Cisco Catalyst PON Series Switches ONT Configuration Guide

First Published: Nov 2020

Last Updated: Oct, 2021

TOC

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

Get Started

Overview of ONT

An Optical Network Terminal (ONT), also referred to as an Optical Network Unit (ONU), is an integrated Passive Optical Network (PON) access device. It provides high performance access services for end users, Small Office Small Home (SOHO) users, small companies, cable TV (CATV), audio and video transmission, and networks where shared high-speed internet access is required.

For more information, refer to the *Cisco Catalyst PON Series Switches Hardware Installation Guide*.

Note

Some features are not supported on all ONT models. Refer the Release Notes for Cisco Catalyst PON Series ONT for the complete list of unsupported features.

Log into ONT

You can access the ONT device through a web-based interface from an IP network; or through the Cisco Catalyst PON Manager.

Prerequisites

- Connect your computer (the remote device accessing the ONT) to a port on the PON network. Configure the IP of your computer to be in the same subnet as the ONT.
- You must know the IP address of the ONT device to login to.

  The ONT device uses a default IP address, 192.168.1.1, with a subnet of /24.

Procedure

1. From your computer, ping the IP address of the ONT device.

   A successful ping indicates that the device can be accessed.

   ```
   C:\Users\Cisco>ping 192.168.1.1
   Pinging 192.168.1.1 with 32 bytes of data:
   Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
   Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
   Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
   Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
   Ping statistics for 192.168.1.1:
   Packets: Sent=4, Received=4, Lost=0(0% loss),
   Approximate round trip times in milli-seconds:
   Minimum=2ms, Maximum=3ms, Average=2ms
   ```

2. Open a browser and enter http://192.168.1.1 or http://<IP address of ONT device> in the address bar.
3. Enter the administrator username and password in the login window.

   Username and password are both case sensitive. By default, the username and password are both “cisco”.

   Create a new username and password after the first login.

After you log in to the device, an ONT configuration window containing the device name and its maintenance menu options appears.

Configure

Configure Local Area Network Connection

You can configure the Local Area Network (LAN) for an ONT device by setting up its interface, port, PoE, and security aspects.

Set Up a LAN Interface

To launch the **LAN Interface Settings** pane, click on **LAN** > **LAN Interface** from the left navigation pane.

Edit LAN Interface Setting

1. Enter the new IP address in the **IP Address** field.
2. Enter the new subnet mask in the **Subnet Mask** field.
3. To enable IGMP snooping, select the **Enabled** radio button on the **IGMP Snooping** tab.

   To disable IGMP snooping, select the **Disabled** radio button.
4. To save and execute the configurations, click **Apply**.
5. If your device supports IPv6 addressing, do the following:
   - Enter the IPv6 address in the **IPv6 Address/Length** field.
   - To enable **MLD Snooping**, select the **Enable** radio button.

Configure a LAN Port

The **Port Settings** pane allows you to edit the basic port configuration and port mirror configuration.

To launch the **Port Settings** pane, click on **LAN** > **Port Settings** from the left navigation pane.

View and Edit the Basic Port Configuration

1. The **Basic Port Configuration** panel displays the following information:

Parameter	Description
Port	Name of the LAN interface.
Link State	Link status of the LAN interface: *up* or *down*.
Enable	Enables the LAN interface.
Flow Control	Flow control feature on the port.
Mode	Transmission mode on the port.

2. To activate a LAN port, select *Enable* from the drop-down list.

   To deactivate a LAN port, select *Disable* from the drop-down list.
3. To enable flow control on a LAN port, select the **Flow Control** check box.
4. To save and execute the configurations, click **Apply**.

Configure Port Mirror

1. On the **Port Mirror Configuration** panel, select the **Enable** check box.
2. Select a destination port from the **Destination Port** drop-down list.
3. To define the ports to be monitored, select the required check boxes on the **Monitored Ports** tab.
4. To save and execute the configurations, click **Apply**.

Configure Power over Ethernet Ports

1. To launch the **Port Settings** pane, click on **LAN** > **PoE Settings** from the left navigation pane.
2. To limit the power per port, select one of the following power modes:
   - **Port Limit**: Limits the power per port to a specified wattage. If the power consumed on the port exceeds the port limit, the port power is cut off.
   - **Class Limit**: Limits the power to the port based on the connected Powered Device. When the power consumed on the port exceeds the class limit, the port power is turned off.
3. The **Global Power Limit** displays the maximum power supported on the port.
4. The **Global Power Consumption** displays the total power consumed by the device.
5. To use local configuration on the device, select the **Enable** check box on the **Configuration Save by Local** tab.

   For the device to inherit the OLT configuration values, do not select the check box.
6. Based on the power mode selected, the **PoE Port Status** panel displays the following information:

Parameter	Description
Interface	Displays the port number.
Status	State of the interface: *enable* or *disable*.
Priority	PoE priority on the port: *high*, *low*, or *critical*.
Class	The power class to which the device belongs.
Power Limit	Maximum supported power on the port. The range is 1 to 30 W.
Power Consumption	Actual power consumed by the port.

7. To save and execute the configurations, click **Apply**.

Edit Port Limit

1. Select the **Port Limit** radio button on the **Power Mode** tab.
2. On the **PoE Port Status** panel, select a port by clicking the corresponding radio button.
3. Click the  button.
4. To enable the selected port as a PoE port, select *Enable* from the drop-down list.

   To disable the port, select *Disable*.
5. Enter the new power limit in Watts in the **Power limit** field. The range is from 1 to 30 W.

6. Select the priority from the **PoE Priority** drop-down list. The available options are:
   - *high*
   - *low*
   - *critical*
7. To save the configuration for the selected port, click **OK**.

Edit Class Limit

1. Select the **Class Limit** radio button on the **Power Mode** tab.
2. On the **PoE Port Status** panel, select a port by clicking the radio button.
3. Click the  button.
4. To enable the selected port as a PoE port, select *Enable* from the drop-down list.
   To disable the port, select *Disable*.
5. Select the priority from the **PoE Priority** drop-down list. The available options are:
   - *high*
   - *low*
   - *critical*
6. To save the configuration for the selected port, click **OK**.

Configure Port Security

You can configure the ONT device for IEEE 802.1x based authentication.

To launch the **802.1X Configuration** pane, click on **LAN** > **Security** from the left navigation pane.

The **Support LAN Port 802.1x** panel displays the following information:

Parameter	Description
Enable MAB	Indicates whether MAC Authentication Bypass (MAB) is enabled or disabled.
Multi-host Mode	Indicates if the port is capable of allowing multiple hosts to access it.
Enable Accounting	Indicates if 802.1X Accounting is enabled or not.
RADIUS Source Interface	Indicates the interface on which the RADIUS client sends requests and receives responses.
RADIUS Server IP	IP address of the RADIUS Server.
RADIUS Authentication Port	Port number of the UDP port connecting to the RADIUS Server. The default port number is 1812.
RADIUS Secret	Password to authenticate on the RADIUS Server.
NAS IP Address	IP Address of the Network Access Server (NAS). NAS first receives the authentication request before the request is passed on to a RADIUS Server.

Parameter	Description
NAS Identifier	Network Access Server identifier (NAS-ID) attribute of a RADIUS packet enables the RADIUS server to identify the access location of the users.

The **Port Table** panel displays the following information:

Parameter	Description
Port	LAN port.
Port State	Status of the LAN port: *Link Up* or *Link Down*.
Administrative State	Indicates the authentication state of the port: *Auto* or *Force Authorized*.

Edit 802.1X Configuration

1. To enable port authorization, select the **Enable Port Auth** check box.
2. To enable MAB, select the **Enable MAB** check box.
3. To enable multi-host mode, select the **Multi-host Mode** check box.
4. To enable RADIUS accounting port, select the **Enable Accounting** check box.
5. To change the IP address, enter the new IP address in the **RADIUS IP** field.
6. To change the port number, enter the new port number in the **RADIUS Authentication Port** field.
7. To change the port accounting number, enter the new port accounting number in the **RADIUS Accounting Port** field.
8. To change the password, enter the new password in the **RADIUS Secret** field.
9. To change the NAS IP address, enter the new IP address in the **NAS IP Address** field.
10. To change the NAS identifier, enter the new identifier in the **NAS Identifier** field.
11. To save and execute the configurations, click **Apply**.

Edit Port Table Configuration

1. On the **Port Table** pane, select the state from the **Administrative State** drop-down list. The available options are:
   - *Auto*
   - *Force Authorized*: Select this for a port without authentication.
2. To save and execute the configurations, click **Apply**.

Configure Wide Area Network Connection Port

You can configure the Wide Area Network (WAN) parameters on the device to enable access to WAN networks, like the Internet.

Note:

This feature is not available when the ONT operates in the Single Family Unit (SFU) mode.

