# cisco\_controller

The example configuration shown in this chapter was obtained from a Cisco 4400 Series Wireless LAN Controller.

#### Initial settings and defining the IP address

In the first phase the controller must be accessed through the Command Line Interface (CLI). When an IP address has been assigned to the controller, further configuration can be done using the web interface, but the CLI can be continued to be used.

Establish access to the controller by using a serial console and configure the initial settings for example as follows.

Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup System Name [Cisco\_b2:e2:83]: <your\_system\_name> Enter Administrative User Name (24 characters max): <your\_username> Enter Administrative Password (24 characters max): <your\_password> Re-enter Administrative Password : <your\_password> Service Interface IP Address Configuration [none][DHCP]: DHCP Enable Link Aggregation (LAG) [yes][NO]: NO Management Interface IP Address: esim. xxx.yyy.zzz.1 Management Interface Netmask: <your\_network\_mask> Management Interface Default Router: <your\_router's\_IP\_address> Management Interface VLAN Identifier (0 = untagged): <0 or 1> Management Interface Port Num [1 to 2]: 1 Management Interface DHCP Server IP Address: esim. xxx.yyy.zzz.2 AP Transport Mode [layer2][LAYER3]: <layer2 if controller and access points are on same subnet; layer3 if routing in between> AP Manager Interface IP Address: esim. xxx.yyy.zzz.3 AP-Manager is on Management subnet, using same values AP Manager Interface DHCP Server (xxx.yyy.zzz.2): Virtual Gateway IP Address: xxx.yyy.zzz.www Mobility/RF Group Name: <choose a suitable name if you have more than one controller. Otherwise, don't care> Enable Symmetric Mobility Tunneling [yes][NO]: NO Network Name (SSID): <Define a test SSID at first> Allow Static IP Addresses [YES][no]: no Configure a RADIUS Server now? [YES][no]: no #Will be done later Warning! The default WLAN security policy requires a RADIUS server. Please see documentation for more details. Enter Country Code list (enter 'help' for a list of countries) [US]: <your country abbreviation> Enable 802.11b Network [YES][no]: no Enable 802.11a Network [YES][no]: YES Enable Auto-RF [YES][no]: YES Configure a NTP server now? [YES][no]: no #Will be done later Configure the system time now? [YES][no]: no #Will be done later Warning! No AP will come up unless the time is set. Please see documentation for more details. Configuration correct? If yes, system will save it and reset. [yes][NO]: yes #When the system has rebooted, familiarize yourself with the CLI by defining (Cisco Controller) >config time ntp server 1 xyz.zyx.zzy.wyz (Cisco Controller) >config time ntp server 2 xyz.zzz.zzy.wyz

After the initial setup, the access control (ACL) list needs to be configured, in order to prohibit unauthorized access to the controller. Choose SECURITY and then Access Control Lists | Access Control Lists and create an ACL by pressing New... The ACL should include at least

- · the networks from which maintenance is carried out
- the address(es) of the monitoring server(s)
- the network(s) from which the APs and the WLAN clients get their addresses
- the address(es) of the RADIUS server(s)
- a rule to always answer ping commands

An example of an ACL is shown below. Inbound means packets towards the controller and outbound means packets towards the WLAN clients.

CILCO	4.9.4			ada norau			0.257-046					
- 45	Acres 6	6.4 U I	1478								1.00017	
515	Sec. N.											
And and the second s			4.14									
Sec. and												
-C-16	1.20		-									
in second		-			Distant.		Provide State	2.1	2.4		Same Same	
0.192	Angle Land			A REAL PROPERTY.	1.14	1000	20	100	2.4		Contract of the	
a succession of the second	1. 1	12	14		1111	17457			-		10.00	
1.0.00	1.7		100			1.000		1	2	100		
11192	1	12	4100			17875	100	1.0				
de arte		1				1.4		1.00	2			
and and a second second	1 Au	12	100					10			1.000	
and the state				10.000		1.000				1		
					11.14	1.74.7.7	10.4 10.4	1.0				
1						i cant	×.	1.0	2		1.00.00	
days of all a line	1. 1	12		· · · · · · · · · · · · · · · · · · ·		17457		-			1000	
iles.						-	×.		· ·		100.11	
Cost.	1 17		1	1.00	1.14		2.4	1.00	2.4			
Land I												

After you have specified the ACL you need to take it into use by first selecting Access Control Lists from the side bar and by choosing your ACL and specifying the CPU ACL Mode to *Wired* or *Both*.

