



GCA-7000

User Manual

Version A1.0. June 17, 2021



Version A1.0, June 17, 2021

Preface

This manual provides information related to the installation and operation of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at INT-support@comtrend.com

For product update, new product release, manual revision, or software upgrades, please visit our website at <http://www.comtrend.com>

Important Safety Instructions

With reference to unpacking, installation, use, and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement). To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.
- Do not stack equipment or place equipment in tight spaces, in drawers, or on carpets. Be sure that your equipment is surrounded by at least 2 inches of air space.
- If you experience trouble with this equipment, you disconnect it from the network until the problem has been corrected or until you are sure that equipment is not malfunctioning.



WARNING (ATTENTION)

- Unplug the power supply from the device before servicing
- For indoor use only
- Do NOT open the casing
- Do NOT use near water
- Keep away from the fire
- For use in ventilated environment / space

- Débranchez l'alimentation électrique avant l'entretien
- Cet appareil est conçu pour l'usage intérieur seulement
- N'ouvrez pas le boîtier
- N'utilisez pas cet appareil près de l'eau
- N'approchez pas du feu
- Veuillez utiliser dans un environnement aéré

Power Specifications (Alimentation) :

Input 12Vdc, 1A

Copyright

Copyright©2021 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>

NOTE: This document is subject to change without notice.

Protect Our Environment



This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

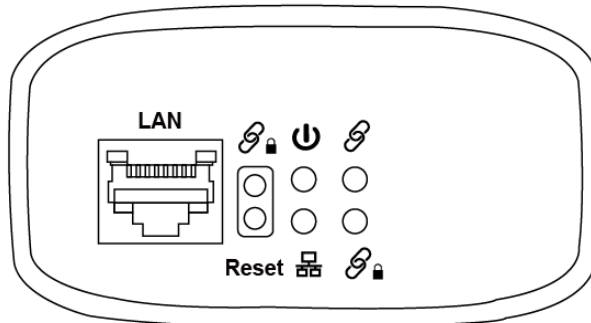
The cardboard box, the plastic contained in the packaging, and the parts that make up this Coax ADAPTER can be recycled in accordance with regionally established regulations. When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separately from domestic waste. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law. Instead, please be responsible and ask for disposal instructions from your local government.





Table of Contents

Chapter 1 Product Information	4
1.1 Front Panel	4
1.2 Front Panel Buttons.....	5
Chapter 2 G.hn/Coax Setup	6
2.1 Logging In	6
Chapter 3 G.hn Interface.....	7
3.1 Basic Configuration	7
3.2 NDIM Configuration	8
3.3 Encryption Configuration via WEB UI.....	8
Chapter 4 IP Interface	9
4.1 IP config	9
Chapter 5 Ethernet Interface	11
Chapter 6 Device Interface	12
6.1 Hardware information	12
6.2 Software information.....	12
6.3 Security	13
6.4 SW update.....	13
6.5 HTTP SW update	13
Chapter 7 Multicast Interface	14
7.1 MCAST Configuration.....	14
Chapter 8 QoS Menu.....	16
8.1 QoS Configuration.....	17
Chapter 9 G.hn spectrum Interface	19
9.1 Notches	19
Chapter 10 Log file Interface.....	21
10.1 Log File	21
Chapter 11 TR069	22
Chapter 12 Advanced Interface	24



Chapter 1 Product Information

1.1 Front Panel LED Indicators



LED	COLOR	MODE	Description
Power 	Green	On	The G.hn Coaxial Adapter is powered on
	Off	Off	The G.hn Coaxial Adapter is powered off or faulty
Connection 	Green	On	The current connection (line rate) is more than 40Mbps
	Orange	On	The current connection (line rate) is between 5Mbps and 40Mbps
	Red	On	The current connection (line rate) is less than 5Mbps
	Off	Off	A connection does not exist
Security 	Green	On	The adapter is secure
		Blink	The adapter is in the process of being secure
	Off	Off	The adapter is not secure
Ethernet 	Green	On	An Ethernet LAN connection is established
		Blink	Data over the Ethernet LAN connection is being transmitted
	Off	Off	An Ethernet LAN connection is not established

1.2 Front Panel Buttons

Security 	Press for more than 2 seconds for enabling data encryption in GCA-7000's. Please refer to GCA-7000_QIG.pdf for details.
Reset 	Press for less than 10 seconds to reset the device. Press for more than 10 seconds to restore factory defaults.

