Predator Connect T7 BE11000 Tri-band Wi-Fi 7 Router

User Manual

V1.0

Revision Apr, 2024

Contents

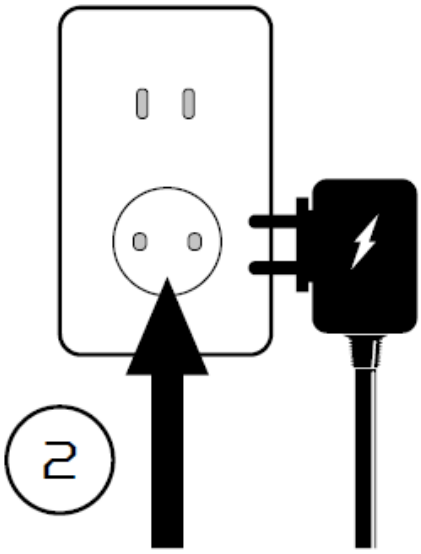
1. Overview

Predator Connect series T7, a whole new Wi-Fi 7 BE11000 wireless router, is optimized for gamers with intensive features and simple setup steps via a 1-2-3 wizard. Unlock the pinnacle of gaming experience with Wi-Fi 7's cutting-edge capabilities, designed for peak data transmission and minimal latency. Wi-Fi 7's MLO is a major technical advancement. Connecting to MLO network enhances throughput, reduces latency, and improves network efficiency. Effectiveness of MLO depends on the AP and STA compatibility. This Wi-Fi router supports band steering Wi-Fi that monitors and organizes the frequency band allocation within a Wi-Fi network. Network Security protection is embedded. Live updates ensure your network is immune from malware and vulnerability threats 24-7. ACS (Automatic Channel Selection) dynamically chooses the most suitable channel for the T7 when you experience interference from nearby SSIDs. Port forwarding profiles for most game consoles (PS5, XBOX, etc.) are readily available inside for gameplay. Hybrid QoS is the best fit for your Predator router, ensuring prioritization of your gaming traffic and bandwidth utilization. The VPN feature provides a secure connection for your device when surfing the website.

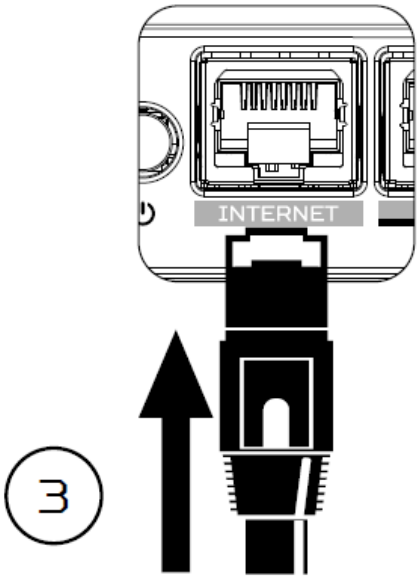
2. Installation and Setup

2.1. Plug in the AC adapter and turn the router power button ON located at the bottom of the device.

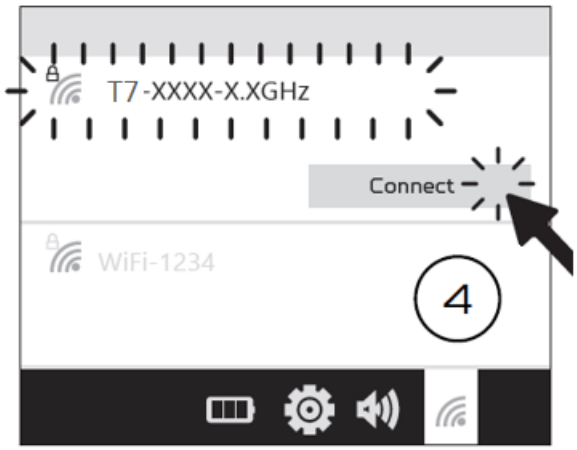
2.2. Plug into an outlet.



2.3 Plug-in Internet cable.



2.4 Connect to Predator T7 Wi-Fi.



2.5 Important info is at the back of the device

2.6 The device can be either setup via Predator Connect mobile App or the browser web admin.

How to setup the router via **Predator Connect Mobile App**:

- Use a mobile device camera to scan the QR code below. Download the Predator Connect mobile App via Play Store or App Store.

Download APP

Available on the App Store

GET IT ON Google Play

- Open the Predator Connect Mobile App and follow the steps for registering an account. Go to your email inbox, review the registration email, and input the 4-digit registration code onto the mobile App. When the whole process is completed, you will be automatically signed in.
- Enable the mobile Wi-Fi function and scan the device QR-code printed on the back label.

The default admin and Wi-Fi password will be automatically exported into the mobile app. (SSID: T7_YYYY)

- Device setup completed.