To launch the **WAN Configuration** pane, click on **WAN** from the left navigation pane.

Create a new WAN connection

1. To select a new link, from the **WAN Connection** drop-down list, select *new link*.

   Note:

   Create separate WAN connections for each service offered by the device.
2. Enter a unique name for the WAN connection in the **WAN Name** field.
3. To open a specified WAN connection, select the **Enable** radio button on the **Admin Status** tab.

   To close a WAN connection, select the **Disable** radio button on the **Admin Status** tab.
4. Choose an appropriate service from the **Service Type** drop-down list:
   - *TR069*: Remote maintenance and management service; can be used to configure ONT management IP address.
   - *INTERNET*: Broadband internet access service.
   - *VOICE*: VoIP service.
   - *TR069_INTERNET*: Both remote maintenance and management service and the internet access service.
   - *VOIP_INTERNET*: Both VoIP service and Internet access service.
   - *TR069_VOICE*: Both remote maintenance and management service and VoIP service.
   - *TR069_VOICE_INTERNET*: All the services together: remote maintenance and management service, VoIP service, and internet access service.
   - *Other*: Any other service.
5. To tag the packets with a VLAN ID, select the **Enable VLAN** check box.

   Do not select this check box if you do not want the packets to be tagged with the VLAN ID.
6. Enter the VLAN ID for the selected network in the **VLAN ID** field.

   Ensure that the VLAN ID matches with the VLAN ID of the OLT. The VLAN ID ranges from 1 to 4094.
7. To define the priority of the data packets, select an 802.1p value from the **802.1p_Mark** drop-down list.

   802.1p priority ranges from 0 to 7, with 7 indicating the highest priority.
8. Enter the multicast VLAN ID in the **Multicast VLAN ID** field.

   Ensure that this ID is the same as the Multicast VLAN ID of the OLT.
9. Enter the size of Maximum Transmission Unit (MTU) in bytes in the **MTU** field.

   MTU is the size of the largest IP packet that an Ethernet frame can contain.
10. Choose an appropriate **Connection Type** that is to be established between the devices in the WAN.
    - To configure a bridge connection, choose **Bridge**. See Configure Bridge as Connection Type, page 13.
    - To configure IP over Ethernet connection, choose **IPoE**. Configure IPoE as Connection Type with Static IP Address, page 13.
    - To configure Point-to-Point over Ethernet protocol-based connection, choose **PPPoE**. See Configure PPPoE as Connection Type, page 14.

11. If your device supports IPv6 addressing, do the following in the **WAN IPv6 Setting** pane:
    To disable IPv6 addressing, select **Disable** from the **Address Mode** drop down list.
    To configure IPv6 DHCP Client:
    a. Select **DHCP** from the **Address Mode** drop-down list.
    b. To obtain the IPv6 address and prefix, select the **Request Address** and **Request Prefix** check boxes.
    c. To obtain a domain name service, select the **Enable** radio button for **Request DNS**.
    d. Enter the **Primary IPv6 DNS** address and the **Secondary IPv6 DNS** address in the fields provided.
    To configure Static IPv6 Addressing Mode:
    a. Select **Static** from the **Address Mode** drop-down list.
    b. Enter the **IPv6 Address** and length in the fields provided.
    c. Enter the **IPv6 Gateway** address.
    d. Enter the **Primary IPv6 DNS** address and the **Secondary IPv6 DNS** address in the fields provided.
    To configure Stateless Address Auto-configuration:
    a. Select **SLAAC** from the **Address Mode** drop-down list.
    b. To obtain the IPv6 address and prefix, select the **Request Address** and **Request Prefix** check boxes.
    c. Enter the **Primary IPv6 DNS address** and the **Secondary IPv6 DNS** address in the fields provided.
12. To save and execute the configurations, click **Apply**.

Configure Bridge as Connection Type

Select bridge to establish a direct connection from the WAN to LAN.

1. On the **Connection Type** tab, select the **Bridge** radio button.
2. To enable Network Address and Port Translation, select **Enable NAPT** check box.
3. To enable IGMP proxy, select the **Enable IGMP-Proxy** check box.
4. To map the LAN port with the WAN port, select the required check boxes on the **Port Mapping** panel.

Configure IPoE as Connection Type with Static IP Address

IP over Ethernet (IPoE) connection delivers traffic across an Ethernet network without using PPP encapsulation. Select IPoE to configure the WAN port with a static IP address or with an IP address obtained through DHCP.

1. On the **Connection Type** tab, select the **IPoE** radio button.
2. To enable Network Address and Port Translation, select **Enable NAPT** check box.
3. To enable IGMP proxy, select the **Enable IGMP-Proxy** check box.
4. On the **WAN IP Settings** panel:
    a. Select the **Fixed IP** radio button on the **Type** tab.
    b. Enter the IP address in the **IP Address** field.
    c. Enter the sub net mask in the **Netmask** field.
    d. Enter the default gateway in the **Default Gateway** field.
5. To map the LAN port with the WAN port, select the required check boxes on the **Port Mapping** panel.

Configure IPoE as Connection Type with DHCP

IP over Ethernet (IPoE) connection delivers traffic across an Ethernet network without using PPP encapsulation. Select IPoE to configure the WAN port with a static IP address or with an IP address obtained through DHCP

1. On the **Connection Type** tab, select the **IPoE** radio button.
2. To enable Network Address and Port Translation, select **Enable NAPT** check box.
3. To enable IGMP proxy, select the **Enable IGMP-Proxy** check box.
4. Select an appropriate IP addressing format from the **IP Protocol** drop-down list.
5. On the **WAN IP Settings** panel:
   a. Select the **DHCP** radio button on the **Type** tab.
   b. To configure DNS,
      - For automatic configuration, select the **Enable** radio button on the **Request DNS** tab.
      - For manual configuration, select the **Disable** radio button on the **Request DNS** tab.

        Enter the DNS server settings in the **Primary DNS Server** and the **Secondary DNS Server** fields.
6. To map the LAN port with the WAN port, select the required check boxes on the **Port Mapping** panel.

Configure PPPoE as Connection Type

Select PPPoE as connection type to configure Point-to-Point over Ethernet (PPPoE) protocol-based connection between the WAN port and the remote device.

1. On the **Connection Type** tab, select the **PPPoE** radio button.
2. To configure the PPP settings, on the **PPP Settings** panel:
   a. Enter the user name in the **UserName** field.
   b. Enter the password in the **Password** field.
   c. Select the type from the **Type** drop-down list. The available options are:
      - *Keep alive*
      - *Connect on Demand*
      - *Manual*
   d. Select the method of authentication from the **Authentication Method** drop-down list. The available options are:
      - *AUTO*
      - *PAP*
      - *CHAP*
      - *MSCHAP*
      - *MSCHAPv2*
   e. Enter the Access Concentrator's name in the **AC-Name** field.
   f. Enter the name of the PPPoE service offered in the **Service-Name** field.
3. To map the LAN port with the WAN port, select the required check boxes on the **Port Mapping** panel.

Configure Wireless Local Area Network Connection

You can configure a wireless local area network (WLAN) for an ONT device by configuring the wireless network parameters and their access controls.

Configure Basic WLAN Parameters

To launch the WLAN Settings pane, click **WLAN** > **Basic Settings** in the left navigation pane.

A **Wireless Table** displays the information about the following parameters of the device:

Feature	Description
Enable	State of the ONT device.
Band	WiFi frequency bands: choose between 2.4GHz and 5GHz.
SSID	Service Set Identifier which is a unique identifier for the WLAN.
WAN Mapping	WAN connection mapping as configured on the WAN page.
Security Mode	Security level for the passwords.
Broadcast SSID	Broadcasting of the device's SSID.
WMM	Wi-Fi Multimedia support
Relay Blocking	Status of relay blocking in the Wireless LAN
Active Client List	Click on **Show** to see the MAC address, transmission, reception packet counters and encrypted status of the selected client.

Add Wireless SSID Settings

To add a new entry to the Wireless Table:

1. Click the + button
2. Enter the **SSID** Name.
3. Select **Enable WLAN**.

   Note:

   Enabling or disabling the WLAN can turn the radios on or off respectively for the default SSID.
4. Choose an appropriate bandwidth from the **Band** drop-down list.
5. To enable broadcast of SSID, select the **Enable** button for **Broadcast SSID**.
6. To enable WiFi Multimedia, select the **Enable** button for **WMM**.
7. To enable the power saving mode, select the **Enable** button for **WMM Power Save**.
8. To enable relay blocking, select the **Enable** button for **Relay Blocking**.

