Security Configure WLANS Current Filter: None [Castos Filter] Create New Control Cont

Il n'y en a ici qu'une seul, le mode de politique de sécurité est WPA2, 802.1X, donc le mode Enterprise, nous allons configurer le mode PSK.

En cliquant sur le « 1 » à gauche il est possible de modifier ce WLAN.

cisco	MONITOR WLANS COM	TROLLER WIJRELESS SECURITY MAMAGEMENT COMMANDS HELP EEEDBACK	Sage Configuration Ping Logout Befrest
WLANs	WLANs > Edit "Intern	al'	< Back Apply
* WLANs WLANs	General Security	QoS Policy-Mapping Advanced	
Advanced	Profile Name	Internal	
	Туре	WLAN	
	SSID	Internal	
	Status	Enabled	
	Security Policies	[WPA2][Auth(802.1X)] (Rodifications done under security tab will appear after applying the changes.)	
	Radio Policy		
	Interface/Interface Group(G)	management V	
	Multicast Vian Feature	C Enabled	
	Broadcast SSID	C Enabled	
	NAS-ID	WLC3	

Nous allons modifier le « Interface Group » pour Internal et non plus pour « management ».

LANs	WLANs > Edit 'Intern	ali < Back Apph
WLANs WLANs	General Security	QoS Policy-Happing Advanced
Advanced	Profile Name	Internal
	Type	WLAN
	SSID	Internal
	Status	C Empled
	Radia Dellari	(Modifications done under security tab will appear after applying the changes.)
	Interface/Interface Group(G)	management V
	Hulticast Vian Feature	Informal
	Broadcast SSID	mangement
	NAS-ID	WLCL

Pour modifier afin d'utiliser le mode PSK, on se rend sur l'onglet « Security »

cisco	MONITOR WLANG CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	2476 Countration Bud College Black
WLANs	WLANs > Edit "Internal"	< Back Apply
WLANS WLANS	General Security QoS Policy-Mapping Advanced	
 Advanced 	Layer 2 Layer 3 AAA Servers Layer 2 Security 4 WMA-WMZ MACFiltering8 Fast Transition Protocolor Protocolor Protocolor Protocolor WMA-WMAA Parameters WMA-WMAA Parameters	ĺ
	WA Patry WA2 Entryption WA2 Entrypti	

Et nous modifions la gestion des clefs d'authentification et sélectionnons PSK :

	BONLOR ADDARS CONTROLLER MIRELESS SECORTLY MERADEMENT COMPANIES HEP DEDBACK	
/LANs	WLANs > Edit 'Internal'	< Back Appl
WLANS WLANS	General Security QoS Policy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	PNF Disabled V WPA+WPA2 Parameters	-
	WRA Reliey WRA 2 Roley WRA 2 Roley WRA 2 Roley Kars Trop Authentication Key Management	
	002.1X Ensable CCOM Ensable PSK I Daole FT 702.1X Esuble FT 705.1X Esuble	
	PSK Format ASCII V	
	WPA gtiv-randomize State Disable V	

On sélectionne aussi le PSK format pour ASCII et on entre un mot de passe et on applique les modifications. Il est possible de modifier le Layer 3 et de modifier le mode d'authentification :



Plusieurs modes sont présents :

-Web Authentication : Après que les clients sans fil ont leurs adresse IP et essaient d'accéder à la page web, ils doivent entrer un nom d'utilisateur et un mode de passe pour s'authentifier.

- Web Passthrough : même chose que Web Authentication mais aucun nom d'utilisateur ou mot de passe n'est requis. Un signal ou déclaration apparaît et le client doit tout simplement accepter pour avoir accès à Internet.

- Conditional et Splash Page, sont des options de redirection web similaire mais qui requière de manière additionnel une authentification 802.1X couche 2.