Chapter 2 G.hn/Coax Setup

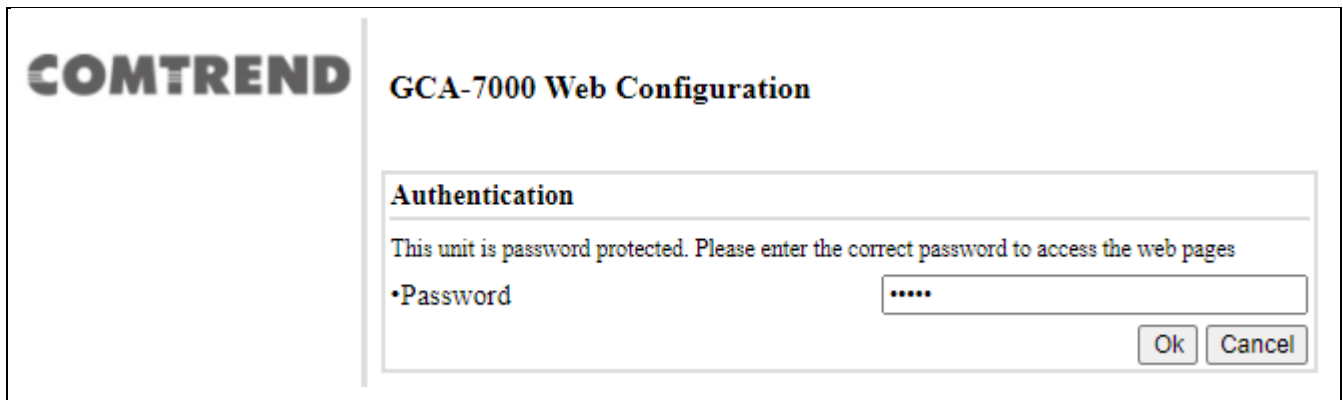
2.1 Logging In

Perform the following steps to login to the web user interface.

STEP 1: Start the Internet browser and input the default IP address for the device in the Web address field. For example, if the default IP address is 192.168.0.5, type <http://192.168.0.5>

STEP 2: A dialog box will appear, such as the one shown below. Input the default Authentication Password.

Authentication Password: **admin**



The screenshot shows a web browser window displaying the COMTREND logo on the left and the title "GCA-7000 Web Configuration" on the right. Below the title is a section titled "Authentication" with a message: "This unit is password protected. Please enter the correct password to access the web pages". There is a text input field labeled "•Password" containing five asterisks. At the bottom right of the dialog are "Ok" and "Cancel" buttons.

Click the **OK** button to continue.

Note:

The Factory Reset password is: **betera**

Chapter 3 G.hn Interface

COMTREND
GCA-7000 Web Configuration
Log Out

[G.hn](#)
[IP](#)
[Ethernet](#)
[Device](#)
[Multicast](#)
[QoS](#)
[G.hn spectrum](#)
[Log file](#)
[TR069](#)
[Advanced](#)

Basic settings

•MAC address c8:d1:2a:f0:8b:65

•Device ID 1

•Domain Name

•Force node Type AUTOMATIC ▾

•Node type* DOMAIN_MASTER

* Node type change can take some time, please refresh page to update state

•G.hn profile COAX 200 MHz ▾

Neighboring Domain Interference Mitigation (NDIM)

•NDIM mode AUTOMATIC ▾

•Domain ID (DOD)

Encryption Configuration

•Encryption is DISABLED

•Pairing password

•Automatic configuration*:

* Pairing can take some time, please refresh page to update state

Available Connections

Device ID	MAC Address	Phy Tx (Mbps)	Phy Rx (Mbps)
<i>Empty list</i>			

3.1 Basic Configuration

- **MAC Address** Displays the MAC address of the device.
- **Device ID** Device ID of this node.
- **Domain Name** string of all nodes in the network.
- **Force node Type** force the modem to have a particular role (END POINT or DOMAIN MASTER or AUTOMATIC)
- **Node Type** Shows the current status of the device.
- **G.hn profile** of all nodes in the network: select which G.hn profile that must be applied to the network (COAX 100MHz and COAX 200MHz).

