

# User Guide

## **Icotera i6800**

Triple play FTTH solution

Published: October 2016

Software version: 1.10.0

Document version: 2.0

# Table of Contents

Change log .....	3
Introduction .....	4
Product Overview .....	5
General Features and Characteristics .....	5
Physical Description .....	5
Configuring and managing the i6800 .....	8
Web interface general overview .....	8
Logging in to the web interface .....	10
Viewing device status information .....	11
Managing the LAN and Wi-Fi settings .....	18
Using network diagnostic tools .....	23
Changing administrator settings .....	26
Managing services .....	28

---

## Change log

Date	Version	Reason for a change	Author
28/10/2016	2.0	First release available to public.	<ijakobik@icotera.com>

---

# Introduction

The Icotera i6800 is a customer premises equipment designed for triple play services, dedicated to FTTH (Fiber To The Home) network in P2P (point-to-point) architecture.

The i6800 integrates Ethernet-based data transmission with Layer 3-4 functionality, voice (IP telephony), wireless 2.4 GHz 802.11b/g/n as well as 5 GHz 802.11a/n/ac transmission, and CATV.

This device features a powerful dual core architecture, where all processor-intensive tasks are handled by a dedicated core, leaving one core available for other immediate tasks. This explicitly means that the system is still responsive, even while doing VoIP, gigabit routing of IPv4/IPv6 with NAT (IPv4) or bridging wirespeed.

Two-channel SIP VoIP with alaw/ulaw fax is supported. Among other supported features local tones and fast dial are included.

The Icotera i6800 provides a wide transparent bandwidth to support CATV analog channels or a combination of analog and digital channels including HDTV broadcast.

---

# Product Overview

This chapter provides a comprehensive overview of the i6800 components, features and characteristics.

## General Features and Characteristics

This section presents a list of features and characteristics of the Icotera i6800 related to its hardware, software and environment of operation.

### Features

- 802.11b/g/n WiFi
- 802.11ac WiFi
- 2 SIP VoIP ports
- Layer 2 - 7 QoS
- Layer 2 - 7 filters
- Customer web interface
- Full band CATV (optional)
- CATV filters (optional)
- USB 2.0 (providing up to 500mA)
- USB 3.0 (providing up to 500mA)

### Uplink Interface

- Dual speed optical uplink with auto detection

### Downlink Interfaces

- 4 x 10/100/1000 RJ45 ports
- Auto-negotiation for speed and duplex
- Auto MDI/MDX

### Performance

- Gigabit routing with NAT and bridging

### Power and Environmental Specifications

- DC12V input
- Power consumption (max): 12 watt
- Operating temperature: 0 – 50°C
- Storage temperature: -15 – 55°C
- Humidity: 10% – 90%

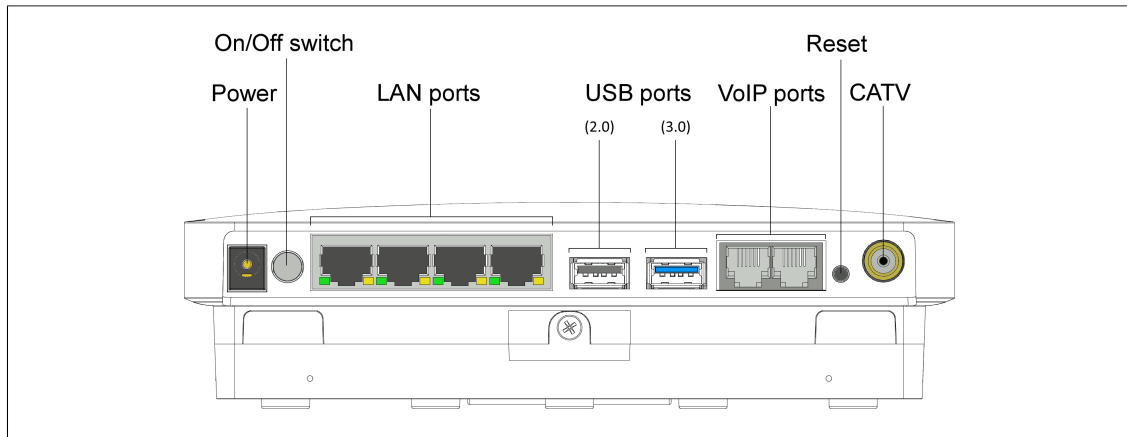
## Physical Description

This section describes the physical components of the i6800, i.e. connectors, LEDs and buttons.

## Front Panel

The Icotera i6800 front panel, shown in the following figure, contains the power port, on/off switch, reset button, connectors and LAN status LEDs. All these items are described in subsequent topics of this section.

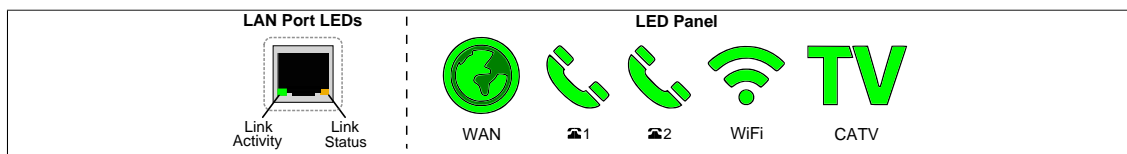
**Figure 1. The Icotera i6800 front panel**



## Status LEDs

There are two types of the Icotera i6800 status LEDs: LAN port LEDs and the LEDs on the LED panel that is located between LAN and POTS ports.

**Figure 2. The Icotera i6800 status LEDs**



The following table shows the status LEDs descriptions for the Icotera i6800.