#### Access Point configuration

If the access points are connected to the same subnet as the controller, they will automatically find the controller and connect to it. If this is not the case, the IP address of the controller must be find from the name server by the name CISCO-LWAPP-CONTROLLER. Once the access point has found the controller, it stores the IP of the controller, and it can connect to it from any network, as long as the network allowed access in the ACL (see previous section).

The next step is to define the wireless network, which has to be done separately for 2,4 GHz and 5 GHz. First, choose WIRELESS and then 802.11b/g/n | Network. Enabling the 802.11b-standard will result in less available capacity on your network and therefore it is recommended to enable only the standards 802.11g and 802.11n. Enable 802.11g according to the figure shown below. If you want to support also the 802.11-b standard, set \_Mandatory\_ for the lowest 802.11b-rate that you want to support (1 Mbps, 2 Mbps, 5.5 Mbps or 11 Mbps), set \_Supported\_ for all data rates higher than this rate and \_Disabled\_ for all rates lower than this rate. If 802.11b needs to be supported, it may pay off to disable the lowest rates, in order to avoid clients being attach to an AP far away, unwilling to roam.

Arelena .	302 11hq Global Parame	1917			19.81
Auros faints a faith a faith	second		VITE KEDIG**		
352	Rolling Wood, Area	H were	1 HLvs	Grandford 🔚	
salenal concernance	621. Hp. 6- (a. 1	EL al vi	210.00	The state of the s	
Me st.	instant and in lines.	59	- C. 1997	Contract M	
HEAP DUNK	A set. Your site	M. week	v HLut	Sin Sites 🔚	
Average (	Segurated in Tracket (Mark)	23.9	100.00	Circles H	
- usuusb/e/s	Difference -	Planse.	12 Page	Desked E	
- MT			Le mois	aparent Se	
di di suori si 1965	CICCI scalars Measurement		12 17 100	autorian -	
243	200.0	L st.vJ	14 K and	T 10 10 10	
4175.418			Do minere	Supporte M	
6. A. A. A.			121.00	Summer -	
Carr			At Same	Page data (B)	
Part Annual of Latin Control (March) County Taxes Fight		<ul> <li>A second s</li></ul>	ing tais ang tais ang tao ang tao ang tao ang tao ang tao ang tao		

Next, switch to enable the standard 802.11a for 5 GHz by selecting 802.11a/n | Network. Configure the settings according to the figure below.

Windows Ands	kibal Parameians			
Ye but South of the South of the South of the Head Company Head Company	and Paralises and Paralises Could off Paralises Paralises Country of the Paralises Country of the Paralises Country of the Paralises Country of the Paralises Country of the Paralises	Chapterson	Prator - M Gan 11 4 0 Gan 11 4 0 F Pair 1	Yek

The only standard left to enable is the standard 802.11n. You can choose to enable it for either 2,4 GHz or 5 GHz. It has been suggested that 802.11n is enabled only on the 5 GHz band, in order to utilise the radio resources effectively, see the Campus Best Practice document on "WLAN network planning and setup" Chapter 6.3. That document, along with a wealth of other WLAN resource planning advice, can be found at GEANT Campus Best Practices - Wireless. To enable 802.11n in the network select 802.11a/n | High throughput (802.11n) and/or 802.11b/g/n | High throughput (802.11n) and configure the settings according to the figure below.

cisco							Con I Account And
	NOTION WORLD	CORRECT MIRLES	1410111	Paradetai		124	
102139	000.11n (\$ G) a) I	igh Throughput					Carely.
Notice Professional							
· Strick Reality :	Grand			MDS (Data D	de-2) Adding	•	
Malifard r	tion node	M CORE		0.14.25	r M	Second of	
100.28 p.c.s.				1 12 24	a H	distant.	
Hell				1 (21 4)	- E	Acres fed	
TRUMP GROUP						S mild	
- HO HLA				1.14.24	а H	discount.	
A 150 A				C 186. V .	5 E	Aug Ini	
1.1	-			4 215 - 22		State	
Transformer				1 220 20		a second	
1000				1 11 24		A control	
Automic Control of Con				1.1.1.1.1	_	Sum 1 d	
2.00							
These sections				12 14, 24		a second	
2.9.6.2101				L (M N)	•. E	Acres led	
des Angelan Guillet				10.11.00	1 M	S. of Lat.	
100.10./10				D 13070	a 14	a support	
Theas				14.1.1994 a	-, E	Aug tel	
a state of				IN 2 HARMS		S. m. i.d.	
1.0							
- 94-19 P		Survey & Shark on Principality	and me	14.100			
Your Street							

At this point you have enabled the radios, but you have not yet defined any network, so don't try to use the access points just yet.

