

# TJ2100N-11G

## User Guide

Version: 1.0



Issue Date: 24-Jan-2024

## Copyright Notice

Copyright © Tejas Networks Ltd. All rights reserved. No part of this book or manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without the express written permission from Tejas Networks Ltd.

## Warning and Disclaimer

This document is a guide for using Tejas Networks products. While every effort has been made to make this document as complete and as accurate as possible, Tejas Networks does not accept any responsibility for poorly designed or malfunctioning networks. The guide contains Tejas Networks proprietary and confidential information and may not be disclosed, used, or copied without the prior written consent of Tejas Networks or set forth in the applicable license agreement. The information provided in this document is on an "as is" basis and is subject to change without prior notice. The author, Tejas Networks, shall have neither liability nor responsibility to any person or entity with respect to any loss or damage arising from the information contained in this document or from the use of equipment or software that might accompany it. The opinions expressed in this document are not necessarily those of Tejas Networks. The users are solely responsible for the proper use of the software and the application of the results obtained. **TEJAS NETWORKS MAKES NO WARRANTY OR REPRESENTATION, EITHER EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENTATION, ITS QUALITY, PERFORMANCE, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.**

## Trademark Acknowledgments

All terms mentioned in this book that are known trademarks or service marks have been appropriately capitalized. All trademarks duly acknowledged. Tejas Networks cannot attest to the accuracy of third-party information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

## Technical Support Information

Tejas customers can contact Tejas Support Center (TSC) 24x7x365 for any assistance through helpline, fax or email.

- Phone(s): +91 80 41719090
- Fax: +91 80 26591079
- Email: support@india.tejasnetworks.com
- Skype: tscsupport123
- Web: www.tejasnetworks.com

## Additional Learning Resources

The help content for all our products including this content is available online at <https://tejdocs.india.tejasnetworks.com/>. Please contact our Sales team to get access to this content or to organize any onsite and/or offsite trainings related to our products or technologies.

## Feedback

Your opinion is of great value and will help us improve the quality of our documentation and related learning resources. Drop a note to docs@tejasnetworks.com and let us know how we can assist you in your learning.

## Revision history

Version	Document ID and Issue Date	Updates
1.0	210-SW0000081-S 24-Jan-2024	Standard release

# Table of contents

<b>1 Document overview</b>	<b>7</b>
1.1 Target audience .....	7
1.2 Safety first .....	7
1.3 Precautions.....	9
<b>2 TJ2100N overview</b>	<b>11</b>
2.1 System overview .....	11
2.2 System features.....	12
2.2.1 Software features.....	12
2.2.2 Upstream .....	13
2.2.3 Downstream .....	13
2.2.4 GPON interface specifications .....	14
2.2.5 Ethernet.....	14
2.2.6 Layer-2 capabilities.....	14
2.2.7 Layer 3/4 hardware NAT/NAPT .....	15
2.2.8 Power saving .....	16
2.2.9 OAM .....	16
2.2.10 Power.....	16
2.2.11 Mechanical and environmental.....	16
<b>3 Hardware interface</b>	<b>17</b>
<b>4 Hardware installation</b>	<b>21</b>
<b>5 User interface configuration</b>	<b>23</b>
5.1 Basic configuration .....	23
5.1.1 Device Info- PON.....	24
5.1.2 Device Info- WAN .....	24
5.1.3 Device Info- Statistics .....	25
5.1.4 Device Info- Route.....	27
5.1.5 Device Info- ARP .....	27
5.1.6 Device Info- DHCP.....	27
5.2 Advanced setup.....	28
5.2.1 LAN .....	28
5.2.2 NAT.....	29
5.2.3 Security .....	32
5.2.4 Parental control.....	35
5.3 Diagnostics.....	36
5.3.1 Ping.....	37
5.3.2 Iperf.....	37
5.3.3 Trace route.....	37
5.3.4 Packet capture .....	37
5.3.5 Connection status.....	38
5.4 Management.....	38
5.4.1 Settings .....	39
5.4.2 System log .....	40
5.4.3 TR-069 Client.....	41
5.4.4 Internet time .....	42
5.4.5 Reboot.....	43
<b>6 Regulatory standard compliance</b>	<b>45</b>

# List of tables

Table 1: Safety sign conventions .....	7
Table 2: Environmental regulatory conventions.....	8
Table 3: ONT interface details .....	11
Table 4: Port description.....	19
Table 5: LED description .....	20
Table 6: PON info parameters.....	24
Table 7: WAN info parameters.....	24
Table 8: LAN and WAN statistics parameters .....	25
Table 9: Route parameters.....	27
Table 10: ARP parameters .....	27
Table 11: DHCP parameters .....	28
Table 12: IPv6 LAN auto configuration parameters .....	28
Table 13: Virtual servers parameters.....	30
Table 14: Port triggering parameters.....	31
Table 15: Add incoming/outgoing IP filtering parameters .....	32
Table 16: DOS configuration parameters.....	35
Table 17: Access control restriction parameters .....	35
Table 18: URL filter parameters .....	36
Table 19: Diagnostics .....	38
Table 20: View system log parameters .....	40
Table 21: System log configuration parameters .....	40
Table 22: TR-069 parameters.....	41
Table 23: Time settings parameters .....	42

This page is intentionally left blank

# 1 Document overview

This document provides an overview of the TJ2100N-11G ONT system, procedure to configure the ONT, and user interface of the device for the service providers.

This document covers both the enterprise (Single Family Unit - SFU) and the residential (Residential Gateway Unit - RGU) user configurations for the TJ2100N-11G ONT.




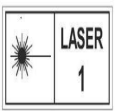
## 1.1 Target audience

This document is intended for operators, engineers, and service providers who use the TJ2100N-11G ONT system.



## 1.2 Safety first

To prevent personal injury, equipment damage, and service interruptions, you must follow all precautionary messages given in the document in addition to all the local safety standards required by your company. The following symbols used in the document at various places represent important situations.