Setup the router via browser:

- Please make sure that the wireless function on your laptop is already enabled.
- Check the device's back label, and find the router's default SSID (T7_YYYY_2.4GHz) and password and then connect.
- Open the browser on your laptop/desktop, input the device web admin URL: http://acer-connect.com or IP: http://192.168.76.1
- The device will automatically redirect to a quick setup wizard. Follow the easy 1-2-3 steps and get ready to access the internet.

Note: The admin login password requires modification within the setup wizard for first-time use. Please create a strong password and keep it in a safe place. (New password cannot be the same as the prior one.)

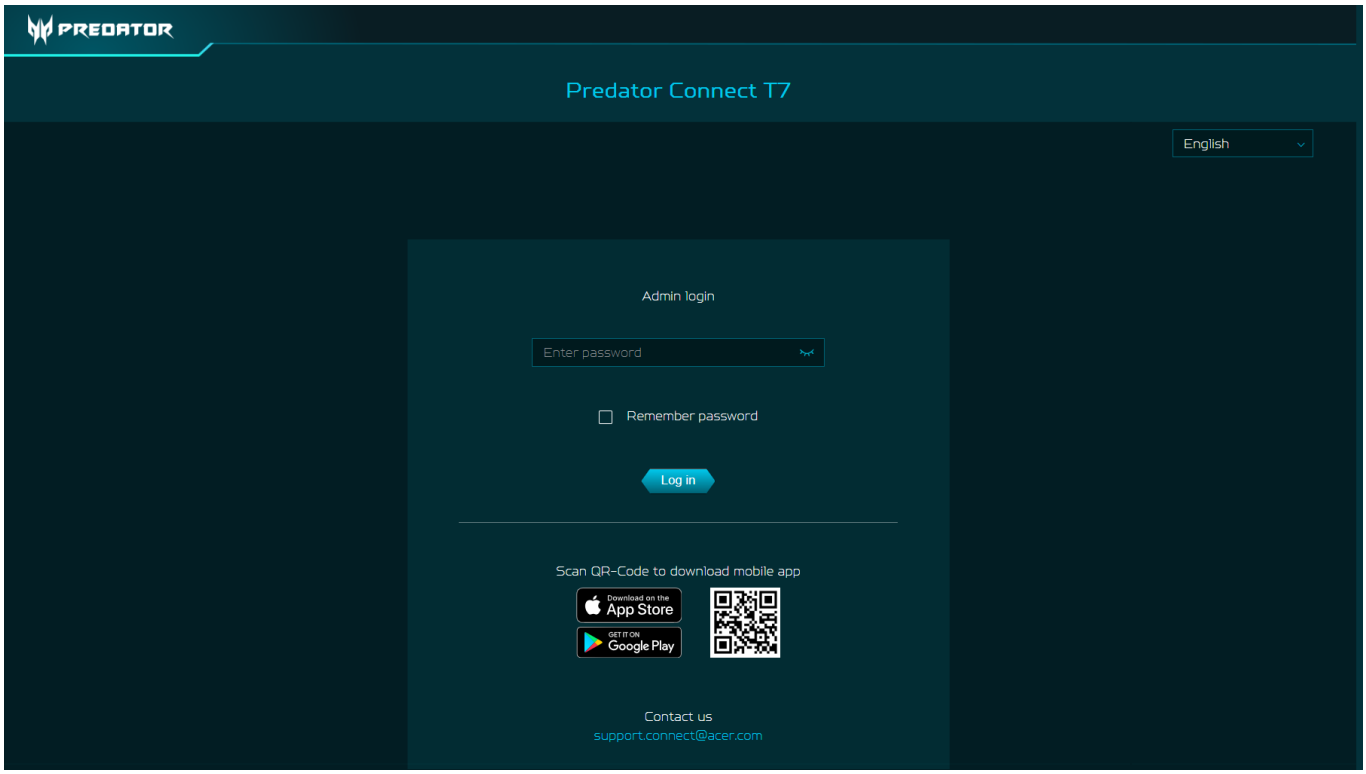
Note: The router web admin portal will automatically lock after five consecutive incorrect attempts. You have to power cycle the router to unlock the web admin.

Note: The SSID Wi-Fi password can't be the same as the admin login password.

Both App & browser can help router to do quick setup. Web UI can execute all functions and settings of router. Mobile App allows the user to remotely control some functions of the router and receive notifications.

3. Initial Configuration

Please log in to the Predator Connect T7 Web Portal (http://acer-connect.com or IP: http://192.168.76.1) by using the current valid Admin password. You can select the language of Web UI by clicking on the drop-down arrow.