Il y a aussi un mode AAA :

cisco	HONITOR WLANS CON	TROLLER WIRELESS SECUR	ITY MANAGEMENT COMMANDS HELP FEEDBACK	Saya Configuration Ping Logout Refres
WLANs	WLANs > Edit 'Intern	aľ		< Back Apply
WLANS	General Security	QoS Policy-Mapping	Advanced	
Advanced	Layer 2 Layer 3	AAA Servers		
	Select AAA servers belo Radius Servers Radius Server Overwrit	w to override use of default serv te interface DEnabled	eers on this WLAN	
	Authentication Servers	Accounting Servers	EAP Parameters	
	Server 1	Enabled Enabled	Enable 🗌	
	Server 2	None V		
	Server 3	None Y		
	Server 4	None V		
	Server 5	None V None V		
	Radius Server Accountin	None V		
	Interim Update	0		
	I DAP Servers			•

Voyons l'onglet QoS :

cisco		TROLLER WIRELESS SECURIT	Y MANAGEMENT	COMMANDS HELP	EEEDBACK	Sage Configuration Bing Legout Befresh
WLANs	WLANs > Edit 'Interna	al*				< Back Apply
WLANS WLANS	General Security	QoS Policy-Mapping A	idvanced			
► Advanced	Quality of Service (QoS) Application Visibility AVC Profile Netflow Nonitor	Silver (best effort) V Trabled Trans V Trans V				
	VolMM Rolley 7820 AP CAC 7920 Client CAC	Allpund V Practical Enabled				

Il faut vérifier que le mode activé est bien le mode Silver (Best Effort).

Il existe d'autres modes comme Gold (Vidéo), Platinum (Voice), Bronze (Background)

Dans l'onglet « advanced » on peut voir différents services :

cisco	MONITOR WLANS CONTR	NOLLER WIRELESS SECURITY MANAGEMENT	COMMANDS HELP FEEDBACK	Sage Configuration Bing Logout Befres
WLANs	WLANs > Edit 'Internal	*		< Back Apply
* WLANS WLANS	General Security	QoS Policy-Mapping Advanced		
Advanced	Allow AAA Override		DHCP	
	Coverage Hole Detection	Enabled	DHCP Server Overnide	
	Aironet IE	Session Timeout (secs)	DHCP Addr. Assignment 🗌 Required	
	Diagnostic Channel	Dtnabled	OEAP	
	Override Interface ACL	IPv4 None V IPv6 None V	Split Tunnel (Printers) Enabled	
	Layer2 Acl	None ¥	Management Frame Protection (MFP)	
	P2P Blocking Action	Disabled		
	Client Exclusion 2	Enabled 60 Timeout Value (secs)	NFP Client Protection ^d Optional V DTIM Period (in beacon intervals)	
	Maximum Allowed Clients	n	002 Illa/n (1 - 255)	
	Static IP Tunneling 11	Enabled	802.11b/a/n (1 - 255) 1	
	Wi-Fi Direct Clients Policy	Disabled V	NAC	
	Haximum Allowed Clients Per AP Radio	200	NAC State None Y	
	Clear HotSpot Configuration	CEnabled	Load Balancing and Band Select	
	4			

Pour créer un nouveau WLAN ou clique sur « Go », nous allons vréer le WLAN Guest.

cisco	MONITOR WLANS C	ONTROLLER WIRELESS SE	CURITY MANAGEMENT COMMANDS	HELP FEEDBACK	Saye Con	liguration ging Logout Befreah
WLANs	WLANs					Entries 1 - 1 of 1
* WLANS WLANS	Current Filter: None	[Chanos Filter] [Clear Fi	liar]	Create New 👻	Go	
Advanced	WLAN ID Type	Profile Name	WLAN SSID	Admin State	us Security Policies	
	L WLAN	Internal	Internal	Enabled	[WPA2][Auth(PSK)]	

On indique le Type, le Profile Name et le SSID, il n'est pas nécessaire qu'il soit identiques.

