



User Guide

Icoteria i6850 Residential Gateway



Contents

Introduction	4
Powerful hardware architecture	4
Next generation Wi-Fi solution.....	4
Innovative feature set	4
Ease of control	4
Integrated Smart Home platform	4
Physical Description	5
Connector Panel	5
Status LEDs	5
Connectors.....	6
100Base-BX/1000Base-BX Optical Port	6
10Base-T/100Base-TX/1000Base-T Ports	6
USB Ports.....	6
POTS Ports.....	7
Power Port	7
On/Off Switch	7
Reset Button	7
Serial Number	7
Configuring and managing the i6850.....	8
Web interface general overview	8
Top bar	8
Menu	8
Management area.....	9
Bottom bar	9
Logging in to the web interface.....	9
Viewing status information	10
General system information.....	10
WAN information	11
LAN information	11
Wi-Fi information	12
Phone information and VoIP call log.....	14
WDS information.....	15
Managing LAN and Wi-Fi settings.....	16
LAN settings.....	16
Wi-Fi settings.....	17
Backup	19
Using network diagnostic tools	20
Ping.....	20
Traceroute	21
Wi-Fi scan	22
Reset.....	22
Configuring administrator settings.....	23
Managing user credentials	23
Managing LEDs behaviour.....	23
Managing remote access.....	23

Managing services	24
Port forwarding	24
DMZ	24
ALG	25
Parental control.....	25
Wake On LAN	26
DDNS	26
UPnP.....	27
NAT type.....	27
IPv6 firewall.....	27

Introduction

The Icotera i6850 FTTH gateway integrates optical Ethernet-based gigabit data transmission with Layer 2-4 functionality, VoIP, 802.11ac & bgn Wi-Fi and USB 3.0.

Powerful hardware architecture

The Icotera i6850 Fiber-to-the-Home (FTTH) gateway demonstrates its great strength by bringing together a wide feature set and flawless performance. Its foundation is built on a powerful, cutting-edge dual-core architecture. This, paired with an ASIC for packet forwarding, ensures the platform is always ready to cope with additional tasks while processing VoIP, Gigabit routing of IPv4 with NAT, IPv6 and stateful filtering, traffic switching/bridging and high speed Wi-Fi.

Next generation Wi-Fi solution

With Wi-Fi becoming the preferred communication technology inside the home, the need for fast and stable wireless connections is becoming ever more important. The i6850 delivers not only backwards compatibility with any 802.11a/b/g/n Wi-Fi certified device, but also includes the very latest standard — 802.11ac. With the added 802.11ac Wave 2 solution, the i6850 is capable of delivering 1700+300 Mbps and more than 1 Gbps of combined throughput in real home and office environment.

Innovative feature set

The i6850 provides exceptional Layer 2 functionality that can effortlessly handle 16 bridging instances, 16 Wi-Fi APs over 2 radios, multiple WAN interfaces, PPPoE and in-band secure management.

Ease of control

A great variety of management protocols (e.g. SNMP v1/v2, syslog, SSH, Telnet and TR-069) is integrated and supported, which guarantees effortless control over the i6850. Paired with our fail-proof, zero-touch auto provisioning mechanism, they provide easy and trouble-free daily operations. To guarantee trouble-free firmware roll-outs in harsh network environments, the i6850 also comes with dual-bank firmware.

Integrated Smart Home platform

The i6850 gateway supports 3rd party Smart Home platforms via state-of-the-art low-consuming wireless technology. A Smart Home platform offers great solutions for end-users within Alarm & Surveillance, Energy Management and Home automation. Via a cloud-based platform the i6850 connects to third party device-hardware, which makes the possibilities for connecting devices close to endless. For the network operator or service provider, a Smart Home platform offers a unique opportunity for additional revenue streams and higher customer loyalty.



Note

A complete list of the i6850 Residential P2P Gateway features can be found in a data sheet document which is available for download from Icotera site at <https://icotera.com/products/p2p-gateway>.

Physical Description

This section describes the physical components of the i6850, i.e. its connectors, LEDs, and buttons.

Connector Panel

The Icotera i6850 connector panel, shown in the following figure, contains the power port, on/off switch, reset button, connectors, and LAN status LEDs. Optical fiber connectors are placed inside the device and are accessible from its bottom part.