**Table 1. The Icotera i6800 status LEDs descriptions**

LED Type	Type	Colour	State	Description
Link Activity	LAN port activity	Green	On	Communications link established
			Blinking	Network activity on the corresponding port
			Off	Bad connection no connection to this port
Link Status	LAN port status	Yellow	On	Corresponding port linked and operating at 1 Gb/s
			Off	Corresponding port set to operate at 10/100 Mb/s
WAN	WAN port activity	N/A	Off	Power down
		Green	Blinking fast	Obtaining IP address
			Blinking slow	Auto detection
			Solid	IP connection established
		Red	Blinking slow	Management or other interface lease fail (depends on LEDs configuration)
			Solid	No signal
☎1/☎2	VoIP registration status/Hook status	N/A	Off	Line disabled
		Green	Blinking fast	Call in progress
			Blinking slow	Off-hook
			Solid	Line registered
		Red	Solid	Line registration error

LED Type	Type	Colour	State	Description
WiFi	WiFi status and activity	N/A	Off	WiFi not configured, disabled or not in use
		Green/Orange	Blinking	WiFi 5 GHz detecting radar (blinks for 60 secs; for channels 120, 124, 128, and 132 blinks for 10 minutes). NOTE: For some production batches radar detecting may be signalled by WiFi LED blinking red. In this case red color does not signal any errors.
		Green	Blinking fast	Connecting new client (blinking 5 s)
			Solid	WiFi configured and enabled
CATV	CATV status	N/A	Off	CATV disabled
		Green	Solid	CATV configured and enabled, signal OK
		Red	Solid	CATV configured and enabled, signal too low (-10.5 dBm) or unavailable
All	Device status	Green	Oscillating	Boot/reboot in progress
All	Device status	Green	Pulsing	Firmware upgrade in progress

**Note**

The LED panel functioning can be adjusted from the web interface. For instructions on how to do this, see *Managing LEDs behaviour* in the *Changing administrator settings* section.

**Connectors**

The Icotera i6800 front panel includes all the local user connectors that are four RJ-45 10Base-T/100Base-TX/1000Base-T ports, two USB ports, two POTS phone ports and one F-type CATV RF output port. Optical fiber connectors are placed inside the device.

**Power Port**

The power port accepts DC 12V power source. It is important to make sure that the proper power adapter is suitable to a particular region.

**On/Off Switch**

The On/Off switch enables you to switch the i6800 on or off, as well as reboot the i6800 and restore the last saved configuration.

**Reset Button**

The **Reset** button has four modes of operation:

- when CPE is operating - **pressed for less than 10 seconds**: restarts CPE.
- when CPE is operating - **pressed for more than 10 seconds**: restores default CPE settings.
- when CPE is off - **power-on with reset button pressed for less than 10 seconds**: restores default CPE settings.
- when CPE is off - **power-on with reset button pressed for more than 10 seconds**: boots CPE from the second bank.

**Serial Number**

The serial number of the Icotera i6800 consists of 16 digits. The format of the serial number is *PPPPVVWWYYXXXXXX*, where *PPPP* is the product ID, *VV* is the product variant, *WW* is the production week, *YY* is the production year, and *XXXXXX* is the running serial number. For example 6801010515123450 would be a serial number of a 01 variant of the i6801 device (i6801-01), produced in the 5th week of 2015, with a running number of 123450.

# Configuring and managing the i6800

This chapter provides a comprehensive overview of the Icotera i6800 configuration and management features. It focuses on managing the device using the web interface, as this interface is the only method of device management available to the end user.

## Web interface general overview

After a successful login, the main window of the web interface is displayed. By default, it is the **System information** submenu of the **Status** menu. The following figure presents the structure of the web interface.

Figure 3. Icotera i6800 web interface



### Top bar

The top bar contains the Icotera logo, device designation, drop-down list which enables to choose interface language, and the **Log out** button.

### Menu

The menu has a form of a collapsible list of available options, which are grouped into two levels: main and secondary. The main level provides access to general i6800 management categories, while the secondary level presents a submenu of available options for a given category. By default all menu options are expanded, but they can be collapsed by clicking chosen main menu entries.



**Figure 4. Collapsing i6800 web interface menu**



## Management area

The management area is where all the i6800 management and status information are displayed and modified. Depending on the selected option, it can display a set of particular configuration options or a list of current i6800 status information.

## Bottom bar

In the centre of the bottom bar, there are three buttons:

- **Reset:** resets all changes made in the current session.
- **Save:** saves all changes made in the current session.
- **Apply:** applies all changes saved during the current session.

The right-hand side of the bottom bar may contain an operator's logo.

## Logging in to the web interface

Complete the following steps to log in to the web interface:

1. Enter the address of your i6800 unit in the address bar of your web browser. The following login prompt will be displayed.

**Figure 5. Icoteria i6800 login prompt**



The screenshot shows a web browser window displaying the 'i6800 Login' page. The page has a green header bar with the text 'i6800 Login' in white. Below the header, the text 'Please input your username and password:' is displayed in a small font. There are two input fields: 'Username:' and 'Password:'. Below the input fields, there are two buttons: 'Log in' and 'Clear'.

2. Enter your username and password in the respective fields.
3. Click the **Log in** button to log in or use the **Clear** button to clear both fields and type your credentials again.



### **Important**

The first time you log in, use the username and password provided by your network operator. After the first login you will be able to change your credentials using the **Administration > UI login password** menu.

---

## Viewing device status information

The **Status** menu provides tools for viewing general device status information, as well as to obtain information about WAN, LAN and wireless interfaces operating on the device. This menu also allows to configure static IP leases for LAN interfaces, and to view VoIP call log.

### Obtaining general system information

To access general information about your i6800 go to **Status > System information**. This menu includes the following information:

The **System information** section:

- **Current time:** The current time and date.
- **Uptime:** The duration the device has been powered up.
- **Firmware version:** The current software version operating on the device.
- **WAN MAC:** The physical address of the device WAN interface.
- **WAN IP:** The IP address of device WAN interface .
- **Device name:** The name of the device.
- **Serial number:** The unit's serial number.
- **Wi-Fi 802.11b/g/n:** The status of the Wi-Fi 802.11b/g/n wireless interface, either **On** or **Off**.
- **Wi-Fi 802.11ac:** The status of the Wi-Fi 802.11ac wireless interface, either **On** or **Off**.

