IP Control Implementation Guide for 2018 LG TV

Change History

Version	Note	Date	Author
0.1	Encryption Protocol	June 9, 2017	Ian Fan
0.2	Added IP Control configuration	June 12, 2017	Ian Fan
0.3	Added details to encryption	June 15, 2017	Ian Fan
0.4	Added key generation	June 23, 2017	Ian Fan
0.5	Added sample app IDs	October 3, 2017	Ian Fan
0.6	Added Wake-On-LAN section	October 30, 2017	Ian Fan
0.7	Added SSDP support	November 9, 2017	Ian Fan
0.8	Added more details Tune command	March 23, 2018	Ian Fan

1. IP Control Configuration

To bring up IP Control configuration, first open up TV's Settings Menu. Keep the Network icon focused as shown in Figure 1, then enter numerical key **828888** using TV's IR Remote. IP Control Configuration menu will be displayed as shown in Figure 2.

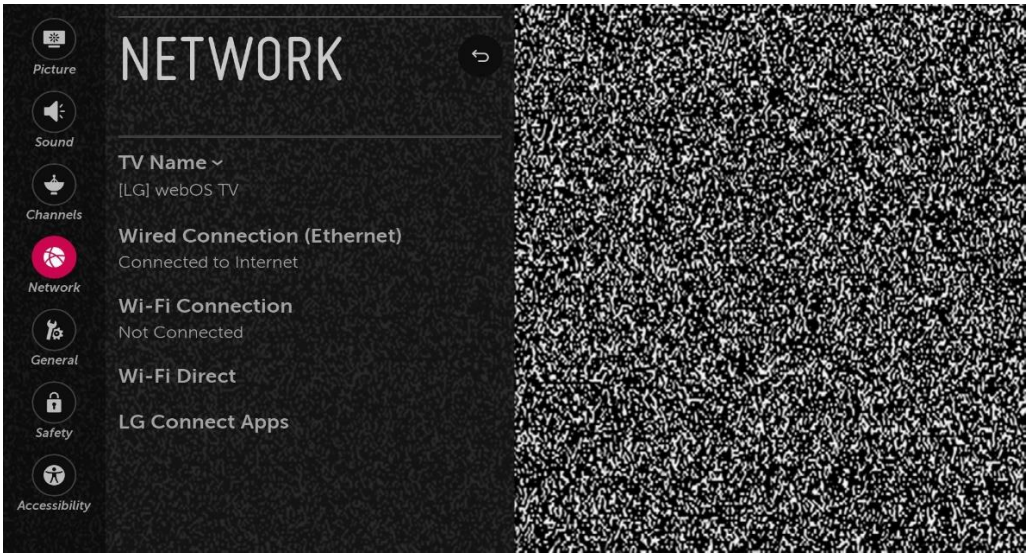


Figure 1 Network Settings

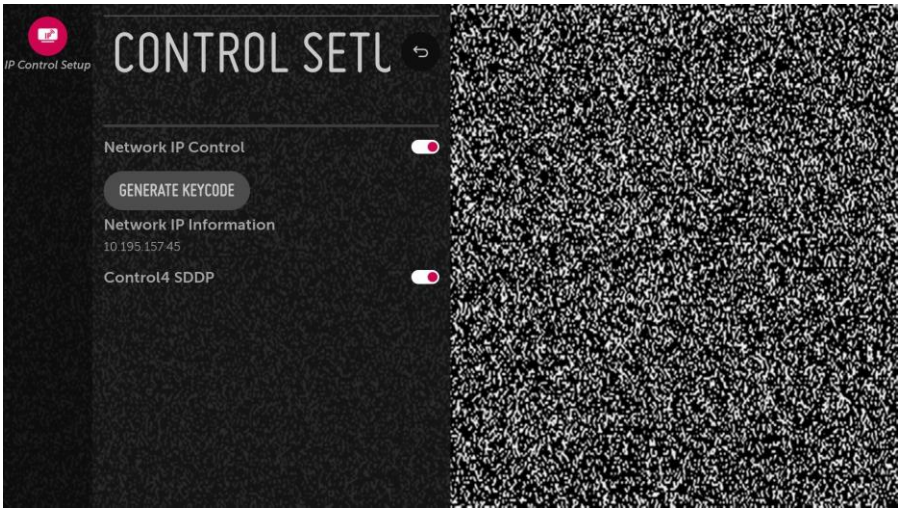


Figure 2 IP Control Configuration

2. Device discovery via SDDP

Simple Device Discovery Protocol (SDDP) is a protocol developed by Control4 Corporation to allow devices to be added to a control system. webOS TV support protocol version 1.0.