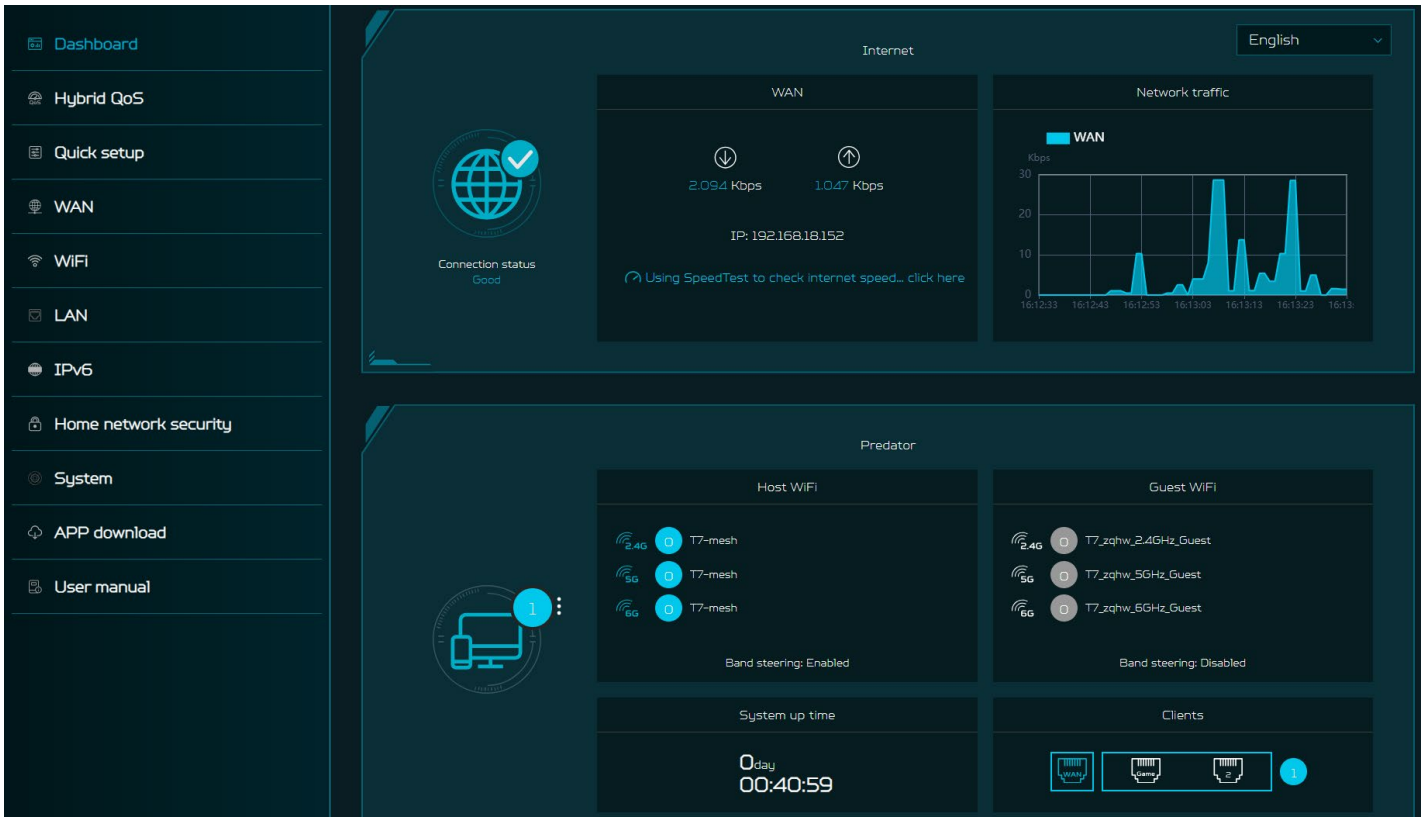


Enter the login password to see the dashboard and other settings of your Predator Connect T7. The router will automatically guide you step by step on how to set up and configure internet access and basic network settings.

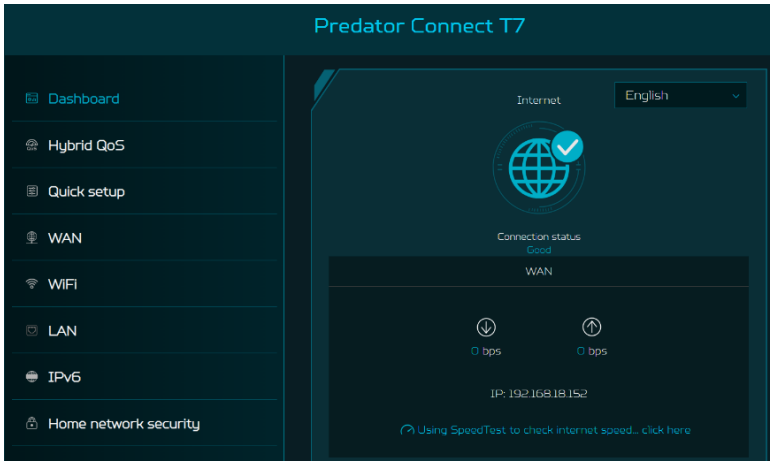
You can scan the QR code (on the login screen using your Android mobile or iPhone) to download the mobile app and manage your router remotely.