The **System counters** section contains statistical information about data entering and leaving the interfaces of the i6800 as well as error and collision counters.

- **Status:** Current status of a given interface, either **Up** or **Down**.
- **Pkts in:** The number of incoming packets in the current session.
- **Pkts out:** The number of outgoing packets in the current session.
- **Errors:** Transmission error counter.
- **Collisions:** Collision counter.
- **Speed:** .

The data under information menu can be refreshed at any time by clicking the **Refresh** button.

As this menu does not include any configurable options the **Reset**, **Save**, and **Apply** buttons are disabled.

**Figure 6. System information section of the Status menu**

System information			
Current time:	2016/10/12 09:10	Device name:	i6800
Uptime:	0 d 20 h 51 m 36 s	Serial number:	6801000915000594
Firmware version:	1.10.0	Wi-Fi 802.11b/g/n:	On
WAN MAC:	00:1e:80:18:1e:21	Wi-Fi 802.11ac:	On
WAN IP:	10.10.0.59		

System counters						
	Status	Pkts in	Pkts out	Errors	Collisions	Speed
LAN 1	Up	232029	360075	0	0	FD1000
LAN 2	Down	0	0	0	0	down
LAN 3	Down	0	0	0	0	down
LAN 4	Down	0	0	0	0	down
WLAN 2.4 GHz	Up	9109 k	52875	-	-	-
WLAN 5 GHz	Up	18169 k	41705	-	-	-
WAN	Up	20696 k	243513	0	0	FD1000

[Refresh](#)

[Reset](#)
[Save](#)
[Apply](#)

## Monitoring the WAN interface

The **WAN** section of the **Status** menu lists basic information about interface as well as the statistics of data carried through the interface.

Click **Status > WAN** menu to open the **WAN** section.

**Figure 7. The WAN section of the Status menu**

WAN			
WAN IP type:	DHCP	Default gateway:	10.10.0.1
IP address:	10.10.0.59	MAC Address:	00:1e:80:18:1e:21
Subnet mask:	255.255.254.0		

WAN counters						
	Status	Pkts in	Pkts out	Errors	Collisions	Speed
WAN	Up	21169 k	293980	0	0	FD1000

[Refresh](#)

[Reset](#)
[Save](#)
[Apply](#)

The **WAN** section presents basic information about the WAN interface:

- **WAN IP type:** The IP address type of the WAN interface.
- **IP address:** The IP address used by the WAN interface.
- **Subnet mask:** The subnet mask used by the WAN interface.

- **Default gateway:** The default gateway configured for the WAN interface.
- **MAC address:** The interface's physical address.

The **WAN counters** section displays statistical information about the data.

The WAN information menu can be refreshed at any with the **Refresh** button.

As this menu does not include any configurable options, the **Reset**, **Save**, and **Apply** buttons are disabled.

## Monitoring the LAN interface

The **LAN** submenu of the **Status** main menu allows user to obtain information about the LAN interface and to configure static IP leases for connected devices.

**Figure 8. The LAN section of the Status menu**

inet\_br

**IP type:** DHCP server  
**IP address:** 192.168.7.1  
**Subnet mask:** 255.255.255.0

**Default gateway:** 192.168.7.1  
**MAC Address:** 00:1e:80:18:1e:21

**Counters**

	Status	Pkts in	Pkts out	Errors	Collisions	Speed
LAN 1	Up	283071	429855	0	0	FD1000
LAN 2	Down	0	0	0	0	down
LAN 3	Down	0	0	0	0	down
LAN 4	Down	0	0	0	0	down
WIFI 1 AP 1	Up	11680 k	80899	0	0	-
WIFI 2 AP 1	Up	23850 k	63253	0	0	-

**Dynamic Leases**

IP address	MAC Address	Hostname	Expires	Remember
192.168.7.37	3c:97:0e:57:59:67	Lenovo-PC	64551	<div style="border: 1px solid #ccc; padding: 2px 5px; display: inline-block;">Make static</div>

**Static Leases**

IP address	MAC Address	Enable	Add/Remove
<input style="width: 150px;" type="text" value="0.0.0.0"/>	<input style="width: 150px;" type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>	<div style="border: 1px solid #ccc; padding: 2px 5px; display: inline-block;">Add</div>

Refresh

Reset

Save

Apply

The **LAN** section contains the following general information about the LAN interface:

- **IP type:** The IP address type of the LAN interface.
- **IP address:** The IP address used to the LAN interface.
- **Subnet mask:** The subnet mask used by the LAN interface.

- **Default gateway:** The default gateway configured for the LAN interface.
- **MAC address:** The interface's physical address.

The **Counters** section displays statistical information about the data

The **Dynamic Leases** section contains information about devices connected to the LAN interface which have a dynamically assigned IP address. Each device is described with the following parameters:

- **IP address:** The IP address assigned to the device.
- **MAC Address:** The physical address of the connected device.
- **Hostname:** The connected device's hostname.
- **Expires:** The lease time of the device's address.
- **Remember:** The dynamic lease can be remembered as a static lease using the **Make static** button. When the button is clicked, the entry will be visible in the **Static Leases** section.

In order to manually add a static lease use the following steps:

1. In the **IP address** field enter the IP address of the device to be connected.
2. In the **MAC address** field enter the **MAC address** of the device.
3. Check the **Enable** box if the lease is to be enabled right away. Leave the box blank if the device will be enabled later.
4. To add the lease to the list click the **Add** button.
5. Save changes by clicking the **Save** button. Clicking the **Apply** button is required to apply the changes to the i6800 database.

The LAN information can be refreshed at any with the **Refresh** button.

## Monitoring the wireless interfaces

The **Wi-Fi 802.11b/g/n** and **Wi-Fi 802.11ac** sections contain information about i6800 wireless interfaces and their access points. These two sections describe separate interfaces, but their layout is the same.

