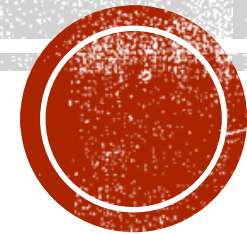


# EDUROAM TECHNICAL SETUP

การตั้งค่า Controller สำหรับ Institute Level



# Wireless AP Controller Configuration



The Controller Configuration : Cisco @ APAN33

\* APAN 33rd Febuary 13-17,2012 at Chiang Mai, Thailand



# Controller Configuration @ APAN33 (1)



Save Configuration | Ping | Logout | Refresh


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Monitor

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Clients
- Multicast

### Summary

25 Access Points Supported



Cisco 5500 Series Wireless Controller Model 5508

#### Controller Summary

Management IP Address	202.29.192.11
Service Port IP Address	0.0.0.0
Software Version	7.0.116.0
Field Recovery Image Version	6.0.182.0
License Level	base
System Name	Cisco5500_1
Up Time	2 days, 15 hours, 2 minutes
System Time	Wed Feb 15 09:55:29 2012
Internal Temperature	+44 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	APAN33
CPU(s) Usage	0%
Individual CPU Usage	0%/0%, 0%/1%, 0%/1%, 0%/1%, 0%/1%, 0%/1%, 0%/0%, 0%/1%, 0%/0%, 0%/1%
Memory Usage	43%

#### Access Point Summary

	Total	Up	Down	
802.11a/n Radios	13	13	0	<a href="#">Detail</a>
802.11b/g/n Radios	13	13	0	<a href="#">Detail</a>
All APs	13	13	0	<a href="#">Detail</a>

#### Client Summary

#### Rogue Summary

Active Rogue APs	19	<a href="#">Detail</a>
Active Rogue Clients	38	<a href="#">Detail</a>
Adhoc Rogues	2	<a href="#">Detail</a>
Rogues on Wired Network	0	

#### Top WLANs

Profile Name	# of Clients	
APAN33-2	167	<a href="#">Detail</a>
eduroam	10	<a href="#">Detail</a>


#### Most Recent Traps

- User a33a293 logged in. Client MAC:78:2e:ef:f4:96:10, Client IP:202.29.197.95, AP MAC:f8:66:f2:c1:56:d
- User a33a344 logged in. Client MAC:00:23:14:19:b6:ec, Client IP:202.29.197.87, AP MAC:f8:66:f2:c1:56:d
- Coverage hole pre alarm for client[1] 60:c5:47:2c:3b:d2 on 802.11b/g interface of AP f8:66:f2:c1:49:80 (A
- AAA Authentication Failure for UserName:APAN33 User Type: WLAN USER
- AAA Authentication Failure for UserName:a33a344 User Type: WLAN USER

[View All](#)

This page refreshes every 30 seconds.

Controller Summary บอก status ต่าง ๆ ของ Controller



# Controller Configuration @ APAN33 (2)

[Save Configuration](#) | [Ping](#) | [Logout](#) | [Refresh](#)



[MONITOR](#) | [WLANs](#) | [CONTROLLER](#) | [WIRELESS](#) | [SECURITY](#) | [MANAGEMENT](#) | [COMMANDS](#) | [HELP](#) | [FEEDBACK](#)

**WLANs**

- ▼ **WLANs**
- WLANs
- ▶ **Advanced**

**WLANs** Entries 1 - 3 of 3

Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#)

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
<input type="checkbox"/>	<a href="#">5</a>	WLAN	APAN33-2	APAN33	Enabled	[WPA2][Auth(PSK)], Web-Auth <input type="button" value="v"/>
<input type="checkbox"/>	<a href="#">6</a>	WLAN	eduroam	eduroam	Enabled	[WPA2][Auth(802.1X)] <input type="button" value="v"/>
<input type="checkbox"/>	<a href="#">7</a>	WLAN	NOC-Service	NOC	Enabled	[WPA2][Auth(PSK)], Web-Auth <input type="button" value="v"/>

WLANs เป็นการ ตั้งค่า WLAN SSID เข้า  
กับ VLAN และ เข้ากับ Profile Name



# Controller Configuration @ APAN33 (3)



[Save Configuration](#) | 
 [Ping](#) | 
 [Logout](#) | 
 [Refresh](#)

[MONITOR](#) | 
 [WLANs](#) | 
 [CONTROLLER](#) | 
 [WIRELESS](#) | 
 [SECURITY](#) | 
 [MANAGEMENT](#) | 
 [COMMANDS](#) | 
 [HELP](#) | 
 [FEEDBACK](#)