3.2 NDIM Configuration

- **NDIM mode** set to Automatic for enabling automatic DOD selection functionality and set to Manual for manual configuration of DOD.
- **Domain ID (DOD)** manually set the DOD number from 1 to 15 to use a different preamble seed than the default 0.

3.3 Encryption Configuration via WEB UI

- **Pairing Password** used for authentication. Write a custom password to manually create a secure domain.

Available Connections

- In this tab table, all the available **G.hn connections** are presented. Remote node DID and MAC address; transmission and reception physical speeds.

Chapter 4 IP Interface

COMTREND
GCA-7000 Web Configuration
Log Out

[G.hn](#)
[IP](#)
[Ethernet](#)
[Device](#)
[Multicast](#)
[QoS](#)
[G.hn spectrum](#)
[Log file](#)
[TR069](#)
[Advanced](#)

IPv4 configuration*

DHCP enabled YES ▾

IPv4 address / netmask /

Default Gateway

DNS

Additional address #1 /

Additional address #2 /

*All changes except the DNS server will have effect after system boot

Ok Cancel

IPv6 configuration*

DHCP enabled NO ▾

IPv6 address / prefix /

Default Gateway

DNS

Additional address #1 /

Additional address #2 /

Additional address #3 /

Additional address #4 /

IPv6 link-local address /

IPv6 SLAAC address /

*All changes except the DNS server will have effect after system boot

Ok Cancel

NTPv4/v6 client configuration

NTPv4/v6 client enabled NO ▾

Resynchronization time (minutes)

NTP IPv4/v6 address

Ok Cancel

4.1 IP config

In the **IP configuration** tab of one G.hn node, the IPv4 and IPv6 settings can be read and changed.

IPv4 subsection:

- **DHCPv4 enabled:** in the case of choosing "NO" IP configuration in the following parameters, the IPv4 Address, Subnet Mask, Default Gateway and DNS should be configured; fill these fields in. In the case of choosing "YES" they will be filled automatically when the configuration is received from the DHCPv4 server.

- **IPv4 address/netmask:** IPv4 address / netmask of this device.
- **Default Gateway:** IPv4 gateway to connect the device to other LAN segments.
- **DNS:** Domain Name Server IP (IPV4).
- **Additional address #1/2:** additional fixed IPv4 addresses that will always be configured at boot time.

IPv6 subsection:

- **DCHPv6 enabled:** in the case of choosing "NO" IP configuration in the following parameters, the IPv6 Address, prefix, Default Gateway and DNS should be configured; fill these fields in. In the case of choosing "YES" they will be filled automatically when the configuration is received from the DHCPv6 server.
- **IPv6 Address / prefix:** IPv6 address / prefix of the device to read the node's DHCPv6 address in case the DHCPv6 is enabled.
- **Default Gateway:** IPv6 gateway to connect the node to other LAN segments.
- **DNS:** Domain Name Server IP (IPV6).
- **Additional address #1/2/3/4:** additional fixed IPv6 addresses that will always be configured at boot time.
- **IPv6 Link-Local Address:** to read the node's Link Local address.
- **IPv6 SLAAC address:** IPv6 address, automatically obtained by means of the SLAAC mechanism.

NTPv4/v6 subsection:

- **NTPv4/v6 client enabled:** Enable/disable NTP client.
- **Resynchronization time:** Configure re-synchronization interval time in minutes.
- **NTP IPv4/v6 address:** Hostname or IP (IPv4 or IPv6) of NTP server.

Chapter 5 Ethernet Interface

The screenshot displays the 'GCA-7000 Web Configuration' page. On the left, there is a navigation menu with links: [G.hn](#), [IP](#), [Ethernet](#), [Device](#), [Multicast](#), [QoS](#), [G.hn spectrum](#), [Log file](#), [TR069](#), and [Advanced](#). The main content area is divided into two sections:

Ethernet

External Interfaces:

Interface	Speed	Duplex	Interface Type	Mode	Internal PHY	Link
ETHA	1000	FULL_DUPLEX	RGMI	MAC	NO	YES
ETHB	2500	FULL_DUPLEX	SGMI	MAC	NO	NO

Powersaving

- Inactivity detection mode: Disabled (dropdown menu)
- Inactivity time(s): 300 (input field)

Buttons: Ok, Cancel

The Ethernet table shows the status & Info of the Ethernet interface; including Interface, Speed, Duplex, Interface Type, Mode, and Internal PHY & Link.