**Figure 9. The Wi-Fi interface tab of the Status menu**

General

**Status:** On

**Mode:** 802.11b/g/n

**Channel:** 1 (auto) Reselect

**TX Power:** 100

**Band:** 20MHz

Access point 1: wifi24ghz\_ap1

**SSID:** my\_default\_ap

**Hidden:** no

**BSSID:** 00:1e:80:18:1e:23

**Encryption:** WPA2 AES-TKIP

**Status:** On

Counters

	Status	Pkts in	Pkts out	Bytes in	Bytes out	Errors	Collisions
AP 1	Up	9368 k	84514	2204 MiB	41987 KiB	0	0

Associated clients

IP address	MAC Address	Hostname	Expires	Mode	Sleep	RSSI	TX bytes	TX rate	TX failed
192.168.1.214	64:bc:0c:59:59:ee	android-bbe0992be83dc50a	35909	BGN	Yes	70	14891 KiB	72.2 Mbps	12
192.168.1.104	d0:92:9e:c7:d9:10	Windows-Phone	42028	BGN	Yes	59	480356 B	72.2 Mbps	1

Refresh

Reset
Save
Apply

The **General** section contains the following general information about the interfaces:

- **Status:** Interface status, either **On** or **Off**.
- **Channel:** The wireless channel on which the interface operates (**Reselect** button allows to reselect channel if **Channel** option in **Settings** section is set to **auto**).
- **Band:** The frequency band used by the interface.
- **Mode:** The wireless mode of the wireless interface.
- **Tx Power:** The Tx power value for the wireless interface.

The **Access point** section contains the following information about a particular Wi-Fi access point:

- **SSID:** The SSID of the access point.
- **BSSID:** The access point BSSID.
- **Status:** The access point status, either **On** or **Off**.
- **Hidden:** The visibility setting of the access point.
- **Encryption:** The data encryption algorithm of the access point.

The **Counters** section contains statistical information about data entering and leaving the interfaces of the access point as well as error and collision counters.

- **Status:** Current status of the given interface, either **Up** or **Down**.
- **Pkts in:** The number of incoming packets in the current session.
- **Pkts out:** The number of outgoing packets in the current session.
- **Bytes in:** The number of incoming bytes in the current session.
- **Bytes out:** The number of outgoing bytes in the current session.
- **Errors:** Transmission error counter.
- **Collisions:** Collision counter.

The **Associated clients** section lists all devices connected to the particular access point. Each device is described with the following parameters:

- **IP address:** The IP address assigned to the device.
- **MAC Address:** The physical address of the connected device.
- **Hostname:** The connected device's hostname.
- **Expires:** The lease time of the device's address.
- **Mode:** Mode of operation.
- **Sleep:** If **Yes**, client is present but does not exchange traffic with host; if **No**, client is present and active.
- **RSSI:** Received Signal Strength Indicator.
- **Tx bytes:** Transmitted bytes.
- **Tx rate:** Transmission rate.
- **Tx failed:** Transmission failures.
- **Rx bytes:** Received bytes.

The wireless interface information tab can be refreshed at any time with the **Refresh** button.

As this tab does not include any configurable options, the **Reset**, **Save**, and **Apply** buttons are disabled.

## Viewing VoIP call log

The **VoIP call log** section gives access to the log of internet telephone calls.

**Figure 10. The VoIP call log tab of the Status menu**

VOIP call log									
Started	Source	Destination	Duration	Status	Codec	Dir.	Max Jitter	Pkts. lost	Type
VOIP call log is empty									

Each call is described by the following data:

- **Started:** Start time and date of a call.
- **Source:** Source phone number.
- **Destination:** Destination call number.



- **Duration:** Call duration.
- **Status:** Call status (e.g. answered, busy)
- **Codec:** Codec used.
- **Dir.:** Call direction (incoming or outgoing).
- **Max Jitter:** Maximal jitter value in seconds.
- **Pkts. lost:** Number of lost packets.
- **Type:** Call type (e.g. voice).

## Managing the LAN and Wi-Fi settings

The **Settings** menu provides advanced configuration options to control the Layer 3 network parameters of your cabled and Wi-Fi network. This menu allows to configure the IP settings of all available interfaces in your home network.

### Managing the LAN settings

The **LAN** submenu contains configurable IP options of LAN interfaces.

In order to manage the IP settings with this menu, use the following steps:

1. Click the **LAN** submenu of the **Settings** menu to open the **LAN** section.

**Figure 11. LAN section of the Settings menu**

The screenshot shows the 'inet\_br' window for LAN configuration. It contains the following fields and values:

- IPv4 Type:** DHCP server (dropdown menu)
- IP address:** 172.22.22.1
- IP netmask:** 255.255.255.0
- Gateway:** 172.22.22.1
- Primary DNS:** 172.22.22.1
- Secondary DNS:** 0.0.0.0
- WINS:** 0.0.0.0
- IP range:** 172.22.22.100 - 172.22.22.250
- Lease time:** 3600
- Max lease time:** 7200

At the bottom of the window are three buttons: **Reset**, **Save**, and **Apply**.

2. Choose LAN interface IP type from the **IPv4 Type:** drop-down menu. If the **DHCP server** option is selected (default configuration), all hosts connected to LAN ports or over WiFi interface will obtain their IP addresses and other necessary information automatically. In order to change this setting choose from the drop-down menu **Static** option and enter all network parameters manually.
3. Use the following fields to configure the IP settings of your network:
  - **IP address:** specifies the IP address of your network.
  - **IP netmask:** specifies your network mask.
  - **Gateway** (only for dynamic IP configuration): specifies the IP address of your network gateway.
  - **Primary DNS** (only for dynamic IP configuration): specifies the primary Domain Name System server to be used to resolve DNS queries.
  - **Secondary DNS** (only for dynamic IP configuration): specifies the secondary Domain Name System server to be used to resolve DNS queries.
  - **Wins** (only for dynamic IP configuration): specifies the IP address of the Windows Internet Name Service server. This server is typically used in office environments.
  - **IP range:** specifies the pool of IP addresses that can be allocated by the DHCP server.

