IPLoC D2-POM-n - Mini Guide

DKTCOMEGA

Table of Content

IPLoC D2-POM-n - Mini Guide 2017-01-02. Ver. 1   Page 2

Specifications are subject to change without notice.
DKT is not responsible for any typographical errors or wrong.

Security Note

To insure proper internet security with an IPLoC, then you need to install the product correct.

As the IPLoC signal use the coaxial cable to transport the IP-signal in all directions, you need to insure that the signal stay inside your network.

To do that you need to install a filter or use IPLoC behind an amplifier.

1. Own house with own antenna

If you have an amplifier on incomimg cable -No need to do anything

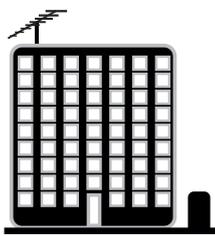If not, install a filter, se example 1

2. Own house with Cable-TV

If you have an amplifier on incomimg cable -No need to do anything
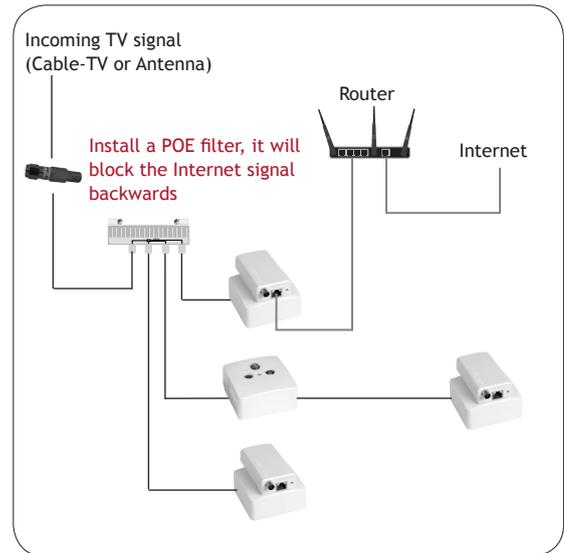
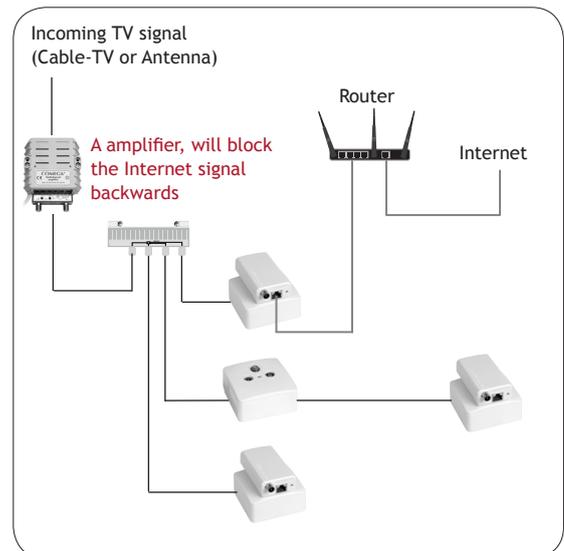If not, install a filter, se example 1

3. Apartments

You need a filter or an amplifier on the incoming cable

See example 1 or 2

Example 1: Filter

Incoming TV signal
(Cable-TV or Antenna)

Router

Install a POE filter, it will block the Internet signal backwards

Internet

Example 2: Amplifier

Incoming TV signal
(Cable-TV or Antenna)

Router

A amplifier, will block the Internet signal backwards

Internet

Example 3: Amplifier HCA-A65 & Filter HCT-114F

Incoming Cable-TV signal

Router

A amplifier, will block the Internet signal backwards

Internet

DKTCOMEGA
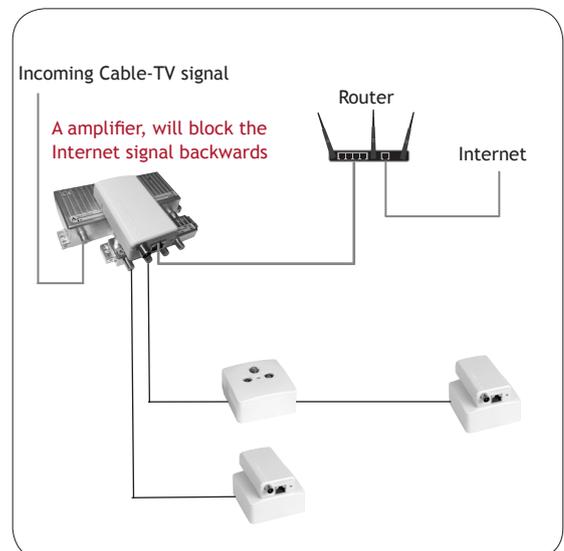
Quick Start Guide for IPLoC without WiFi

The following items should be found in your package:

1 pcs
IPLoC
push-on
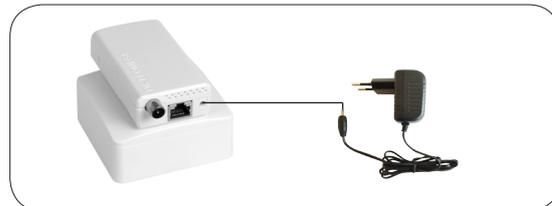module

1 pcs
Power supply
with DC-con-
nector

Plug in IPLoC to the existing ADSL / Broadband router with an Ethernet cable in LAN socket.
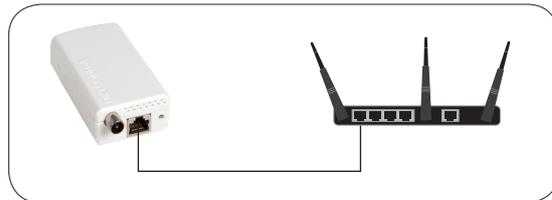
Install the IPLoC on the existing TV socket.
(if you have a TV cord in the socket, remove it and put it in the IPLoC instead).
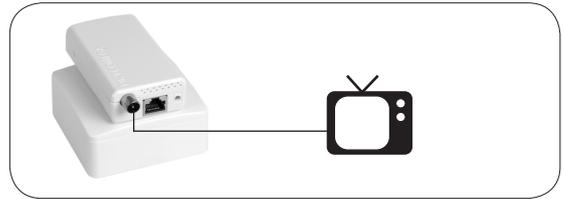
Plug the supplied mains adapter to IPLoC

To connect an additional device, open an second unit and connect the device to the TV socket in which you want an Internet connection.