Powersaving

Ethernet powersaving can be disabled, enabled by Ethernet link or enabled by Ethernet activity; idle timer can be configured as well.

Chapter 6 Device Interface

The screenshot displays the 'GCA-7000 Web Configuration' interface. On the left, there is a navigation menu with links: [G.hn](#), [IP](#), [Ethernet](#), [Device](#), [Multicast](#), [QoS](#), [G.hn spectrum](#), [Log file](#), [TR069](#), and [Advanced](#). The main content area is divided into several sections:

- Hardware information:**
 - Device name: GCA-7000
 - Device description: G.hn 2000 Coax Adapter
 - Device manufacturer: Comtrend
 - Serial number: 1966010XXXF-AA000060
 - MAC address: c8:d1:2a:f0:8b:65
 - HW version: 2_0
- Software information:**
 - FW version: GCA-7000-78R61938CTUHN-C01_R01
 - System uptime: 0 days, 13h 49m 17s
- Security:**
 - New Configuration password:
- SW update:**
 - Status: Ready: initial status
 - Protocol:
 - Server IPv4/v6:
 - FTP User:
 - FTP Password:
 - OSUP Filename:
- HTTP SW update:**
 - Upgrade file:

6.1 Hardware information

In this tab, basic information such as MAC Address and Serial Number of the selected node is shown.

6.2 Software information

Shows the FW version and system uptime.

6.3 Security

The nodes in the network: to change the configuration password string from the default ("admin") to another; decided by the user.

6.4 SW update

Current loaded firmware version is shown. Any flash section can be upgraded; the first flash section should be selected and after clicking on the "OK" button the corresponding file should be chosen. Usually, a reboot should be performed afterwards to make sure the changes are effective.

The protocol is by FTP client or TFTP client. L2 is proprietary and is reserved for future use.

6.5 HTTP SW update

STEP 1: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

STEP 2: Click the **OK** button once to upload and install the file.

NOTE1: The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the [Device Interface](#) screen with the firmware version installed, to confirm the installation was successful.

NOTE2: The Power LED indicates the status of firmware update progress. Please **DO NOT** power off the device when Power LED is flashing or the device will be damaged.

Chapter 7 Multicast Interface

The screenshot shows the 'COMTREND GCA-7000 Web Configuration' interface. On the left is a navigation menu with links: [G.hn](#), [IP](#), [Ethernet](#), [Device](#), [Multicast](#), [QoS](#), [G.hn spectrum](#), [Log file](#), [TR069](#), and [Advanced](#). The main content area is titled 'Multicast Configuration*' and contains the following settings:

- IGMP Snooping: YES
- MLD snooping: NO
- IGMP/MLD broadcast report: NO
- IGMP/MLD broadcast report mode: 0
- Filter unknown multicast traffic: YES
- IGMP Multicast ranges:

Minimum IP address	Maximum IP address
224 . 0 .0.0	239 . 254 .255.255
0 . 0 .0.0	0 . 0 .255.255
0 . 0 .0.0	0 . 0 .255.255
0 . 0 .0.0	0 . 0 .255.255

Below the Multicast Configuration section is the 'Broadcast suppression' section with the following setting:

- Broadcast xput limit (Mbps): 2

Buttons for 'Ok' and 'Cancel' are present at the bottom of each configuration section.

7.1 MCAST Configuration

In the **MCAST Configuration** tab of "My Network", **IGMP snooping and MLD** features can be enabled or disabled. Also, IGMP multicast IP addresses ranges which the G.hn PLC network will sniff; can be configured.