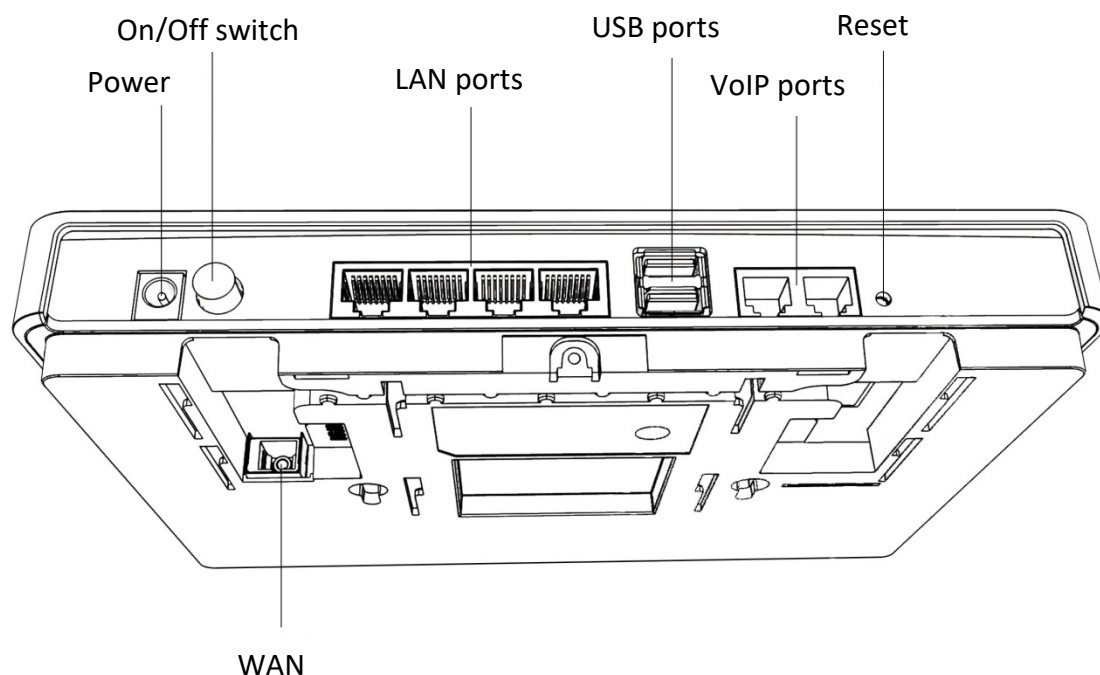


Figure 1. The Icotera i6850 connectors

Status LEDs

The status LEDs are located on the LAN ports and on the front panel of the device.

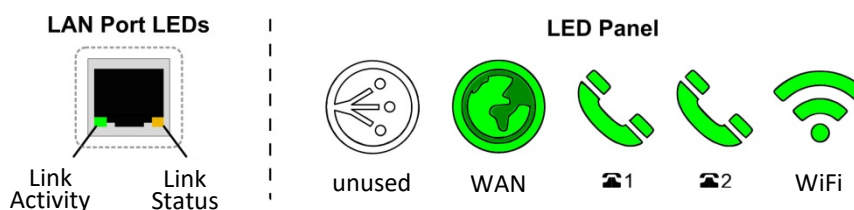
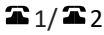


Figure 2. Status LEDs

The following table shows status LEDs descriptions.

Table 1. The status LEDs descriptions

LED type	Type	Colour	State	Описание
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
GPON	-	-	-	Not used

LED type	Type	Colour	State	Описание
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 interface lease fail
			Solid	No signal
	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
		WiFi	WiFi status and activity	N/A
Green/Orange	Blinking			WiFi 5 GHz detecting radar (blinks for 60 secs; for channels 120, 124, 128, and 132 blinks for 10 minutes). ЗАБЕЛЕЖКА: 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
Green	Solid			WiFi configured and enabled
	All status LEDs			Device status
All status LEDs	Device status	Green	Pulsing	Firmware upgrade in progress



Note

Please note that for some configurations the 5 GHz WiFi interface may be unavailable for up to 10 minutes due to –prolonged radar detection mechanism, which is signalled by the WiFi LED blink- ing. If the 2.4GHz WiFi is enabled, it will operate normally.

Connectors

The i6850 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. Optical fiber connectors are placed inside the device.

100Base-BX/1000Base-BX Optical Port

The i6850 uses standard SC port connectors to attach 9/125 micron single mode fiber optic cables. For data it is an SC/PC connector with a TX wavelength of 1310 nm and an RX wavelength of 1550 nm.

10Base-T/100Base-TX/1000Base-T Ports

The Icotera i6850 uses 10Base-T/100Base-TX/1000Base-T RJ-45 (8-pin modular) port connectors. The 10Base-T/100Base-TX/1000Base-T port connectors are configured as MDI-X (Medium Dependent Interface – Crossover). The CPE uses auto sense ports that are designed to operate at 10 Mb/s, 100 Mb/s, or at 1000 Mb/s, depending on the connecting device. These ports support the IEEE 802.3u auto negotiation standard, which means that when a port is connected to another device that also supports the IEEE 802.3u standard, then the two devices negotiate the best speed and duplex mode. The 10Base-T/100Base-TX/1000Base-T RJ-45 switch ports also support half- and full-duplex mode operation and can connect to 10 Mb/s, 100 Mb/s or 1000 Mb/s Ethernet segments or nodes.

USB Ports

The Icotera i6850 is equipped with one USB 3.0 and one USB 2.0 port that supply 5 V at 500 mA. Both ports are prepared for Z-Wave, ZigBee, CAT-iq, and printers and support NTFS and FAT32 file systems.

POTS Ports

The Icotera i6850 uses FXS RJ-11 (2-pin modular) port connectors for POTS (VoIP) connections. The CPE has two FXS ports, so it is possible to configure two independent telephone numbers.

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 i6850 on or off, as well as reboot it 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; use only in case of recommendation from technical support

Serial Number

The serial number of the Icotera CPE 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 6850004718000123 would be a serial number of a 00 variant of the i6850 device, produced in the 47th week of 2018, with a running number of 123.

Configuring and managing the i6850

This chapter provides a comprehensive overview of the Icotera i6850 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. To connect to the initial network by WiFi see the username and password from the bottom of the device or use cable.

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.

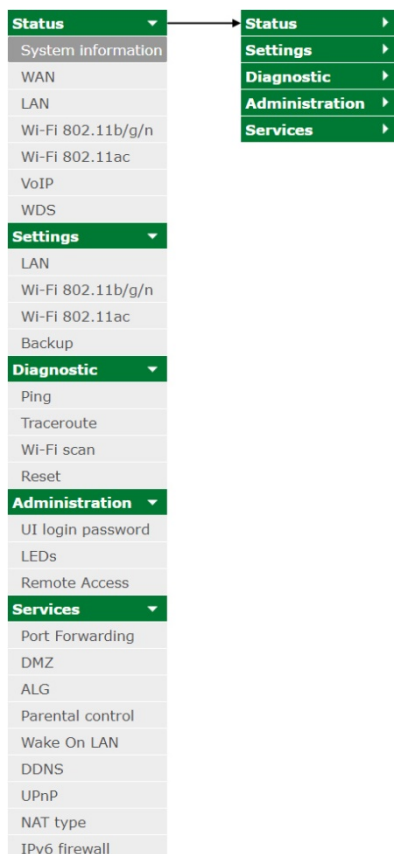


Figure 3. Web Interface main screen

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 i6850 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.