**Table 1: Safety sign conventions**

Symbols	Meaning	Represents
	Caution	Situations that could result in equipment damage or loss of data.
	Danger	Situation that could cause physical injury. Failure to observe this precaution may result in personal injury, death, or equipment damage.
	Hot surface	Situation that could result in personal physical injury including burns.
	Optical safety	Staring directly into the optical connector output beam may cause irreparable damage to your eyes. It could even lead to loss of eye sight.

**Table 1: Safety sign conventions**

Symbols	Meaning	Represents
	Electric shock risk	Observe this precaution to prevent personal injury, or death. This can cause equipment damage.
	Static discharge warning	Handle the equipment wearing an anti-static ESD wrist strap properly grounded to discharge the static buildup. Failure to observe this precaution may result in equipment damage.

**Table 2: Environmental regulatory conventions**

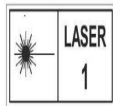
Symbols	Meaning	Represents
	European Conformity	Abbreviation of original French words <i>Conformité Européenne</i> which translates to European Conformity.  CE Marking on a product is a manufacturer's declaration that the product complies with the essential requirements of the relevant European health, safety and environmental protection legislation.
	China RoHS	China RoHS chasing arrow symbol with a <i>50</i> indicating that hazardous material is not released into the environment until 50 years after the date of manufacture.
	China RoHS	China RoHS chasing arrow symbol with a <i>10</i> indicating that hazardous material is not released into the environment until 10 years after the date of manufacture.
	WEEE	The WEEE- Waste of electrical and electronic equipment - under Article 11(2) of the WEEE Directive. It is also prescribed by European standard EN50419:2005.  This symbol indicates the need for separate collection for products.



## 1.3 Precautions

Take the following precautions while using the ONT:

- Use Tejas supplied electrical power adapter specifically designed Tejas ONTs.
- Use the green color SC-APC optical connector.
- Before inserting the fiber into the ONT, clean the fiber with Iso-Propyl alcohol.
- Place the ONTs away from any heat generating devices.
- Do not allow the dust to accumulate in, on, and around the ONT.
- Do not make direct eye contact with a live fiber.
- Ensure that the fiber does not have any sharp bends.
- Place the ONT out of reach of children.
- Avoid exposing the ONT to direct sunlight.



**Optical safety:** Do not stare or look directly into the optical connector output beam, as this can cause irreparable damage to your eyes and even result in loss of eye sight.

---

This page is intentionally left blank

## 2 TJ2100N overview

The TJ2100N model covered in this guide is Optical Network Terminal (ONT) installed at the customer premises in a GPON network. Their primary function is to provide broadband connectivity to the enterprise or residential users using GPON technology.

Tejas offers a series of advanced GPON ONT elements designed for next-generation Optical Access networks deployed in Fiber-To-The-Home (FTTH) and Fiber-To-The-Building (FTTB) formats. It addresses the rapidly growing service provider needs for flexible, high-capacity fixed-line broadband solutions to support emerging high bandwidth video applications (For example, IPTV, Mobile backhaul, MTU, and VOD) in enterprise, residential deployments, aggregation of backhaul traffic from LTE cell sites, enterprise VPN services, and SD-WAN networks based on NFV paradigm.

Tejas provides a full GPON solution that includes both TJ1400 Optical Line Terminal (OLT) and TJ2100N-11G Optical Network Terminal (ONT) platforms.

TJ2100N-11G is a versatile ONT product supports four 10/100/1000 Mbps Ethernet interfaces. TJ2100N-11G is compliant to ITU-T G984, G988, and TR069 standards.

### 2.1 System overview

The ONT is placed inside the plastic enclosures to protect the hardware. The ONT operates in non-air condition and is powered by 12 V DC, 1 A +/-5% power adaptor. An AC-DC adaptor is provided to support working with 110-240 V, 50/60 Hz, AC supply. The ONT can be positioned on a tabletop or mounted on a wall. The TJ2100N-11G model is specifically intended for indoor environments.

Use Tejas supplied adaptor only with the Tejas ONTs.

The ONT has WAN (GPON) and LAN side interfaces, LAN ports are provisioned with RJ-45 connectors supporting 10/100/1000 BaseT.

The following table provides the interface details of the ONT:

**Table 3: ONT interface details**

Model	Configuration
TJ2100N-11G	4x10/100/1000 Ethernet ports

## 2.2 System features

The following are the system features of the TJ2100N-11G ONT:

- Serves as an access terminal to provide a broadband connection.
- Supports GPON access technology, providing up to 2.5 Gbps downstream rate and 1.25 Gbps upstream rate at the network side.
- Provides 4x10/100/1000 Base-T full-duplex Ethernet ports, enabling various IP related services like Internet, IPTV, VOD, and over the top services.
- Supports remote software upgrade from OLT or TR69 server or ONT UI.
- Provides Dying Gasp support for power loss indication.

### 2.2.1 Software features

The following are the software features of the TJ2100N-11G ONT:

- Compliant to ITU-TG.984, G.988, and TR069 set of standards
- Real-time DBA (mode 0)
- Advanced L2/3/4 classifier
- IGMPv2 support and IPv6 ready
- 256 entry MAC table
- 64 entry VLAN table
- Wire speed Network Address Port Translation (NAPT) even in PPPoE mode
- Firewall and Access Control List (ACL) to prevent MAC address spoofing and limit the number of MAC/IP addresses per port
- 256 multicast groups
- IEEE 802.3x based on Ethernet flow control
- Per VLAN based bandwidth management and Quality of Service (QoS)
- 802.1p bridging
- Piggy-back Dynamic Bandwidth Reporting (DBRu) report mode 0
- Idle-GEM DBA
- Concurrent support of Piggy-back DBRu and Idle-GEM DBA

- Traffic Container (TCONT) type-1 to type-5
- Bandwidth control per User Network Interface (UNI) port is available
- Advanced Encryption Standard (AES)
- Number of TCONTs: 5 on ONT side
- TJ2100N-11G is configured to accept following types of frames from end users:
  - \* Customer VLAN tagged frames
  - \* Untagged frames
  - \* 802.1p mode
- G.984.1 - Examples of services and UNIs include:
  - \* Ethernet and IPTV on RJ-45 based ports (4xGE)