cisco	MONITOR WLANS C	ONTROLLER WIRELESS	SECURITY MANAGEM	ent c <u>o</u> mmands	HELP	EEEDBACK	Saye Configuration	Bng	Logout Befresh
WLANs	WLANs > New						< 8	lack	Apply
₩LANS WLANS	Type Bacfile transp	WLAN V							
Advanced	SSID	Guest							
	1D	2 ¥							

On arrive ensuite à cette page :

սիսիս			Saye Configuration Ping Logout Balfrash
WLANs	WLANs > Edit 'Guest	NULER MIRELESS ZECURIT NYHNOENETT (YMMHNOS MEY" EEUBWUR	< Back Apply
 ₩LANS WLANS Advanced 	General Security Profile Name Type SSID Status Geounty Policies Radio Policy Interface/Interface Grang(I) Multicost Vite Feature Broadcast SSID NAS-ID	QoS Policy-Happing Advanced Guest WLNN Guest Enabled (WPA2](Auth(002.1X)) (MPA2](Auth(002.1X)) (MPA2](Auth(002.1X)) (MPA2)(Auth(002.1X)) (MPA2](Auth(002.1X)) (MPA2)(Auth(002.1X)) (MPA2)(Auth(002.1X)) (MPA2)(Auth(002.1X))	

Il doit être changé différents paramètres. Le « status » doit être activé. Et le l'interface Group doit aussi être changé pour « Guest ». On change aussi le mode d'authentification pour PSK comme vu précédemment.

Les deux WLAN sont à présent bien présent comme on peut voir :

cisco		ELANS CON	TROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS	HELP EEEDBACK		Saye Configuration	Ping	Logaut	Befresh
WLANs	WLANs							Enl	tries 1 -	2 of 2
* WLANS	Current Filter:	None	(Change Filter) [Clear Filter]		Create New 💌	50				
Advanced	U WLAN ID	Туре	Profile Name	WLAN SSID	Admin Status	Security Policies				
	01	WLAN	Internal	Internal	Enabled	[WPA2][Auch(PSK)]				
	0 2	WLAN	Guest	Guest	Enabled	(WPA2](Auth(PSK))				

Lorsqu'un client se connecte aux point d'accès on peut voir que le nombre de client augmente.

cisco	MONITOR W	II ANS	CONTROLI		SS SECURE					tion <u>Ping</u> Logout Befresh	
Monitor	-dudu cisco		4///		17211		and Comparison				
Summary						eter Model 2504					
Access Points				1	1 10						
Cisco CleanAir		2000				P					
Statistics	Controller S	unnina	ry			Rogue summary					
+ CDP	Hanagement D	P Addres	8 192-168	1.100		Active Rogue APs	185	5	Detail		
h Roomer	Field Recovery	Image	7.0.120.			Active Rogue Clients	2		Detail		
Climate	Version		7.6.101.	1		Adhoc Rogues	12		Retail		
Chemiss Clients	System Name		WLC1			Rogues on Wired Network	0				
Sieeping Cients	Op Time		U days, I	nouns, 24 min	utes 14						
Applications	Redundancy M	ode	N/A			Top WLANs					
Applications	Internal Tempe	rature	+34 C			Profile Name		# of Clies	nts		
Local Proning	802.118 Netwo	ork State	Enabled			Internal		2	Detail		
	802.11b/g Net	work Sta	ste Enabled			Guest		1	Detail		
	Local Hobility G	Group	group	group							
	CPU(s) Usage		0%			Most Recent Traps					
	Individual CPU	Usape	0%/0%	0%/1%							
	Nemory Usage		43%			Rogue AP: b2:72:bf:78:81:39	detected on Base Radio NAC:	08:d0:9fred:e	ec:70 Interface no: 0(802.1	In(2.4 GHz)) Channel: 11	
						Noise Profile Paried for Base Rac	tio NAC: 08:00:91:ed:ec:70 a	and slotNo: 0			
	Access Point	t Sumr	nary			Negoti er i peroviceren strou removes nom base Natio Punu i verovisriesreci/u interace no(0(802.118(2.4.982)) Posta 10 - 04-72-98-12-87-as, removad from Sana Padio NAT - 08-d7-95-ad-ar-70 (starfare no:0(802.116(2.4.682))					
		Total	Un	Dran		Bosue 4P : 90-a2-Sh-e8-fe-h2	removed from Base Badio M	AC + 08:40-96	educe: 70 Interface no:0180	(2.116(2.4 GHz))	
	002.11a/n/ac	2	. 2	• •	Detail	View All					
	B02.11b/g/n Badios	2	• 2	• 0	Datail	Top Applications					
	Dual-Band	0		• 0	Detail	Application Name	Packet Count	Byte Count			
	All APs	2	• 2	• 0	Detail						
	Client Summ	ary									
	Current Clients	3			Detai						
	Excluded Client	ts 0	6		Detai						
	Disabled Client	× 0	6		Detail						