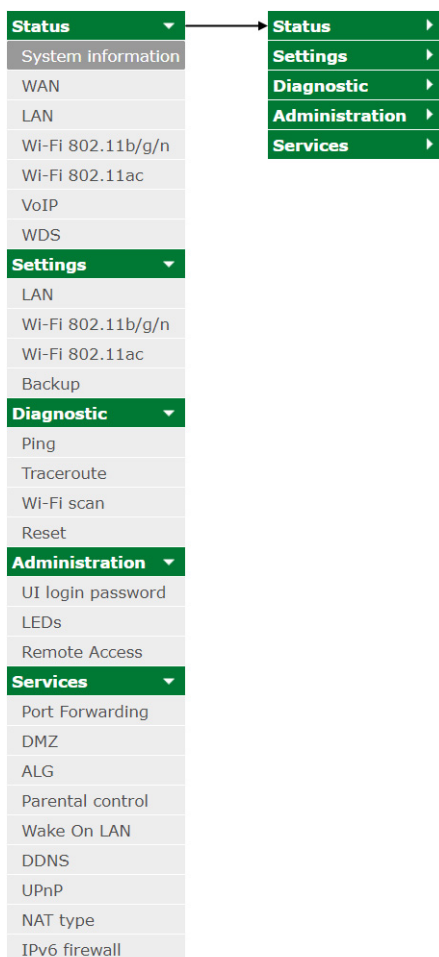


Figure 4. Collapsing web interface menu

Management area

The management area is where all the i6850 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 CPE 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.

Logging in to the web interface

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

1. Enter the IP address of your i6850 in the address bar of your web browser. The following login prompt will be displayed.

Figure 5. Logging into the web interface

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



Note

The first time you log in, use username *admin* and password *admin*. After the first login you will be able to change your password under the **Administration/UI login password** menu. After successfully connected to the initial network, you need to load: >> <http://192.168.1.1>.

Viewing status information

The **Status** menu provides tools for viewing general i6850 system information, as well as to obtain information about WAN, LAN and wireless interfaces operating on the device. It also allows to view phone info, VoIP call log, as well as information about WDS status and associated clients.

General system information

To access general information about the CPE go to the **Status/System information** menu item.

System information	
Current time:	2019/03/20 15:34
Uptime:	0 d 4 h 47 m 40 s
Firmware version:	6850-1.16.0
WAN MAC:	00:1e:80:70:a1:10
WAN IP:	10.104.1.148
Configuration mode:	Unconfigured
Device name:	i6850
Serial number:	6851005217000122
Wi-Fi 802.11b/g/n:	On
Wi-Fi 802.11ac:	On

System counters						
	Status	Pkts in	Pkts out	Errors	Collisions	Speed
LAN 1	Up	8366	24604	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	144715	603	-	-	-
WLAN 5 GHz	Up	0	0	-	-	-
WAN	Up	32928	7508	0	0	FD1000

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

This menu item includes the following information:

The **System information** section contains general information about i6850 state:

- **Current time:** current time and date,
- **Uptime:** duration the device has been powered up,
- **Firmware version:** current software version operating on the device,
- **WAN MAC:** physical address of the device's WAN interface,
- **WAN IP:** IP address of device's WAN interface,
- **Configuration mode:** **Unconfigured** (no steering or configuration propagation between i6850 and i3550) or **Master** (steering and configuration propagation active between i6850 and i3550).
- **Device name:** name of the device,
- **Serial number:** 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 i6850, as well as error and collision counters:

- **Status:** current status of a given interface, either **Up** or **Down**,
- **Pkts in:** number of incoming packets in the current session,
- **Pkts out:** number of outgoing packets in the current session,
- **Errors:** transmission error counter,
- **Collisions:** collision counter,
- **Speed:** negotiated speed (**FD1000** - Full Duplex, 1000Mbps; **HD100** - Half Duplex, 100Mbps; **HD10** - Half Duplex, 10Mbps).

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.

WAN information

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

WAN						
WAN IP type:	DHCP	Default gateway:	10.104.0.1			
IP address:	10.104.1.241	MAC Address:	00:1e:80:80:01:b8			
Subnet mask:	255.255.254.0	DNS:	81.18.219.100 0.0.0.0			

WAN counters						
	Status	Pkts in	Pkts out	Errors	Collisions	Speed
WAN	Up	46801	10310	0	0	FD1000

Figure 7. **WAN** item of the **Status** menu

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

- **WAN IP type:** IP address type of the WAN interface,
- **IP address:** IP address used by the WAN interface,
- **Subnet mask:** subnet mask used by the WAN interface,
- **Default gateway:** default gateway configured for the WAN interface,
- **MAC address:** interface's physical address,
- **DNS:** two IP addresses are displayed; 0.0.0.0 is shown if DHCP server option provided only single DNS server.

The **WAN counters** section displays statistical information about data:

- **Status:** current status of a given interface, either **Up** or **Down**,
- **Pkts in:** number of incoming packets in the current session,
- **Pkts out:** number of outgoing packets in the current session,
- **Errors:** transmission error counter,
- **Collisions:** collision counter,
- **Speed:** negotiated speed (**FD1000** - Full Duplex, 1000Mbps; **HD100** - Half Duplex, 100Mbps; **HD10** - Half Duplex, 10Mbps).

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

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

LAN information

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

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

- **IP type:** IP address type of the LAN interface,
- **IP address:** IP address used to the LAN interface,
- **Subnet mask:** subnet mask used by the LAN interface,
- **Default gateway:** default gateway configured for the LAN interface,
- **MAC address:** interface's physical address.