Computer

TV

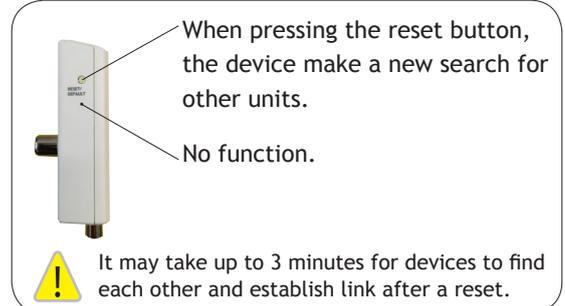Connect the network cable to the device.
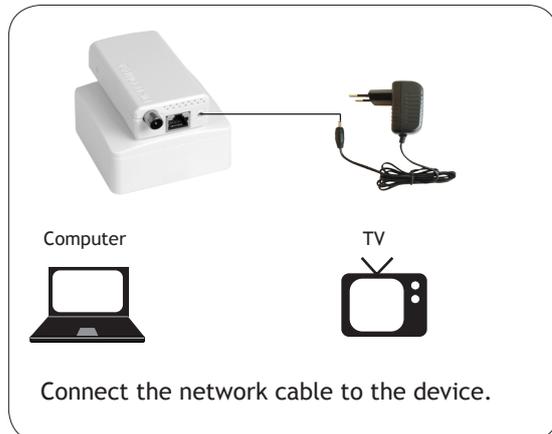
if you have a TV cord in the socket, remove it and put it in the IPLoC instead

When the second device is connected, it will be configured automatically. Could take up to 3 min. For the function of the device, please check the LED indicator lights on the side of IPLoC

Name:	Status:	Indication:
Power	Green	Power on
	Off	Power off
MoCA	Green	Link
	Off	No link
LAN	Green	Ethernet connected
	Blinking	Activity

IPLoC push-on module has a Reset/Default function.

When pressing the reset button, the device make a new search for other units.

No function.

⚠ It may take up to 3 minutes for devices to find each other and establish link after a reset.

IPLoC - example

Gateway, delivery point

Router

TV-signal

Internet

Smart-TV

TV

Internet

DKT COMEGA
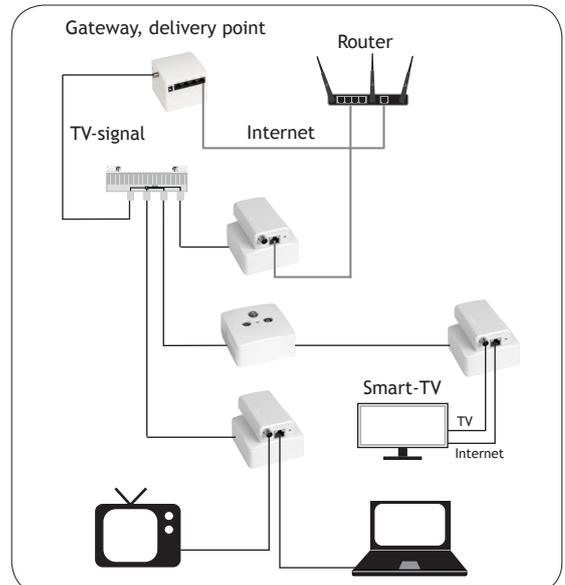
Introduction

Overview

IPLoC D2-POM-n is a Ethernet over Coax Adapter with WiFi wich bridges the Ethernet traffic present on its Ethernet port to other IPLoC D2-POM connected to the home coaxial wiring.
It is compatible with the MoCA®2.0 standard (Multimedia over Coax Alliance).

With IPLoC D2-POM-n you can use your existing coax network in your home and turn it in to an Ethernet Network for distributing Internet with WiFi access point.

It will make a stabil link for Ethernet traffic with high demand such as 4K-TV streaming and at the same time be used as an access point for your WiFi home network.

IPLoC D2-POM-n Features

- AP, Client, Bridge mode
- 64/128/152 WEP, WPA-PSK/WPA2-PSK,WPA/WPA2
- 2412 MHz-2484MHz(channel 1 - channel 14)
- IEEE802.11B/G/N transmission up to 150MBPs