## 2.2.2 Upstream

The following are the upstream specifications:

- Upstream FEC, RS(255,239)
- Normal queues for PLOAM and CPU packets performance monitoring, faults and alarm, including BER rate monitor

## 2.2.3 Downstream

The following are the downstream specifications:

- Downstream AES-128 encryption and key exchange process
- Downstream FEC and RS(255,239)
- Dedicated independent TX queues for PLOAM and CPU packets

## 2.2.4 GPON interface specifications

The following are the GPON interface specifications of the TJ2100N-11G ONT:

- Connector: SC/APC
- Transmission: ITU-T G.984
- Optical module: Class B+
- Optical transmit power: +0.5 to +5 dBm
- Receive sensitivity: -28 dBm
- Data rates: 2488 Gbps downstream and 1244 Gbps upstream
- Ranging and activation process support
- Wavelength: 1490 nm/1310 nm
- Distance: 20 km, depending on the split ratio of the optical signal

## 2.2.5 Ethernet

The following are the Ethernet interface specifications of the TJ2100N-11G ONT:

- Meets 802.3 specifications 4x10/100/1000 Mbps
- Equipped with RJ-45 connector
- Full-duplex operation
- 10/100/1000Mbps auto-negotiation
- MDI/MDIX auto detection

## 2.2.6 Layer-2 capabilities

The following are the Layer-2 capabilities of the TJ2100N-11G ONT:

- Ethernet frame filtering based on port, source/destination IP and MAC addresses
- IEEE 802.3as
- Maximum MTU size: 2000 Bytes
- IEEE 802.1d bridging
- Ingress/egress IEEE 802.1p tagging, replacement, and stripping
- IEEE 802.1ad double tagging

- Traffic class forwarding to GEM Port and TCONT
- QoS based on 802.1p and 802.1q
- IEEE 802.1p marking based on DSCP
- Multicast: IGMP v2, v3, IGMP snooping

## **2.2.7 Layer 3/4 hardware NAT/NAPT**

The following are the L3 and L4 hardware specifications of the TJ2100N-11G ONT:

- Port Forwarding
- Port/VLAN bridging
- IPv4/IPv6 flow routing for policy rate
- IPOE/DHCP/PPPoE WAN hardware forward

## **2.2.8 Power saving**

As per ITU-T 984.3 (03/2020) of ONU power management aspects

## **2.2.9 OAM**

The following are the OAM specifications of the TJ2100N-11G ONT:

- Management: G.988 (OMCI), Telnet, TR069
- LED: LED indicators
- Alarm: Alarm report and suppression (ARC)
- Firmware: Firmware upgrade, active and alternative firmware images

## **2.2.10 Power**

12 V DC, 1 A +/- 5%, Round barrel-type connector with 110-240 V AC, 50/60 Hz input.

## **2.2.11 Mechanical and environmental**

The following are the mechanical and environmental specifications of the TJ2100N-11G ONT:

- Table top and wall mount enclosure design
- Operating temperature: -5°C to 55°C
- Dimensions: L190mm\*W117mm\*H43mm
- Altitude: 4,000m operations
- Humidity: 5 to 93% RH non-condensing



### 3 Hardware interface

---

**Note:** ONT images are shown for reference only, the actual color and appearance may vary in the final product.

---

#### Top view

Figure-1 shows the top view of TJ2100N-11G ONT along with the LEDs.

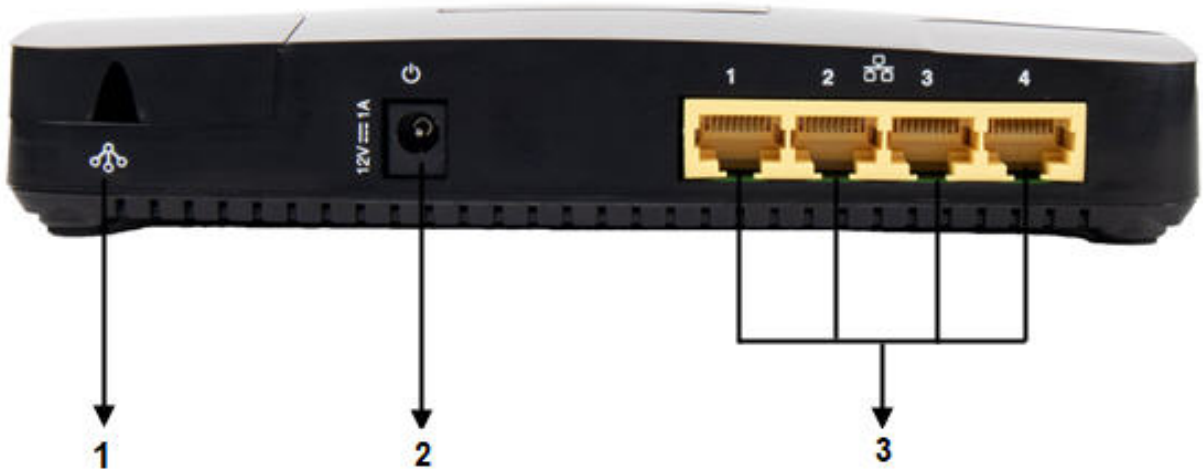
**Figure 1: Top view**



### Rear view

Figure-2 shows the rear view of TJ2100N-11G ONT.

**Figure 2: Rear view**



### Front view





Figure-3 shows the front view of TJ2100N-11G ONT.

