Configure Cisco AP 1200 Series (802.11g Radio) for RADIUS

By Fariborz Entezami, August 2014

The configuration examples were tested based on a Cisco Series 1200 with an 802.11g Radio Module enabled with IOS version:

```
Cisco IOS Software, C1200 Software (C1200-K9W7-M), Version 12.3(8)JA2,
RELEASE SOFTWARE (fc1)
```

Setting the Name and IP address

First, an IP address on the BVI interface (the IP address that this Access Point will have for accessing resources like the RADIUS server) needs to be configured. Also a unique name for this Access Point (ap1200) is configured.

```
ap#configure terminal
ap#hostname ap1200
ap1200(config)#interface BVI 1
ap1200(config-if)# ip address 192.168.10.200 255.255.255.0
```

RADIUS/AAA section

In the authentication, authorisation and accounting configuration parameters (AAA), at least one group needs to be defined (radsrv), which will be assigned later for the several AAA operations. More groups can be defined if needed for various purposes; one for authentication, another for accounting, and so on. In this example the RADIUS server has the IP address 192.168.10.253.

```
ap1200(config)#aaa new-model
ap1200(config)#radius-server host 192.168.10.253 auth-port 1812 acct-port 1813 key
ap1200(config)#aaa group server radius radsrv
ap1200(config-sg-radius)#server 192.168.10.253 auth-port 1812 acct-port 1813
ap1200(config-sg-radius)#!
ap1200(config-sg-radius)#aaa authentication login eap_methods group radsrv
ap1200(config)#aaa authorization network default group radsrv
ap1200(config)#aaa accounting send stop-record authentication failure
ap1200(config)#aaa accounting session-duration ntp-adjusted
ap1200(config)#aaa accounting update newinfo periodic 15
ap1200(config)#aaa accounting network default start-stop group radsrv
ap1200(config)#aaa accounting network acct_methods start-stop group radsrv
```

Configuring the SSIDs

For each SSID one dot11 ssid <SSID NAME> must be configured. In this section the default VLAN for the SSID will be configured as well as the authentication framework, the accounting and, if desired, the SSID to be broadcast (guest-mode).

```
ap1200(config)#dot11 ssid eduroam
ap1200(config-ssid)#vlan 909
ap1200(config-ssid)#authentication open eap eap_methods
ap1200(config-ssid)#authentication network-eap eap_methods
ap1200(config-ssid)#authentication key-management wpa optional
ap1200(config-ssid)#accounting acct_methods
ap1200(config-ssid)#guest-mode
```

More SSIDs can be configured. An open SSID for giving information about the institution and/or how to connect to the eduroam SSID:

```
ap1200(config)#dot11 ssid guest
ap1200(config-ssid)#vlan 903
ap1200(config-ssid)#authentication open
ap1200(config-ssid)#accounting acct_methods
```

The Radio Interface

Now the configured SSID's will be mapped to the radio interface, and it will be specified what ciphers will be used/allowed on each VLAN. If dynamic VLANs are planned, the ciphers for those VLANs must also be configured even if there is no direct mapping on any SSID (this example shows the usage of the VLANs 906 and 909 for eduroam users)

```
ap1200(config)#interface Dot11Radio 0
ap1200(config-if)# encryption vlan 906 mode ciphers aes-ccm tkip wep128
ap1200(config-if)# encryption vlan 909 mode ciphers aes-ccm tkip wep128
ap1200(config-if)#ssid eduroam
```

To bind extra SSID's the previous command, for each SSID to be bound, needs to be repeated. The following command sets the maximum time (e.g. 300 seconds, which is recommended) for rekeying/reauthentication:

```
dot1x reauth-period 300
```

VLAN interfaces

For each VLAN to be used for wireless clients, two virtual interfaces need to be defined: one on "the air" (DotRadio) and another on the "wire" (FastEthernet) then they need to be bridged together with the same bridge group. These VLANs are always tagged with the proper VLAN identifier.

An administrative VLAN needs to be configured as well (for maintenance/management and authentication/accounting traffic). This VLAN is usually untagged (the command defining the VLAN has to be suffixed with the keyword "native") and belongs to bridge-group 1. The Radio virtual interface for this VLAN does not need to be defined since the default will keep the physical interface (Dot Radio 0) in bridge-group 1.

Because VLANs can be from 1 to 4094 and bridge-groups from 1 to 255, it is not necessary to have the same bridge-group id as the vlan id.

```
ap1200(config)#interface dot11Radio 0.903
ap1200(config-subif)#encapsulation dot1Q 903
ap1200(config-subif)#bridge-group 3
ap1200(config)#interface fastEthernet 0.903
ap1200(config-subif)#encapsulation dot1Q 903
ap1200(config-subif)#bridge-group 3
ap1200(config)#interface dot11Radio 0.909
ap1200(config-subif)#encapsulation dot1Q 909
ap1200(config-subif)#bridge-group 9
ap1200(config)#interface fastEthernet 0.909
ap1200(config-subif)#encapsulation dot1Q 909
ap1200(config-subif)#bridge-group 9
```

Configure Cisco IOS Client (192.168.1.1) to authenticate with Radius Server (192.168.1.250)