- On TV startup, TV sends NOTIFY ALIVE message.
- When Control4 SDDP is enabled on IP Control Setup screen, it generates NOTIFY IDENTIFY message.
- Before TV is powered off, it sends NOTIFY OFFLINE.
- WebOS TV will also respond to SEARCH request method.

3. Device discovery via SSDP

LG webOS TV supports Simple Device Discovery Protocol (SSDP) defined by UPnP Forum. There are three standard device and service types currently available for discovery:

```
urn:schemas-upnp.org:device:Basic:1
urn:schemas-upnp.org:service:dial:1
urn:schemas-upnp.org:device:MediaRenderer:1
```

From the Basic device, Manufacturer, TV's IP address, and Model Number can be obtained.

Each device/services also generate SSDP NOTIFY ssdp:alive and ssdp:byebye events upon powered up and down, respectively.

4. Encryption Protocol for IP Control Message Exchange

4.1 Encryption Specification

For IP Control message exchange, AES (Advanced Encryption Standard) is used with following specification:

- Block Length: 128 bit
- Key length: 128 bit
- Initialization Vector (IV) length: 128 bit.
- Block Cipher Mode: Cipher Block Chaining (CBC)

4.2 Encryption Key

Eight (8) digits (alphanumeric) password will be shown on IP Control Setting menu. IP Control client encrypts the password with PBKDF2 (Password-Based Key Derivation Function 2) method. First 16 Bytes of encrypted password are AES128 key. Following parameters must be used:

Algorithm: sha256

Salt: 0x63,0x61,0xb8,0x0e, 0x9b,0xdc,0xa6,0x63,0x8d,0x07,0x20, 0xf2,0xcc,0x56,0x8f,0xb9

Number of Iteration: 2**14

Note: on current developmental firmware, a hard-coded password string ("12345678") is used. Generated key is 9B B9 91 16 DD C1 33 E0 B0 5B 76 D8 BA 71 3A B0

TCP port number **9761** is used on TV to receive all IP control commands.

4.3 IV generation

IV is 16 byte string and must be randomly generated for each command encryption.

2.4 Operation

1) Clear text message must be terminated with '\r' (0x0d). Use VOLUME_MUTE on command as example.

V	O	L	U	M	E	_	M	U	T	E		o	n	'\'	

2) If the length of the message is not multiple of 16, then padding is required.

V	O	L	U	M	E	_	M	U	T	E		o	n	'\r'	'\1'

The value to be padded is the number of bytes to be padded. In this case, it is 1. The entire 16 byte text in hex is 56 4f 4c 55 4d 45 5f 4d 55 54 45 20 6f 6e 0d 01.

3) Apply AES-128 encryption algorithm. This will result in the follow cipher string in hex:

d2	d3	2b	fe	ac	13	f4	43	5e	6f	2f	54	2e	ea	9c	18

Output of AES 128 encryption is a string of length as input with padding

4) Send to receiver with IV prefixed. Since IV is 16 bytes. Total length is (16 + olen)

Encrypted IV (AES ECB)	Encrypted message (AES CBC)

0 15 (15+olen)

IV must be encrypted using AES-128 ECB mode. If IV is 16 0s, the encrypted IV is:
D2 B2 1C A0 AD 64 86 CB 20 56 A8 B8 15 03 35 08

Send only the Encrypted message. In this case, it is byte streams: DF E7 7A 7D E0 56 03 A5 9E D5 31 6E C5 52 FA C1. On Linux, this is can done through command echo and nc as follows:

```
echo -e '\xd2\xd3\x2b\xfe\xac\x13\xf4\x43\x5e\x6f\x2f\x54\x2e\xea\x9c\x18 |
nc <TV IP>  9761
```