9. To configure the security settings for the SSID, choose the **Security Mode** from the drop-down list:
    a. To have no authentication, choose **NONE**; any host with a wireless network card can be connected.
    b. To configure WEP encryption. choose **WEP**.
        i. By default, **Auto** Authentication mode is selected. Select the **Key Length**, **Key Format** from the respective drop-down lists and enter the **Encryption Key** value.
        ii. To change the authentication mode, select **Open System** or **Shared Key** buttons as per your network requirements.
    c. To configure a pre-shared key and encrypt the data before transmission, choose **WPA2** and configure the following:
        i. Select from **None**, **Capable** or **Required** modes of **IEEE 802.11w**, according to your network requirements.
        ii. To configure a RADIUS Server for authentication, select **Enterprise(RADIUS)** as the **Authentication Mode** and enter the **RADIUS Server** attributes and the **Backup RADIUS Server** attributes.
        iii. To configure a pre-shared key for authentication, select **Personal(Pre-Shared Key)** as the **Authentication Mode** and enter the pre-shared key format and the pre-shared key in the fields provided.
        iv. Enter the **Group Key Update Timer**.
    d. To configure a hybrid authentication mode, choose **WPA2 Mixed**.
        i. To configure a RADIUS Server for authentication, select **Enterprise(RADIUS)** as the **Authentication Mode** and enter the **RADIUS Server attributes** and the **Backup RADIUS Server** attributes.
        ii. To configure a pre-shared key for authentication, select **Personal(Pre-Shared Key)** as the **Authentication Mode** and enter the pre-shared key format and the pre-shared key in the fields provided.
        iii. Enter the **Group Key Update Timer**.

    Note:

    We recommend configuring WPA2 or WPA2 Mixed as the security mode instead of WEP as WEP security mode is outdated.
10. To save and execute the configurations, click **Apply**.

Edit Wireless SSID Settings

To edit an entry in the **Wireless Table**:

1. Select the SSID entry.
2. Click the  button.
3. Modify the field values.
4. To save and execute the configurations, click **Apply**.

Delete a Wireless SSID

To delete an entry in the **Wireless Table**:

1. Select the SSID entry.
2. Click the  button.

3. Click **Apply**.

Configure Advanced WLAN Parameters

To configure parameters of the 2.4GHz or 5GHz WiFi spectrums, do the following:

Warning:

Perform these steps only if you know the effect of these settings on your Access Points.

1. To launch the Advanced Settings pane, click **WLAN** > **Advanced Settings** in the left navigation pane.
2. Choose the appropriate bandwidth: **2.4GHz** or **5GHz**.
3. Enter the **Fragment Threshold**. It ranges from 256 to 2346.
4. Enter the **RTS Threshold**. It ranges from 0 to 2347.
5. Enter the **Beacon Interval**. It ranges from 20 to 1024 milliseconds.
6. Enter the **DTIM Period**. It ranges from 1 to 255.
7. Choose an appropriate **Data Range** from the drop-down list.
8. Choose an appropriate **Preamble Type** from the **Long Preamble** or **Short Preamble** buttons.
9. Enable or Disable **Protection** according to your network requirements.
10. Enable or Disable **Aggregation** according to your network requirements.
11. Enable or Disable **Short GI** according to your network requirements.
12. Enable or Disable **802.11k Support** according to your network requirements.
13. If you enable 802.11k Support, enable or disable the **802.11v Support** according to your network requirements.
14. If you have selected 5GHz bandwidth, in addition to the above parameters, configure **TX beamforming** and **MU MIMO parameters**.
15. To save and execute the configurations, click **Apply**.

Configure Wireless Local Area Network Access Control

You can configure Access Control List (ACL) for a device, to permit or block the packets from a specified MAC address in the WLAN.

1. To launch the **WLAN Access Control** pane, click **WLAN** > **Access Control** in the left navigation pane.
2. Choose an appropriate bandwidth: **2.4GHz** or **5GHz**.
3. Select the **Access Mode** from these options in the drop-down list:
   a. To disable the ACL function, select **Disabled**.
   b. To prevent the packets from the specified MAC address to reach the device, select **Deny Listed**.
   c. To allow the packets from the specified MAC address to reach the device, select **Allow Listed**.
4. To add an entry to the Current Access Control List, click the  button and enter the MAC address.
5. To modify an entry in the Current Access Control List, click the  button and modify the list.
6. To delete an entry from the Current Access Control List, select the entry and click the  button.
7. To save and execute the configurations, click **Apply**.

Configure Different Services

You can configure the following services on the device:

- DHCP
- Dynamic DNS
- Universal Plug and Play
- DHCPv6
- Router Advertisement

Note:

DHCP, Dynamic DNS, Universal Plug and Play Services, DHCPv6, and Router Advertisement are not available when the ONT operates in the Single Family Unit (SFU) mode.

Configure the Device as a DHCP Server

Configure the device as a DHCP server to provide and assign IP addresses and other network parameters, to the client devices. DHCP Server uses the Dynamic Host Configuration Protocol (DHCP) to correspond with the client devices.

To launch the **DHCP Settings** pane, click on **Services** > **DHCP** from the left navigation pane.

Configure DHCP Settings

1. To enable the device as a DHCP server, select the **Enable** radio button on the **DHCP Mode** tab.
2. Enter the starting IP address and the ending IP address in the **IP Pool Range** fields.
3. Enter the subnet mask for the IP addresses in the **Subnet Mask** field.
4. Enter the maximum lease time in the **Max Lease Time** field.

   Once the lease time for an IP address expires, the IP address is available to be assigned to other network devices. The range is from 0 to 604800 seconds. A Max Lease Time of 0 indicates that the IP address that is leased to the client doesn't expire. Default lease time is 86400 seconds.
5. Enter the gateway address for the client network in the **Gateway Address** field.
6. To configure a DNS Proxy Server for the network, do the following:
   - To configure DNS proxy server automatically, select the **DNS Proxy** radio button.
   - To configure DNS proxy server manually, select the **Set Manually** radio button.

     Enter the DNS server information in the **DNS1**, **DNS2**, and **DNS3** fields.
7. To save and execute the configurations, click **Apply**.

View the DHCP Client Information

To see the IP address, MAC address, and Lease Time for each of the active clients, click **Show DHCP Client**.

The **Active DHCP Clients** window displays the following information:

Parameter	Description
IP Address	IP address of the DHCP client.
MAC Address	MAC address of the DHCP client.
Lease Time	Lease time configured for the DHCP client.

Configure DHCP Port-Based Filter

Configure a certain port to not obtain an IP address from the DHCP Server.

1. To launch the **Port-Based Filter** window, click the **DHCP Port-Based Filter** button.
2. On the **Port-Based Filter** pane, select the required check boxes.
3. To save the selection, click **Apply**.

Configure DHCP MAC-Based Assignment

Configure a static IP address to a MAC address.

1. To launch the **MAC-Based Assignment** window, click the **DHCP MAC-Based Assignment** button.
2. To add an entry:
   a. Click the  button.
   b. Enter the MAC address in the **MAC Address** field.
   c. Enter the IP address that will be bound to the MAC address, in the **IP Address** field.
3. To edit an entry:
   a. Select the entry.
   b. Click the  button.
   c. Modify the field values as required.
4. To delete an entry:
   a. Select the entry.
   b. Click the  button.
5. To update the table, click **Apply**.

Disable DHCP

1. To disable the device as a DHCP server, select the **Disable** radio button on the **DHCP Mode** tab.
2. To save and execute the configurations, click **Apply**.

Configure Dynamic Domain Name System for the Device

Dynamic Domain Name System (DNS) automatically updates the DNS server records when IP address of the device changes. Dynamic DNS automatically updates the association between the IP address and the hostnames.

To launch the **Dynamic DNS Configuration** pane, click on **Services** > **Dynamic DNS** in the left navigation pane.

View the Dynamic DNS Information

The **Dynamic DNS Table** displays the following information:

Parameter	Description
State	Status of the Dynamic DNS service: *Enabled* or *Disabled*.

Parameter	Description
Hostname	Hostname of the service provider.
Interface	The interface on which the service is enabled.
Username/Email	Username to login to the service provide network.
Password/Key	Password to login to the service provider network.
Service	Service Provider that provides the Dynamic DNS addresses: *No-IP* or *DynDNS.org*.
Status	Displays the status of the Dynamic DNS Service. Status can be: ▪ Successfully updated ▪ Connection error ▪ Authentication failure ▪ Wrong option ▪ Handling DDNS request packet ▪ Cannot connect to provider

Configure Dynamic DNS Entries

1. To add an entry:
   a. Click the + button.
   b. Select your service provider from the **Service** drop-down list. The available options are:
      - *No-IP*
      - *DynDNS.org*
   c. Enter the following details of the service provider that you select.
      - **Hostname**
      - **Username**
      - **Password**
   d. Select the interface on which the service is enabled from the **Interface** drop-down list.
   e. Select an appropriate value from the **State** drop-down list. The available optons are:
      - *Enable*
      - *Disable*
   f. To save the entry, click **Apply**.