- **Lease time:** specifies the DHCP lease renewal time in seconds. The value in this field must range from 60 to 86400 and cannot be higher than the value in the **Max lease time** field. It is recommended to leave this value at its default setting.
  - **Max lease time:** specifies the maximum time in seconds that can be assigned to the client, if he asks for a longer lease time than the standard lease time. The value in this field must range from 60 to 86400 and cannot be lower than the value in the **Lease time** field. It is recommended to leave this value at its default setting.
4. Click the **Save** button to save your changes.

After applying these settings with the **Apply** button, the network configuration will be changed.

### Notes

- During DHCP configuration, take special care to ensure that the **IP address**, **Netmask**, **Gateway** and **Range** settings match each other. Under normal circumstances the IP address and the gateway address should be the same.
- It is recommended to leave **Primary DNS** and **Secondary DNS** fields at their default settings, which will allow you to use your operator's DNS servers. However, these addresses can be changed to use other servers, e.g. Open DNS.

## Managing the wireless settings

The **Wi-Fi** sections of the **Settings** menu allow to configure general settings of the wireless interfaces, as well as access lists.

### Global Wi-Fi settings

Figure 12. The global settings of the Wi-Fi tab

The screenshot shows the 'Global Settings' for the 'Wi-Fi 802.11b/g/n' interface. The settings are:

- Enable:** ☒
- Channel:** 1
- Channel width:** 20 MHz
- Mode:** 802.11b/g/n
- Tx Power:** 100 %

The **Global Settings** section provides you with the general Wi-Fi performance settings, common for all 802.11b/g/n or 802.11ac interfaces. Use the following steps to configure them:

1. Check the **Enable** checkbox to enable the interface, or leave it blank to disable the interface.
2. Use the **Channel** drop-down list to set the channel number (or choose **auto** option).
3. Use the **Channel width** drop-down list to set the channel width in MHz.
4. Use the **Mode** drop-down list to select the available networking modes.



**Note** The lists of available networking modes might vary depending on the CPE model.

5. Use the **TX power** drop-down list to specify the Tx power level (in percentage).

- Confirm your changes by clicking the **Save** button on the bottom bar.

## Access point settings

The **APs** section provides configuration options for the Wi-Fi access points. Use the following steps to configure the APs interfaces:

- Click the **Wi-Fi 802.11b/g/n** or **Wi-Fi 802.11ac** submenu of the **Settings** menu to open the Wi-Fi settings section.
- Go to the tab containing the desired AP configuration.

**Figure 13. The access point settings in the Wi-Fi settings section**

The screenshot displays the 'Wi-Fi 802.11b/g/n APs' configuration window. At the top, there are two tabs: 'AP 1' and 'AP 2'. The 'AP 1' tab is selected. Below the tabs, the following settings are visible for AP 1:

- Enable:** A checkbox that is checked.
- SSID:** A text input field containing the value 'Icoteria'.
- Encryption:** A dropdown menu currently showing 'WPA2 TKIP-AES'.
- Encryption key:** A text input field filled with dots. To its right is a 'Show password' checkbox, which is currently unchecked.
- Hidden:** An unchecked checkbox.
- Client isolation:** An unchecked checkbox.
- Enable WPS:** A checked checkbox.

- If you are going to use the particular AP, check the **Enable** checkbox.
- Use the **SSID** field to edit the SSID of your AP. SSID is the AP name you will see when scanning for available Wi-Fi networks on your computer. It can be any combination of letters and digits.
- Use the **Encryption** drop-down list to select the type of encryption key and the encryption algorithm used to secure the Wi-Fi transmission between your computer and the i6800. Available choices are **None**, **WEP-64**, **WEP-128**, **WPA TKIP**, **WPA AES**, **WPA TKIP-AES**, **WPA2 TKIP**, **WPA AES** and **WPA TKIP-AES**. Please note that **None** leaves the wireless AP unsecured and open for access from any Wi-Fi device. The recommended encryption type is **WPA2**.
- Specify the encryption key in the **Encryption key** field. The key characters will be displayed, when the **Show password** checkbox is checked.
- If you want to prevent your AP from being detected by simple network scanning, check the **Hidden** checkbox. However it is recommended to leave this box blank, since hiding the AP doesn't provide any layer of security.
- If you want to block traffic between clients of the access point, check the **Client isolation** checkbox. This option may be used to create "guest" access point, so all devices connected to that AP will be isolated from one another.
- If you want to enable WPS based procedure for a given access point, check the **Enable WPS** checkbox.
- Confirm your changes by clicking the **Save** button on the bottom bar.

## WPS section

WPS section allows to perform WPS based procedure. WPS function is activated by pressing the **Start WPS** button.

**Figure 14. The WPS section**

WPS:

Please press the WPS button to activate WPS function.

Start WPS

## Access lists

Each access list provides an Ethernet layer 2 filter, which can be used either to allow or to deny particular users to connect based on their Wi-Fi adapters MAC address. In order to configure the Access list for your interfaces, complete the following steps:

1. Click the **Wi-Fi 802.11b/g/n** or **Wi-Fi 802.11ac** submenu of the **Settings** menu to open the Wi-Fi settings section.
2. Go to the **ACL settings** area which contains the access list for AP.