**Figure 3: Front view**








The following table details the ports function of the TJ1200N-11G:

**Table 4: Port description**

Sl. No.	Symbol	Port	Function
1		PON port	SC-APC connector: To provide one PON access port, which is used to connect to the PON network for providing integrated access services
2		Power input	Input requirement: 12V DC, 1A
3		ETH port	1x4 RJ45 connector: It provides 10/100/1000 BaseT interface (UNI)
4		RST Switch	Push button: To reset ONT or factory default

The following table details the LED status of the TJ2100N-11G:

**Table 5: LED description**

LED	Name	Status	Description
	Power	Off	No power supply to the ONT.
		On	The ONT is powered On.
	PON link indicator	Off	No link is established with the OLT.
		On	The ONT has successfully established link with the OLT.
	Alarm indicator	Off	Default indication.
		Red	Indicates the presence of alarm On the ONT.
		Green	Indicates that there is no alarm On the ONT.
	LAN status (ETH1 to ETH4)	Off	LAN is not connected.
		Blinking	LAN connected but the traffic transfer is in progress.
		On	LAN connected but there is no traffic.
	Internet	Off	WAN connection is not created on ONT.
		On	WAN connection is created on ONT.

## 4 Hardware installation

Install TJ2100N-11G on tabletop or wall-mounted enclosure suitable for indoor environments. The installation location should be free of dust accumulation for better connectivity.

### Prerequisite

- Use 2.1x5.5x11 mm jack Tejas power adapter supplied along with the ONT.
- Use Isopropyl alcohol to clean the optical connector.

### Procedure

1. Find an appropriate location to install the ONT. Clean the optic fiber with Isopropyl alcohol.
2. Use the SC-APC green optical connector to connect the optic fiber and the ONT.
3. Ensure the ONT is placed away from any kind of heat-generating device.

This page is intentionally left blank

# 5 User interface configuration

This chapter details the configurations to be performed in each of the following menus:

1. Basic configuration
2. Advanced setup
3. Diagnostics
4. Management

## 5.1 Basic configuration

Perform the following steps to do the basic configuration on the ONT:

1. Connect a PC or laptop to any one of the Ethernet ports on the ONT.
2. Configure the PC or laptop in DHCP mode and connect it to one of the LAN ports on the TJ2100N-11G to get an IP from the residential gateway.
3. Open the **command prompt** on the connected laptop and check the IP by typing ***ipconfig*** in windows or ***ifconfig*** in Linux. Verify if the IP is from class 192.168.1.1 subnet.
4. Open a Internet browser on the connected laptop/PC and browse the site: *http://192.168.1.1*. The Login page appears.
5. Enter the **user name** and the **password**. The default user name and password is ***admin***.
6. Click **OK**. The gateway configuration page appears.
7. Configuration page lists the system and interface information details. This page also appears if you navigate to **System Info > Summary**. Click **Logout** button to log out of the node. Click **Refresh** button to refresh or reload the page.

### 5.1.1 Device Info- PON

To view the configured Wide Area Network (WAN) details, select **Device Info > PON Info** from the navigation menu. The **PON Info** page appears.

**Table 6: PON info parameters**

Parameter	Description
ONT MAC Address	Displays the MAC address of the ONT.
ONT Model	Displays the model name of the ONT.
ONT Serial Number	Displays the serial number of the ONT.
ONT Activation Status	Displays the activation status of the ONT.
RX Optical Power	Displays the power (dBm) of the received signal.
TX Optical Power	Displays the power (dBm) of the transmitted signal.
Laser Voltage	Displays the laser voltage (mV) of the ONT.
TxBias Current	Displays the Tx Bias current (uA) of the ONT.
Temperature	Displays the temperature (C) of the ONT.
WAN Interface 1	Displays the service type of the WAN interface 1.
WAN MAC address	Displays the MAC address of the WAN interface 1.
WAN Interface 2	Displays the service type of the WAN interface 2.
WAN MAC address	Displays the MAC address of the WAN interface 2.

### 5.1.2 Device Info-CPU

To view the configured Wide Area Network (WAN) details, select **Device Info > CPU Info** from the navigation menu. The **CPU Info** page appears.

**Table 7: CPU info parameters**

Parameter	Description
CPU temperature	Displays the temperature (C) of the CPU
V0.85_1	Displays the voltage for V0.85_1 CPU voltage pin
V0.85_2	Displays the voltage for V0.85_2 CPU voltage pin
V1.0	Displays the voltage for V1.0 CPU voltage pin
V1.8	Displays the voltage for V1.8 CPU voltage pin
V3.3	Displays the voltage for V3.3 CPU voltage pin
VIN	Displays the voltage for VIN CPU voltage pin



### 5.1.3 Device Info- WAN

To view the configured Wide Area Network (WAN) details, select **Device Info > WAN** from the navigation menu. The **WAN Info** page appears.

**Table 8: WAN info parameters**

Parameter	Description
Interface	Displays the configured wireless interface name.
Description	Displays the WAN service description.
MAC Address	Displays the MAC Address of the ONT.
Type	Displays the WAN service type.
VlanMuxId	Displays the identifier of VLANMux.
IPv6	Displays the IPv6 address.
Igmp Pxy	Displays whether IGMP Proxy is enabled or disabled.
Igmp Src Enbl	Displays whether IGMP Source is enabled or disabled.
MLD Pxy	Displays whether MLD Proxy is enabled or disabled.
MLD Src Enbl	Displays whether MLD Source is enabled or disabled.
NAT	Displays whether Network address translation (NAT) is enabled or disabled.
Firewall	Displays whether firewall is enabled or disabled.
IPv4 Status	Displays the status of the IPv4.
IPv4 Address	Displays the IPv4 address.
IPv6 Status	Displays the status of the IPv4 address.
IPv6 Address	Displays the IPv6 address.

### 5.1.4 Device Info- Statistics

To view the statistics of Local Area Network (LAN), select **Device Info > Statistics > LAN Stats** from the navigation menu. The **Statistics > LAN** page appears.

To view the statistics of Wide Area Network (WAN), select **Device Info > Statistics > WAN Stats** from the navigation menu. The **Statistics > WAN** page appears.

To view the statistics of Gem Counter, select **Device Info > Statistics > Gem Counter** from the navigation menu. The **Statistics > Gem Port** page appears.

To view the statistics of Queue, select **Device Info > Statistics > Queue** from the navigation menu. The **Statistics > Queue** page appears.

Click **Reset Statistics** button on respective pages to reset the desired statistics.