2. To edit an entry:
   a. Select the entry.
   b. Click the  button.
   c. Modify the field values as required.
   d. To save the changes, click **Apply**.
3. To delete an entry:
   a. Select the entry
   b. Click the  button.

Configure the Device as Universal Plug and Play

When you enable Universal Plug and Play (UPnP), the system acts as a daemon. By default, UPnP is disabled.

To launch the **Dynamic DNS Configuration** pane, click on **Services** > **UPnP** in the left navigation pane.

Configure UPnP

1. To enable UPnP on the device, select the **Enable** radio button on the **UPnP** tab.
2. Select a WAN interface from the **WAN Interface**drop-down list.
   The selected WAN interface uses the UPnP.
3. To save and execute the configuration, click **Apply**.

View the UPnP Information

The **UPnP Dynamic Table** displays the following information:

Parameter	Description
UserDefined Application	Application defined by the user.
IP Address	IP Address of the device which is a part of UPnP.
Protocol	Protocol used for UPnP.
Local Port	The local port on the device.
Public Port	The port that receives the messages from the external network.
Interface	The interface on which UPnP is configured.

Disable UPnP

1. To disable UPnP on the device, select the **Disable** radio button on the **UPnP** tab.
2. To save and execute the configuration, click **Apply**.

Configure the Device as a DHCPv6 Server

Configure the device as a DHCPv6 server to provide and assign IPv6 addresses and other network parameters to the client devices. DHCPv6 Server uses Dynamic Host Configuration Protocol (DHCP) to correspond with the client

devices.

To launch the **DHCPv6 Settings** pane, click **Services** > **DHCPv6** in the left navigation pane.

Configure DHCPv6 Server Manually

1. To enable manual configuration of DHCPv6 Server, select the **DHCPServer(Manual)** radio button on the **DHCPv6 Mode** tab.
2. Enter the starting IPv6 address and the ending IPv6 address in the **IP Pool Range** fields.
3. Enter the **Prefix Length** of the IPv6 addresses.
4. Enter a **Valid Lifetime** in seconds.

   After the lifetime for an IP address expires, the IP address is available to be assigned to other network devices. A **Valid Lifetime** of 0 indicates that the IP address that is leased to the client doesn't expire. Default lifetime is 20000 seconds.
5. To configure a DNS Proxy Server for the network, do the following:
   - To configure DNS proxy server automatically, select the **DNS Proxy** radio button on the **DNS Option** tab.
   - To configure DNS proxy server manually, select the **Set Manually** radio button on the **DNS Option** tab.

     Enter the DNS server information in the **DNS1**, **DNS2**, and **Domain** fields.
6. To save and execute the configurations, click **Apply**.
7. To see the IP Address, MAC address and lease time for each of the active clients, click **Show Client**.

   The **Active DHCPv6 Clients** window displays the following parameters in a **DHCPv6 Client Table**:

Parameter	Description
IP Address	IP address of the DHCPv6 client.
Client DUID	MAC address of the DHCPv6 client.
Expired Time	Lease time configured for the DHCPv6 client.

Configure Router Advertisement for the Device

You can advertise the device as a router by configuring Router Advertisement.

To launch the Router Advertisement pane, click **Services** > **Router Advertisement** in the left navigation pane.

1. To enable router advertisement, select the **Enable** checkbox.
2. Enter the **Advertisement Interval** in seconds. Default is 30 seconds. The range is 10 to 1800 seconds.
3. To obtain an IPv6 address from the DHCPv6 server, select the *on* button for the **Managed Flag**; to turn it off, select the *off* button.
4. To obtain other non-address network parameters from the DHCPv6 server, select the *on* button for the **Other Flag**; to turn it off, select the *off* button.
5. To specify the maximum transmission units that are to be used in the router advertisement messages, enter the **MTU**. The range is 1280 to 1500 bytes. Default is 1492 bytes.
6. To specify the time for which the advertisement messages exist on the route, enter the **Router Lifetime**. It ranges from 0 to 9000 seconds. Default is 1800 seconds.
7. Select the **Router Preference** from the drop-down list. It could be **High**, **Medium**, or **Low**.

8. To save and execute the configurations, click **Apply**.
9. A **Prefix Table** displays the following information about prefix advertisement:

Parameter	Description
Prefix Mode	The mode could be Manual or Prefix Delegation (PD).
IPv6 Prefix	The network prefix of the IPv6 addresses.
Prefix Length	The prefix length of the IPv6 addresses.
Lifetime	Time period for which the IPv6 address remains valid.

Add an Entry to the Prefix Table

1. To add an entry to the Prefix Table, click the button.
2. Select **PD** or **Manual** from the **Prefix Mode** drop-down list, according to your network requirements.
3. Enter the **IPv6 Prefix**.
4. Enter the IPv6 address **Prefix Length**.
5. Enter the **Lifetime** in seconds.
6. To save and add the entry, click **Apply**.

Modify an Entry in the Prefix Table

1. To edit an entry in the Prefix Table, select the entry.
2. Click the button.
3. Modify the required field values.
4. To save and execute the changes, click **Apply**.

Delete an Entry from the Prefix Table

1. To delete an entry from the Prefix Table, select the entry.
2. Click the button.
3. Click **Apply**.

Configure Layer 2 and Routing

You can perform the following tasks to configure the device for Layer 2 and Routing aspects:

- View the ARP Table Entries
- Configure MAC Address Aging
- Configure Routing Parameters
- Configure Loop Detection
- Configure Spanning Tree

View the ARP Table Entries of the Device

The Address Resolution Protocol (ARP) Table stores the association between an IP Address and a MAC Address.

Note:

This feature is not available when the ONT operates in the Single Family Unit (SFU) mode.

To launch the **ARP Table** pane, click on **Advanced** > **ARP Table** from the left navigation pane.

The **User List** panel displays the following information:

- **IP Address**
- **MAC Address**

Configure the MAC Address Aging Time for the Device

MAC Address aging time specifies the time after which an entry in the MAC Address table expires and is discarded from the table.

To launch the **MAC Table** pane, click on **Advanced** > **Mac Table** from the left navigation pane.

Edit Aging Time

1. On the **MAC Address Aging Time** panel, enter a new value in the **Aging Time** field.
   Aging Time can range between 0 and 65535 seconds. By default, the aging time is 300 seconds.
2. To save and execute the configuration, click **Apply**.

View MAC Address Information

The **MAC Address Table** displays the following information:

Parameter	Description
Port	The port on the device.
MAC Address	MAC Address of the device.
Aging Timer	Aging time configured for the device.

Configure Routing Information

The device forwards packets using the information from the IP Route Table or the Static Route Table.

Note:

This feature is not available when the ONT operates in the Single Family Unit (SFU) mode.

To launch the **Routing Configuration** pane, click on **Advanced** > **Routing** from the left navigation pane.

Configure Route Data

1. To add a new route data:
   a. On the **Static Route Table** panel, click the + button.
   b. Select the **Enable** check box.
   c. Enter the following information
      - **Destination IP Address**: IP address of the destination host.
      - **Subnet Mask**: subnet mask for the IP address.
      - **Next Hop**: IP address of the next hop.
      - **Metric**: determines which route to choose.
      - **Interface**: the interface that routes the packets.
   d. Click **Apply** to save the entry in the table.
2. To edit a route data:
   a. On the **Static Route Table** panel, click the button.
   b. Modify the field values as required.
   c. Click **Apply**.
3. To delete a route data:
   a. To delete a route data from the **Static Route Table**, click the button.
   b. To save the changes, click **Apply**.

View IP Route Information

The **IP Routing Table** displays the following information:

Parameter	Description
State	Status of the entry in the Routing Table: *Enabled* or *Disabled*.
Destination	IP address of the destination host.
Subnet Mask	Subnet mask for the IP address of the destination.
Next Hop	IP address of the next hop, which is the gateway IP address.
Metric	Determines which route to choose. Default is 0.
Interface	The interface that routes the packets.

Configure IPv6 Routing Information

The device forwards packets using the information from the IPv6 Route Table or the Static Route Table.

To view and manually configure the IPv6 Static Route Table, launch the **IPv6 Static Routing Configuration** pane.

View IPv6 Static Routing Information

Click on **Advanced** > **IPv6 Routing** in the left navigation pane. The **IPv6 Static Routing Table** displays the following parameters:

Parameter	Description
State	Status of the entry in the Routing Table: *Enabled* or *Disabled*.
Destination	IPv6 address of the destination host.
Next Hop	IPv6 address of the next hop, which is the gateway IP address.
Metric	Determines which route to choose. Default is 0.
Interface	The interface that routes the packets. Options are *Management*, *Internet*, and *Any*.