**Figure 15. Access list settings**

ACL settings

☐ Client limit 0 client(s)

Access list behavior

☐ allow  
☐ deny  
☒ none

No.	Name	MAC Address	Enabled	Action
1			<input type="checkbox"/>	Clear
2			<input type="checkbox"/>	Clear
3			<input type="checkbox"/>	Clear
4			<input type="checkbox"/>	Clear
5			<input type="checkbox"/>	Clear
6			<input type="checkbox"/>	Clear
7			<input type="checkbox"/>	Clear
8			<input type="checkbox"/>	Clear
9			<input type="checkbox"/>	Clear
10			<input type="checkbox"/>	Clear
11			<input type="checkbox"/>	Clear
12			<input type="checkbox"/>	Clear
13			<input type="checkbox"/>	Clear
14			<input type="checkbox"/>	Clear
15			<input type="checkbox"/>	Clear
16			<input type="checkbox"/>	Clear

Reset
Save
Apply

3. In order to set a limit of clients that may be connected to your APs, check the **Client limit** checkbox and enter the desired client limit value. The maximum value is 32 clients.
4. Use the **Access list behavior** radio buttons to define the desired behaviour of the access list:
  - **allow**: allows only the devices in the access list to connect to the AP.
  - **deny**: prevents the devices in the access list from connecting to the AP and allows all the other devices to connect to it.
  - **none**: completely disables the access list.
5. Check the appropriate checkbox in the **Enabled** column to activate the access list entry for editing. Use the following options to add the Wi-Fi device to the access list:
  - **Name**: this field is used for your reference. It should be set to a meaningful string that allows to identify a particular device, e.g. "my Lenovo laptop" or "my iPhone".
  - **Mac Address**: physical address of the wireless adapter in your device. The valid address must be specified as a string of six octets separated by colons or hyphens, e.g. 02:00:54:FF:4E:01 or 02-00-54-FF-4E-01. The method to determine this address varies depending on the device. For more information on how to determine this address, please refer to your device manual.
  - **Enabled**: check this check box to include the device in the current access list. To temporarily exclude the device from the access list, uncheck it.
  - **Clear**: use this button if you want to permanently remove the device from the access list.
6. After you have finished editing access list entries, click the **Save** button to save changes.

To update access list configuration, click the **Apply** button.



The maximum number of allowed connected clients is 255.

---

## Using network diagnostic tools

The **Diagnostic** menu contains **Ping**, **Traceroute**, **Wi-Fi scan**, and **Reset** options, which can be used to troubleshoot connection problems and to reboot the i6800.

### Ping option

To use the network **Ping** tool, complete the following steps:

1. Click the **Ping** submenu in the **Diagnostic** menu to open the **Ping** section.

**Figure 16. Ping section of the Diagnostic menu**

**Ping**

Ping address:

Use predef. val: ☐

Packet size:

Packet count:

**Results:**

Status: Not running

```

40 bytes from 212.77.100.101: seq=5 ttl=245 time=5.997 ms
40 bytes from 212.77.100.101: seq=6 ttl=245 time=5.997 ms
40 bytes from 212.77.100.101: seq=7 ttl=245 time=5.997 ms

--- 212.77.100.101 ping statistics ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 5.997/6.122/6.996 ms
  
```

2. In the **Ping address** field enter the IPv4 address to be pinged. Check the **Use predef. val** checkbox, if you want to use the default ping parameters (64 data bytes and 10 packets). If the **Use predef. val.** box is unchecked, you can specify custom ping parameters: data size in bytes in the **Packet size** field and the number of packets in the **Packet count** field.
3. Click the **Ping** button to send the ping packets to the specified address. The output of the Ping operation will be displayed continuously in the **Results** field. To interrupt the running Ping operation, click the **Stop** button.

### Traceroute option

To use the network **Traceroute** tool, complete the following steps:

1. Click the **Traceroute** submenu in the **Diagnostic** menu to open the **Traceroute** section.
2. Enter the destination host address in the **Address** field. Click the **Diag** button to start tracing route to the entered host. The output of the Traceroute operation will be displayed continuously in the **Results** field. To interrupt the running Traceroute operation, click the **Stop** button.

**Figure 17. Traceroute section of the Diagnostic menu**

**Traceroute**

**Address:**

**Results:**

**Status:** Not running

5	p1-szz01a-ra2-ae0-2139.aorta.net (84.116.252.158)	6.996 ms	5.997 ms	5.997 ms
6	p1-gdn01a-rd2-ae2-2141.aorta.net (84.116.252.166)	7.996 ms	7.996 ms	8.996 ms
7	p1-gdn01a-rd1-ae23-2108.aorta.net (84.116.252.34)	5.997 ms	9.996 ms	15.992 ms
8	upc-cio4.10ge.task.gda.pl (153.19.0.5)	25.988 ms	21.989 ms	5.997 ms
9	wp-jro4.10ge.task.gda.pl (153.19.102.6)	6.997 ms	5.997 ms	5.997 ms
10	rtr2.rtr-int-1.adm.wp-sa.pl (212.77.96.65)	6.997 ms	6.996 ms	6.997 ms
11	www.wp.pl (212.77.100.101)	6.997 ms	5.997 ms	5.997 ms

## Wi-Fi scan option

**Figure 18. Wi-Fi scan section of the Diagnostic menu**

**Wi-Fi 802.11ac**

**Network scan**

Press the Scan button to execute site survey:

Please be aware that a site survey will disrupt all Wi-Fi communication for up to 10 seconds

**Site survey:**

Ch	Type	SSID	BSSID	Encryption	Signal [dBm]
36	AP	NATed-Vlan1000-5GHz	00:0f:15:01:01:c9	WPA2-PSK	-73
36	AP	Icotera-Scrum	00:0f:15:01:01:c8	WPA2-PSK	-74
36	AP	Icotera-Enterprise	00:0f:15:01:01:ca	WPA/WPA2	-74
36	AP	GPON_SSID5_AP1	00:1e:80:11:0b:44	WPA2-PSK	-75
36	AP	GPON_SSID5_AP2	00:1e:80:11:0b:45	WPA2-PSK	-75
40	AP	NATed-Vlan1000-5GHz	00:1e:80:11:02:b9	WPA2-PSK	-77
40	AP	Icotera-Enterprise	00:1e:80:11:02:ba	WPA/WPA2	-77
40	AP	Icotera-Support&Testing	00:1e:80:11:02:b8	WPA2-PSK	-78
36	AP	i6800_wifi_5_test	00:1e:80:19:98:4a	Open	-79
40	AP	Icotera-Enterprise	00:1e:80:18:1c:c3	WPA/WPA2	-79
40	AP	Icotera-Service	00:1e:80:18:1c:c1	WPA2-PSK	-79
48	AP	WoBa-i6800-WiFi	00:0f:15:06:f6:20	WPA2-PSK	-82
36	AP	23PNwep128	00:1e:80:18:1e:d1	WEP	-82
36	AP	pn	00:1e:80:18:1e:d2	WEP	-82
36	AP	Icotera-Hardware	00:1e:80:18:13:a0	WPA2-PSK	-84