WLANs

▼ WLANs  
 WLANs  
 ▶ Advanced

WLANs > Edit 'eduroam'

< Back

Apply

[General](#) | 
 [Security](#) | 
 [QoS](#) | 
 [Advanced](#)

Profile Name	eduroam
Type	WLAN
SSID	eduroam
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All ▼
Interface/Interface Group(G)	eduroam ▼
Multicast Vlan Feature	<input checked="" type="checkbox"/> Enabled
Multicast Interface	eduroam ▼
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

**Foot Notes**

- 1 Web Policy cannot be used in combination with IPsec
- 2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured
- 5 Learn Client IP is configurable only when HREAP Local Switching is enabled
- 6 WMM and open or AES security should be enabled to support higher 11n rates
- 7 Multicast Should Be Enabled For IPV6.
- 8 Band Select is configurable only when Radio Policy is set to 'All'.
- 9 Value zero implies there is no restriction on maximum clients allowed.
- 10 MAC Filtering is not supported with HREAP Local authentication
- 11 MAC Filtering should be enabled.
- 12 Guest tunneling, Local switching, DHCP Required should be disabled.
- 13 Max-associated-clients feature is not supported with HREAP Local Authentication.



# Controller Configuration @ APAN33 (4)

Save Configuration | Ping | Logout | Refresh
CISCO

MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK

WLANs > Edit 'eduroam'
< Back
Apply

General
Security
QoS
Advanced

Layer 2
Layer 3
AAA Servers

Layer 2 Security <sup>6</sup> WPA+WPA2

<sup>10</sup>MAC Filtering

---

**WPA+WPA2 Parameters**

WPA Policy

WPA2 Policy

WPA2 Encryption  AES  TKIP

Auth Key Mgmt 802.1X

เป็นการเลือก Authentication  
Key และการเข้ารหัส

**Foot Notes**

- 1 Web Policy cannot be used in combination with IPsec
- 2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured
- 5 Learn Client IP is configurable only when HREAP Local Switching is enabled
- 6 WMM and open or AES security should be enabled to support higher 11n rates
- 7 Multicast Should Be Enabled For IPV6.
- 8 Band Select is configurable only when Radio Policy is set to 'All'.
- 9 Value zero implies there is no restriction on maximum clients allowed.
- 10 MAC Filtering is not supported with HREAP Local authentication
- 11 MAC Filtering should be enabled.
- 12 Guest tunneling, Local switching, DHCP Required should be disabled.
- 13 Max-associated-clients feature is not supported with HREAP Local Authentication.



# Controller Configuration @ APAN33 (5)

Save Configuration | Ping | Logout | Refresh
CISCO

[MONITOR](#) | [WLANs](#) | [CONTROLLER](#) | [WIRELESS](#) | [SECURITY](#) | [MANAGEMENT](#) | [COMMANDS](#) | [HELP](#) | [FEEDBACK](#)

WLANs > Edit 'eduroam'
< Back
Apply

General
Security
QoS
Advanced

Layer 2
Layer 3
AAA Servers

Layer 3 Security None

Web Policy <sup>1</sup>

**Foot Notes**

- 1 Web Policy cannot be used in combination with IPsec
- 2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured
- 5 Learn Client IP is configurable only when HREAP Local Switching is enabled
- 6 WMM and open or AES security should be enabled to support higher 11n rates
- 7 Multicast Should Be Enabled For IPV6.
- 8 Band Select is configurable only when Radio Policy is set to 'All'.
- 9 Value zero implies there is no restriction on maximum clients allowed.
- 10 MAC Filtering is not supported with HREAP Local authentication
- 11 MAC Filtering should be enabled.
- 12 Guest tunneling, Local switching, DHCP Required should be disabled.
- 13 Max-associated-clients feature is not supported with HREAP Local Authentication.



# Controller Configuration @ APAN33 (6)



Save Configuration | Ping | Logout | Refresh

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANS

WLANS

WLANS

Advanced

WLANS > Edit 'eduroam'

< Back

Apply

General Security **QoS** Advanced

Layer 2 Layer 3 **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface  Enabled

Authentication Servers

Enabled

Accounting Servers

Enabled

Server 1

IP:202.29.192.6, Port:1812

IP:202.29.192.6, Port:1813

Server 2

None

None

Server 3

None

None

LDAP Servers

Server 1 None

Server 2 None

Server 3 None

Local EAP Authentication

Local EAP Authentication  Enabled

Authentication priority order for web-auth user

AAA Servers เป็นการตั้งค่า server ที่จะ เป็น  
พอร์ท Authentication และ Accounting ในที่นี้คือ  
IP Address: 202.29.192.6  
Port 1812 , 1813