Add a new IPv6 Static Routing Entry

1. Click on **Advanced** > **IPv6 Routing** in the left navigation pane.
2. In the **IPv6 Static Routing Table**, click the button.
3. Select the **Enable** checkbox.
4. Enter the following information:
   - **Destination** IPv6 address
   - Its **Next Hop** IPv6 address which is the gateway address
   - **Metric** which determines which route to choose
   - **Interface** that routes the packets
5. To save and add the entry, click **Apply**.

Modify an IPv6 Static Route Entry

1. Click on **Advanced** > **IPv6 Routing** in the left navigation pane.
2. In the **IPv6 Static Routing Table**, click the button.
3. Enter the changes required.
4. To save and update the route data, click **Apply**.

Delete an IPv6 Static Route Entry

1. Click on **Advanced** > **IPv6 Routing** in the left navigation pane.
2. In the IPv6 Static Routing Table, click the button.
3. To save the changes, click **Apply**.

Configure MLD Proxy on the Device

To configure the device as a Multicast Listener Discovery (MLD) proxy, launch the MLD Proxy Configuration pane.

1. To launch the **MLD Proxy Configuration** pane, click on **Advanced** > **MLD Proxy** in the left navigation pane.
2. Enter the **Robust Count**.
3. Enter the **Query Interval** in seconds.
4. Enter the **Query Response Interval** in milliseconds.
5. Enter the **Response Interval of Last Group Member** in seconds.
6. To save and execute the configuration, click **Apply**.

Configure Loop Detection on the Device

Loop Detection helps you identify loops in a network. A network loop occurs when there is more than one path between the same set of source and destination.

When an interface is configured for loop detection, the device sends loop detection packets through the interface. If a loop is detected and the device receives the same packet, it shuts down the interface that received the packet.

Note:

Loop Detection is enabled by default.

Define the following parameters to set up loop detection:

- **Detection Interval:** sets the time period between sending loop packets.
- **Interface Recovery Interval**: sets the period that the device waits before reenabling the interface that was shut down because of loop detection.

Note:

You cannot enable Loop Detection and Spanning Tree together on the device.

To launch the **Loop Detection** pane, click on **Advanced** > **Loop Detection** from the left navigation pane.

Configure Loop Detection

1. To enable loop detection, select the **Enable** radio button on the **Loop Detection Enable** tab.
2. Enter the detection interval in seconds in the **Detection Interval** field.
   By default, the detection interval is 5 seconds.
3. Enter the recovery interval in seconds in the **Recovery Interval** field.
   By default, the recovery interval is 300 seconds.
4. To save and execute the configuration, click **Apply**.

View Loop Detection Information

The **Loop Detection Status** panel displays the following information:

Parameter	Description
LAN Port	Displays the LAN port.
Loop Status	Displays the loop status of the LAN port.

Disable Loop Detection

1. To disable loop detection, select the **Disable** radio button on the **Loop Detection Enable** tab.
2. To save and execute the configuration, click **Apply**.

Configure Spanning Tree

Spanning Tree is disabled by default.

Note:

You cannot enable Loop Detection and Spanning Tree together on the device.

To launch the **Spanning Tree** pane, click on **Advanced** > **SpanningTree** from the left navigation pane.

View Spanning Tree information

To view spanning tree information, select the **Enable** radio button on the **Spanning Tree State** tab.

The **STP Interface Info Table** displays with the following information:

Parameter	Description
Interface	The device interface on which STP is enabled.
Port State	State of the interface: *Enabled* or *Disabled*.
Designated Bridge ID	Identifier of the root bridge.

Disable Spanning Tree

1. To disable spanning tree, select the **Disable** radio button on the **Spanning Tree State** tab.
2. To save and execute the configuration, click **Apply**.

Configure QoS Traffic Limiting

Traffic Limiting regulates the traffic flow by imposing a maximum traffic rate for each port's egress queue. Packets that exceed the threshold are placed in the queue and are transmitted later. Traffic limiting rate is configured in kilobits per second (kbps).

Note:

This feature is not available when the ONT operates in the Single Family Unit (SFU) mode.

To launch the **IP QoS Traffic Limiting** pane, click on **IP QoS** > **QoS Traffic** from the left navigation pane.

Configure Total Upstream Bandwidth Limit

1. On the **Total Upstream Bandwidth Limit** panel, select the **Enable** radio button.
2. Enter the bandwidth limit in kbps in the **Total Upstream Bandwidth Limit** field.
   By default, the total upstream bandwidth is 100000 kbps.
3. To save and execute the configuration, click **Apply**.

Disable Total Upstream Bandwidth Limit

1. On the **Total Upstream Bandwidth Limit** panel, select the **Disable** radio button.
2. To save and execute the configuration, click **Apply**.

Configure IP QoS Traffic Limiting

1. On the **IP QoS Enable** tab, select the **Enabled** radio button.
   The **IP QoS Traffic Limiting** panel displays the following information:

Parameter	Description
IP Version	IPv4 or IPv6 versions of Internet Protocol.
Interface	The interface on which the Traffic Shaping is applied. This is a WAN interface on the device.
Direction	Traffic direction: Upstream or Downstream traffic.
Protocol	The protocol packets that are affected by Traffic Shaping. You can choose from *TCP*, *UDP*, or *ICMP*. *ANY* specifies that Traffic Shaping is applied to all protocol packets.
Source IP	IP address and subnet mask of the egress interface.
Destination IP	IP address and subnet mask of the destination interface.
Source Port	The egress port on which the traffic originates.
Destination Port	The port on which the traffic terminates.
Rate	Maximum Traffic rate specified in kilobits per second (kbps).

2. To add an entry:
   a. Click the + button.
   b. Enter the required QoS parameters.
   c. Click **Apply**.
3. To edit an entry:
   a. Select an entry
   b. Click the edit button.
   c. Modify the field values as required.
   d. Click **Apply**.
4. To delete an entry:
   a. Select an entry
   b. Click the delete button.

Disable IP QoS Traffic Limiting

1. On the **IP QoS Enable** tab, select the **Disabled** radio button.
2. To save and execute the configuration, click **Apply**.

Configure Voice Over IP

You can configure the device to deliver voice communications and multimedia sessions over the IP network.

Note:

This feature is not available on the CGP-ONT-4P model.

Configure Port Parameters on the Device for Voice over IP

You can configure the Foreign Exchange Subscriber (FXS) ports on the device to support VoIP traffic. FXS ports allow you to connect analog devices to a VoIP system. Both FXS1 and FXS2 ports have similar configurations.

To launch the **Port1** pane, click on **VoIP** > **Port1** from the left navigation pane. To launch the **Port2** pane, click on **VoIP** > **Port2**.

View the Proxy Settings

The **Proxy** panel displays the following information:

Parameter	Description
Name	An easily identifiable name for the VoIP port.
Phone Number	Phone number of the user.
User ID	Login identity of the user that registers with the SIP Proxy.
Password	Password for the User ID.
Proxy	Enable or disable the primary SIP Proxy function.
Proxy Addr	IP address of the primary SIP Proxy Server that is provided by the Internet Service Provider (ISP).
Proxy Port	Port number that is used for the communication between the primary SIP Proxy Server and the VoIP terminal, provided by the ISP. Proxy Port numbers range between 1024 and 65535. The default proxy port is 5060.
SIP Subscribe	Enable or disable the call reminder function.
SIP Domain	Domain name of the SIP Proxy Server.
Reg Expire	The period (in seconds) for which the registration of the client with the SIP Proxy server is valid. The default time is 3600 seconds.
Outbound Proxy	Enable or disable the secondary SIP Proxy function.
Outbound Proxy Address	IP Address of the secondary SIP Proxy Server, which is provided by the ISP.
Outbound Proxy Port	The port that is used for communication between the secondary SIP proxy server and the VoIP terminal. This port is provided by the ISP. The port number ranges from 1024 to 65535. By default, 5060 is the outbound proxy port.
Enable Session Timer	Enable or disable a timer for the SIP session.
Session Expire(sec)	Time (in seconds) after which the SIP session expires. By default, the session expires after 1800 seconds.