- **IGMP Snooping:** Enable or Disable.
- **MLD Snooping:** Enable or Disable.
- **IGMP/MLD broadcast report (allowed):** set to **NO** for enabling reports dropping until the video source is detected, this is a recommended setting when IGMP/MLD is enabled. Set to **YES** for broadcasting reports until the video source is detected; this implies the multicast video stream is sent as broadcast and it is the recommended state when IGMP/MLD is disabled.
- **IGMP/MLD broadcast report mode:** Report broadcast forwarding behavior when the MCAST.GENERAL.REPORT_BROADCAST_ALLOWED is enabled.
 - If 0 then broadcast reports only when the video source is unknown.
 - If 1 then broadcast reports always.
 - If 2 then broadcast reports always if IGMPv3 and only when video source is unknown in others.

The term 'video source' refers to the node whose Ethernet port is connected directly to the Home Gateway.

- **Filter unknown multicast traffic:** Enables the Multicast Filtering feature.

If enabled, all the unsolicited multicast traffic will be blocked.

In IPv4 multicast traffic, only the traffic between the IP ranges defined in the MCAST.GENERAL.IGMP_IP_RANGES_DEF and the packets are unsolicited, these packets will be dropped.

Warning: This feature implies a higher CPU load, so it is advisable to enable it only in the Video Source. Only 100 Kbps of broadcast traffic could be managed in this mode.

IGMP Multicast ranges configuration: 4 multicast IP address ranges can be configured defining the minimum and maximum IP addresses of each range. Only multicast traffic within these ranges will be processed.

Broadcast Suppression: Maximum throughput allowed without suppressing broadcast traffic. The accuracy of this parameter depends on size of packets (big packets -> more accuracy). Value 0 deactivates this functionality.

Chapter 8 QoS Menu

COMTREND
GCA-7000 Web Configuration
Log Out

[G.hn](#)
[IP](#)
[Ethernet](#)
[Device](#)
[Multicast](#)
[QoS](#)
[G.hn spectrum](#)
[Log file](#)
[TR069](#)
[Advanced](#)

QoS Configuration

QoS criterion DSCP

Type of frame Ethernet frame

Packet detection 1 None

Offset 0

Bitmask 0x0000

Pattern 0x0000

Packet detection 2 None

Offset 0

Bitmask 0x0000

Pattern 0x0000

Packet classification

•Default prio 0

•TCP Ack Class in IPv4 0 NO

•TCP Ack Class in IPv6 0 NO

•ARP Class 0 NO

DSCP Class

0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	2
3	3	3	3	3	3	3	3	3
4	4	4	4	4	4	4	4	4
5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6
7	7	7	7	7	7	7	7	7

PC	Offset	Bitmask	Pattern	Priority
Rule 1	0	0x0000	0x0000	0
Rule 2	0	0x0000	0x0000	1
Rule 3	0	0x0000	0x0000	2
Rule 4	0	0x0000	0x0000	3
Rule 5	0	0x0000	0x0000	4
Rule 6	0	0x0000	0x0000	5
Rule 7	0	0x0000	0x0000	6
Rule 8	0	0x0000	0x0000	7

8.1 QoS Configuration

In the **QoS** configuration tab, the packet classifier can be managed to define a QoS rule for incoming Ethernet traffic, and assign a priority to be used in the G.hn network. Press the “**Ok**” button to load the newly configured settings:

- **QoS CRITERION:** a general criterion can be chosen among "None" (no QoS), "Custom" and "802.1p".
- **Type of Frame:** with this parameter the type of Ethernet traffic being transmitted by the G.hn network should be selected. Based on this parameter, the internal offsets in the system are adjusted. In the QoS tab, Ethernet frame offsets should set a **counting number** as they appear in the sniffer SW (for instance, the same field will be in a different position if normal Ethernet frames or 802.1Q tagged frames exist).
- **Packet detection 1:** first packet detection rule can be configured (offset, bitmask and pattern). Packets which accomplish it will be sent to the classification module.
- **Packet detection 2:** if second packet detection is also enabled, both, first and second detection criteria must be accomplished to pass packets to the classification module.
- **Packet classification:** up to 8 classification rules can be defined in this section for packets which have previously been correctly detected. For 802.1p only priorities can be managed, offset, bitmask and pattern are predefined to sniff the PCP field.
- **Default priority:** select default priority; which will be applied to non classified incoming packets. Priority 7 is the highest. Priority 0 is the lowest.
- **TCP Ack Class in IPv4:** Mapping TCP ACK (IPv4) to a Class Value.
- **TCP Ack Class in IPv6:** Mapping TCP ACK (IPv6) to a Class Value.
- **ARP Class:** Mapping ARP to a Class Value.
- **DSCP Class:** Mapping of each DSCP value to a Class Value.