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

- **Status:** current status of a given interface, either **Up** or **Down**,
- **Pkts in:** number of incoming packets in the current session,
- **Pkts out:** number of outgoing packets in the current session,
- **Errors:** transmission error counter,
- **Collisions:** collision counter,
- **Speed:** negotiated speed (**FD1000** - Full Duplex, 1000Mbps; **HD100** - Half Duplex, 100Mbps; **HD10** - Half Duplex, 10Mbps; **Down** - not active).

inet_br						
IP type:	DHCP server		Default gateway:	192.168.7.1		
IP address:	192.168.7.1		MAC Address:	00:1e:80:80:01:ba		
Subnet mask:	255.255.255.0					
Counters						
	Status	Pkts in	Pkts out	Errors	Collisions	Speed
LAN 1	Up	20148	76525	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	353448	1347	0	0	-
WIFI 2 AP 1	Up	0	0	0	0	-
Dynamic Leases						
IP address	MAC Address	Hostname	Expires	Remember		
192.168.7.147	80:ce:62:3f:bb:12	LAPTOP-3JJ1B272	84574	<input checked="" type="checkbox"/>	<input type="button" value="Make static"/>	
Static Leases						
IP address	MAC Address	Hostname	Enable	Add/Remove		
<input type="text" value="0.0.0.0"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add"/>		
<input type="button" value="Refresh"/>						
<input type="button" value="Reset"/> <input type="button" value="Save"/> <input type="button" value="Apply"/>						

Figure 8. LAN item of the *Status* menu

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

- **IP address:** IP address assigned to a device,
- **MAC Address:** physical address of a connected device,
- **Hostname:** connected device's hostname,
- **Expires:** lease time of the device's address,
- **Remember:** dynamic lease can be turned into 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 apply the following steps:

1. In the **IP address** field enter IP address of a device to be connected.
2. In the **MAC Address** field enter MAC address of the device.
3. In the **Hostname** field enter the device's name.
4. Check the **Enable** box if the lease is to be enabled right away. Leave the box blank if the device will be enabled later.
5. To add the lease to the list click the **Add** button.
6. Save changes by clicking the **Save** button. Clicking the **Apply** button is required to apply changes to the database. The LAN information can be refreshed at any with the **Refresh** button.

Wi-Fi information

The **Wi-Fi 802.11b/g/n** and **Wi-Fi 802.11ac** menu items contain information about i6850 wireless interfaces and their access points. They describe separate interfaces, but their layout is the same.

The **General** section contains the following information about the Wi-Fi interfaces:

- **Status:** interface status, either **On** or **Off**,
- **Channel:** wireless channel on which the interface operates (**Reselect** button allows to reselect channel if **Channel** option under the **Settings/Wi-Fi** menu item is set to **auto**),
- **Band:** frequency band used by the interface,
- **Mode:** wireless mode of the wireless interface (802.11b/g/n or 802.11a/n/ac),
- **Tx Power:** transmission power value (percentage) for the wireless interface.

General

Status: On Mode: 802.11a/n/ac
Channel: 48 TX Power: 100
Band: 80MHz

Access point 1: ap2

SSID: Icotera-i6800 Hidden: no
BSSID: 00:1e:80:80:01:c0 Encryption: WPA2 AES-TKIP
Status: On

Counters

AP 1	Status	Pkts in	Pkts out	Bytes in	Bytes out	Errors	Collisions
AP 1	Up	0	0	0	0	0	0

Associated clients

IP address	MAC Address	Hostname	Expires	Mode	Sleep	RSSI	Tx bytes	Tx rate	Tx failed	Rx bytes

Figure 9. *Wi-Fi 802.11ac* item of the *Status* menu

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

- **SSID**: Service Set Identifier of the access point,
- **BSSID**: MAC address of the access point (Basic Service Set Identifier),
- **Status**: access point status, either **On** or **Off**,
- **Hidden**: visibility setting of the access point,
- **Encryption**: data encryption algorithm of the access point.

The **Counters** section contains statistical information about data entering and leaving the interfaces of the access point:

- **Status**: current status of a given interface, either **Up** or **Down**,
- **Pkts in**: number of incoming packets in the current session,
- **Pkts out**: number of outgoing packets in the current session,
- **Bytes in**: number of incoming bytes in the current session,
- **Bytes out**: 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**: IP address assigned to the device,
- **MAC Address**: physical address of the connected device,
- **Hostname**: connected device's hostname,
- **Expires**: lease time of the device's address,
- **Mode**: mode of operation (**BGN** or **AC**),
- **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 section can be refreshed at any time with the **Refresh** button.

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

Phone information and VoIP call log

The **VoIP** menu item contains phone information and gives access to the log of internet telephone calls.

Phone info		
	Phone 1	Phone 2
Display name		
Hook	On Hook	
Registration	Request Sent	Disabled
SIP Proxy	proxy.example.org	
<input type="button" value="Refresh"/>		

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

Figure 10. **VoIP** item of the **Status** menu

Each of the two phone lines is described by the following data:

- **Display name**: subscriber phone number or other data set by the ISP,
- **Hook**: headset state as **On hook** or **Off hook**,
- **Registration**: subscription status,
- **SIP Proxy**: SIP server status.

The **Phone info** section can be refreshed at any time with the **Refresh** button. Each

call is described by the following data, which is recorded in the VoIP call log:

- **Started**: start time and date of a call,
- **Source**: source phone number,
- **Destination**: destination call number,
- **Duration**: call duration in seconds,
- **Status**: call status (e.g. **Answered**, **Busy**, **No answer**),
- **Codec**: codec used (e.g. **Alaw**, **G722**),
- **Dir.:** call direction (**In** or **Out**),
- **Max Jitter**: maximal jitter value in milliseconds,
- **Pkts. lost**: number of lost packets,
- **Type**: call type (e.g. **Voice**).

WDS information

The **WDS** menu item contains information about connected slave access points and associated clients.

The screenshot shows three sections of a web interface:

- WDS Information:** A green header with a 'Refresh' button. Below it, 'Number of slaves: 0' is displayed.
- BSS/Backbone Information:** A green header with a 'Refresh' button. Below it is a table with columns: BSSID, Uplink rate, Role, Band, Channel, FAT, Slave MAC, and MDID.
- Associated clients:** A green header with a 'Refresh' button. Below it is a dropdown menu set to 'All' and a table with columns: MAC Address, Mode, Band, SS, BSSTr, Associated to, RSSI, TX bytes, TX rate, TX failed, and RX bytes.