View the SIP Advanced Settings

The **SIP Advanced** panel displays the following information:

Parameter	Description
SIP Port	The port that is used for communication between the SIP proxy server and the VoIP terminal. The port number ranges from 1024 to 65535. By default, the SIP port number is 5060.
Media Port	The port that is used for communication between the SIP proxy server and the VoIP terminal. The port number ranges from 1024 to 65535. By default, the Media port number is 9000.
DTMF Relay	Dual Tone Multifrequency (DTMF) tones relayed between the end points on a SIP call. Options available are RFC2833, SIP INFO, Inband, DTMF_delete.
DTMF RFC2833 Payload Type	RTP Payload type number that indicates that the transmitted packets contain DTMF digits. The default number is 96.
DTMF RFC2833 Packet Interval (msec)	The duration of DTMF event is determined by the DTMF packet interval, which is denoted in milli seconds. It is 10 milli seconds by default.
Use DTMF RFC2833 PT As Fax/Modem	Enables the DTMF payload to be a Fax or a Modem.
Fax/Modem RFC2833 Payload Type	RFC 2833 specified payload type for Fax or Modem. Default payload type number is 101.
Fax/Modem RFC2833 Packet Interval (msec)	DTMF packet interval when Fax or Modem is the payload type. Default packet interval is 10 milli seconds.
SIP INFO Duration (ms)	Minimum signal duration when SIP INFO method is used for DTMF tone generation. Default value is 250 milliseconds.
Call Waiting	Call waiting supplementary service allows incoming calls to come through even if your phone is busy.
Call Waiting Caller ID	Call Waiting Caller ID service displays the phone number of the incoming call.
Reject Direct IP Call	Restricts the users from making a direct call to another VoIP phone, by dialing its IP address. A direct IP call does not connect through a server.
Send Caller ID Hidden	This service prevents the phone number of the caller being displayed on the receiver's phone.
Call Transfer	Call Transfer service allows you to transfer the call to another phone.
Three-way Conference	Three-way conference service allows three users to communicate on the same call.
Conference On Server/ONT	Use either the SIP Server or ONT as a bridge for a conference call.

Parameter	Description
Conference-uri	A SIP conference is identified by its unique Uniform Resource Identifier (URI). This URI identifies the focus that is responsible for the conference.

View the Dial Plan Settings

The **Dial Plan** panel displays the following information:

Parameter	Description
Enable Dialplan	You can define a custom Dialplan for a SIP Call or let the default Dialplan process and route the SIP call.
Dial Plan	Defines a custom Dialplan.

Edit the Port Parameters for Voice over IP

1. In the **Proxy** panel, enter the required proxy settings in the relevant fields.
2. In the **SIP Advanced** panel, enter the required SIP Advanced settings in the relevant fields.
3. In the **Dial Plan** panel, enter the required Dial Plan settings in the relevant fields.
4. To save and execute the configuration, click **Apply**.

Configure SIP Support for T.38 FAX Media Session

T.38 is an ITU standard that defines the process for carrying fax services across IP networks.

1. To launch the **T.38** pane, click on **VoIP** > **Other** from the left navigation pane.
2. To configure the network for T.38 protocol, select the **Enable** check box.
3. Select a country from the **Country** drop-down list.
4. To save the configuration, click **Apply**.

Configure Firewall

You can enhance the security of the device by setting up a firewall, which includes the following tasks:

- Configure Port Filtering
- Configure MAC Filtering
- Configure Port Forwarding
- Configure URL Blocking
- Configure Parental Control
- Configure DMZ

Note:

This feature is not available when the ONT operates in the Single Family Unit (SFU) mode.

Configure Port Filtering on the Device

IP Filtering or Port Filtering firewall lets you restrict certain types of data packets from entering the device. You can set up rules to permit or deny packets that contain certain IP Addresses or ports. IP Filtering or Port Filtering helps in securing your local network.

To launch the **IP/Port Filtering** pane, click on **Firewall** > **IP/Port Filtering** from the left navigation pane.

Set the Default Action

1. To set the default action to allow, select the **Allow** radio button on the **Default action** panel.
   To set the default action to deny, select the **Deny** radio button.
2. To save the configuration, click **Apply**.

Configure Current Filter Table

1. To add an entry:
   a. Click the  button.
   b. Select the protocol whose packets need to be filtered, from the **Protocol** drop-down list. The available options are:
      - *TCP*
      - *UDP*
      - *ICMP*
      - *ANY* : Applies the filtering rules to all the protocols.
   c. Enter the following information:
      - **Source IP Address**
      - **Source Port**
      - **Destination IP Address**
      - **Destination Port**
      - **Rule/Action**
   d. To save the entry, click **Apply**.
2. To edit an entry:
   a. Select the entry
   b. Click the  button.
   c. Modify the field values as required.
   d. To save the entry, click **Apply**.
3. To delete an entry:
   a. Select the entry.
   b. Click the  button.
   c. Click **Apply**.

Configure MAC Filtering

MAC Filtering lets you prevent unauthorized devices from accessing your network. You can configure a list of devices that have access to your network (Allowed List) or configure a list of devices that are not permitted to access your network (Blocked List).

To launch the **MAC Filtering** pane, click on **Firewall** > **MAC Filtering** from the left navigation pane.

Configure Allowed List or Blocked List

Note:

You can select only one mode at a time.

1. To configure an allowed list, select the **Allowed List** radio button on the **Mode** panel.
   To configure a blocked list, select the **Blocked List** radio button on the **Mode** panel.
2. To save and execute the configuration, click **Apply**.

Configure Current Filter Table

1. To add an entry:
   a. Click the + button.
   b. Enter the MAC address of the device that you want to either permit or deny access to in the **MAC Address** field.
   c. Repeat Steps a and b to add more entries.
   d. To save the configuration, click **Apply**.
2. To edit an entry:
   a. Select the entry.
   b. Click the edit button.
   c. Modify the field values as required.
   d. To save the configuration, click **Apply**.
3. To delete an entry:
   a. Select the entry.
   b. Click the delete button.
   c. Click **Apply**.

Configure Port Forwarding

The Port Forwarding service automatically redirects common network services to a specific device behind the Network Address Translation (NAT) firewall. Use port forwarding when you want to host a server on your private local network behind your gateway's NAT firewall.

To launch the **Port Forwarding** pane, click on **Firewall** > **Port Forwarding** from the left navigation pane.

Enabling or Disabling Port Forwarding

1. To enable port forwarding, select the **Enable** radio button on the **Port Forwarding** panel.
   To disable port forwarding, select the **Disable** radio button.
2. To save and execute the configuration, click **Apply**.

View the Current Forwarding Table Information

The **Current Port Forwarding Table** displays the following information:

Parameter	Description
Predefined Application	Applications predefined in the system: *DNS*, *NTP*, *AUTH*, *NNTP*, *Mail*, *SSH*, *FTP*, *SNMP*, *TFTP*, *HTTP*, and so on.
UserDefined Application	Application defined by the user.
IP Address	IP address of the interface.
Protocol	Protocol used by the application: *TCP*, *UDP*, or *Both*.
Local Port	Port that receives the forwarded packets.
Public Port	Port that forwards the packets.
Interface	WAN interface of the device.

Configure Current Forwarding Table

1. To add an entry:
   a. Click the + button.
   b. Select a service from the **UserDefined Application** drop-down list.
   c. Enter the IP Address of the interface in the **IP Address** field.
   d. Select the protocol used by the service, from the **Protocol** drop-down list. It can be *TCP*, *UDP* or *Both*.
   e. Enter the range of the port numbers that get the forwarded packets, in the **Local Port** field.
   f. Enter the range of port numbers from which the packets are forwarded, in the **Public Port** field.
   g. Select the WAN interface on the device from the **Interface** drop-down list.
   h. To save the configuration, click **Apply**.
2. To edit an entry:
   a. Select the entry.
   b. Click the edit button.
   c. Modify the field values as required.
   d. To save the entry, click **Apply**.
3. To delete an entry:
   a. Select the entry.
   b. Click the delete button.

Configure URL Blocking

You can configure the device to block certain webpages based on their URLs or the keywords present in the webpages. Update the **URL Blocking Table** with details of the website address and update the **Keyword Filtering Table** with the keyword to block.

To launch the **URL Blocking** pane, click on **Firewall** > **URL Blocking** from the left navigation pane.

Enable or Disable URL Blocking

1. To enable URL blocking, select the **Enable** radio button on the **URL Blocking** panel.
   To disable URL blocking, select the **Disable** radio button.
2. To save and configure the configuration, click **Apply**.

Configure URL Blocking Table

1. To add a domain name that is to be blocked:
   a. On the **URL Blocking Table** panel, click the + button.
   b. Enter the **Domain name**.
   c. To save the configuration, click **Apply**.
2. To edit an entry in the **URL Blocking Table**:
   a. Select the entry.
   b. Click the edit button.
   c. Modify the field values as required.
   d. To save the entry, click **Apply**.
3. To delete an entry from the **URL Blocking Table**:
   a. Select the entry.
   b. Click the delete button.
   c. Click **Apply**.

Configure Keyword Filtering Table

1. To add a keyword to be filtered:
   a. On the **Keyword Filtering Table** panel, click the + button .
   b. Enter the keyword in the **Filtered Keyword** field.
   c. To save the configuration, click **Apply**.
2. To edit an entry in the **Keyword Filtering Table**:
   a. Select the entry.
   b. Click the edit button.
   c. Modify the field values as required.
   d. To save the entry, click **Apply**.

3. To delete an entry from the **Keyword Filtering Table**:
   a. Select the entry.
   b. Click the  button.
   c. Click **Apply**.