4. Dashboard

Once you have successfully logged in, the following key information will be displayed on the Predator Connect T7 dashboard.



Connection Status: shows the current connection status of Internet.

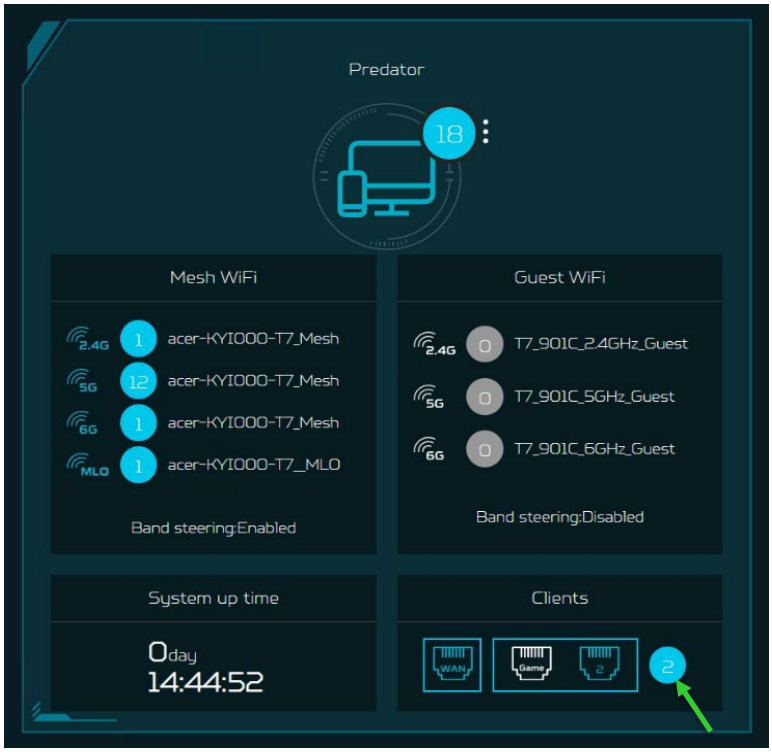


WAN Status: shows WAN connectivity and Download/Upload speed and WAN IP.

Wi-Fi Status: shows the number of wireless client devices connected with 2.4GHz, 5GHz and 6GHz bands. By enabling band steering Wi-Fi, the router monitors and organizes the frequency band allocation within a Wi-Fi network.

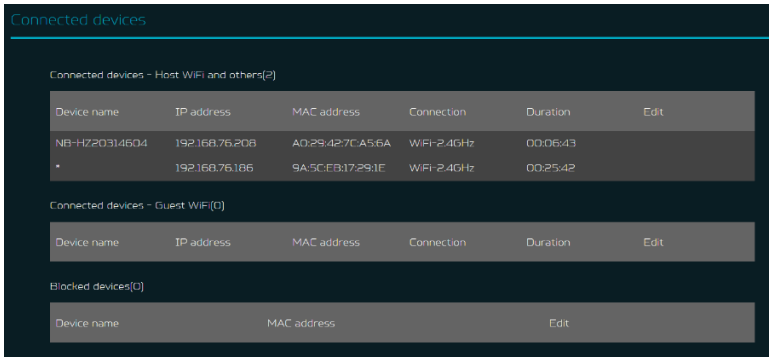
LAN Status: quickly indicates the status of LAN ports. Predator Connect T7 has one WAN port, one Game port and one LAN port. The "icon" (at the far right) represents the number of devices connected to the T7 router. Clicking on this icon will display the table shown below.

System Uptime: shows the system Uptime since the last reboot.

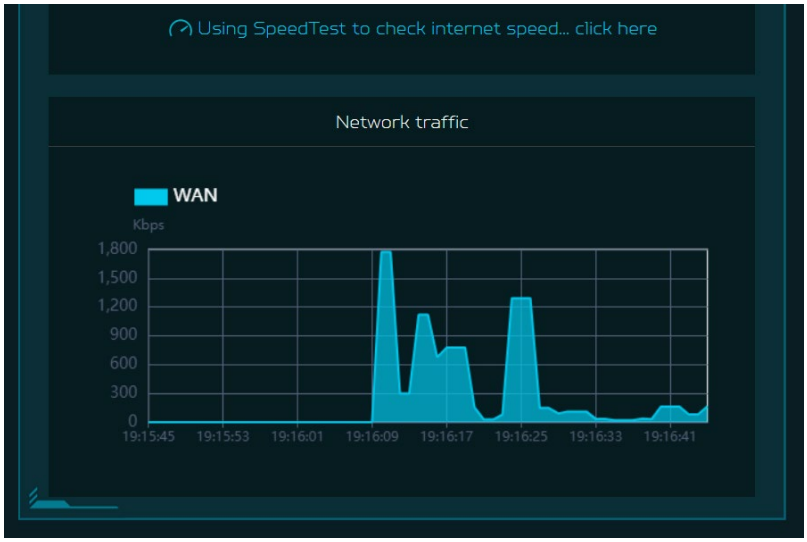


Connected Devices: shows how many client's devices are connected with your Predator Connect T7 through Wi-Fi or LAN. You can also modify the device name by clicking on the pencil icon.