---

**Note:** Queue statistics are not supported in this release.

---

For parameter description, refer to ***LAN and WAN statistics parameters table***.

**Table 9: LAN and WAN statistics parameters**

Parameter		Description
Interface		Displays the name of the wireless interface.
Description		Displays the type of the wireless interface.
<b>Transmitted/Received</b>		
Total	Bytes	Displays the total number of bytes transmitted/received.
	Pkts	Displays the total number of packets transmitted/received.
	Errs	Displays the total number of errors transmitted/received.
	Drops	Displays the total number of drops transmitted/received.
Multicast	Bytes	Displays the multicast bytes transmitted/received.
	Pkts	Displays the multicast packets transmitted/received.
Unicast	Pkts	Displays the unicast packets transmitted/received.
Broadcast	Pkts	Displays the broadcast packets transmitted/received.

## 5.1.5 Device Info- Route

To view the routing details, select **Device Info > Route** from the navigation menu. The **Device Info- Route** page appears.

**Table 10: Route parameters**

Parameter	Description
Destination	Displays the destination IP address.
Gateway	Displays the gateway IP address.
Subnet mask	Displays the subnet mask.
Flag	Displays the flags status as: <ul style="list-style-type: none"> <li>• U - up</li> <li>• ! - reject</li> <li>• G - gateway</li> <li>• H - host</li> <li>• R - reinstate</li> <li>• D - dynamic (redirect)</li> <li>• M - modified (redirect)</li> </ul>
Metric	Displays the metric.
Service	Displays the service name.
Interface	Displays the interface name.

## 5.1.6 Device Info- ARP

To view the Address Resolution Protocol (ARP) details, select **Device Info > ARP** from the navigation menu. The **Device Info- ARP** page appears.

**Table 11: ARP parameters**

Parameter	Description
IP address	Displays the IP address.
Flags	Displays the flag status as, complete or not.
HW Address	Displays the MAC address.
Device	Displays the device name.

## 5.1.7 Device Info- DHCP

To view the Dynamic Host Configuration Protocol (DHCP) details, select **Device Info > DHCP** in the navigation menu. The **Device Info - DHCP Leases** page appears.

**Table 12: DHCP parameters**

Parameter	Description
Hostname	Displays the host name of the DHCP server.
MAC Address	Displays the MAC address of the DHCP server.
IP Address	Displays the IP address of the DHCP server.
Expires In	Displays the DHCP lease expiry time. When DHCP lease expires, it must renew the lease and potentially receive a new IP address.

## 5.2 Advanced setup

### 5.2.1 LAN

The LAN option is to configure the broadband router IP address and subnet mask for LAN interface.

#### 5.2.1.1 VLAN Setup

Perform the following steps to configure the VLAN:

1. Click **Advanced Setup > LAN > Lan VLAN Setting** in the navigation pane. The **Local Area Network (LAN) VLAN Setup** page appears.
2. Select a **LAN port** from the drop down.
3. Select **Enable VLAN Mode** check box to enable VLAN.
4. Click **Add** button to add new VLANs and enter **Vlan Id** and **Pbits**. Click **Apply/Save** button.

To delete the configured VLANs, select the check box under the **Remove** parameter against the desired VLAN ID and click **Remove** button.

#### 5.2.1.2 IPv6 LAN auto configuration

Perform the following steps to configure the IPv6 LAN:

1. Click **Advanced Setup > LAN > IPv6 Autoconfig** in the navigation pane. The **IPv6 LAN Auto Configuration** page appears.
2. Select or enter the desired values and click **Save/Apply** button.

**Table 13: IPv6 LAN auto configuration parameters**

Parameter	Description
<b>Static LAN IPv6 address configuration</b>	
Interface Address	Enter the IP address (prefix length must be 64).

**Table 13: IPv6 LAN auto configuration parameters**

Parameter	Description
<b>IPv6 LAN applications</b>	
Enable DHCPv6 Server	Select the check box to enable DHCPv6 Server.
Enable RADVD	Select the check box to enable Router Advertisement Daemon (RADVD). Once enabled, <b>Enable ULA Prefix Advertisement</b> , <b>Randomly Generate</b> , and <b>Statically Configure</b> parameters appears. When <b>Statically Configure</b> radio button is selected, enter the <b>Prefix</b> , <b>Preferred Life Time (hour)</b> and <b>Valid Life Time (hour)</b> .
Enable MLD snooping	Select the check box to enable MLD snooping.

## 5.2.2 NAT

Network Address Translation (NAT) allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network.

### 5.2.2.1 Virtual servers

Virtual server is to direct incoming traffic from WAN side (identified by protocol and external port) to the internal server with private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

To view the added virtual servers, click **Advanced Setup > NAT > Virtual Servers** in the navigation pane. The **NAT > Virtual Servers Setup** page appears.

Perform the following steps to add the virtual servers:

1. Click **Advanced Setup > NAT > Virtual Servers** in the navigation pane. The **NAT > Virtual Servers Setup** page appears.
2. Click **Add**. The **NAT - Virtual Servers** page appears.
3. Select or enter values by referring to the **Virtual servers parameters table**.
4. In the **Service Name**, select either **Select a Service** to select predefined services or **Custom Service** to create a service name.
5. Click **Apply/Save** to forward IP packets for this service to the specified server.
6. Select or enter the values for **External Port Start**, **External Port End**, **Protocol**, **Internal Port Start**, and **Internal Port End** parameters by referring to the **Virtual servers parameters table**.
7. Click **Apply/Save**.

To delete the configured virtual servers, select the check box under the **Remove** parameter against the desired server name and click **Remove** button.

---

**Note:** The **Internal Port End** cannot be modified directly. Normally, it is set to the same value as **External Port End**. However, if you modify **Internal Port Start**, then **Internal Port End** will be set to the same value as **Internal Port Start**. Remaining number of entries that can be configured is 32.