MoCA Coax Network - Example
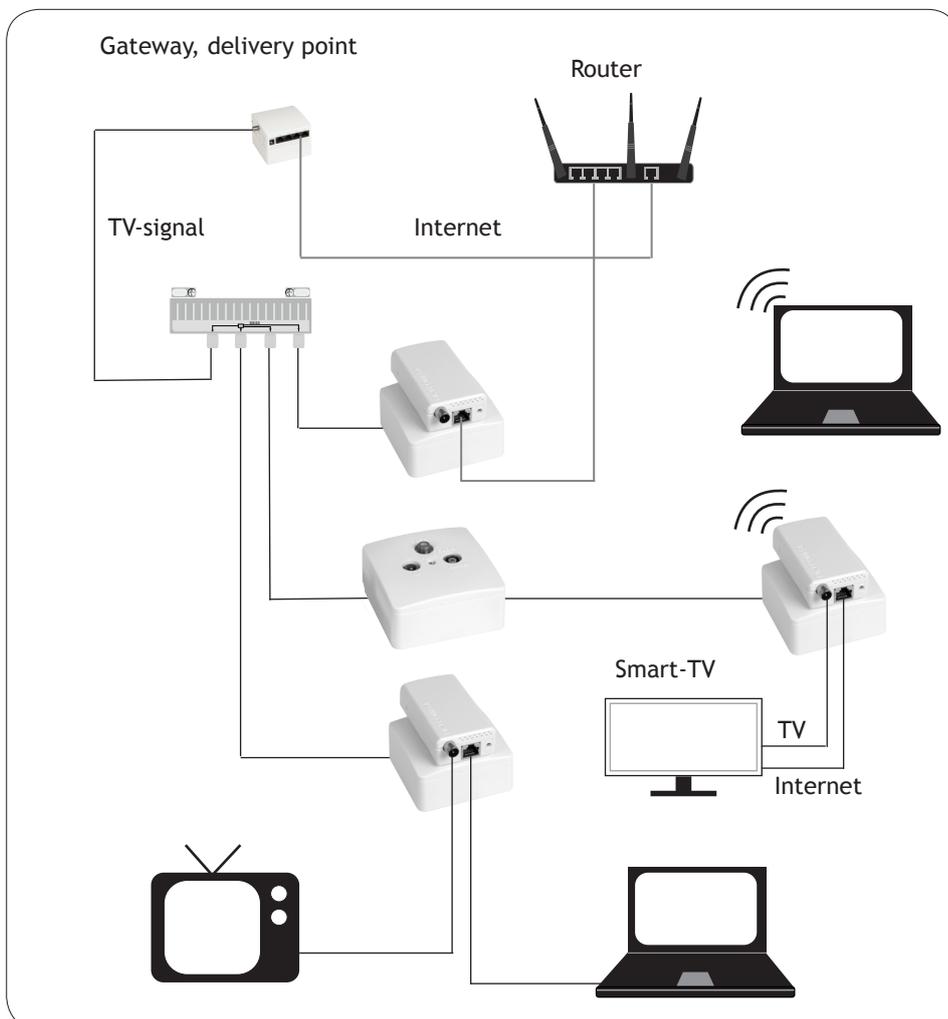
Purpose

This "mini guide" will focus on how to connect an IPLoC with Wi-Fi to another IPLoC unit in an existing MoCA network and integrated it with the existing Wi-Fi router in a home network.

For setting up/configuration of an IPLoC without Wi-Fi, see "Quick Start Guide for IPLoC without WiFi" on page 4.

For more information about the Web interface on IPLoC D2-POM-n see "IPLoC WiFi GUI Guide"

Existing MoCA network

Gateway, delivery point

Router

TV-signal

Internet

New WiFi unit
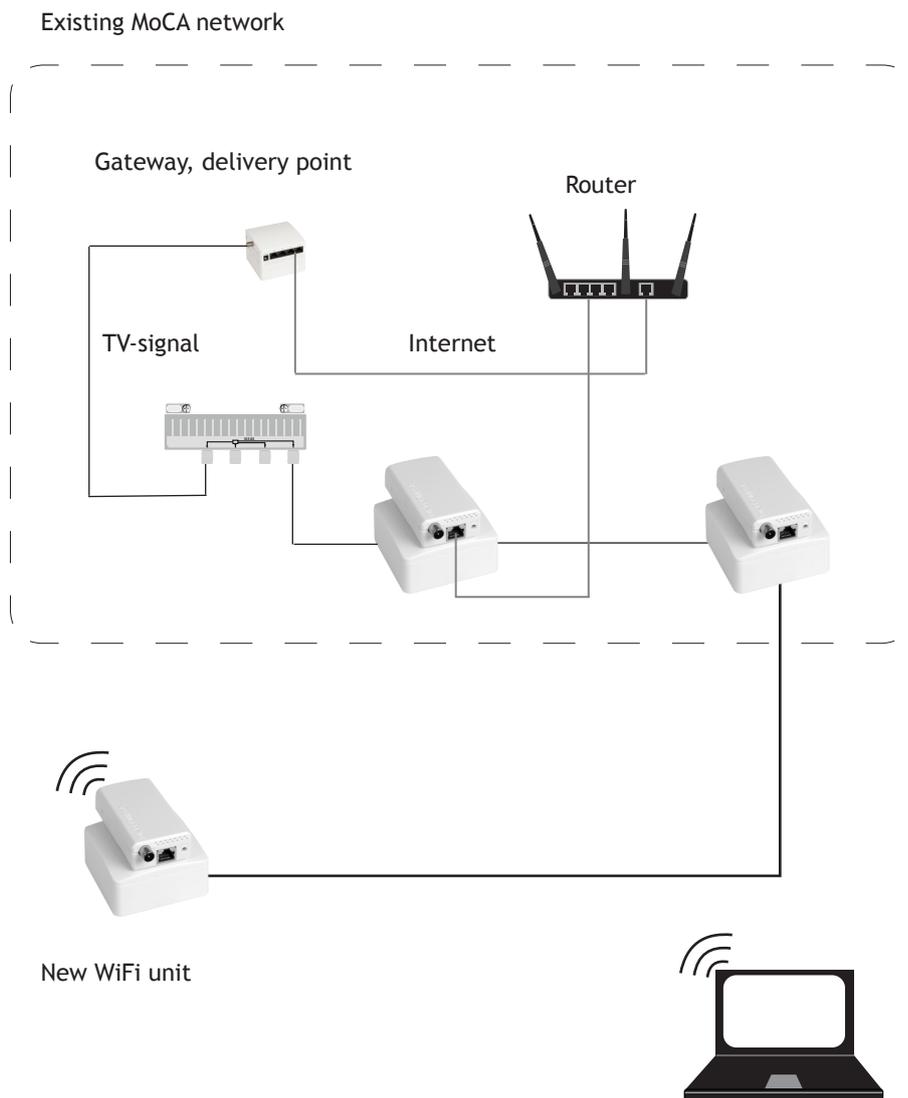
Interface
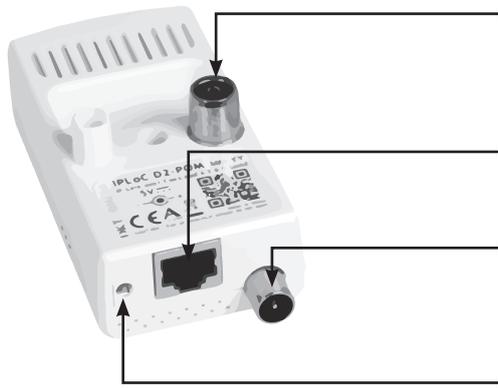
IEC Female Connector:
- Input for TV signal
- Output for MoCA Link