At the bottom of the interface are three buttons: 'Reset', 'Save', and 'Apply'.

Figure 12. **WDS** item of the **Status** menu

The **WDS Information** section shows information about connected slave access points:

- **Number of slaves:** number of i3550 devices working in a slave mode.

The **WDS Information** section can be refreshed at any time with the **Refresh** button. The

BSS/Backbone information section contains the following information:

- **BSSID:** Basic Service Set Identifier of a slave access point,
- **Uplink rate:** WDS link rate
- **Role:** role of the Basic Service Set member,
- **Band:** wireless band supported by the BSS member,
- **Channel:** channel used by the BSS member,
- **FAT:** individual Free Air Time indicator calculated for BSS member,
- **Slave MAC:** MAC address of a slave device,
- **MDID:** Mobility Domain ID used by the members of the Backbone.

The **BSS/Backbone information** section can be refreshed at any time with the **Refresh** button.

The **Associated clients** section lists all devices connected to the device's access points. Each device is described by the following parameters:

- **MAC Address:** MAC address of a connected device,
- **Mode:** mode of operation: BGN or AC,
- **Band:** frequency band used by the client,
- **SS:** number of spatial streams supported by the host,
- **BSSTr:** support for 802.11v BSS Transition management by the host,
- **Associated to:** MAC address of a connected device,
- **RSSI:** Received Signal Strength Indicator,
- **TX bytes:** transmitted bytes,
- **TX rate:** transmission rate,
- **TX failed:** transmission failures,
- **RX bytes:** received bytes.

The **Associated clients** section can be refreshed at any time with the **Refresh** button.

Managing LAN and Wi-Fi settings

The **Settings** menu provides advanced configuration options to control Layer 3 network parameters of the cabled and Wi-Fi network. It also allows to upload and download configuration files.

LAN settings

The **LAN** item of the **Settings** menu allows to modify parameters of the Local Area Network:

- **IPv4 Type:** 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 the **Static** option from the drop-down menu and enter all network parameters manually,
- **IP address:** specifies IP address of your network,
- **IP netmask:** specifies network mask,
- **Gateway** (only for dynamic IP configuration): specifies IP address of your network gateway,
- **Primary DNS** (only for dynamic IP configuration): specifies primary Domain Name System server to be used to re- solve DNS queries,
- **Secondary DNS** (only for dynamic IP configuration): specifies secondary Domain Name System server to be used to resolve DNS queries,
- **WINS** (only for dynamic IP configuration): specifies IP address of the Windows Internet Name Service server. This server is typically used in office environments,
- **IP range:** specifies pool of IP addresses that can be allocated by the DHCP server,
- **Lease time:** specifies 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 maximum time in seconds which can be assigned to a client, if it asks for a longer lease time than the standard one. 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.

inet_br

IPv4 Type: DHCP server ▾

IP address: 192.168.7.1

IP netmask: 255.255.255.0

Gateway: 192.168.7.1

Primary DNS: 192.168.7.1

Secondary DNS: 0.0.0.0

WINS: 0.0.0.0

IP range: 192.168.7.2 - 192.168.7.250

Lease time: 86400

Max lease time: 86400

Enable Local Easy HostName:

1	router	<input type="checkbox"/>
2	gateway	<input type="checkbox"/>
3	i4850	<input checked="" type="checkbox"/>
4		<input type="checkbox"/>
5		<input type="checkbox"/>
6		<input type="checkbox"/>
7		<input type="checkbox"/>
8		<input type="checkbox"/>

IPv6 Router Advertisement: Enable ▾

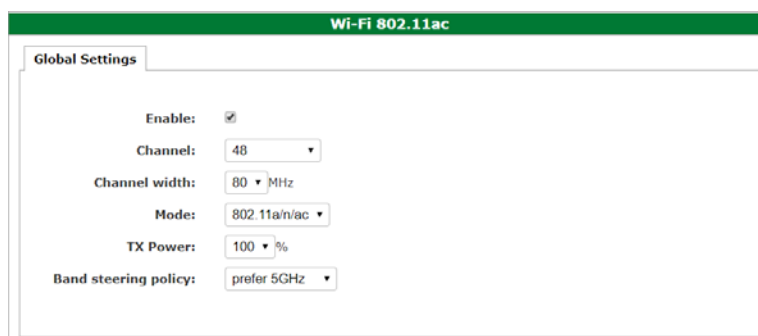
Reset Save Apply

Figure 13. **LAN** item of the **Settings** menu

- **Enable Local Easy HostName:** when this box is checked, web browser will recognize selected names from the list below and open i6850 web interface after any of these names is entered in the address bar of a browser.
- **IPv6 Router Advertisement:** when enabled, messages are sent by the router periodically and in response to Neighbor Solicitation packets.
- **Reset:** resets all changes made during the current session; **Save:** saves all changes made during the current session; **Apply:** applies all changes saved during the current session.

Wi-Fi settings

The **Wi-Fi** sections of the **Settings** menu allow to configure general settings of the wireless interfaces, set access point parameters, as well as define Wi-Fi schedules and access lists.



The screenshot shows the 'Global Settings' section for 'Wi-Fi 802.11ac'. The settings are as follows:

Setting	Value
Enable	<input checked="" type="checkbox"/>
Channel	48
Channel width	80 MHz
Mode	802.11a/n/ac
TX Power	100 %
Band steering policy	prefer 5GHz

Figure 14. **Global settings** section of the **Wi-Fi** item of the **Settings** menu

The **Global Settings** section provides general Wi-Fi performance settings, common for both 802.11b/g/n and 802.11ac interfaces:

- **Enable:** enables or disables the interface,
- **Channel:** sets channel number or relies on one of the auto options,
- **Channel width:** channel width in MHz,
- **Mode:** available networking mode,
- **TX power:** Tx power level (percentage),
- **Band steering policy:** allows to choose one of the available options:
 - * **force 2.4GHz:** redirects dual-band clients to 2.4 GHz,
 - * **force 5GHz:** redirects dual-band clients to 5 GHz,
 - * **prefer 2.4GHz:** redirects dual-band clients to 2.4 GHz, unless they persist,
 - * **prefer 5GHz:** redirects dual-band clients to 5 GHz, unless they persist,
 - * **disable:** no band steering policy.