---

**Table 14: Virtual servers parameters**

Parameter	Description
Use Interface	Select the use interface.
Select a service	Select a service name from the drop-down list.
Custom Service	Enter the custom service name.
Server IP Address	Enter the IP address of the virtual server.
External Port Start	Enter the external port start number of the virtual server.
External Port End	Enter the external port end number of the virtual server.
Protocol	Select a protocol from the drop-down list.
Internal Port Start	Enter the internal port start number of the virtual server.
Internal Port End	Enter the internal port end number of the virtual server.

### 5.2.2.2 Port triggering

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port trigger dynamically opens up the *Open Ports* in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the *Triggering Ports*. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the *Open Ports*. A maximum 32 entries can be configured.

To view the added port triggering, click **Advanced Setup > NAT > Port Triggering** in the navigation pane. The **NAT > Port Triggering Setup** page appears.

Perform the following steps to configure the port triggering:

1. Click **Advanced Setup > NAT > Port Triggering** in the navigation pane. The **NAT - Port Triggering Setup** page appears.
2. Click **Add**. The **NAT - Port Triggering** page appears.
3. Select or enter values by referring to the **Port triggering parameters table**.
4. In the **Application Name**, select either **Select an Application** to select pre-defined applications or **Custom Application** to create a application name.
5. Click **Save/Apply** to add the application.

6. Select or enter the values for the **Trigger Port Start, Trigger Port End, Trigger Protocol, Open Port Start, Open Port End,** and **Open Protocol** parameters by referring to the ***Port triggering parameters table***.
7. Click **Apply/Save**.

To delete the configured port triggering, select the check box under the **Remove** parameter against the desired application name and click **Remove** button.

---

**Note:** Some applications such as games, video conferencing, remote access applications, and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this page by selecting an existing application or creating your own (Custom application)

---

**Table 15: Port triggering parameters**

Parameter	Description
Use Interface	Select the use interface.
Select an application	Select an application name from the drop-down list.
Trigger Port Start	Enter the trigger port start number of the serve.
Trigger Port End	Enter the trigger port end number of the serve.
Trigger Protocol	Select a trigger protocol from the drop-down list.
Open Port Start	Enter the open port start number of the serve.
Open Port End	Enter the open port end number of the serve.
Open Protocol	Select a open protocol from the drop-down list.

### 5.2.2.3 DMZ host

The ONT forwards IP packets from the WAN that do not belong to any of the applications configured in the virtual servers table to the DMZ host.

Perform the following steps to activate DMZ host:

1. Click **Advanced Setup > NAT > DMZ Host** in the navigation pane. The **NAT - DMZ Host** page appears.
2. Enter the PCs IP address in the **DMZ Host IP Address**
3. Click **Save/Apply** to save and activate the DMZ host.

---

**Note:** Clear the IP address field and click **Save/Apply** to deactivate the DMZ host.

---

## 5.2.3 Security

Security section details the procedures to configure IP filtering, MAC filtering, WAN access control, LAN access control, and DOS configuration.

### 5.2.3.1 IP filtering

IP filtering allows you to configure the incoming and outgoing IP Filters.

#### Outgoing IP filtering

By default, outgoing IP filtering allows all IP traffic from the LAN. Setting up filters blocks the specific IP traffic.

To view the added outgoing IP filtering, Click **Advanced Setup > Security > IP Filtering > Outgoing** in the navigation pane. The **Outgoing IP Filtering Setup** page appears.

Perform the following steps to configure outgoing IP filters:

1. Click **Advanced Setup > Security > IP Filtering > Outgoing** in the navigation pane. The **Outgoing IP Filtering Setup** page appears.
2. Click **Add** button. The **Add IP Filter -- Outgoing** page appears.
3. Select or enter the desired values by referring to the **Add incoming/outgoing IP filtering parameters table**.
4. Click **Apply/Save** to save and activate the filter.

To delete the added outgoing IP filter, select the check box under the **Remove** parameter against the desired filter name and click **Remove** button.

**Table 16: Add incoming/outgoing IP filtering parameters**

Parameter	Description
Filter name	Enter the name for the new filter.
IP Version	Select an IP version from the drop-down list. <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
Protocol	Select a protocol version from the drop-down list. <ul style="list-style-type: none"> <li>• TCP/UDP</li> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>
Source IP address [/ Prefix Length]	Enter the source IP address.
Source Port (port or port:port):	Enter the port number of the source IP.



**Table 16: Add incoming/outgoing IP filtering parameters**

Parameter	Description
Destination IP Address [/Prefix Length]	Enter the destination IP address.
Destination Port (port or port:port):	Enter the port number of the destination IP.

### Incoming IP filtering

All the incoming IP traffic is blocked when the firewall is enabled on a WAN or LAN interface. Setting up filters accepts the specific IP traffic.

To view the added outgoing IP filtering, Click **Advanced Setup > Security > IP Filtering > Incoming** in the navigation pane. The **Incoming IP Filtering Setup** page appears.

Perform the following steps to configure incoming IP filters:

1. Click **Advanced Setup > Security > IP Filtering > Incoming** in the navigation pane. The **Incoming IP Filtering Setup** page appears.
2. Click **Add** button. The **Add IP Filter - Incoming** page appears.
3. Select or enter the desired values by referring to the **Add incoming/outgoing IP filtering parameters table**.
4. Click **Apply/Save** to save and activate the filter.

To delete the added incoming IP filter, select the check box under the **Remove** parameter against the desired filter name and click **Remove** button.

### 5.2.3.2 MAC filtering

MAC filtering is to configure the MAC filter on the interfaces and to change the policy of the interfaces. Click **Advanced Setup > Security > MAC Filtering** in the navigation pane. The **MAC Filtering Setup** page appears.

Perform the following steps to configure the MAC filtering rules:

1. Open **MAC Filtering Setup** page.
2. Click **Add**. The **Add MAC Filter** page appears.
3. Enter the Source MAC Address.
4. Select the LAN Interfaces.
5. Click **Save/Apply** to save or activate the filter.

To delete the added MAC IP filter, select the check box under the **Remove** parameter against the desired filter name and click **Remove** button.

---

**Warning:** Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED. AUTOMATICALLY! You need to create new rules for the new policy.