Configure Parental Control

You can set up parental controls on your network to restrict internet access for certain IP Addresses and MAC Addresses for a specified time period. Update the **Parental Control Table** with the IP addresses of the devices that are not permitted to access the internet on a certain day, between a certain time period.

To launch the **Parental Control** pane, click on **Firewall** > **Parental Control** from the left navigation pane.

Enable or Disable Parental Control

1. To enable parental control, select the **Enable** radio button on the **Parental Control Enable** panel.
   To disable parental control, select the **Disable** radio button.
2. To save and execute the configuration, click **Apply**.

View Current Parent Control Table Information

The **Current Parental Control Table** displays the following information:

Parameter	Decription
Name	Unique name for the record.
Specified PC	A PC specified by IP address or MAC address.
Start IP	The starting IP in the range of host IP address.
End IP	The ending IP in the range of host IP address.
MAC Address	MAC Address of the PC.
Days	Specifies the day(s)of the week.
Start Time	Start time of parental control.
End Time	End time of parental control.

Configure Current Parent Control Table

1. To add an entry:

   a. On the **Current Parental Control Table** panel, click the  button.
   b. Enter a unique name for this entry in the **Name** field.
   c. To specify the device, do the following:

      - To specify the device based on the IP address, select the IP address from the **Specified IP** drop-down list.

        Enter the range of IP addresses in the **Start IP** and **End IP** fields.
      - To specify the device based on the MAC address, select the MAC address from the **Specified IP** drop-down list.

        Enter the MAC address of the device in the **MAC Address** field.

   d. To select the days of the week, select the required check box in the **Days** column.
   e. To set the time period, enter the **Start Time** and **End Time** in hours:minutes format.
   f. To save the configuration, click **Apply**.
2. To edit an entry in the **Current Parental Control Table**:

   a. Select the entry and click the  button.
   b. Modify the field values as required.
   c. To save the edit, click **Apply**.
3. To delete an entry from the **Current Parental Control Table**:

   a. Select the entry and click the  button.
   b. Click **Apply**.

Configure Demilitarized Zone for the Network

A Demilitarized Zone (DMZ) is a sub-network that is behind a firewall but is open to the public. By placing public services like Web server, or SMTP email server, or DNS server on the DMZ, you can let unrestricted access to these services while restricting access to the local private network.

1. To launch the **DMZ** pane, click on **Firewall** > **DMZ** from the left navigation pane.
2. To activate the DMZ host, select the **Enable** radio button on the **DMZ-host** tab.

   To disable the DMZ host, select the **Disable** radio button.
3. To configure DMZ on a host device, enter the IP address of the host in the **DMZ-host IPaddress** field.
4. To save and execute the configuration, click **Apply**.

Monitor

View the Status of a Device

The **Device Status** pane allows you to monitor and troubleshoot the device.

To launch the **Device Status** pane, click on **Status and Statistics** > **Device Status** from the left navigation pane.

The **Device Status** pane displays the following information:

Section	Parameters Displayed
System	**Device Name**: Name of the device being monitored. **PON Serial Number**: Unique identification number of the PON device. **Uptime**: Time period for which the device has been up and running. **Current System Time**: Displays the current time in GMT. **Firmware Version**: Version of firmware installed on the device. **Firmware MD5 Checksum**: A 32-character hexadecimal number that helps in ensuring digital integrity and security of the firmware. **CPU Usage**: The percentage of CPU utilization. **Memory Usage**: The percentage of memory utilization.
LAN Configuration	**IP Address**: IP address of the device. **Subnet Mask**: Subnet mask for the network. **DHCP Server**: Status of the DHCP server: *Enabled* or *Disabled*. **MAC Address**: MAC Address of the device.
POTS Register Status	Status of the telephone ports: **POTS1**: Status of POTS1 connection: *Enabled*, *Disabled*, *Registered*, or *Register Fail*. **POTS2**: Status of POTS2 connection: *Enabled*, *Disabled*, *Registered*, or *Register Fail*.

Section	Parameters Displayed
WAN Configuration	A WAN Configuration table displays the following parameters: **WAN Name**: Name of the WAN network. **Interface**: Interface that is configured as a WAN port. **VLAN ID**: Identity number of the VLAN. **Service Type**: The type of service provided by the WAN network through this port: *INTERNET*, *VOICE*, *TR069*, *TR069_INTERNET*, *VOIP_INTERNET*, *TR069_VOICE*, *TR069_VOICE_INTERNET* . **Connection Type**: Type of connection that is established by this WAN port with other devices. **IP Address**: IP address configured on this WAN port. **Gateway**: IP address of the gateway. **Primary DNS**: The IP addresses of the Primary DNS Server. **Secondary DNS**: The IP addresses of the Secondary DNS Server. **Status**: State of the interface: *Up* or *Down*.
Interface Statistics Table	Statistics of the number of packets transmitted and received on an interface.
PON Statistics Table	Overall statistics of the number of packets transmitted and received on the device. This includes the unicast packets, multicast packets, and broadcast packets.

View the Status of the PON network

The **PON Status** pane allows you to monitor the PON network.

To launch the **PON Status** pane, click on **Status and Statistics** > **PON Status** from the left navigation pane.

The **PON Status** pane displays the following information:

Parameter	Description
Temperature	Working temperature of the device.
Voltage	Supply voltage for the device.
Transmitting Power	The transmitting power of the device, in dBm.
Receiving Power	The receiving power of the device, in dBm.
Bias Current	Bias current of the device.
ONT State	Status of the ONT device.
ONT ID	Identity number of the ONT device.

View the Unique Device Identification (UDI) Information

The **UDI Status** pane allows you to view the device information. This information is unique to a device.

To launch the **UDI Status** pane, click on **Status and Statistics** > **UDI Status** from the left navigation pane.

The **UDI Status** pane displays the following information:

Parameter	Description
Product ID	Unique identifier of the device
Product Serial Number	Serial number of the device
Hardware version	Hardware version of the device

View the Status of Cable TV Network

The **CATV Status** pane allows you to monitor the Cable TV network.

To launch the **CATV Status** pane, click on **Status and Statistics** > **CATV Status** from the left navigation pane.

The **CATV Status** pane displays the following information::

- **Rx Power**: Receiving Power of CATV in dBm.
- **Tx Voltage**: Transmitting Voltage of CATV in dBuV

Note:

This feature is not available on the CGP-ONT-4PV and CGP-ONT-4P models.

View the IPv6 Status

You can view the IPv6 status of the device on the IPv6 Status pane.

To launch the IPv6 Status pane, click **Status and Statistics** > **IPv6 Status** in the left navigation pane.

You can view the LAN configuration, WAN configuration and Prefix Delegation information.

The **LAN Configuration** section displays the following parameter values:

Parameter	Description
IPv6 Status	Status of IPv6: *Enabled* or *Disabled*
IPv6 Address	IPv6 address of the device.
IPv6 Link-Local Address	IPv6 link-local address.

The **WAN Configuration** table displays the following parameter values:

Parameter	Description
WAN Name	Name of the Wide Area Network.
Interface	Interface that is configured as a WAN port.
VLAN ID	Identity number of the VLAN.

Parameter	Description
Service Type	Type of service that is provided by the WAN network through the WAN port. It could be any of the following: ▪ INTERNET ▪ VOICE ▪ TR069 ▪ TR069_INTERNET ▪ VOIP_INTERNET ▪ TR069_VOICE ▪ TR069_VOICE_INTERNET
Connection Type	Type of connection that is established by the WAN port with other devices.
IP Address	IP address of the WAN port.
Gateway	IP address of the gateway.
DNS1	IP address of the Primary DNS Server.
DNS2	IP address of the Secondary DNS Server.
IPv6 Link-Local Address	IPv6 link-local address on this WAN port.
Status	Status of the interface : Up / Down.

View Status of Wireless Local Area Network

The **WLAN Status** page displays the current status of the wireless local area network.

To launch the WLAN Status pane, click **WLAN** > **Status** in the left navigation pane.

You can view the details of the following parameters of the WLAN configuration:

Parameter	Description
Mode	AP by default.
Band	WiFi network frequency band.
SSID	Service Set Identifier.
Channel Number	The number of the WLAN channel that is configured in the network.
Encryption	Type of encryption.
BSSID	Broadcast Service Set Identifier.
Associated Clients	Number of users connected.

Maintain

Upgrade Firmware

To launch the **Firmware Upgrade** pane, click on **Administration** > **Firmware Upgrade** from the left navigation pane.

Note:

Do not power off the device during the upgrade.

1. To select the file from its saved location, select one of the following radio buttons:
   - **Select file from PC**
   - **Select file from USB storage**
2. To reset all configurations and restore factory settings after the upgrade, select the **Reset all configurations/settings to factory defaults** check box.
3. To locate and select the firmware file to upgrade, click the **Browse** button.

   Select the upgrade file and click the **Open** button.
4. Click the **Upgrade** button.