RJ 45 Connector:
- Input/Output for Ethernet signal (LAN)

IEC Male Connector:
- Output for TV signal

DC Connector:
- Input 5V DC

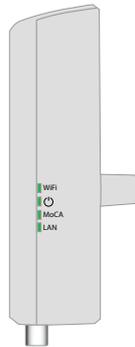| Name:	Status:	Indication:
WiFi	Green	Ready
	Blinking	IP address are unassigned
Power	Green	Power on
	Off	Power off
MoCA	Green	Link
	Off	No link
LAN	Green	Ethernet connected
	Blinking	Activity

The function of the external button are:
- MoCA Reset : 3~9 seconds
- Revert all MoCA settings to factory default : > 10 seconds

The function of the button in the pinhole are:
- Allow devices to connect to WiFi by means of WPS: <1 second
- Reset Wifi module : 3~9 seconds
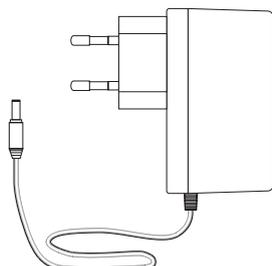
Power Supply
- Input 100-240VAC, 0,2A max
- Output 5VDC, 2A

DKTCOMEGA

Installation of IPLoC D2-POM-n

Overview

The IPLoC D2-POM-n can be installed into any home with coaxial cables by simply connecting the device to a coaxial cable outlet as the IPLoC D2-POM-n is pre-configured with default parameters that will allow operation without any additional configuration with anaother IPLoC unit. Up to 16 units is possible in a MoCA network.

⚠️ *Default setting:*
For using the Wi-Fi unit as an access point there has to be a router with DHCP server in the home network otherwise the unit will not receive an IP address.

Advanced: Static IP and other settings can be configured through the WEB GUI.

Minimum installation

Using 1 pcs of IPLoC D2-POM and 1 pcs of IPLoC D2-POM-n with a single coaxial cable for distribute Ethernet signal and IPLoC D2-POM-n as an access point.

This is not a normal way, only to show minimum configuration of a MoCA coax network with an access point.
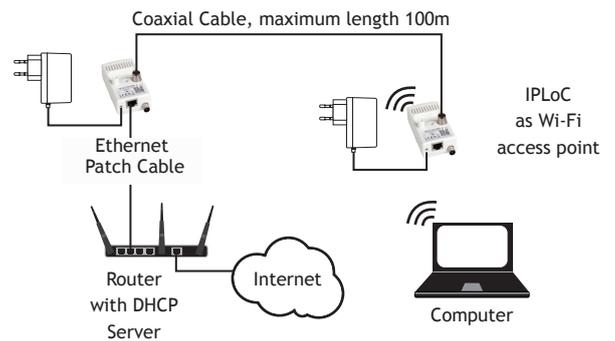
Installation example in this guide