---

To change the policy of the MAC filter, select the check box under the **Change** parameter against the desired LAN interface and click **Change Policy** button.

---

**Note:** FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.

---

### 5.2.3.3 DOS configuration

Perform the following steps to configure the Denial of Service (DOS) configuration:

1. Click **Advanced Setup > Security > DOS Configuration** in the navigation pane. The **DOS Configuration** page appears.
2. Select the check box against the desired parameters by referring the **DOS configuration parameters table**.
3. Click **Apply**.

**Table 17: DOS configuration parameters**

Parameter	Description
Prevent LAND Attack	Click checkbox to prevent the LAND attack.
Prevent ICMP Redirection Attack	Click checkbox to prevent the ICMP redirection attack.
Block Packets With Bogus TCP Flags	Click checkbox to block the packets with bogus TCP flags.
Drop all ICMP Packets to Prevent Ping Flood	Click checkbox to drop all ICMP Packets to prevent a ping flood.
Block XMAS Packets	Click checkbox to block the XMAS packets.
Block SYN Flood	Click checkbox to block the SYN flood.

### 5.2.4 Parental control

This section describes the configuration of parental controls in the WiFi access points.

#### Time Restriction

Perform the following steps to configure the time restriction:

1. Click **Advanced Setup > Parental Control > Time Restriction** in the navigation pane. The **Access Time Restriction** page appears.
2. Click **Add** to configure time restriction. The **Access Time Restriction** page appears.
3. Select or enter the values by referring to **Access control restriction parameters table**.
4. Click **Apply/Save** to add the time restriction.

**Table 18: Access control restriction parameters**

Parameter	Description
User Name	Enter the user name.
Browser's MAC Address	Automatically displays the MAC address of the LAN device where the browser is running.
Other MAC Address	Enter the MAC address of the other LAN device.

**Table 18: Access control restriction parameters**

Parameter	Description
Days of the week	Select the days of the week in the check box.
Start Blocking Time (hh:mm)	Enter the start blocking time.
End Blocking Time (hh:mm)	Enter the end blocking time.

**Url filter**

Perform the following steps to configure the URL filter:

1. Click **Advanced Setup > Parental Control > Url Filter/Keyword Filter** in the navigation pane. The **URL Filter** page appears.
2. Select the **Exclude** or **Include** radio button against **URL List Type**.

---

**Note:** Select the list type first then configure the list entries. Maximum 100 entries can be configured.

---

3. Click **Add** button to configure the URL List. The **Parental Control- URL Filter Add** page appears.
4. Enter the values by referring to **URL filter parameters table**.
5. Click **Apply/Save** button to add the entry to the URL filter.

**Table 19: URL filter parameters**

Parameter	Description
URL Address	Enter the URL address.
Port Number	Enter the port number. Default value for port number is 80

---

**Note:** When the **Port Number** field is left empty, default value will be applied.

---

## 5.3 Diagnostics

This chapter describes about the diagnostics that help user and network administrators in scanning, diagnosing, and identifying problems within a computer network.

### 5.3.1 Ping

Perform the following steps to ping the IP:

1. Click **Diagnostics > Ping** in the navigation pane. The **Ping Test** page appears.
2. Enter a valid IP Address.
3. Click **Ping** to ping to the requested IP. This enables the user to know the reachability of any adjacent nodes by putting the IP address in the specified box.

### 5.3.2 Iperf

Perform the following steps to configure the Iperf:

1. Click **Diagnostics > Iperf** in the navigation pane. The **Iperf** page appears.
2. Select the IPERF utility to test bandwidth.
3. Click **start**.

### 5.3.3 Trace route

Perform the following steps to configure the traceroute:

1. Click **Diagnostics > TraceRoute** in the navigation pane. The **Trace Route** page appears.
2. Enter a valid IP Address.
3. Click **TraceRoute**. This enables the user to know the number of hops or distance required to reach any other adjacent node in the network.

### 5.3.4 Packet capture

Perform the following steps to capture the packets on interface:

1. Click **Diagnostics > Packet Capture** in the navigation pane. The **Packet Capture** page appears.
2. Select the packet capture from drop-down list.
3. Click **Start**.

### 5.3.5 Connection status

To view the connection status page, click **Diagnostics > Connection Status** in the navigation pane. The **Diagnostics** page appears.

This page lists the interfaces with the test results as **PASS** or **FAIL**. If a test displays a **FAIL** status, click **Rerun Diagnostic Tests** button to ensure the **FAIL** status is consistent.

**Table 20: Diagnostics**

Parameter	Description
PASS	Indicates that the Ethernet interface from your computer is connected to the LAN port of your Broadband Router. A flashing or solid green LAN LED on the router also signifies that an Ethernet connection is present and that this test is successful.
FAIL	Indicates that the Broadband Router does not detect the Ethernet interface on your computer.

If the test continues to fail, click **Help** link and follow the troubleshooting procedures listed below and rerun the diagnostics tests by clicking on the **Rerun Diagnostic Tests** button.

1. If you are not able to access **Ethernet Connection Test** page, verify that the Ethernet cable from your computer or your hub is connected to the LAN port on DSL Router. Reset the cable by unplugging both ends and reconnecting them to their respective ports.
2. Turn off the Broadband Router, wait 10 seconds and turn it back ON.
3. Ensure you use the Ethernet wire that supplied with your DSL router.
4. With the router on, press the reset button on the Broadband Router for at least five seconds and release it. This resets the Broadband Router to its default settings. Wait for the Broadband Router to initialize, then close and restart your Web browser. To reconfigure the router, type your DSL Account username and password.

If all the tests pass, close and restart your Web browser to access the Internet. Contact Technical Support if you have tried all of the above and still are experiencing a fail condition.

## 5.4 Management

This section explains the procedures to perform backup settings, restore default settings, update software, and reboot the router and also explains the configurations of SNMP.

## 5.4.1 Settings

This section explains the backup settings, update settings and restore default settings.