The network scan tool enables the i6800 to execute a site survey for all wireless networks in the neighborhood. As a result of this survey, a list of scanned networks will be presented. In order to execute the site survey from your CPE complete the following steps:

1. Press the **Scan** button in the **Network Scan** section.
2. Wait for the site survey to complete. This might take up to 10 seconds and temporarily disrupts Wi-Fi communication with the i6800.

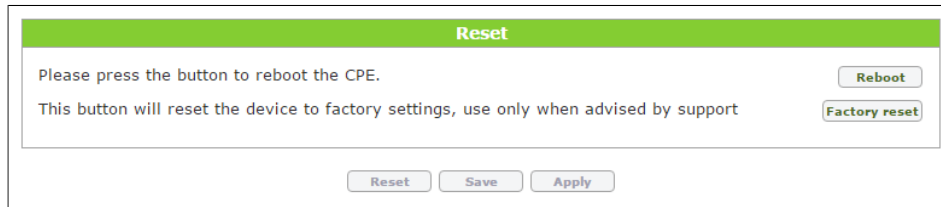


3. After the site survey has been completed, the table of networks will be displayed, which contains the following information:
  - **CH**: operating channel number of the neighboring network.
  - **Type**: connection type.
  - **SSID**: SSID of the neighboring network.
  - **BSSID**: BSSID of the neighboring network.
  - **Encryption**: encryption type and method used by the neighboring network.
  - **Signal [dBm]**: signal quality of the neighboring network in dBm.
4. In order to refresh the table, press the **Scan** button again.

## Reset option

The **Diagnostic** menu also contains the **Reset** submenu, from which the CPE can be rebooted with the **Reboot** button or reset to factory settings with the **Factory reset** button.

**Figure 19. Reset section of the Diagnostic menu**



**Reset**

Please press the button to reboot the CPE. **Reboot**

This button will reset the device to factory settings, use only when advised by support **Factory reset**

**Reset** **Save** **Apply**

## Changing administrator settings

The **Administration** menu provides configuration options for controlling user credentials and managing LEDs behaviour.

### Managing your username and password

Use the following steps to manage your username and password:

**Figure 20. UI login password section of the Administration menu**

- Under the **UI login password** section complete the following steps:
  - Type your new user name in the **User name** field.
  - Enter your old password in the **Old Password** field.
  - Type your new password in the **New Password** field.
  - Repeat your new password in the **Retype new password** field.
- Confirm your changes by clicking the **Save** button on the bottom bar or click **Reset** button to restore default settings.

After applying these settings with the **Apply** button, the user credentials will be changed and will take effect during the next login.

### Managing LEDs behaviour

Use the following steps to manage i6800 LEDs behaviour:

- In the **Administration** menu click the **LEDs** submenu to go to the **LEDs** section.

**Figure 21. LEDs section of the Administration menu**

- From the **LEDs** drop-down list choose the preferred LEDs behaviour:
  - turn on** - LEDs remain turned on all the time.
  - turn off - LEDs will be turned on again only if an event occurs** - LEDs remain turned off except in case of an error.
  - turn off - LEDs will be turned on again only if an event occurs** - LEDs remain turned off except in case of an event.

From the **LEDs' brightness** drop-down list choose the preferred LEDs brightness level:

- **high** - LEDs are visible in daylight.
  - **medium** - LEDs are barely visible in daylight.
  - **low** - LEDs are visible in darkness but not in daylight.
3. Confirm your changes by clicking the **Save** button on the bottom bar or click **Reset** button to restore default settings.

After confirming new settings with the **Apply** button, LEDs behaviour and brightness will be changed accordingly.

## Managing services

The **Services** menu provides configuration options for controlling port forwarding, DMZ, ALG, parental control settings, Wake-on-LAN function, and DDNS configuration.

### Managing port forwarding

Use the following steps to manage port forwarding:

1. In the **Services** menu click the **Port Forwarding** submenu.

**Figure 22. Port Forwarding section of the Services menu**

Port Forwarding							
No.	Name	Protocols	Ext. ports	Int. IP	Int. port	Loopback	Enabled
1	portForward1	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
2	portForward2	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
3	portForward3	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
4	portForward4	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
5	portForward5	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
6	portForward6	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
7	portForward7	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
8	portForward8	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
9	portForward9	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
10	portForward10	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
11	portForward11	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
12	portForward12	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
13	portForward13	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
14	portForward14	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
15	portForward15	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
16	portForward16	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
17	portForward17	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
18	portForward18	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
19	portForward19	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
20	portForward20	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
21	portForward21	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
22	portForward22	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
23	portForward23	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
24	portForward24	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
25	portForward25	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
26	portForward26	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
27	portForward27	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
28	portForward28	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
29	portForward29	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
30	portForward30	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
31	portForward31	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
32	portForward32	UDP ▼	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>

2. Complete the following steps to manage port forwarding:
  - Click checkbox in the **Enabled** column to enable a chosen port forwarding rule for editing.
  - In the **Name** field enter the name for a given rule. Chose protocol (**UDP** or **TCP**) from the drop-down list in the **Protocols** column. In the **Ext. ports** field enter external ports

range, and in the **Int. IP** field type internal IP address. Then, in the **Int. port**, type internal port number.