DKTCOMEGA

Practical installation of the IPLoC unit

- Find the TV-Outlet there you want to have your Wi-Fi access point.
- You also need a 220V outlet for the power supply.
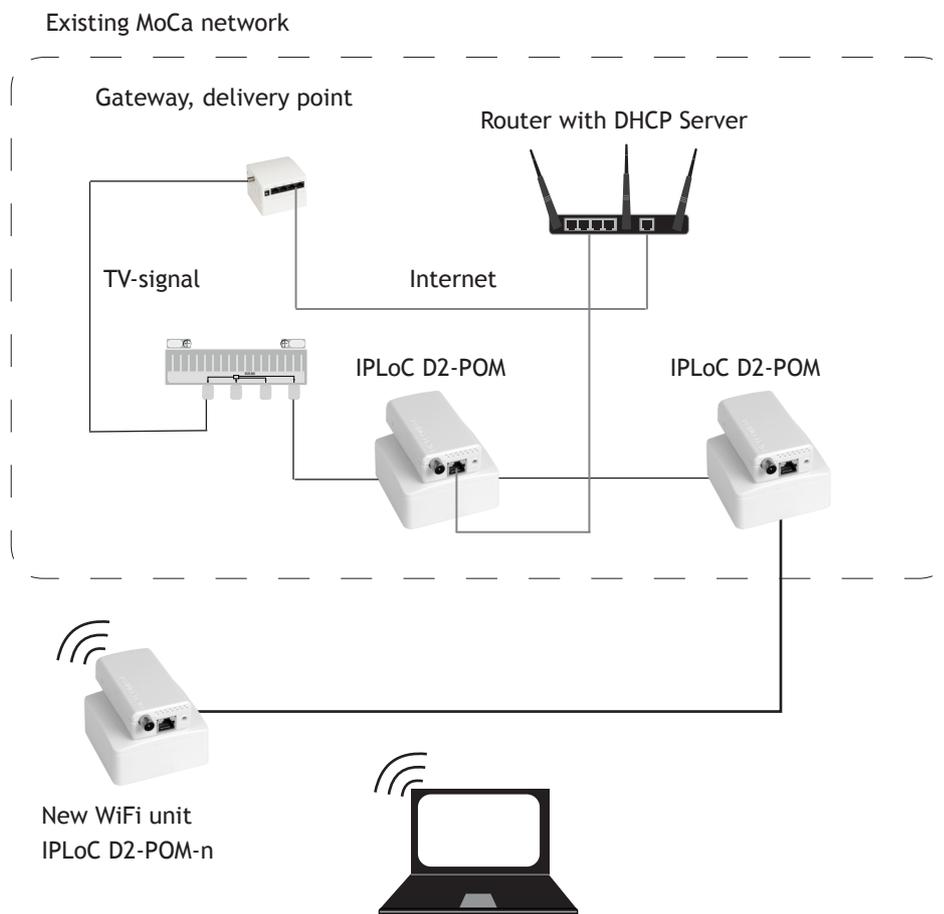- If you have a antenna cable in the outlet to a TV set, remove that and push on the IPLoC D2-POM-n and re-install the TV-set cable in the IPLoC D2-POM-n unit
- Connect the power supply unit.
  The diode for power will light up green.
- When you have powered up your IPLoC D2-POM-n there should be a green MoCA diode Green LAN blinking and a green Wi-Fi diode if everything is ok.
 Note! It can take up to 3 minutes before there is a link.
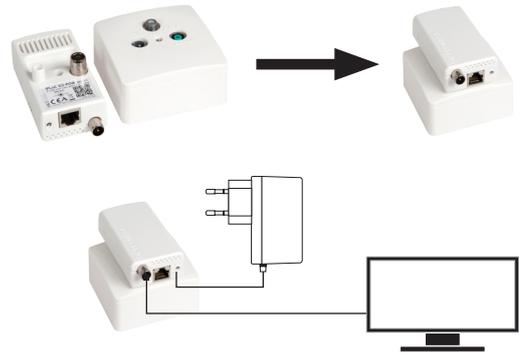
⚠ If you use the FM or DATA port on the outlet, you can mount the IPLoC unit "Upside Down" or use a jumper cable.

IPLoC unit as Accesspoint

Installation

When the unit is connected to a network with a DHCP server it will receive an IP address from the server automatically. When it has received the address it will create a Wi-Fi network which is by the default:
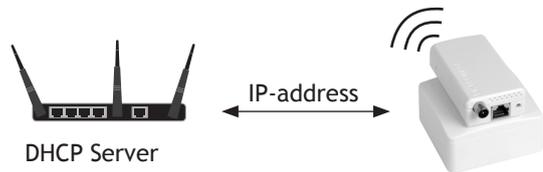
Broadcast name:	IPLoC-xxxx were xxxx are the last 4 digits of the WiFi MAC address printed on the unit
Default WiFi Password:	12345678

So far the unit work as a separate Wi-Fi access point in the home network with its own broadcast name and password. This is however not the most common use since it is more convenient if WiFi access points in the home has same network settings as the primary router.

The advantage of using same WiFi settings in the IPLoC as the main router is that all client devices (phones, computers, tablets etc) that have previously connected to the primary router can also connect to the IPLoC WiFi without the need to setup all devices one by one.

To be able to integrate the IPLoC unit in the existing network and allow other devices to jump seamlessly from router to IPLoC. You first need to change some settings on the IPLoC to match the router configuration.

In this guide the Router has following settings, It will be an advantage to have following information ready for your own router prior to this setup:

	Example of router settings:	Your router settings:
SSID:	HomeNetwork	
Encryption type:	WPA2 PSK	
Encryption key:	abcd1234	
Channel:	1	
Network mode:	b/g/n	
Band Width:	40MHz	

You may need to refer to router documentation for advice on how to view or change settings for your model.

IPLoC D2-POM-n - Mini Guide 2017-01-02. Ver. 1

Page 9

Specifications are subject to change without notice.
DKT is not responsible for any typographical errors or wrong.

DKTCOMEGA

IP Address on IPLoC WiFi

The intent with the WPS is that you can push a paperclip to the hole for ~1sec and the IPLoC will allow mobile devices to connect to wifi without the need to enter encryption key.

The WPS has never been meant to grap settings from the primary router.

So first of all you need to find the IP-address on the unit which it has received from the DHCP server. To do that, you can either look in your routers DHCP table or you need some software that can find an IP address in a Wi-Fi network. e.g.

Android phone and Tablets	https://goo.gl/tsNaf8
iPhone and iPad	https://goo.gl/maf6rQ
Windows, Linux and Mac	https://goo.gl/ZVFvo3

If you do a Net scan with software you will receive information for all the devices that are connected to the router.

Look for information from vendor DKT A/S. Then you will find a MAC-address and that shall be the same as your IPLoC which is written on the unit.

Look for the IP-address for that MAC-Address. This is the address you need to be able to access your IPLoC.

Now when you have found the IP-address, connect to your home network, open a browser and enter the IP-address. The login screen will appear.

Username: root
Password: admin

IP-Address   MAC-Address (Label on IPLoC unit)

192.168.100.166   00:19:9f:20:06:08
DKT A/S
22 23 80

Ports   Vendor name

← → C   ① 192.168.0.112/cgi-bin/luci

Authorization Required

Please enter your username and password.

Username	root
Password	

Reset   Login

Denmark | DKT A/S | Fanoevej 6 | DK-4060 Kirke Saaby | Denmark | e-mail: info@dktcomega.com | Phone: +45 4646 2626

Now that we are able to log on to the IPLoC unit will we make some change in the Wi-Fi configuration so that the unit will be integrated in the home network.