Pour afficher les clients ont clique sur l'onglet client on peut voir affiché leurs informations :

cisco		CONTROLLER	WIRELESS SECURITY	MANAGEMENT COMMAND	OS HELP FEEDBACK	Save	Configuration Ping Logsut Refresh
Monitor Summary Access Points Cisco CleanAir	Clients Current Filter	None	[Change Filter] [Clear Filter]	1			Entries 1 - 3 of 3
Estatistics	Client NAC Addr	IP Address	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol Statu
) CDP	7a:20:9c:2a:c8:6c	10.0.0.2	AP0464.1350	.8243 Internal	Internal	Usknown	802.11an Associ
k Roques	a4:83:e7:b9:fd:4a	10.0.0.3	AP649e.f390	.53ef Internal	Internal	Unknown	802.11an Associ
Clients Sleeping Clients Multicast Applications Local Profiling							

On peut aussi afficher les points d'accès avec leurs informations :

cisco	MONITOR MLANS CONTROLLER	WIRELESS SECUR		COMMANDS HELP FEEDBACK	Saye C	configuration Ping I	Logout Refresh
Wireless	All APs					Entr	ries 1 - 2 of 2
 Access Points All APs Radios 802.11a/m/ac 	Current Filter Number of APs	None 2		[Change Piter] [Clear Piter]			
BU2.11brg/n Dual-Band Radios Global Configuration	AP Name	IP Address	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status
Advanced	AP0464.135b.8243	192.168.1.82	AIR-CAP3502E-E-K9	c4:64:13:5b:82:43	0 d, 04 h 25 m 25 s	Enabled	REG
Mesh	AP549e.f390.53ef	192.168.1.83	ATR-CAP35021-E-K9	64:9e:f3:90:53:ef	0 d, 04 h 25 m 22 s	Enabled	REG
RF Profiles FlexConnect Groups FlexConnect ACLs b 802.11a/n/ac b 802.11b/g/n b Hedia Stream Application Visibility							
 And Control Country Timers Netflow QoS 							

Pour modifier les paramètres de l'un des points d'accès on clique sur l'un d'eux :