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured
- 5 Learn Client IP is configurable only when HREAP Local Switching is enabled
- 6 WMM and open or AES security should be enabled to support higher 11n rates
- 7 Multicast Should Be Enabled For IPV6.
- 8 Band Select is configurable only when Radio Policy is set to 'All'.
- 9 Value zero implies there is no restriction on maximum clients allowed.
- 10 MAC Filtering is not supported with HREAP Local authentication
- 11 MAC Filtering should be enabled.
- 12 Guest tunneling, Local switching, DHCP Required should be disabled.
- 13 Max-associated-clients feature is not supported with HREAP Local Authentication.





# Controller Configuration @ APAN33 (7)



Save Configuration | Ping | Logout | Refresh

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

▼ WLANs  
WLANs  
► Advanced

WLANs > Edit 'eduroam'

< Back

Apply

General Security QoS **Advanced**

Allow AAA Override  Enabled  
 Coverage Hole Detection  Enabled  
 Enable Session Timeout  36000  
 Session Timeout (secs)  
 Aironet IE  Enabled  
 Diagnostic Channel  Enabled  
 IPv6 Enable   
 Override Interface ACL   
 P2P Blocking Action   
 Client Exclusion  Enabled 60  
 Timeout Value (secs)  
 Maximum Allowed Clients   
 Static IP Tunneling  Enabled

Off Channel Scanning Defer

Scan Defer Priority  0  1  2  3  4  5  6  7  
 Scan Defer Time(msecs)

DHCP

DHCP Server  Override  
 DHCP Addr. Assignment  Required

Management Frame Protection (MFP)

MFP Client Protection

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)   
 802.11b/g/n (1 - 255)

NAC

NAC State

Load Balancing and Band Select

Client Load Balancing   
 Client Band Select

Passive Client

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured
- 5 Learn Client IP is configurable only when HREAP Local Switching is enabled
- 6 WMM and open or AES security should be enabled to support higher 11n rates
- 7 Multicast Should Be Enabled For IPV6.
- 8 Band Select is configurable only when Radio Policy is set to 'All'.
- 9 Value zero implies there is no restriction on maximum clients allowed.
- 10 MAC Filtering is not supported with HREAP Local authentication
- 11 MAC Filtering should be enabled.
- 12 Guest tunneling, Local switching, DHCP Required should be disabled.
- 13 Max-associated-clients feature is not supported with HREAP Local Authentication.



# Controller Configuration @ APAN33 (8)

- Security
- AAA
  - General
  - RADIUS
    - Authentication**
    - Accounting
    - Fallback
  - TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
  - Disabled Clients
  - User Login Policies
  - AP Policies
  - Password Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- Advanced

### RADIUS Authentication Servers

Call Station ID Type <sup>1</sup>

Use AES Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">1</a>	202.29.192.2	1812	Disabled	Enabled <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">2</a>	202.29.192.6	1812	Disabled	Enabled <input checked="" type="checkbox"/>

1. Call Station ID Type will be applicable only for non 802.1x authentication only.

เป็นหน้าแสดงผลรวมของ server radius ในที่นี้  
 202.29.192.2 คือ Web Authentication ของ APAN33  
 202.29.192.6 คือ eduroam



# Controller Configuration @ APAN33 (9)



[Save Configuration](#) | [Ping](#) | [Logout](#) | [Refresh](#)

[MONITOR](#) | [WLANs](#) | [CONTROLLER](#) | [WIRELESS](#) | **[SECURITY](#)** | [MANAGEMENT](#) | [COMMANDS](#) | [HELP](#) | [FEEDBACK](#)

## Security

### AAA

- General
- ▼ RADIUS
  - Authentication
  - Accounting
  - Fallback
- ▶ TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies

### ▶ Local EAP

### ▶ Priority Order

### ▶ Certificate

### ▶ Access Control Lists

### ▶ Wireless Protection Policies

### ▶ Web Auth

### ▶ Advanced

## RADIUS Authentication Servers > Edit

< Back

Apply

Server Index	2
Server Address	202.29.192.6
Shared Secret Format	ASCII ▼
Shared Secret	●●●
Confirm Shared Secret	●●●
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled ▼
Support for RFC 3576	Enabled ▼
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable



# EDUROAM TECHNICAL SETUP



การตั้งค่า Controller สำหรับ Institute Level