DKTCOMEGA

Changing default settings - Password

A good thing is to change the default password on the unit. To do that, go to tab "System" and sub-tab "Administration".
Enter a new password under password and type it again under confirmation. Press save and apply

Changing default settings - Network

Changing default settings - Network

Now we will give the unit the same network parameters as existing WiFi router.

In this guide the Router has following settings:

SSID:	HomeNetwork
Encryption type:	WPA2/PSK
Encryption key:	abcd1234
Channel:	1
Network mode:	b/g/n
Band Width:	20MHz

Our router is on channel 1 and we shall not have the same channel as our router.

You will of course use your Router settings, except the same channel.
When you have all the information go to tab "Network" and Sub-Tab "WiFi" and select edit.

IPLoC D2-POM-n - Mini Guide 2017-01-02. Ver. 1

Page 11

Specifications are subject to change without notice.
DKT is not responsible for any typographical errors or wrong.

General Configuration "General Setup" change:

Network Mode:

You can choose between:

- 802.11a
- 802.11b
- 802.11g
- 802.11b/g
- 802.11g/n

- 802.11a/n
- 802.11b/g/n
- 802.11a/an
- 802.11a/an/ac

Default is *802.11b/g/n*

In our case we do not change:
802.11b/g/n
because it is default and the same
as we have in our router.

Channel:

Default is "auto"

You can choose between:

- auto
- 2412MHz (Channel 1)
- 2417MHz (Channel 2)
- 2422MHz (Channel 3)
- 2427MHz (Channel 4)
- 2432MHz (Channel 5)

- 2437MHz (Channel 6)
- 2442MHz (Channel 7)
- 2447MHz (Channel 8)
- 2452MHz (Channel 9)
- 2457MHz (Channel 10)
- 2462MHz (Channel 11)

In our case we change to:
2417MHz (Channel 2)

Our router is on channel 1 and we
shall not have the same channel
as our router.

Band Width

Default is "40MHz"

You can choose between:

- 20MHz
- 40MHz

In our case we change to:
20MHz

Specifications are subject to change without notice.
DKT is not responsible for any typographical errors or wrong.

Interface Configurations "General Setup" change:

ESSID:

Default is IPLoC-xxxx were xxxx are the last 4 digits of the WiFi MAC address printed on the unit.

If you want to use your existing network name, you change to that.

If you not change to the same network name as your router, your devices must log on to 2 separate networks.
Sometimes ESSID is called SSID, Network name.

In our case we change to: HomeNetwork

Mode:

Default is "Access Point"
You can choose between:
Access Point and Client

We do not change

Interface Configurations "Wireless Security" change:

Encryption:

Default is "WPA2-PSK"

You can choose between:

- No Encryption
- WEP Open System
- WEP Shared Key

- WPA-PSK
- WPA2-PSK
- WPA-PSK/ WPA2-PSK Mixed Mode

- WPA-EAP
- WPA2-EAP
- WPA-EAP/ WPA2-EAP Mixed Mode

- 8021x

⚠ Same as your current Wi-Fi router

We do not change

Wi-Fi Protected Access (WPA) is the most common wireless encryption method used today. This is the recommended wireless security option.
WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP).
Personal requires only the use of a pass-phrase for security.

Cipher:

Default is "Force CCMP (AES)"

You can choose between:

- Force TKIP
- Force CCMP (AES)
- Force TKIP and Force CCMP (AES)

⚠ Same as your current Wi-Fi router

Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), and Both (TKIP and AES)

Key:

Default is 12345678

⚠ Same as your current Wi-Fi router

This is the encryption key for the home network. In our case we change to:
abcd1234

Now you can Click:
Save and Apply and wait for 60 seconds before doing anything else.

Now your IPLoC WiFi unit has the same security settings as your router and it is integrated in the home Network. Client devices (Phones, tablets, PC's etc.) can use the WiFi of both the router and IPLoC WiFi. Remember that you just changed the setting of the IPLoC WiFi, the accesspoint named IPLoC-xxxx is no longer avalible.

Web Interface

The Web interface has 4 main tabs with sub tabs.

Status with Sub tabs

System with Sub tabs

Network with Sub tabs

Logout

There are no Sub-Tabs under Logout. When you click on "Logout" you will exit the GUI direct and you have to logon again. The screen below appears

The following pages only show Network - Wi-Fi - Configurations GUI

Network - WiFi

If you click on Edit you can change your settings.

There are 3 tabs for Devivice Configuration:
- General Setup
- Advanced settings
- HT Physical Mode

And 2 tabs for Interface Configuration:
- General Setup
- Wireless Security

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable).

Per network settings like encryption or operation mode are grouped in the Interface Configuration.

Device Configuration - General Setup

Status:

Information on present configuration.

Radio on/off:

You can turn on or off the radio

You can turn off the radio to disable access through this device.
This can be helpful for configuration, network tuning, or troubleshooting.

Network Mode:

You can choose between:

- 802.11a
- 802.11b
- 802.11g
- 802.11b/g
- 802.11g/n
- 802.11a/n
- 802.11b/g/n
- 802.11a/an
- 802.11a/an/ac

Default is 802.11b/g/n

⚠️ This unit only support 802.11b/g/n if your router is set to Auto it is recommended to also set the router to 802.11b/g/n.

Channel:

Default is "auto"
You can choose between:

- auto
- 2412MHz (Channel 1)
- 2417MHz (Channel 2)
- 2422MHz (Channel 3)
- 2427MHz (Channel 4)
- 2432MHz (Channel 5)
- 2437MHz (Channel 6)
- 2442MHz (Channel 7)
- 2447MHz (Channel 8)
- 2452MHz (Channel 9)
- 2457MHz (Channel 10)
- 2462MHz (Channel 11)
- 2467MHz (Channel 12)
- 2472MHz (Channel 13)

Our router is on channel 1 and we shall not have the same channel as our router.