Access Doints						
All APs	General Cred	ientials Interfaces	High Availability	Inventory Advanced		
802.11a/n/ac 802.11b/n/n	General			Versions		
Dual-Band Radios	AP Name	APc464.135b.8243		Primery Software Version	7.6.120.0	
Advanced	Location	default location		Backup Software Version	0.0.0.0	
Novenceo	AP MAC	c4:64:13:5b:02:43		Predownload Status	None	
Mesn	Race Radio MAC	ed:0a:chi64:24:60		Predownloaded Version	None	
RF Promes	Admin Status	Enable M		Predownload Next Retry Tir	THE TUP	
FlexConnect ACLs	AP Mode	local Y		Predownload Retry Count	NA.	
802.11a/n/ac	AP Sub Node	None Y		Boot Version	15.2.2.4	
802.11b/g/n	Operational			105 Version	15.2(4)JB5\$	
Media Stream	Status	KEG		Mini 105 Version	7.0.112.74	
Application Vicibility	Port Number	LAG		IP Config		
And Control	Venue Group	Unspecified V		IP Address	192.168.1.82	
Country	Venue Type	Unspecified ¥		Static 1P		
limers	Venue Name	<u> </u>		Time Statistics		
Netflow	Language			Time Statutes		
QoS	Spectrum	E2082E47E17FE788F7A3CA	CE478D3A26	UPTime	0 d, 04 h 36 m 35 s	
	Interface Key			Controller Associated Time	0 0, 00 h 35 m 09 5	
				Controller Association Later	ity 00,0312511375	
	Hardware Reset		Set to Facto	ry Defaults		
	Perform a hardwa	are reset on this AP	Clear com	figuration on this AP and reset it t	o fectory	
	Reset AP Now	a	defaults			
		-	Clear A	II Config		

Sur la partie AP Mode on peut changer le mode de configuration, flexconnect, RogueDetector, Sniffer, etc.. comme vu auparavant.

i cicaa	All Al o > Dotalio I	101 Pd 0404.1000.0240				K BUCK Apply
Access Points All APs	General Crede	entials Interfaces	High Availability	Inventory Advanced		
Radios 802.11e/n/ac 802.11b/o/a	General			Versions		
Dual-Band Radios	AP Name	APo464.135b.8243		Primary Software Version	7.6.120.0	
disanced	Location	default location		Beckup Software Version	0.0.0.0	
tuvunceu	AP MAC	04164113150182143		Predownload Status	None	
iesn	Race Radio MAC	ad-0a-da-64-34-90		Predownloaded Version	None	
de promes	Admin Status	Proble Y		Predownload Next Retry Time	NA	
NexConnect ACLs	AP Mode			Predownload Retry Count	NA.	
02.11a/n/ac	AP Sub Mode	local		Boot Version	15.2.2.4	
02.11b/g/n	Operational	monitor		IOS Version	15.2(4)085\$	
tedia Stream	Status	Ropue Detector		Mini 105 Version	7.0.112.74	
opplication Visibility	Port Number	Bridge		IP Config		
and Control	Venue Group	se-connect v		IP Address	192.168.1.02	
ountry	Venue Type	Unspecified ¥		Static IP		
imers	Lanzuage			Time Statistics		
letflow	Network			UP Time	0 d. 04 h 36 m 55 s	
ios	Spectrum Interface Key	E2082E47E17FE788F7A3CA0	E478D3A26	Controller Associated Time	0 d, 00 h 38 m 09 s	
				Controller Association Latency	0 d, 03 h 25 m 37 s	
	Hardware Reset		Set to Facto	ry Defaults		
	Perform a hardwar	re reset on this AP	Clear con	Iguration on this AP and reset it to f	factory	
	Reset AP Now	1	defaults			

Sur l'onglet Management on peut voir différents paramètres, comme par exemple la version de SNMP activé, le mode HTTP activé, Syslog, SSH, etc.

cisco	MONITOR WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	Save Configuration	Ping	Logout	Refres
Management	Summary											
Summary	SNMP Protocols	v1:Disa	bled v2c:Enabl	ed v3:Enabled								
> SNMP	Syslog	Disabled	1									
HTTP-HTTPS	HTTP Mode	Enabled										
Telnet-SSH	HTTPS Mode	Enabled										
Serial Port	New Telnet Sessions Allow	wed No										
Local Management	New SSH Sessions Allowe	d Yes										
Users	Management via Wireless	Disabled	1									
User Sessions					-							
Logs												
Momt Via Wireless												
Software Activation												
Tach Support												
P Tech Support												

Telnet est ici désactivé comme on peut le voir :



On peut activer un mode pour que les clients d'un point d'accès puisse avoir accès à la gestion du contrôleur.