Note

Band steering policy setting is shared by 2.4 and 5GHz radio interfaces. If settings for both interfaces are changed during web UI session, then policy defined in the 802.11ac section take precedence.

ap2

Enable:

SSID:

Encryption:

Encryption key: Show password

Hidden:

Client isolation:

Enable WPS:

WPS:

Please press the WPS button to activate WPS function.

Wifi Schedule

Enabled:

Schedule the interface access intervals in a 24-hour hh:mm notation.

Enabled	Day of week	From	To
<input type="checkbox"/>	Sunday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Monday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Tuesday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Wednesday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Thursday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Friday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Saturday	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Everyday	<input type="text"/>	<input type="text"/>

ACL settings

Client limit client(s)

Access list behavior

allow

deny

none

No.	Name	MAC Address	Enabled	Action
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="Clear"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="Clear"/>
15	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="Clear"/>
16	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="Clear"/>

Figure 15. Access point settings of the *Wi-Fi* item of the *Settings* menu

The **APs** sections, common for both 802.11b/g/n and 802.11ac interfaces, provide the following settings:

- **Enable:** enables or disables particular access point,
- **SSID:** access point name that will be seen when scanning for available Wi-Fi networks,
- **Encryption:** type of encryption key and encryption algorithm used to secure Wi-Fi transmission between access point and its clients. Available choices are **None**, **WEP-64**, **WEP-128**, **WPA TKIP**, **WPA AES**, **WPA TKIP-AES**, **WPA2 TKIP**, **WPA AES** and **WPA TKIP-AES** (depending on a chosen Wi-Fi interface). Please note that **None** leaves the wireless AP unsecured and open for access from any Wi-Fi device. The recommended encryption type is **WPA2**.
- **Encryption key:** password used for connecting to the access point. Entered characters will be displayed, when the **Show password** checkbox is checked.
- **Hidden:** if checked, chosen access point will not be detected by simple network scanning. It is however recommended to leave this box unchecked, since hiding AP does not provide any layer of security.
- **Client isolation:** if checked, traffic between clients of the access point will be blocked. This option may be used to create “guest” access point, so all devices connected to that AP will be isolated one from another.
- **Enable WPS:** enables or disables WPS based procedure for a given access point.

The **WPS** section allows to perform WPS based procedure:

- **Start WPS:** activates WPS procedure.

The **Wi-Fi Schedule** section allows to define AP access intervals for days of a week.

- **Enabled:** activates Wi-Fi access scheduling:
 - * **Enabled:** enables access interval for a particular day,
 - * **Day of week:** day of week or everyday,
 - * **From:** start of access time in a 24-hour hh:mm format,
 - * **To:** end of access time in a 24-hour hh:mm format.

The **ACL settings** section provides an Ethernet layer 2 filter, which can be used either to allow or to deny particular clients to connect to the chosen AP, based on their MAC addresses:

- **Client limit:** limit of clients that may be connected to the access point; check the checkbox and enter desired client limit. The maximum value is 32 clients.
- **Access list behavior:** defines desired behaviour of the access list:
 - * **allow:** allows only devices in the access list to connect to the AP,
 - * **deny:** prevents devices in the access list from connecting to the AP and allows all the other devices to connect,
 - * **none:** disables access list.
- **Name:** meaningful string that allows to identify a particular device, e.g. **my smartphone**, used as a quick reference.
- **MAC Address:** physical address of wireless adapter in a client 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**.
- **Enabled:** includes device in the current access list. To temporarily exclude the device from the access list, uncheck it.
- **Clear:** removes device from the access list.



Note

The maximum number of allowed connected clients is 255.

- **Reset:** resets all changes made to access point settings during the current session; **Save:** saves all changes made during the current session; **Apply:** applies all changes saved during the current session.

Backup

The **Backup** item of the **Settings** menu provides tools for uploading and downloading CPE configuration files.

The screenshot shows a web interface for configuration backup. It is divided into two main sections: 'Upload config from local file' and 'Download file'. In the 'Upload' section, there is a label 'Upload file' followed by a 'Choose file' button. Below this, the 'Status' is shown as 'no operation done.'. The 'Download file' section has a label 'Click to download config:' followed by a 'Save' button. At the bottom of the interface, there are three buttons: 'Reset', 'Save', and 'Apply'.

Figure 16. **Backup** item of the **Settings** menu

The **Upload config from local file** sections allows to read configuration from a local file:

- **Upload file:** press **Choose file** button to select configuration file from a local drive,
- **Status:** status of upload operation (eg. **no operation done** or **nothing to change**). The

Download file section allows to save current configuration to a local drive:

- **Click to download config:** press **Save** button to generate and save file with the current CPE configuration.

Using network diagnostic tools

The **Diagnostic** menu contains **Ping**, **Traceroute**, **Wi-Fi scan**, and **Reset** items, which can be used to troubleshoot connection problems and to reboot the i6850. As this menu does not include any configurable options the **Reset**, **Save**, and **Apply** buttons are disabled.

Ping

Ping diagnostic tool is used for testing reachability of a host in an IP network.

- **Ping address:** IPv4 address or host name to be pinged,
- **Use predef. val:** uses default ping parameters (64 data bytes and 10 packets). If **Use predef. val** box is not checked, it is possible to specify custom ping parameters:
 - * **Packet size:** data size in bytes,
 - * **Packet count:** number of packets to be sent.
- **Ping:** starts sending ping packets to the specified address,
- **Stop:** interrupts ping command,
- **Results:** output of ping operation is displayed continuously in this field.

