# How to determine the managed Access Points behavior in case the controller fails

- 2018-02-09 - BAT, WLC (HiLCOS)

When we have APs managed by a controller, what happens to them in the case the controller fails ?

There are different answers depending on the used topology.
- controller and APs are in the same LAN (Layer 2 topology)
- controller and APs are in different LANs, clients roam between APs in different LANs (Layer 3 topology with layer 3 roaming)

Layer 2 Topology:

When the AP looses connection to the controller, the applied profile remains active as long as the time configured in the "logical WLAN network" settings of the WLAN profile in "AP standalone time" field.

Notice: The default setting here is zero. This setting causes the AP to switch off immediately its radio module after loss of contact to the WLAN Controller (there is a timeout of 1 min for the communication with the controller te be seen as "down" so in practical the radio are switched off after 1 min). The configuration parameters are deleted and have to be communicated again in full after the connection to the WLAN Controller has been re-established. Although this is a time consuming procedure, it ensures that the security parameters in a stolen AP cannot be misused.
With any setting greater than zero, configuration parameters are stored in the AP. This allows connections to associated clients to be maintained until the time set here expires. After the interval is elapsed the configuration parameters are deleted in turn.
The value 9999 has a particular effect. No matter how long contact to the WLAN Controller is lost, the AP continues to work in its current configuration.

In case there is a redundant controller:
If the "AP standalone time" set is 0, the AP will remain approximatively 10 sec without profile (it has to establish the communication with the redundant controller and fully load its profile again)

If the "AP standalone time" is higher than 0, the AP will remain with an inactive profile approximatively 3 sec when the timer elapses and the AP establishes the communication with the redundant controller.

Layer 3 Topology:

Having a L3 topology and layer 3 roaming, it doesn't make any sense for an AP to keep a profile active given that the CAPWAP tunnel to the WLC is interrupted when the WLC is lost. In this case, without redundant controller, the loss of the main controller leads immediately to a general loss of the communications.

In the case there is a redundant controller:
The "AP standalone time" must then be set to 0.
When the AP detect that the CAPWAP tunnel is down it immediately tries to establish a connection with the redundant controller.
It takes around 30 seconds for an AP to detect that the CAPWAP tunnel is down, establish the communication with the new controller, get and load a profile from the redundant controller (less than 500 ms planned in future).