### Defining the RADIUS server

Define the RADIUS server to be used in the eduroam network by selecting SECURITY and then AAA | RADIUS | Authentication. Define the IP address, the shared secret and the other parameters according to figure. Please note that your first server will naturally have a server index of one.

alarta cisco	SHICK MAR DOING	ана мраная <mark>знанах</mark> идеонана оде	Several Array Local Array Marka Helji
Security	RADUIS Arthurtication 8	anvers :- Neve	Shah dada
<ul> <li>ANA</li> <li>Provide a straight of the straightof the straight of the straight of the straight of the straigh</li></ul>	Security and Provide Security Nature (Materia) Nature (Materia) Security (Materia) Security (Materia) Security (Materia) Security (Materia) Security (Materia) Security (Materia) Security (Materia) Security (Materia)	2 9	n guargia - 527 i Kara an
F advanced			

## Defining a wireless network

Select WLANs and then WLANs | WLANs from the sidebar. Create a new network and name it as shown in the figure below.

սիսիս					Sage	Configuration	Sing Logaut Befrech
CISCO	MONITOR	WLANS	CONTROLLER	WPELESS	SECONDA	NUNNCEMENT	COMMANDS HELP
WLANs	V	VLANs >	New			< Back	Apply
* WLANS		Туре		WLAN	×		
+ Advenced		Profile Rat	794	eduraans			
		5510		edurears			
		10		3 🕶			

After defining the eduroam network, click on the WLAN ID number to start defining the settings for the network. Set the General settings according to the figure below, then click the Security tab.



In order to enable only WPA2-AES, fill in the security settings as shown in the figure below.

oliolio cisco	HONETON WANN CONTR	Saya Configuration (Eng. Logout (Enf CLURK VOPPLIES (SECURITY HIGHWORT COPINIADS HELP
WLANs	WLANs > Edit	< Back Apply
* WLANs	General Security 0	as Alvanced
Advanced	Lever 2 Lever 3	AAA Servers
	Layer 2 Security # NYA	A DAGEN
	WTR+NTAJ Parameters	AC Fibering
	WPR Policy	0
	WP82 Palicy	E
	WPR2 Encryption	EAS TRP
	Auth Kay Mgnt	802.1X ×

After this, click on the AAA Servers tab and select the RADIUS server that you defined earlier to be used in eduroam.



Next, click on the QoS tab and make sure that you have set the WMM Policy to either Required or Allowed. Otherwise, the higher transmission rates associated with the 802.11n-standard will not work. Then select the Advanced tab and adjust the settings as shown in the figure below. By choosing the parameter P2P Blocking Action to have the value Forward-UpStream, you can prevent WLAN clients to communicate directly, without involving the AP, as recommended in the Campus Best Practice document on "WLAN Information Security" Chapter 2.2 and 2.3. MFP Client Protection is known to have caused problems and can be disabled.

Al Aline Pér-	- 20 A - A
See Street See Street	
distantia in the second	100
the state in a 2 more	Mittheor Carago
den a	Article Council of Strategy
Table Select Carlos	Temperate Committee (article)
n andreas and an and an and an and an and an an and an	And the second s
Character Zmark Concernance	10.1071 MI 1
tothe south the set of proper	Patrations for 1997 1
President and a state of the state	The David

At this stage, click Apply. In the Advanced-tab, the Client Exclusion timeout value was set to 60s. While this is a suitable value, the rules for client exclusion are a bit too strict. Hence, it pays off to adjust the rules by selecting SECURITY and then Wireless Protection Policies | Client Exclusion Policies from the sidebar and uncheck all other options except for "IP Theft or IP Reuse".

These are the basic settings for the Cisco controller. More advanced settings can be found from the upcoming Campus Best Practice document on "WLAN infrastructure", to be published in the first half of 2011.