Figure 17. **Ping** tool of the **Diagnostic** menu

Traceroute

The *Traceroute* diagnostic tool is used for displaying route and measuring transit delays of packets across an IP network.

Traceroute

Address:

Results:

Status: Not running

```

traceroute to icotera.com (104.31.84.139) from 192.168.1.1, 30 hops max, 38 byte packets
 1 10.104.0.1 (10.104.0.1) 0.000 ms 1.000 ms 0.000 ms
 2 81.18.219.97 (81.18.219.97) 0.000 ms 1.000 ms 0.000 ms
 3 81.18.219.53 (81.18.219.53) 1.000 ms 1.000 ms 1.000 ms
 4 89.75.18.209 (89.75.18.209) 1.000 ms 1.000 ms 1.000 ms
 5 84.116.252.158 (84.116.252.158) 11.000 ms 11.000 ms 11.000 ms
 6 84.116.252.166 (84.116.252.166) 12.000 ms 11.000 ms 11.000 ms

```

Figure 18. *Traceroute* tool of the *Diagnostic* menu

- **Address:** destination IPv4 address or host name,
- **Diag:** starts tracing route to the entered host,
- **Stop:** interrupts running of the traceroute operation,
- **Results:** output of the traceroute operation is displayed continuously in this field.

Wi-Fi scan

The **Wi-Fi scan** tool enables to execute a site survey for all wireless networks in the neighbourhood. As a result of this survey, a list of scanned access points is presented.

- **Scan**: starts site survey process,
- **Site survey**: information about detected networks:
 - * **CH**: operating channel number of a network,
 - * **Type**: connection type,
 - * **SSID**: access point name,
 - * **BSSID**: MAC address of the access point,
 - * **Encryption**: encryption type and method used by the network,
 - * **Signal [dBm]**: signal quality of the network in dBm.

Wi-Fi 802.11ac

Network scan

Press the Scan button to execute site survey: Scan

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	i6800_5G	00:11:22:33:44:5d	UNSECURED	-76
36	AP	AirOne	00:1e:80:70:a0:28	WPA2-PSK	-97
40	AP	27-HighSpeed	00:1e:80:27:63:5d	WPA2-PSK	-92
104	AP	magicTestTime	00:1e:80:70:9e:30	WPA2-PSK	-97
104	AP	WiFi-i6800	00:1e:80:80:02:c8	WPA2-PSK	-70
104	AP	Icotera-i6800	00:1e:80:70:a1:60	WPA2-PSK	-70
104	AP	IcoteraAP	00:1e:80:70:a1:61	WPA2-PSK	-70
104	AP	31-AR17M-HighSpeed	00:1e:80:70:05:d8	WPA2-PSK	-86
104	AP	FTTH_AR2323	00:1e:80:75:3e:e8	WPA2-PSK	-97
104	AP	IcoteraAP	00:1e:80:70:07:c4	WPA2-PSK	-73
104	AP	ICONS-#2/1-0.14	00:1e:80:70:a1:fc	WPA2-PSK	-91
104	AP	PS4 test	00:1e:80:70:a1:18	WPA2-PSK	-73
104	AP	Icotera Office	00:1e:80:71:44:68	WPA2-PSK	-97
104	AP	dzwony_5	00:1e:80:80:3e:38	WPA2-PSK	-97
104	AP	FTTH_HZ7921	00:1e:80:75:30:24	WPA2-PSK	-72
104	AP	DemWifi5	00:1e:80:70:9f:c8	WPA2-PSK	-97
104	AP	Dem Wifi	00:1e:80:75:31:ec	WPA2-PSK	-97

Figure 19. **Wi-Fi scan** tool of the **Diagnostic** menu

In order to refresh site survey list press the **Scan** button again.

Reset

The **Diagnostic** menu also contains the **Reset** item, from which the i6850 can be rebooted with the **Reboot** button or reset to factory settings with the **Factory reset** button.

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

Figure 20. **Reset** item of the **Diagnostic** menu

The resetting or rebooting of the i6850 has to be confirmed by the user.

i4850 Warning

Reboot requested. Click to reboot CPE.

Ok Cancel

Figure 21. Request for reboot confirmation



Figure 22. Request for reset confirmation

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

Configuring administrator settings

The **Administration** menu provides options for changing user credentials, managing LEDs behaviour and configuring remote access to the CPE. All these setting can be restored to default configuration with the **Reset** button, confirmed with the **Save** button or introduced with the **Apply** button.

Managing user credentials

The **UI login password** item of the **Administration** menu allows to change user's password by filling out the following fields:

- **Old password**,
- **New password**,
- **Retype new password**.

Figure 23. Changing password in the **Administration** menu

Managing LEDs behaviour

LEDs behaviour can be controlled from under the **LEDs** item of the **Administration** menu:

- **LEDs**: 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 event,
 - * **turn off - LEDs will be turned on again only if an error occurs**: LEDs remain turned off except in case of an error.
- **LEDs' brightness**: 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.

Figure 24. **LEDs** item of the **Administration** menu

Managing remote access

The **Remote Access** item of the **Administration** menu allows to configure access to the router from a WAN interface.

- **HTTPS setting**:
 - * **Enable**: enables or disables HTTPS protocol on a given port.
 - * **Port**: port number (default is 443).

- **Remote access from Internet:**
 - * **Enable:** enables or disables operator's filters. This option can be checked only if HTTPS is enabled.
 - * **Public URLs:** the URL of Web UI accessible from public Internet.

Figure 25. **Remote Access** item of the **Administration** menu

Remote access setting can be restored to default configuration with the **Reset** button, confirmed with the **Save** button or introduced with the **Apply** button.

Managing services

The **Services** menu provides configuration options for controlling port forwarding, DMZ, ALG, parental control settings, Wake-on-LAN function, DDNS, UPnP, NAT type and IPv6 firewall.