This tab displays the client device name, the IP address allocated by the router, MAC address, mode of connection (whether the device is connected with the router through Ethernet or Wi-Fi), and the duration of device connectivity with the router. You can even block the device from accessing the Internet by clicking on the "block" button.



Network Traffic: helps indicate real time status of the Download (DL) and Upload (UL) speeds across the WAN.



Network Speed Test:

1) Powered by Ookla. A push of the "GO" button tests the speed of the WAN connectivity.
2) You can even manually select the server option. Click on the dropdown arrow and it will display the available servers.
3) Clicking the "Go" Button will test the network speed and display the results as shown in the image below.

It will test and clearly show the network download and upload speed in Mbps, ping rate, and jitter in milliseconds. After getting the speed test results, you have the option to run the speed test again.

5. Hybrid QoS

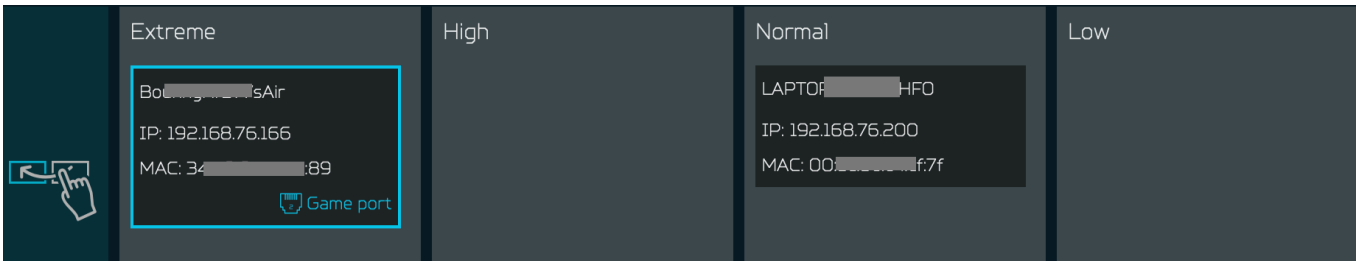
Hybrid QoS combines application priority and device priority. The Killer-Enabled PC can set applications priority and send packets with DSCP values to the Predator Connect T7 router, then the router will classify packets and set priority for all different applications based on the below definition.
For non-Killer-Enabled devices, Predator Connect T7 can identify game consoles, streaming devices, computers, smartphones, and IoT devices in the network and allocate them a priority group according to the default settings, or the user can manually set priority for devices connected to the router.

*Note: Device identification requires the network security engine option enabled.
Application-based QoS* priority: (Enabled by default)

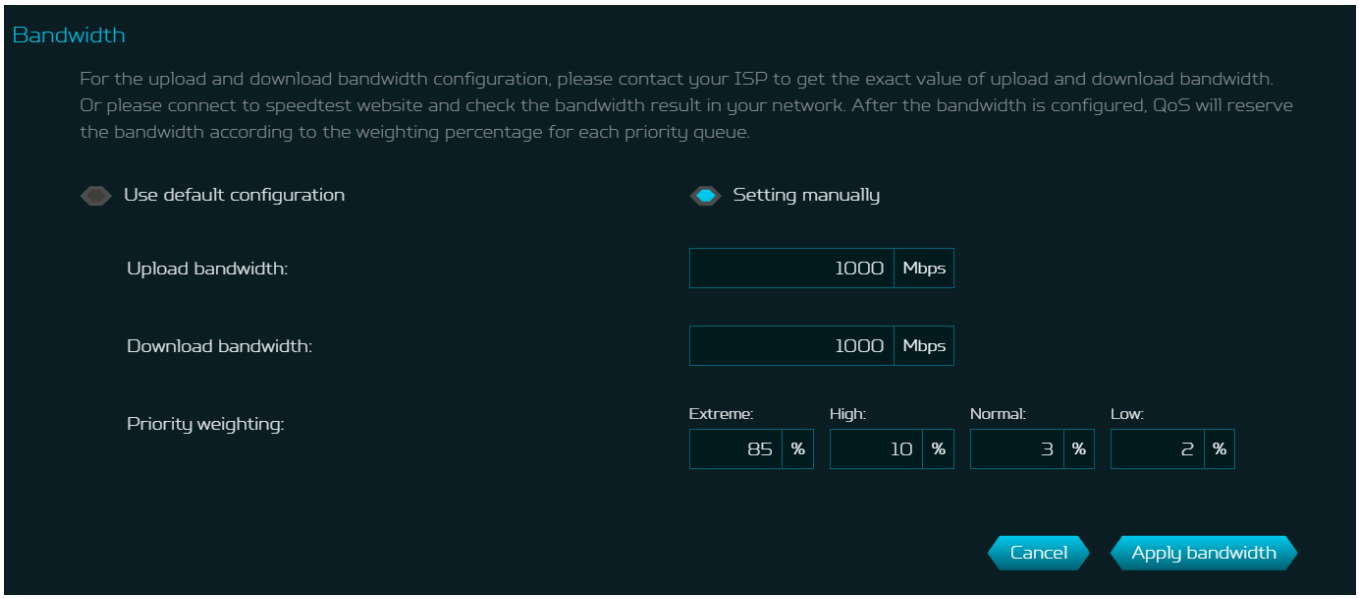
*Note: Application Priority will use the DSCP value in the IP header for packet classification. Laptop/desktop with Killer™ embedded traffic priorities in four grades by application. I.e. Extreme (Games), High (Streaming), Normal (Browsing), Low (Download).