### Backup settings

With this option, perform settings in Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Perform the following steps to configure the Backup Settings:

1. Navigate to **Management > Settings > Backup** in navigation pane. The **Settings - Backup** page appears.
2. Click **Backup Settings**. The **Opening backupsettings.conf** dialog box appears. Choose **Save File**.
3. Select a convenient network location where you can retrieve this file in the future as needed.
4. Click **Save**.

### Restore default settings

This option is required to restore broadband router settings to the factory defaults.

Perform the following steps to configure the restore settings:

1. Go to **Management > Settings > Restore Default** in the navigation pane. The **Tools - Restore Default Settings** page appears.
2. Click **Restore Default Settings**. *Are you sure you want to restore factory default settings?* message appears.
3. Click **OK**.

## 5.4.2 System log

Perform the following steps to view the system log:

1. Click **Management > System log** in the navigation pane. The **System Log** page appears.
2. Click **View System Log** displays the system log details in the local browser. For parameter description refer to **View system log parameters table**.

**Table 21: View system log parameters**

Parameter	Description
Date/Time	Displays the date and time.
Facility	Displays the facility.
Severity	Displays the severity of the message.
Message	Displays the message.

Perform the following steps to configure the system log:

1. Click **Management > System log** in the navigation pane. The **System Log** page appears.
2. Click **Configure System Log**. The **System Log - Configuration** page appears.
3. Select or enter the desired values by referring to **System log configuration parameters table**.
4. Click **Apply/Save** to configure the system log.

**Table 22: System log configuration parameters**

Parameter	Description
Log	To enable or disable the system log configuration.
Log Level	Select the log level from the drop-down list.
Display Level	Select the display level from the drop-down list.
Mode	Select the mode from the drop-down list.
Server IP Address	Enter the server IP address.
Server UDP Port	Enter the server UDP port number.

### 5.4.3 TR-069 Client

Perform the following steps to configure the TR-069 client:

1. Click **Management > TR-069 Client** in the navigation pane. The **TR-069 client - Configuration** page appears.
2. Select or enter the desired values by referring to **TR-069 parameters table**.
3. Click **Apply/Save** to save the time configuration.

**Table 23: TR-069 parameters**

Parameter	Description
Inform	To enable or disable the periodic inform.
Inform Interval	Enter the inform interval that defines a frequency of communication with the ACS.
ACS URL	Enter the Internet address of the ACS, which is accessible from the device.
ACS User Name	Enter the ACS user name.
ACS Password	Enter the ACS password.
ACS Connectivity Status	Displays the ACS connectivity status.



**Table 23: TR-069 parameters**

Parameter	Description
WAN Interface used by TR-069 client	Select the WAN interface from the drop down menu.
Connection Request Authentication	Select the check box to enable the connection request authentication.
Connection Request User Name	Enter the user name of the connection.
Connection Request Password	Enter the password of the connection.
Connection Request URL	Displays the URL of the connection.

### 5.4.4 Internet time

Internet time option is to set the time on the router.

Perform the following steps to configure the time on the router:

1. Click **Management > Internet Time** in the navigation pane. The **Time settings** page appears.
2. Select or enter the desired values by referring to **Time settings parameters table**.
3. Click **Apply/Save** to save the time configuration.

**Table 24: Time settings parameters**

Parameter	Description
Automatically synchronize with Internet time servers	Select the check box to synchronize with Internet time servers automatically.
Following parameters appears if <b>Automatically synchronize with Internet time servers</b> check box is selected.	
First NTP time server	Select the first time server from the drop-down list. <ul style="list-style-type: none"> <li>• clock.fmt.he.net</li> <li>• clock.nyc.he.net</li> <li>• clock.sjc.he.net</li> <li>• clock.via.net</li> <li>• ntp1.tummy.com</li> <li>• time.cachenetworks.com</li> <li>• time.nist.gov</li> <li>• Other</li> </ul>

**Table 24: Time settings parameters**

Parameter	Description
Second NTP time server	Select the second time server from the drop-down list. <ul style="list-style-type: none"> <li>• None</li> <li>• clock.fmt.he.net</li> <li>• clock.nyc.he.net</li> <li>• clock.sjc.he.net</li> <li>• clock.via.net</li> <li>• ntp1.tummy.com</li> <li>• time.cachenetworks.com</li> <li>• time.nist.gov</li> <li>• Other</li> </ul>
Third NTP time server	Select the third time server from the drop-down list.
Fourth NTP time server	Select the fourth time server from the drop-down list.
Fifth NTP time server	Select the fifth time server from the drop-down list.
Time zone offset	Select the time zone offset with respect to the synchronization server from the drop-down list.

### 5.4.5 Reboot

Perform the following steps to reboot the router:

1. Click **Management > Reboot**.
2. Click **Reboot** button to reboot the router.

## 6 Regulatory standard compliance

The list of technical standards provided in this chapter is not exhaustive. The standards listed are generally regarded as the primary applicable electromagnetic compatibility (EMC) and safety standards. The conformity status on additional national and international standards are not listed in this section can be provided upon request.

Specification	Standard compliance
EMI/EMC	ICES-003
	EN 300 386
	EN 55022 / CISPR-22
	EN 55032 / CISPR-32
	EN 55024 / CISPR-24
	EN 55035 / CISPR-35
	(EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6)
Safety	EN 61000-4-11, EN 61000-3-2, and EN 61000-3-3 (applicable to AC power supply products)
	Certified for CB – Scheme.
	IEC 62368-1 / EN 62368-1 UL 62368-1
Laser Safety	IEC 60825-1 / EN 60825-1
	IEC 60825-2 / EN 60825-2
	21 Code of Federal Regulations (CFR)1040
Environment	ETS 300 019-1-1, Class 1.2 Storage
	ETS 300 019-1-2, Class 2.3 Transportation
	ETS 300 019-1-3, Class 3.2 Operating stationary use
	QM333 – Functional for Environmental testing of Electronic equipment's for Transmission and switching use.
RF	FCC Part-15, subpart-C 15.207, 15.209, and 15.407.
	EN 300 328
	EN 302 502
	EN 301 893
RoHS compliant	Directive 2011/65/EU and 2015/863/EU