As shown above, if QoS criterion: DSCP, all other options are grayed out, and follow the QoS rules below. According to G.9960 specs, the priority mapping recommended by [IEEE 802.1D] sub clause 7.7.3 is presented in Table III.1. for four priority queues.

PCP	Priority	Acronym	Traffic Types
1	0 (Third)	BK	Background
0	1 (lowest)	BE	Best Effort
2	2 (lowest)	EE	Excellent Effort
3	3 (Third)	CA	Critical Applications
4	4 (second)	VI	Video, < 100 ms <u>latency</u> and <u>jitter</u>

5	5 (second)	VO	Voice, < 10 ms latency and jitter
6	6 (highest)	IC	Internetnetwork Control
7	7 (highest)	NC	Network Control

In summary, the sequence of priority queue, (7,6) > (5,4) > (3,0) > (2,1)

Chapter 9 G.hn spectrum Interface

COMTREND **GCA-7000 Web Configuration** [Log Out](#)

[G.hn](#)
[IP](#)
[Ethernet](#)
[Device](#)
[Multicast](#)
[QoS](#)
[G.hn spectrum](#)
[Log file](#)
[TR069](#)
[Advanced](#)

Notches Configuration

Notch index	Start freq (KHz)	Stop freq (KHz)	Depth (dB)	Type
0	0	1954	100	Regulation

Add new user notch

- Index (0..9)
- Start frequency (KHz)
- Stop frequency (KHz)
- Depth (0..40dB, 100 removes notch)

Remove user notch

- Index (0..9)

9.1 Notches

In this tab a table with all configured **Notches** of selected node will be shown. The table is composed of next columns for every notch: Notch Number, Type of notch, Start Frequency (KHz), Stop Frequency (KHz), Depth (in dB).

The first 13 notches (Regulation) are Read Only, **RO**, in the system and they can be neither removed nor modified. The next 40 notches (Vendor) are defined by the vendor using SDK and they are also RO. The last 10 notches (User) are R/W and they can be added/removed by user using this tool.

To add new notches the user should fill the "**Add a new User Notch**" fields, setting Start and Stop frequencies in KHz and depth in dB of notch and then press the "**Ok**" button. They will be added in first User free position from number 0 to 9. (If successful, you can see a record in the Type column).

To remove a User Notch, the "**Remove a User Notch**" section should be used, setting notch number to be removed from 0 to 9 and pressing the "**Ok**" button.

Chapter 10 Log file Interface

The screenshot shows the 'GCA-7000 Web Configuration' interface. On the left is a navigation menu with links: [G.hn](#), [IP](#), [Ethernet](#), [Device](#), [Multicast](#), [QoS](#), [G.hn spectrum](#), [Log file](#), [TR069](#), and [Advanced](#). The main content area is titled 'Log File Configuration' and contains the following settings:

Setting	Value
•Enable Log File	NO
•Data capture interval (s)	1
•FTP server URL	
•FTP server login	
•FTP server password	
•Upload to server interval (min)	5

Buttons for 'Ok' and 'Cancel' are located at the bottom right of the configuration area. A 'Log Out' button is in the top right corner of the main window.

10.1 Log File

In the **Log File** configuration the following settings can be read, and changed by clicking on the corresponding "OK" button for the selected node:

- **Enable Log File:** set to YES for enabling Log File functionality in the node and set to NO for disabling it.
- **Data Capture: Interval** sets the interval of time in seconds to capture data.
- **FTP Server URL:** configures the url for the remote FTP server where the files will be uploaded.
- **FTP Server Login:** configures the user for the FTP server.
- **FTP Server Password:** configures the password for the FTP server.
- **Upload to Server Interval:** sets the interval of time in minutes to send the captured file to the remote server.