Priority	Extreme (Games)	High (Streaming)	Normal (Browsing)	Low (Download)
Applications (DSCP) Intel Killer Teams/Zoom, GT-Booster	· Killer Priority 1 (Games) · Killer Priority 2 (Real Time)	· Killer Priority 3 (Streaming)	· Killer Priority 4 (Browsing)	· Killer Priority 5 & 6 (Cloud Download)
	· Teams/Zoom Voice	· Teams/Zoom Video	· Teams Shared Screen	
Devices	· Game Port Connected · Game Console: PS, Xbox, Switch	· Chromecast, FireTV, Roku · SmartTV	· Computers, Smartphones · Other Devices	· IoT Devices, Wearable

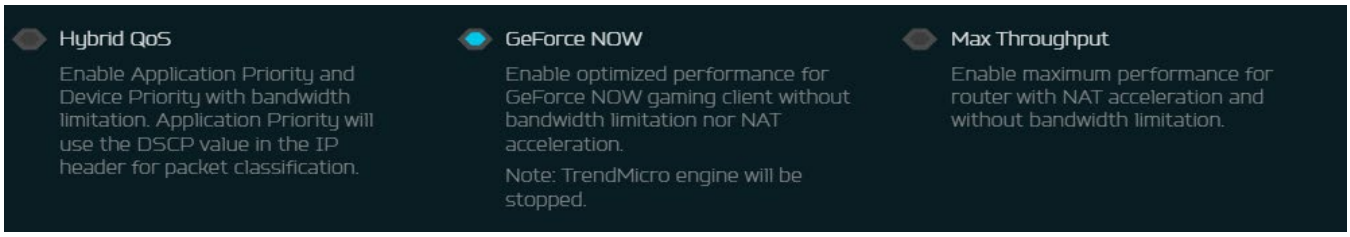
Device priority:
Note 1: Killer-Enabled PC is set to default extreme priority whether connected by wired Ethernet or by wireless.
Note 2: You may drag and drop connected clients into the desired priority level. The change is effective immediately.



For the upload and download **bandwidth** configuration, please contact your ISP to get the exact value of the upload and download bandwidth. Once the bandwidth is configured, QoS will reserve the bandwidth according to the weighting percentage of each priority queue.



You may select “use default configuration” and click on “Apply bandwidth”. you can select “setting Otherwise, manually” and enter the required upload and download bandwidth with priority weighting.



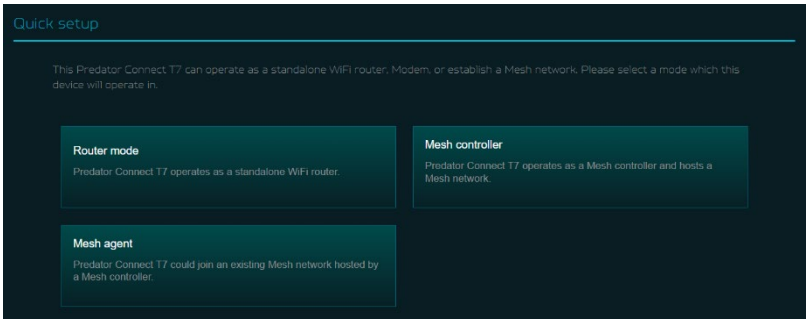
You can select **GeForce NOW** option to enable optimized performance for GeForce NOW gaming clients without bandwidth limitation or NAT acceleration.
Note: TrendMicro engine will be stopped.

For enabling router maximum performance with NAT acceleration and without bandwidth limitation, please select the option “**Max Throughput**” in this case.