Using same channel as the router is not a good idea, in fact the only parameter that should be different from the router is the channel number, suggestion is that all devices with same SSID has different channel number assigned and to maintain that Auto should not be used on any device.

For optimal performance it can be a good idea to check which channels are already occupied in the area, this can be done with:

Android	https://goo.gl/9TqbNW
IOS	not available
Windows Linux Mac	https://goo.gl/04ww9w (It is Not a freeware)

Band Width

Default is "40MHz"
You can choose between:
- 20MHz
- 40MHz

Band width controls how large of a "pipe" is available to transfer data. However, larger channels are more subject to interference and more likely to interfere with other devices.

DKT COMEGA

WiFi - Advanced settings

DKTCOMEGA

Status | System | **Network** | Logout

Interfaces | **Wifi** | DHCP and DNS | Hostnames | Static Routes | Firewall | Diagnostics

Wireless Network: Client " IPLoC-xxxx " (ra0)

The *Device Configuration* section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

Device Configuration

General Setup | **Advanced Settings** | HT Physical Mode

Country Code	US
Support Channel	CH1~11
BG Protection Mode	auto
Beacon Interval	100
Data Beacon Rate	1
Fragment Threshold	2346
RTS Threshold	2347
TX Power	100
Short Preamble	Enable
Short Slot	Enable
Tx Burst	Enable
Pkt_Aggregate	Enable
IEEE 802.11H Support	Enable
Tx Beamforming	Disable
IGMP Snooping	Enable

Interface Configuration

General Setup | Wireless Security

ESSID	IPLoC-xxxx
Mode	Access Point
Network	☑ lan: 📶 📶 🖥 ☐ create:
	Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.
WMM Mode	Enable
APSDCapable	Disable

Reset | Save | Save & Apply

Denmark | DKT A/S | Fanoevej 6 | DK-4060 Kirke Saaby | Denmark | e-mail: info@dktcomega.com | Phone: +45 4646 2626

Device Configuration - Advanced settings

Country Code:

IDefault is "US"

You can choose between:

US, JP, FR, TW, IE, HK, None

Support Channel:

Default is "CH1~10"

You can choose between:

- CH1~10
- CH1~11
- CH10~11
- CH13
- CH1~14
- CH3~9
- CH5~13

BG Protection Mode:

Default is "auto"

You can choose between:

auto, on, off

Protection mode refers to a mechanism for the G radio. Since a legacy B radio device would not decode radio signals at G rates, a protection mechanism was developed for the new G radio and the B radio to co-exist on the same network.

Beacon Interval:
  Default is "100"
  You can choose between:
  20 to 1024 (ms)

A beacon is a packet broadcast sent by the router that synchronizes the wireless network. Adjustments may be necessary if there is a significant lag in wireless speed.

Data Beacon Rate:
  Default is "1"

Controls the data rate of beacon being sent. The setting range is 1~255 and 1ms is usually used.

Fragment Threshold:
  Default is "2346"
  You can choose between:
  256 to 2346

This is the maximum size of packet a client can send. Smaller packets improve reliability, but they will decrease performance. Reducing the fragmentation threshold is not recommended. Use default settings (2346).

RTS Threshold:
  Default is "2347"
  You can choose between:
  0 to 2347

RTS stands for 'Request to send' and it is send by the client to the access point – asking for permission to send the next data packet. The lower the threshold, the more stable your Wi-Fi network will be. If you don't have problems with your Wi-Fi, make sure that the RTS Threshold is set to the maximum allowed 2347.

TX Power:
  Default is "100"

TX power is set in percent.
Accepted value are 100, 70, 50, 35 and 15%

Short Preamble:
  Default is "Enable"
  You can choose between:
  Enable and Disable

Preamble Type setting means that it adds some additional data header strings to help check the wifi data transmission errors. Short Preamble Type uses shorter data strings that adds less data to transmit the error redundancy check which means that it is much faster.

Short Slot:
  Default is "Enable"
  You can choose between:
  Enable and Disable

When you enable short slot time, only the wireless devices with clients associated to the 802.11g, 2.4-GHz radio support slot time. Enabling short slot time increases throughput on the 802.11g, 2.4-GHz radio."

Tx Burst:
  Default is "Enable"
  You can choose between:
  Enable and Disable

It reducing some of the overhead or the skippable data transmissions in between multiple unicast. Normally it should be set to enable. Tx Bursting does not apply to wireless N or AC networks.

TPkt_Aggregate:
  Default is "Enable"
  You can choose between:
  Enable and Disable

Numerous packets can be transmitted in one MPDU by enabling this function.

DKT COMEGA

IEEE 802.11H Support:

Default is "Enable"
You can choose between:
Enable and Disable

802.11h refers to the amendment added to the IEEE 802.11 standard for Spectrum and Transmit Power Management Extensions. It solves problems like interference with satellites and radar using the same 5 GHz frequency band

Tx Beamforming

Default is "Disable"
You can choose between:
Enable and Disable

Beamforming allows an access point to effectively concentrate its signal at the clients location. This results in a better signal, SNR and potentially a great throughput.

IGMP Snooping:

Default is "Enable"
You can choose between:
Enable and Disable

When enabled, IGMP Snooping monitors IGMP communications among devices and optimizes wireless multicast traffic.

WiFi - HT Physical Mode

Device Configuration - Physical Mode

20/40 Coexistence:

Default is "Disable"

You can choose between:

Enable and Disable

Only use 20 Mhz / 40 Mhz combination if one of your devices require it.

Extension Channel:

Default is "Above"

You can choose between:

Above and Below

When 20/40MHz channel bandwidth has been set, the extension channel option will be enabled. The extension channel will allow you to get extra bandwidth.