5) Receiver applies decryption with received IV, and encrypted message. For "VOLUME_MUTE on" command, the response from the server is:
`ce 53 7c e4 b8 82 98 c6 a4 3e 21 89 af 5f 20 2f` and after decryption:
`4f 4b 0a 00 7d 7d 7d 7d 7d 7d 7d 7d 7d 7d 7d.`
`O K '\n' } } } } } } } } } } }`
For now, just ignore characters after '\n'

5. New Commands

3.1 Get current channel

Input: CURRENT_CH

Return: combination of Channel Name and Channel Number (Major and Minor Number)

For example:

CH:KRON-HD 4-1

If there's no Channel Name, it would be shown as UNKNOWN

If there is another application is launched, not liveTV, it would return NONE.

3.2 Get current app

Input: CURRENT_APP

Return: App ID.

For example: APP:youtube.leanback.v4

3.3 Get current vol

Input: CURRENT_VOL

Return: VOL:<numerical value>

For example: VOL:3

3.4 Get mute state

Input:MUTE_STATE

Return: on| off

For example: MUTE:off

3.5 Get MAC address

Input: GET_MACADDRESS wire|wifi

Return: MAC address in MM:MM:MM:SS:SS:SS format

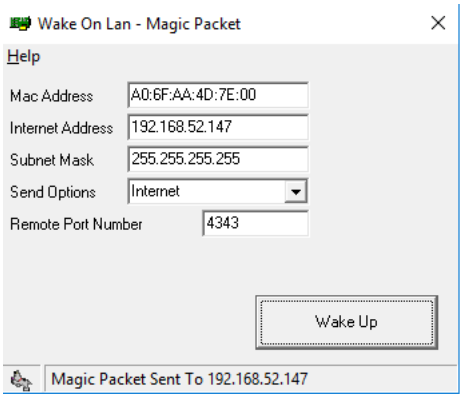
For example: E8:5B:5B:82:60:7C for wired or a0:6f:aa:4d:7e:00 wifi

6. Wake-on-LAN

Wake-on-LAN is performed by sending a magic packet to the TV's mac address to power it on. For that to work, both TV and the other device must be connected to the same subnet.

To enable Wake on LAN, go to Settings->General->Mobile TV On and set"Turn on via Wi-Fi" to on.

One way to test WOL is to use test tool from Depicus (https://www.depicus.com/wake-on-lan/wake-on-lan-gui).



The wake procedure for Wake on Wireless LAN (WoWLAN) is the same as in wired case. Only you will need a wifi MAC address. The router needs to support Wireless Multimedia Extensions (WME or WMM) for WoWLAN to work.

The *magic packet* is a broadcast frame containing 6 bytes of all 255 (FF FF FF FF FF FF in hexdecimal), followed by sixteen repetitions of the target TV's 48-bit MAC address, for a total of 102 bytes.

Port number 4343 or any number can be used. TV's IP address or broadcast IP address can be used for destination address. For example, if your TV's IP address is 192.168.52.147, you would use 192.168.5.255.

When testing WoWLAN, wired Ethernet cable must be disconnected.

7. Command Reference List

7.1 TV Control Commands

	Function	**Command**	**Discrete/ Toggle**	**Note**
1	Power	POWER off	Discrete	
2	Aspect Ratio	ASPECT_RATIO 4by3|16by9|setbyoriginal	Discrete	
3	Screen Mute	SCREEN_MUTE screenmuteon|videomuteon|allmuteoff screenmuteon: mute OSD and video videomuteon: mute video only allmuteoff: all mute are off.	Discrete	

