# TRANSLATION2

When the device is getting access to the router’s dhcp to get IP, the script will be triggered to run wdctl add\_online\_client. This will check if the device have already been certificated in other routers and enables walk-through. If yes, the device will be automatically added into the certification list (check by iptables -t mangle -L -n), simultaneously, the same one on the other router will be disable.

Roaming request interface

GET http://authserv\_hostname:port/authserv\_path/roam?gw\_id=gwid&mac=macaddress&channel\_path=cpath

The format of macaddress is；

50:7b:9d:19:1b:12

Feedback；

If the device is unable to roam, the feedback information will be like {"roam":"no"}; If yes, the feedback information will be like {"roam":"yes","client":{"token":"token\_value","first\_login":"first\_login\_value"}}. And the token value will be the one when the device first be certificated, first\_login is the time-stamp when the device first be certificated.

Tip: the device should be offloaded from the original router through the auth port.

THE CERTIFICATION OF APFREE WIFIDOG IN KUNTENG FIRMWARE CAN BE ACTIVE OR INACTIVE

Start Roaming

wifidog\_roam enable

Disable Roaming

wifidog\_roam disable

The script of wifidog\_roam

#!/bin/sh

[ -x /etc/init.d/wifidog ] || exit 1

[ $# != 1 ] && {

echo "$0 enable|disable"

exit

}

case $1 in

enable)

uci set wifidog.@wifidog[0].roam=1

uci commit wifidog

;;

disable)

uci set wifidog.@wifidog[0].roam=0

uci commit wifidog

;;

\*)

echo "no valid param $1"

;;

esac

Configure **dnsmasq, the script will be run when the user is allocated an IP address by dhcp server**

Plus dhcpscript

config dnsmasq

option domainneeded 1

option boguspriv 1

option filterwin2k 0 # enable for dial on demand

option localise\_queries 1

option rebind\_protection 1 # disable if upstream must serve RFC1918 addresses

option rebind\_localhost 1 # enable for RBL checking and similar services

#list rebind\_domain example.lan # whitelist RFC1918 responses for domains

option local '/lan/'

option domain 'lan'

option expandhosts 1

option nonegcache 0

option authoritative 1

option readethers 1

option leasefile '/tmp/dhcp.leases'

option resolvfile '/tmp/resolv.conf.auto'

#list server '/mycompany.local/1.2.3.4'

#option nonwildcard 1

#list interface br-lan

#list notinterface lo

#list bogusnxdomain '64.94.110.11'

option localservice 1 # disable to allow DNS requests from non-local subnets

option dhcpscript '/usr/sbin/roam\_check'

The script of roam\_check is used to run wdctl add\_online\_client

#!/bin/sh

WDCTL=/usr/bin/wdctl

UCI=/sbin/uci

action=$1

[ $action = "add" -o $action = "old" ] && {

# For the equipments in landi MAC address block

command -v landi-robot >/dev/null 2>&1 && landi-robot $2

[ -x $WDCTL ] || exit

roam=`$UCI get wifidog.@wifidog[0].roam 2> /dev/null`

[ $roam = 1 ] && {

$WDCTL add\_online\_client {\"mac\":\"$2\",\"ip\":\"$3\",\"name\":\"$4\"}

}

}