Dans l'onglet « Security » on peut configurer une ACL :

cisco	MONITOR WLANS CONTROLLE	r Wireless <u>s</u> ecurety	MANAGEMENT COMMAN	DS HELP TEEDBACK	Sage Configuration Fing Logout Befresh
Security	Access Control Lists				New Apply
AAA General RADILIS Authenbication Accounting Falback DNS TACACS+ LDAP	Enable Counters 🗌 Name Type				
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Papaword Palicies					
Local EAP					
Priority Order					
Certificate					
Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs Layer2 ACLs					
 Wireless Protection Policies 					
▶ Web Auth					
TrustSec SXP					
Local Policies					
Advanced					

On donne un nom à l'ACL :

aludu			Sage Configuration Ping Logout Befresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAG	EMENT COMMANDS HELP EEEDBACK	
Security	Access Control Lists > New		< Back Apply
	Access Control List Name ACL Type IPv4 OIPv6]	
TrustSec SXP Local Policies			
Advanced			

L'ACL est bien crée mais n'a pas de règle, on ajoute des règles en cliquant sur « add new rule »

						Save Configuration Ping Logout Refresh
CISCO	MONITOR WLANS	CONTROLLER WIRELE	SS SECURITY MANAGEMENT	COMMANDS HELP	FEEDBACK	
Security	Access Control	Lists > Rules > New				< Back Apply
▼ AAA General	Sequence	10	IP Address	Netmask		
	Source	IP Address 💙	192.168.1.0	255.255.255.0		
Fallback DNS	Destination	IP Address 💙	IP Address 192.168.1.100	Netmask 255.255.255.255		
LDAP Local Net Users	Protocol	Any 🗸				
MAC Filtering Disabled Clients	DSCP	Any 🗸				
User Login Policies AP Policies	Direction	Any 💙				
Local EAP	Action	Permit 💙				
Priority Order						
▶ Certificate						
 Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs Layer2 ACLs 						
Wireless Protection Policies						
▶ Web Auth						
TrustSec SXP						
Local Policies						
Advanced						

On crée 3 règles comme suit :

AAA General KADIUS Authentication Accounting Tailback DNS	Acce	ss Cont	rol Lists > Edit								< Back	Add New Ro
	Gene	ral										
	Access Deny (List Name Counters	MANAGEMEN 0	IT_ACL								
TACACS+	Seq	Action	Source IP/Hask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits		
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Ŧ	Permit	192.168.1.0 / 255.255.255.0	192.168.1.100 / 255.255.255.255	Алу	Any	Any	Any	Any	D	•	
	2	Permit	10.0.0.0 / 255.255.255.0	192.168.1.100 / 255.255.255.255	Any	Any	Any	Any	Any	D	•	
Local EAP Priority Order Certificate	ı	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Алу	Απγ	Any	Any	Алу	D	۰	
Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs Layer2 ACLs												
Wireless Protection Policies												
Web Auth TrustSec SXP Local Policies												

Pour faire Appliquer ces ACL on clique sur : « CPU Access Control Lists » Puis on sélectionne Enable CPU ACL et on clique sur Apply pour appliquer les modifications.

cisco	MONITOR WLANS	CONTROLLER	WIRELESS S	ECURITY MAN	AGEMENT COMP	ANDS HELP	FEEDBACK		Logout Befresh
Security	CPU Access Con	trol Lists							Apply
AAA General Gaturestication Accounting Palback DNS TrGACS+ LDAP Local Net Users MAC FileIng Disabled Clients User Logn Polyies	Enable CPU ACL ACL Name	(Z						
AP Policies Password Policies Local EAP									
Priority Order Certificate									
Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs Layer2 ACLs									
Wireless Protection Policies									
Web Auth TrustSec SXP									
Local Policies									