4	Volume Mute	VOLUME_MUTE on|off	Discrete	
5	Volume Control	VOLUME_CONTROL [0 to 100]	Discrete	
6	Picture Mode	PICTURE_MODE vivid/eco/normal/game/cinema/sports Eco->APS Normal->Standard	Discrete	
7	Backlight	PICTURE_BACKLIGHT [0 to 100]	Discrete	
8	Contrast	PICTURE_CONTRAST [0 to 100]	Discrete	
9	Brightness	PICTURE_BRIGHTNESS [0 to 100]	Discrete	
10	Color/Colour	PICTURE_COLOUR [0 to 100]	Discrete	
11	Tint	PICTURE_TINT [0 to 100] 0-> R50 50->0 100->G50	Discrete	
12	Sharpness	PICTURE_SHARPNESS [0 to 50]	Discrete	The only one picture setting tha has 0 -50 range.
13	Colour Temperature	PICTURE_COLOUR_TEMPERATURE [0 to 100] 0 -> W50 50 -> 0 100 - >C50	Discrete	
14	Remote Control Lock Mode	REMOTECONTROLER_LOCK on|off	Discrete	
15	Audio Balance	AUDIO_BALANCE [0-100] 0 -> L50 50->0 100 ->R50	Discrete	
16	Audio Equalizer	AUDIO_EQUALIZER [1 to 5][0 to 20] 1 = 100 Hz 2 = 300 Hz 3= 1kHz 4= 3kHz 5=10kHz Value range 0 to 20 is mapped to -10 to +10 0 -> -10 1-> -9, etc	Discrete	Sound /Sound Mode Settings /Equalizer must be ON
17	Energy Saving	ENERGY_SAVING auto|screenoff |Maximum|medium|minimum|off	Discrete	
18	Tune Command	CHANNEL_SETTING_ATSC_ATV [Channel Number] antenna CHANNEL_SETTING_ATSC_ATV [Channel Number] cable CHANNEL_SETTING_ATSC_DTV [Channel Number] cablemaj	Discrete	ex) CHANNEL_SETTING_ATSC_ATV 1 antenna
		CHANNEL_SETTING_ATSC_DTV [Maj. Channel Number] [Min.Channel Number] antennanotphy CHANNEL_SETTING_ATSC_DTV [Maj.	Discrete	ex) CHANNEL_SETTING_ATSC_DTV 1 2 antennanotphy

		Channel Number] [Min.Channel Number] cablenotphy		
19	Channel Add/ Del	CHANNEL_ADD_DELETE add|delete	Discrete	
20	Key	KEY_ACTION exit|channelup|channeldown|volumeup|Volumedown|arrowright|arrowleft|volumemute|deviceinput|sleepreserve|livetv|previouschannel|favoritechannel|teletext|teletextoption|returnback|avmode|captionsubtitle|arrowup|arrowdown|myapp|settingmenu|ok|quickmenu|videomode|audiomode|channellist|bluebutton|yellowbutton|greenbutton|redbutton|aspectratio|audiodescription|programmorder|userguide|smarthome|simplelink|fastforward|rewind|programminfo|programguide|play|slowplay|soccerscreen|reord|3d|autoconfig|app||screenbright|number0|number1|number2|number3|number4|number5|number6|number7|number8|number9	Toggle	
21	OSD	OSD_SELECT on|off	discrete	
22	Input Select	INPUT_SELECT dtv|atv|cadtv|catv|avav1|component1|hdmi1|hdmi2|hdmi3	discrete	APP_LAUNCH is preferred method for HDMI input select
23	3D (only 3D models)	PICTURE_3D	toggle	
24	Extended 3D (on 3D models)	PICTURE_3D_EXTENSION	toggle	
245	Launch app	LAUNCH_APP appid	discrete	See Section 5 for sample application IDs.

7.2 Status Query Commands

	Function	**Command**	**Discrete/Toggle**	**Note**
1	MAC Address	GET_MACADDRESS wired|wifi	discrete	
2	Mute State	MUTE_STATE	discrete	
3	Current Volume	CURRENT_VOL	discrete	
4	Current App	CURRENT_APP	discrete	
5	Get IP Control State	GET_IPCONTROL_STATE Return ON if server is healthy. Otherwise, the command will time out.	discrete	

8. Sample Application Identifications

The following are samples of application IDs the currently available on webOS 4.0.

Applications	**Identifications (ID)**
Amazon	amazon
Google Play	googleplaymovieswebos
Hulu	com.hulu.hulu
Netflix	netflix
Sling TV	com.movenetworks.app.sling-tv-sling-production
Youtube	youtube.leanback.v4
Vudu	vudu

The following are samples of system built-in applications on webOS 4.0

Applications	Identifications (ID)
Settings	com.palm.app.settings
Photo & Video	com.webos.app.photovideo
Music	com.webos.app.music
Guide	com.webos.service.iepg
Browser	com.webos.app.browser