Port forwarding

Port forwarding rules can be configured under the **Port forwarding** item of the **Services** menu.

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"/>
126	portForward126	UDP	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
127	portForward127	UDP	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>
128	portForward128	UDP	0	0.0.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>

Figure 26. **Port forwarding** item of the **Services** menu

It is possible to define up to 128 rules:

- **Name:** name for a given rule,
- **Protocols:** one of the available protocols:
 - * **TCP,**
 - * **UDP,**
 - * **BOTH.**
- **Ext. ports:** external ports range,
- **Int. IP:** internal IP address,
- **Int. port:** internal port number,
- **Loopback:** enables or disables 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.
- **Enabled:** enables or disables chosen port forwarding rule for editing.

DMZ

Demilitarized zone can be configured under the **DMZ** item of the **Services** menu.

Figure 27. **DMZ** item of the **Services** menu

- **Enable:** activates or deactivates DMZ,
- **DMZ destination IP:** IP address of the DMZ destination,
- **Description:** DMZ description (up to 64 characters).

ALG

Application-level gateway options are available under the **ALG** item of the **Services** menu. Click appropriate checkbox to activate or deactivate any of the following protocols:

- **ALG SIP,**
- **ALG RTSP,**
- **ALG FTP,**
- **ALG PPTP,**
- **ALG L2TP,**
- **ALG IPSEC.**

Figure 28. **ALG** item of the **Services** menu

Parental control

Parental control settings can be configured under the **Parental control** item of the **Services** menu.

No.	Domain	Exact matching	Enabled
1		Suffix matching	<input type="checkbox"/>
2		Suffix matching	<input type="checkbox"/>
3		Suffix matching	<input type="checkbox"/>
30		Suffix matching	<input type="checkbox"/>
31		Suffix matching	<input type="checkbox"/>
32		Suffix matching	<input type="checkbox"/>

Figure 29. **Parental control** item of the **Services** menu

- **Use parental control:** activates parental control feature,
- **Use DNS jail:** blocks unauthorized DNS servers requests,
- **Use custom DNS:** activates **Primary DNS** and **Secondary DNS** fields,
- **Primary DNS:** IP address of a primary DNS server which would provide list of blocked domains,
- **Secondary DNS:** IP address of a secondary DNS server which would provide list of blocked domains,
- **Use DNS filtering:** activates fields in the **Enabled** column,
- **Enabled:** activates **Domain** and **Exact matching** fields,
- **Domain:** domain name which would be blocked,
- **Exact matching:** matching method for domain name:
 - * **Suffix matching:** only suffix will be matched,
 - * **Exact matching:** exact domain name will be matched.

Wake On LAN

The **Wake On LAN** feature allows to send magic packet to a chosen device:

- **Destination MAC:** MAC address to which a magic packet will be sent. 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 present on the list (connected to LAN port but not operating),
- **Source interface:** interface from which a magic packet will be sent.
- **Send magic packet:** sends magic packet.

MAC	Hostname	Type	Interface
80:ce:62:3f:bb:12	LAPTOP-3311B272	Dynamic	inet_br
80:ce:62:3f:bb:12		ARP	inet_br

Figure 30. **Wake On LAN** item of the **Services** menu

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

DDNS

The **DDNS** feature allows to manage Dynamic DNS feature.

Help: Show help

Following sequences in custom service URL have special meaning and are substituted with configuration data:

- [USERNAME] User login used for authentication
- [PASSWORD] User password used for authentication
- [DOMAIN] Domain name configured by user
- [IP] System IP

Figure 31. **DDNS** item of the **Services** menu with help displayed



Note

The Dynamic DNS feature should be configured only by the advanced users.

To configure DDNS feature fill the following fields:

- **Enabled,**
- **Update interval,**

- **Force update interval,**
- **Select active profile,**
 - * **custom,**
 - * **opendns,**
 - * **no-ip,**
 - * **freedns,**
 - * **changeip,**
 - * **dynu,**
- **User login,**
- **User password,**
- **User domain,**
- **Service URL,**
- **Show help:** displays information about special sequences which can be entered in the fields of this section. These sequences will be substituted by appropriate configuration data.

UPnP

Universal Plug-and-Play feature can be activated under the **UPnP** item of the **Services** menu:

Figure 32. **UPnP** item of the **Services** menu

NAT type

NAT type masquerade can be selected under the **NAT type** item of the **Services** menu:

Figure 33. **NAT type** item of the **Services** menu

- **Nat type:** one of the available types:
 - * **Symmetric:** recommended for day-by-day routine,
 - * **Port restricted cone:** less secure and should be used only in situations when gaming console issues occur.

IPv6 firewall

The **IPv6 firewall** item of the **Services** menu allows to manually specify exceptions to the stateful IPv6 firewall.

No.	Description	Protocols	Destination ports	Source IPv6	Destination IPv6	Enabled
1		ANY	0 - 0	:: / 0	:: / 0	<input type="checkbox"/>
2		ANY	0 - 0	:: / 0	:: / 0	<input type="checkbox"/>
3		ANY	0 - 0	:: / 0	:: / 0	<input type="checkbox"/>
30		ANY	0 - 0	:: / 0	:: / 0	<input type="checkbox"/>
31		ANY	0 - 0	:: / 0	:: / 0	<input type="checkbox"/>
32		ANY	0 - 0	:: / 0	:: / 0	<input type="checkbox"/>

Figure 34. **IPv6** item of the **Services** menu

- **Use firewall exceptions:** activate IPv6 firewall exceptions,
- **Description:** description of a given rule,

- **Protocols:** one of the available protocols:
 - * **TCP,**
 - * **UDP,**
 - * **ANY.**
- **Destination ports:** single destination port or range of ports,
- **Source IPv6:** source IPv6 address,
- **Destination IPv6:** destination IPv6 address,
- **Enabled:** - enables or disables chosen exception.

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.

coolbox

national phone number

0800 45 845