6. Quick Setup

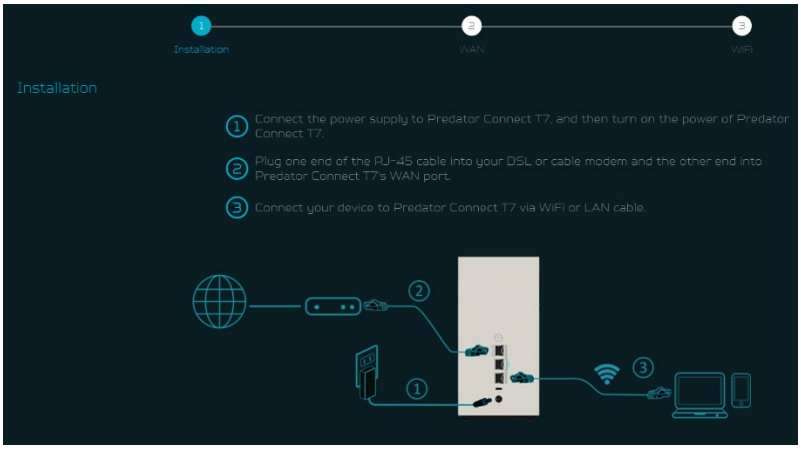
The Predator Connect T7 can operate as a standalone Wi-Fi router or establish a Mesh network. Please select a mode which this device will operate in:

1) Router Mode
2) Mesh Controller
3) Mesh Agent



In **Router mode**, plug one end of the RJ-45 cable into your DSL or cable modem and the other end into Predator Connect T7's WAN port.

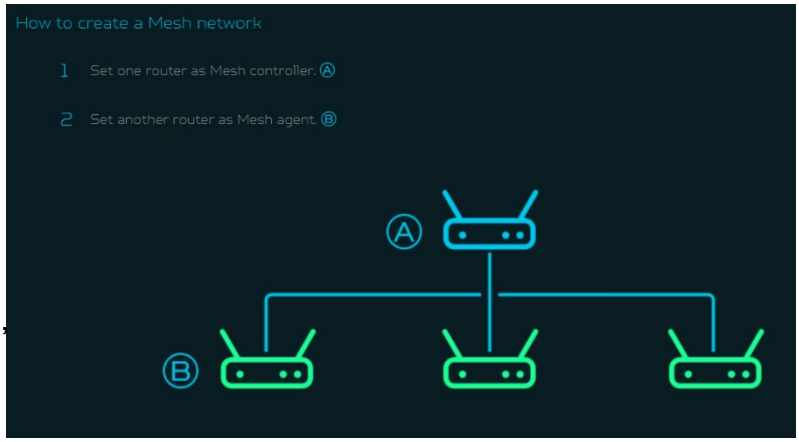
Connect your device to Predator Connect T7 via Wi-Fi or LAN cable.



6.1 How to create a Mesh network

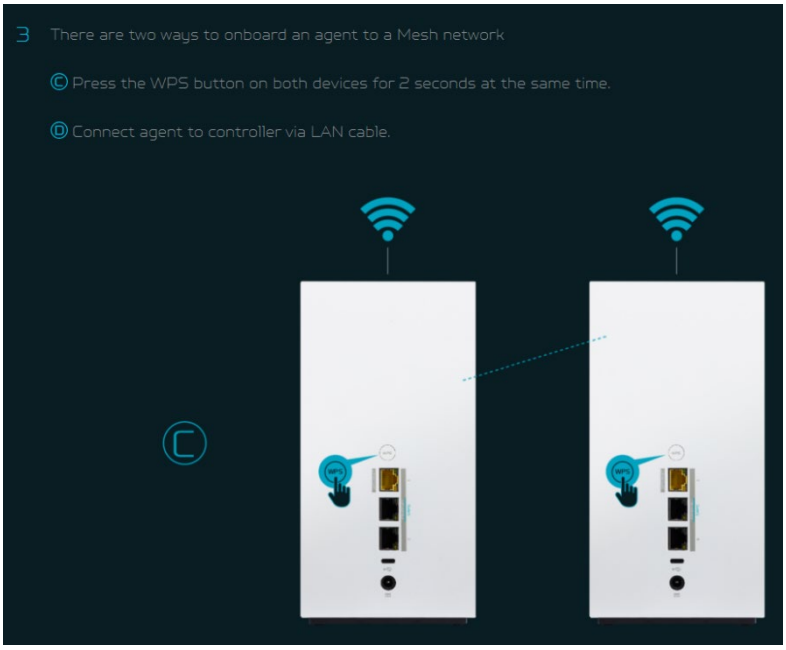
To create a mesh network,
set one router as a Mesh controller (A) and set another router as a Mesh agent (B)

To ensure better performance, it is recommended not to use wireless to connect more than 2 agents in series, but you can connect multiple agents behind the controller. Or you can use LAN cable to connect more than 2 agents in series.



Following are the steps to create a Mesh network;

1. Go to quick setup and set the main router as Mesh controller.
2. Power on the other Predator router and set it as Mesh Agent.
3. Place both routers close to each other.