Perform Diagnostic Functions

You can test whether a device is reachable or not. You can also trace the IP route of the device.

Note:

This feature is not available when the ONT operates in the Single Family Unit (SFU) mode.

To launch the **Ping or Trace on IP Address** pane, click on **Administration** > **Diagnostics** from the left navigation pane.

Ping an IP Address

1. Select the **Interface** from which a ping is sent out.
2. Enter the IP address of the device in the **IP Address** field or the domain name of the device in the **Domain Name** field.
3. To test whether the device is reachable or not, click the **Ping** button.

   The ONT device pings the specified address and shows the output of the ping.

Trace an IP Address

1. Select the **Interface** on which a traceroute command is executed.
2. Enter the IP address of the device in the **IP Address** field or the domain name of the device in the **Domain Name** field.
3. To trace the IP route of the device, click the **Traceroute** button.

   The ONT device executes the `traceroute` command on the specified IP address or domain name and displays the output of the command.

Perform a Backup and Restore the Settings

You can save the current configuration of the device to a file for reuse. You can import a configuration file to restore the settings on a device.

To launch the **Backup and Restore Settings** pane, click on **Administration** > **Backup/Restore** from the left navigation pane.

Import a Configuration File

1. To select the file from its saved location, select one of the following radio buttons:
   - **Select file from PC**
   - **Select file from USB storage**
2. To locate and select the firmware file to upgrade, click the **Browse** button.

   Select the upgrade file and click the **Open** button.
3. To save and execute the configuration, click **Apply**.

Export a Configuration File

1. To export or backup the device configuration, select one of the following buttons:
   - To backup the device configuration to a computer, click **Backup to PC**.
   - To backup the device configuration to a USB device, click **Backup to USB**.
2. To save and execute the configuration, click **Apply**.

Reboot the Device

You can reboot the device after committing the changes to the system memory or reboot the device to restore the factory default settings on the device.

1. To launch the **Reboot** pane, click on **Administration** > **Reboot** from the left navigation pane.
2. To reboot the device, select the **Reboot the device** radio button.
3. To restore the factory settings after reboot, select **Return to factory default settings after reboot** radio button.

4. For the ONT device to operate as a Home Gateway Unit after reboot, select the **Change to HGU** check box.

   An ONT device can operate either as a Home Gateway Unit (HGU) or a Single Family Unit (SFU).

   An HGU supports Layer 2 bridging, Layer 3 routing, and Layer 4 Network Address Translation (NAT). An SFU supports only Layer 2 bridge forwarding.

   This table mentions the operating modes of the Cisco Catalyst ONT models:

ONT Model	Operating Mode
CGP-ONT-4P	HGU or SFU. Default mode is SFU.
CGP-ONT-4PVC	HGU or SFU. Default mode is HGU.
CGP-ONT-4PV	HGU or SFU. Default mode is HGU.
CGP-ONT-4TVCW	HGU
CGP-ONT-1P	SFU

   CGP-ONT-4P can switch to HGU mode after rebooting.

   Beginning from 1.1.3.17 release, CGP-ONT-4PVC and CGP-ONT-4PV can switch to SFU mode after rebooting.

   When you switch between SFU and HGU mode, we recommend that you clear all configurations and return to factory default settings.

5. Click the **Reboot** button.

   The ONT device restarts.

Administer

Set the Logical ID and Password

A Logical ID (LOID) is a unique identifier for the device, which is provided by the ISP.

Resetting or configuring the LOID and password might result in authentication failure. Exercise caution before performing this configuration.

1. To launch the **GPON Settings** pane, click on **Administration** > **GPON Settings** from the left navigation pane.
2. The existing **LOID** and **LOID Password** are displayed.

   You can modify the LOID and password as required.
3. To save the settings, click **Apply**.

Set Up an Account to Access the Web Server

1. To launch the **Password Configuration** pane, click on **Administration** > **Password** from the left navigation pane.
2. To change the username, enter the new user name in the **New User Name** field.
3. To change the Password, enter the following:
   a. The old password in the **Old Password** field.
   b. The new password in the **New Password** field and the **Confirmed Password** field.

      Note:

      - The password cannot be the same as the user name.
      - The password must be a minimum of eight characters. The eight characters must contain a minimum of three characters that are either numeric, upper case, lower case, or a special character.
4. To save the information, click **Apply**.

View and Export System Logs

You can view the system logs which contain events that are updated by the operating system components. Events are categorised as critical, emergency, error, debug, warning, and so on.

You can set the category of event you want to see and save them for analysis and corrective action.

To launch the **System Log** pane, click on **Administration** > **System Log** from the left navigation pane.

Configure System Logs

1. On the **System Log** tab, select the **Enable** radio button.
2. Select the level of the log from the **Log Level** drop-down list. The available options are:
   - *Emergency*
   - *Alert*
   - *Critical*
   - *Error*
   - *Warning*
   - *Notification*
   - *Informational*
   - *Debugging*
3. Select the category of logs that are displayed on the device console, from the **Display Level** drop-down list. The available options are:
   - *Emergency*
   - *Alert*
   - *Critical*
   - *Error*
   - *Warning*
   - *Notification*
   - *Informational*
   - *Debugging*
4. Select the mode of display from the **Mode** drop-down list. The available options are:
   - *Local*: Displays the logs only on the local device.
   - *Remote*: Displays the logs on a remote device specified by the **Server IP Address** and **Server UDP Port**.
   - *Both*: Displays the logs on the remote and the local device.
5. To save the logs to a USB device connected to the device, select **Enable** on the **Save to USB Automatically** tab.
6. To save and execute the configuration, click **Apply**.

Disable System Logs

1. On the **System Log** tab, select the **Disable** radio button.
2. To save and execute the configuration, click **Apply**.

View the Logs

To see the logs, click the **Show Logs** button.

The **Log Table** displays the following information:

Parameter	Description
Date/Time	Date and time of the message or event.
Facility	The facility to which the message refers (for example, SNMP, SYS, and so forth). A facility denotes the source or the cause of the system message.
Level	Defines the severity of the message or event: *Emergency*, *Alert*, *Critical*, *Error*, *Warning*, *Notification*, *Informational*, and *Debugging*
Message	Event that is recorded in the log table.

Export the Logs

1. To save the logs, click the **Export Logs to PC** button.
2. Provide a location to store the logs when prompted.

Clear Logs

1. To delete the logs, click the **Clear Log** button.
2. Click **Close** when prompted.

Manage Access

You can set the parameters that define different types of access to a device.

1. To launch the **Device Access Settings** pane, click on **Administration** > **Device Access** from the left navigation pane.
2. To set the WAN interface on the device to block public pings, select the **Enable** check box on the **Block WAN Ping** tab.
3. To let a local user telnet access to the device, select the **Enable** check box on the **Local Telnet** tab.
4. To let a user log in to the device remotely and use the web interface, select the **Enable** check box on the **Remote Web Management** tab.

   To select the protocol type, select the **HTTP** and **HTTPS** check boxes.
5. To allow a range of remote IP addresses that can access your device, do one of the following:
   - To allow all IP addresses to access the device, select **Any IP Address** radio button in the **Allowed Remote IP addresses** tab.
   - To allow a fixed set of IP address, enter the IPv4 address range in the **Allowed Remote IP addresses** tab.
6. To save and execute the configuration, click **Apply**.

Set the System Time and Time Zone

Note:

This feature is not available when the ONT operates in the Single Family Unit (SFU) mode.

To launch the **Time** pane, click on **Administration** > **Time** from the left navigation pane.

Configure the System Time and Time Zone

1. Select a new time zone from the **Time Zone** drop-down list.
2. To set the device to obtain the time automatically from an NTP server, select the **Auto** radio button in the **Set Date and Time** tab.
   - To set the device to obtain the time from Default NTP servers, select the **Default** radio button.
   - To define a Custom NTP Server, select the **User Defined** radio button.
     Enter the NTP server details in the **NTP Server 1** and **NTP Server 2** fields.
3. To manually set the system date and time, select the **Manual** radio button in the **Set Date and Time** tab.
   Enter the date and time in the **Enter Date and Time** field.
4. To save and execute the configuration, click **Apply**.

Configure Daylight Savings

1. Select the **Daylight Saving Time** check box.
2. To select the daylight saving mode, do the following:
   - To set the daylight saving for a certain period, select **By Date** .
     Select the dates in **From** and **To**.
   - To set the daylight saving for a recurring period, select **Recurring**.
     Select the dates in **From** and **To**.
3. Select the offset time in **Daylight Saving Offset**.
4. To save and execute the configuration, click **Apply**.

Configure USB Interface

You can enable or disable the USB interface on the device.

To launch the USB Interface pane, click **Administration** > **USB Interface** in the left navigation pane.

To enable the USB interface, select the **Enable** button.

To disable the USB interface, select the **Disable** button.