- Click checkbox in the **Loopback** column to enable loopback feature for a given port. The NAT loopback, also known as NAT hairpinning, is a feature which permits access to service via the WAN IP address (often public IP address) from inside the local network. By default NAT loopback option for each port forwarding rule is disabled
3. Confirm your changes by clicking the **Save** button on the bottom bar or click **Reset** button to restore previously saved settings.

To activate port forwarding, click **Apply** button.

## Managing DMZ

Use the following steps to manage the demilitarized zone:

1. In the **Services** menu click the **DMZ** submenu.

**Figure 23. DMZ section of the Services menu**

2. Check **Enable** checkbox to activate DMZ. Then, in the **DMZ destination IP** field enter the IP address of the DMZ destination, and in **Description** field type DMZ description (up to 64 characters).
3. Confirm your changes by clicking the **Save** button on the bottom bar or click **Reset** button to restore previously saved settings.

To activate DMZ, click **Apply** button.

## Managing ALG

Use the following steps to manage the application-level gateway:

1. In the **Services** menu click the **ALG** submenu.

**Figure 24. ALG section of the Services menu**

2. Check chosen checkboxes to activate application-level gateway for SIP, RTSP, FTP, PPTP, L2TP, and/or IPSEC protocols.

3. Confirm your changes by clicking the **Save** button on the bottom bar or click **Reset** button to restore previously saved settings.

To activate ALG settings click **Apply** button.

## Managing Parental control

Use the following steps to manage Parental control settings:

1. In the **Services** menu click the **Parental control** submenu.

**Figure 25. Parental control section of the Services menu**

**Parental control**

**inet\_br**

**Parental control**

Use parental control: ☐

**Custom DNS**

Use DNS jail: ☐

Use custom DNS: ☐

Primary DNS:

Secondary DNS:

**DNS filtering**

Use DNS filtering: ☐

No.	Domain	Exact matching	Enabled
1	<input type="text"/>	Suffix matching ▼	<input type="checkbox"/>
2	<input type="text"/>	Suffix matching ▼	<input type="checkbox"/>
3	<input type="text"/>	Suffix matching ▼	<input type="checkbox"/>
4	<input type="text"/>	Suffix matching ▼	<input type="checkbox"/>
5	<input type="text"/>	Suffix matching ▼	<input type="checkbox"/>
...			
27	<input type="text"/>	Suffix matching ▼	<input type="checkbox"/>
28	<input type="text"/>	Suffix matching ▼	<input type="checkbox"/>
29	<input type="text"/>	Suffix matching ▼	<input type="checkbox"/>
30	<input type="text"/>	Suffix matching ▼	<input type="checkbox"/>
31	<input type="text"/>	Suffix matching ▼	<input type="checkbox"/>
32	<input type="text"/>	Suffix matching ▼	<input type="checkbox"/>

**Reset** **Save** **Apply**

2. Complete the following steps to manage parental control feature.
  - Check **Use parental control** checkbox to activate parental control.
  - Check **Use DNS jail** checkbox to .
  - Check **Use custom DNS** checkbox to activate **Primary DNS** and **Secondary DNS** fields. .
  - Fill **Primary DNS** field with IP address of a primary DNS server which would provide list of blocked domains.
  - Fill **Secondary DNS** field with IP address of a secondary DNS server which would provide list of blocked domains.

- Check **Use DNS filtering** checkbox to activate fields in **Enabled** column.
  - Check **Enabled** checkbox to activate **Domain** and **Exact matching** fields.
  - Fill **Domain** field with domain name which would be blocked.
  - From the **Exact matching** drop-down list chose matching method for domain name (**Suffix matching** or **Exact matching**).
3. Confirm your changes by clicking the **Save** button on the bottom bar or click **Reset** button to restore previously saved settings.

To activate Parental control settings click **Apply** button.

## Wake On LAN section

Use the following steps to use Wake On LAN feature and send magic packet to the chosen device.

1. In the **Services** menu click the **Wake On LAN** submenu.

**Figure 26. Wake On LAN section of the Services menu**

Wake On LAN

Destination MAC:  Source interface:

No packet sent

Click a lease row to set destination parameters

MAC	Hostname	Type	Interface
90:e7:c4:c4:a2:d1	android-8bd5afacad7c4bc8	Dynamic	inet_br
00:0b:6b:02:8d:20	war-HP-ProBook-470-G1	Dynamic	inet_br
3c:97:0e:57:59:67	Lenovo-PC	Dynamic	inet_br
3c:97:0e:57:59:67		ARP	inet_br

2. Complete the following steps to send magic packet.
  - Start typing MAC address into the **Destination MAC** field. At any moment you can click a matching entry from a list of MAC addresses below to set destination parameters. It is also possible to send magic packet to a host which is not visible on the list (connected to LAN port but not operating)
  - Choose source interface from a drop-down list.
  - Click **Send magic packet** button.

As this tab does not include any configurable options, the **Reset**, **Save**, and **Apply** buttons are disabled.

## Managing DDNS feature

Use the following steps to manage Dynamic DNS feature.

1. In the **Services** menu click the **DDNS** submenu.

**Figure 27. DDNS section of the Services menu**

2. Complete the following steps to manage the DDNS.
  - Check the **Enabled** checkbox to enable DDNS service
  - Enter update interval.
  - Enter forced update time interval.
  - From the drop-down list choose active profile.
  - Enter service URL.
  - Enter user login.
  - Enter user password.
  - Enter user domain.
  - Click **Show help** link to display information about special sequences which can be entered in the fields of this section. These sequences will be substituted by appropriate configuration data.

**Figure 28. Help for DDNS feature**

3. Confirm your changes by clicking the **Save** button on the bottom bar or click **Reset** button to restore previously saved settings.

To activate DDNS settings click **Apply** button.



---

The information contained in this document represents the current view of Icotera on the issues discussed as of the date of publication. Because Icotera must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Icotera, and Icotera cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. Icotera MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Icotera

Icotera may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Icotera, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2016 Icotera. All rights reserved.