The screenshot shows the COMTREND GCA-7000 Web Configuration interface. On the left, there is a navigation menu with links: [G.hn](#), [IP](#), [Ethernet](#), [Device](#), [Multicast](#), [QoS](#), [G.hn spectrum](#), [Log file](#), [TR069](#), and [Advanced](#). The main content area is titled "GCA-7000 Web Configuration" and includes a "Log Out" button in the top right corner. The interface is divided into two main configuration sections: "TR069 Configuration" and "STUN Configuration".

TR069 Configuration

- ACS url:
- Username:
- Password:
- PeriodicInformEnable: YES
- PeriodicInformInterval:
- Conn Req Username:
- Conn Req Password:

STUN Configuration

- STUNEnable: YES
- STUNServerAddress:
- STUNServerPort:
- STUNUsername:
- STUNPassword:
- STUNMaxKeepAlivePeriod:
- STUNMinKeepAlivePeriod:

Both sections have "Ok" and "Cancel" buttons at the bottom right.

TR069 Configuration

- **ACS url:** URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The “host” portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
- **Username:** Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
- **Password:** Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
- **PeriodicInformEnable:** When set to YES, the modem should periodically send information to the ACS using the Inform method call.
- **PeriodicInformInterval:** The duration in seconds of the interval in which the CPE MUST attempt to connect with the ACS and call the Inform method.

- **Conn Req Username:** Username used to authenticate an ACS making a Connection Request to the modem.
- **Conn Req Password:** Password used to authenticate an ACS making a Connection Request to the modem.

STUN Configuration

- **STUNEnable:** Enables(YES) or disables(NO) the use of STUN. This applies only to the use of STUN in association with the ACS to allow UDP Connection Requests.
- **STUNServerAddress:** Host name or IP address of the STUN server to send Binding Requests if STUN is enabled via the STUN_ENABLE parameter. If it is an empty string and STUN_ENABLE is YES, the modem should use the address of the ACS extracted from the host portion of the ACS URL.
- **STUNServerPort:** Port number of the STUN server to send Binding Requests if STUN is enabled via STUN_ENABLE. By default, this should be equal to the default STUN port, 3478.
- **STUNUsername:** If it is not an empty string, the value of the STUN USERNAME attribute to be used in Binding Requests (only if message integrity has been requested by the STUN server). If it is an empty string, the modem will not send STUN Binding Requests with message integrity.
- **STUNPassword:** The value of the STUN Password to be used in computing the MESSAGE-INTEGRITY attributes to be used in Binding Requests (only if message integrity has been requested by the STUN server).
- **STUNMaxKeepAlivePeriod:** If STUN is enabled, the maximum period, in seconds, that STUN Binding Requests must be sent for the purpose of maintaining the binding in the Gateway. This applies specifically to Binding Requests sent from the UDP Connection Request address and port. A value of -1 indicates that no maximum period is specified.
- **STUNMinKeepAlivePeriod:** If STUN is enabled, the minimum period, in seconds, that STUN Binding Requests can be sent for the purpose of maintaining the binding in the Gateway. This limit applies only to Binding Requests sent from the UDP Connection Request address and port, and only those that do not contain the BINDING-CHANGE attribute. This limit does not apply to retransmissions following the procedures defined in [RFC3489].

Chapter 12 Advanced Interface

The screenshot displays the 'GCA-7000 Web Configuration' interface. At the top left is the 'COMTREND' logo. At the top center is the title 'GCA-7000 Web Configuration'. At the top right is a 'Log Out' button. On the left side, there is a vertical menu of links: [G.hn](#), [IP](#), [Ethernet](#), [Device](#), [Multicast](#), [QoS](#), [G.hn spectrum](#), [Log file](#), [TR069](#), and [Advanced](#). The main content area contains two sections. The first section is titled 'Hardware Reset' and has a 'Hardware Reset' button. The second section is titled 'Factory Reset*' and contains a 'Password' field with the text '•Password' to its left. Below the password field is a warning message: '*Warning! Current configuration will be lost'. At the bottom right of this section are 'Ok' and 'Cancel' buttons.

Hardware Reset: Click on this button to perform a reboot in the node.

Factory Reset: Input the password: **betera** and click the **OK** button to perform a factory reset. The current configuration will be lost.