Operating Mode:

Default is "Mixed Mode"

You can choose between:

Mixed Mode and Green Mode

The "greenfield" mode is designed to improve efficiency by eliminating support for 802.11a/b/g devices in an all draft-n network. In green mode the network ignore all earlier standards.

Guard Interval:

Default is "Auto"

You can choose between:

Auto and Long

The guard interval(GI) between symbols helps receivers overcome the effects of multipath delays. 802.11 a/b/g requires GI to be 800 ns (Long).

Reverse Direction Grant(RDG)

Default is "Enable"

You can choose between:

Enable and Disable

When enables Reverse Direction Grant, the wireless AP can reduce the transmitted data packet collision by using the reverse direction protocol.

Space Time Block Coding (STBC):

Default is "Enable"

You can choose between:

Enable and Disable

STBC is supported when the value is enable

Aggregation MSDU(A-MSDU):

Default is "Enable"

You can choose between:

Enable and Disable

MAC Service Data Unit (MSDU) aggregation group several data frames into one large frame. The concept of A-MSDU is to allow multiple MSDUs (MAC Service Data Units) to be sent to the same receiver concatenated in a single MPDU.

Auto Block ACK:

Default is "Enable"

You can choose between:

Enable and Disable

Decide whether Block ACK will be transmitted automatically.

Decline BA Request:

Default is "Disable"

You can choose between:

Enable and Disable

Decide whether user wants to decline Block ACK request.

HT Disallow TKIP:

Default is "Enable"

You can choose between:

Enable and Disable

Decide whether to operate in 802.11g, if using TKIP

DKTCOMEGA

HT LDPC:

   Default is "Disable"
   You can choose between:
   Enable and Disable

The low-density parity check (LDPC) code is defined as an option in 802.11n. It offers a coding gain when compared to convolutional codes. It can increases signal-to-noise ratio.

HT TxStream:

   Default is "2"
   You can choose between:
   1, 2, 3 and 4

HT TxStream - HT means High Throughput. The number of HT TxStream means how many antennas will transmit data simultaneously.

HT RxStream:

   Default is "2"
   You can choose between:
   1, 2, 3 and 4

HT RxStream - HT means High Throughput. The number of HT RxStream means how many antennas will receive data simultaneously.
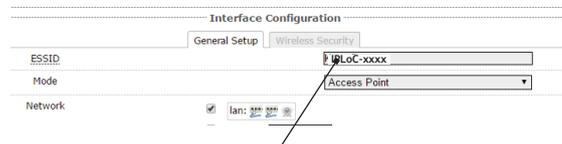

Interface Configuration - General Setup

ESSID:

   Extended Service Set Identification (ESSID)
   Default is "IPLOC-0615"

   If you want to use your existing network name, you change to that.

   If you not change to the same network name as your router, your devices must log on to 2 separate networks.

⚠ Same as your current Wi-Fi router

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID), but may still be referred to as SSID

Mode:

   Default is "Access Point"
   You can choose between:
   Access Point and Client

Network:

   Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network

---

WMM Mode:

   Default is "Enable"
   You can choose between:
   Enable and Disable

Wireless Multimedia Extensions(WMM), It provides basic Quality of service (QoS) features to networks. WMM prioritizes traffic such as voice, video, best effort and background.

APSDCapable:

   Default is "Disable"
   You can choose between:
   Enable and Disable

WMM APSD stands for Wi-Fi Multimedia (WMM) Automatic Power Save Delivery. It is basically a feature mode that allows your mobile devices to save more battery while connected to your wifi network.

DKT COMEGA

Interface Configuration - Wireless Security

Reverse Direction Grant(RDG)	Enable
Space Time Block Coding (STBC)	Enable
Aggregation MSDU(A-MSDU)	Enable
Auto Block ACK	Enable
Decline BA Request	Disable
HT Disallow TKIP	Enable
HT LDPC	Disable
HT TxStream	2
HT RxStream	2

Interface Configuration

General Setup | Wireless Security

Encryption	WPA2-PSK
Cipher	Force CCMP (AES)
Key Renewal Interval(seconds)	
Key	•••••••••

⊗Reset ⊘Save ▣Save & Apply

Encryption:

Default is "WPA2-PSK"

You can choose between:

- No Encryption
- WEP Open System
- WEP Shared Key

- WPA-PSK
- WPA2-PSK
- WPA-PSK/ WPA2-PSK Mixed Mode

- WPA-EAP
- WPA2-EAP
- WPA-EAP/ WPA2-EAP Mixed Mode
- 8021x

⚠ Same as your current Wi-Fi router

Wi-Fi Protected Access (WPA) is the most common wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP). Personal requires only the use of a pass-phrase for security.

Cipher:

Default is "Force CCMP (AES)"

You can choose between:

- Force TKIP
- Force CCMP (AES)
- Force TKIP and Force CCMP (AES)

⚠ Same as your current Wi-Fi router

Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), and Both (TKIP and AES)

Key Renewal Interval(seconds):

Default is ""

A normal value is 3600

One of the strengths of WPA2 encryption is that it self-generates a new key based on the original encryption key you entered. By enabling this field, you can control the time interval between the creation of the new encryption keys.

Key:

Default is 12345678

⚠ Same as your current Wi-Fi router

The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?&_) and spaces. This key must be the exact same key entered on your wireless router.*

IPLoC D2-POM-n - Mini Guide 2017-01-02. Ver. 1

Specifications are subject to change without notice.
DKT is not responsible for any typographical errors or wrong.

Page 23

DKTCOMEGA

The most recent version of the Mini guide:

https://goo.gl/AWu46I

The most recent version of the User guide:

https://goo.gl/MKnx8F

The most recent version of the Quick Start-guide:

https://goo.gl/RAe4mI

DKTCOMEGA