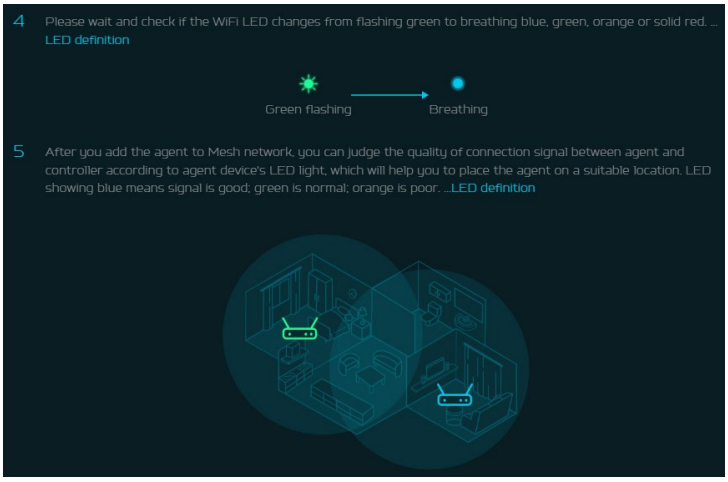
There are two ways to onboard an agent to a Mesh network.

I. Press the WPS button on both devices for 2 seconds at the same time.
II. Connect agent to the controller via LAN cable.

If the agent onboard to a controller successfully, the LED will be breathing blue, otherwise, LED will become solid red color.

Power off the agent device, move it to another place, and then power ON. Then observe the agent's LED color. (Agent's LED color shows RSSI indication between a controller and agent.

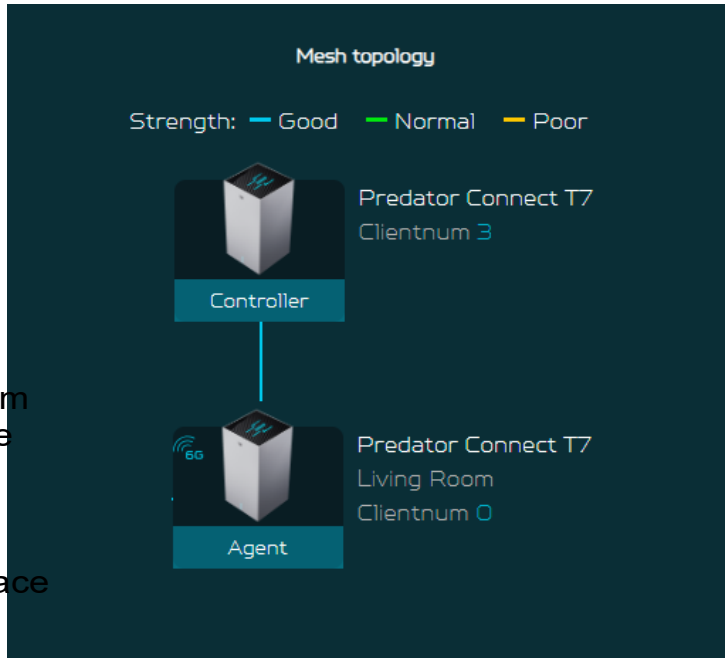
The Blue color means RSSI is good, Green color means RSSI is normal, Orange color means RSSI is poor, Red color means disconnected.



6.1.1 Mesh Topologies

Following are the mesh topologies:

- Topology – One agent
- Start topology – 3 agents
- Daisy chain topology – 2 agents
- Tree topology – 3 agents

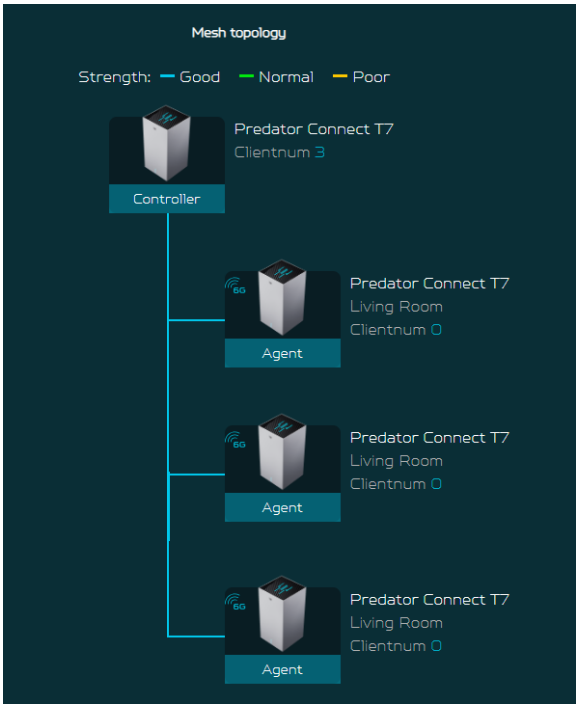


Topology – One Agent

In one agent topology, a controller is connected with one agent, and the medium between a controller and the agent can be wireless or wired connectivity.
Blue color line indicates the good signal strength between a controller and the agent, so it is always recommended to place an agent close to the controller.

Star topology – 3 agents

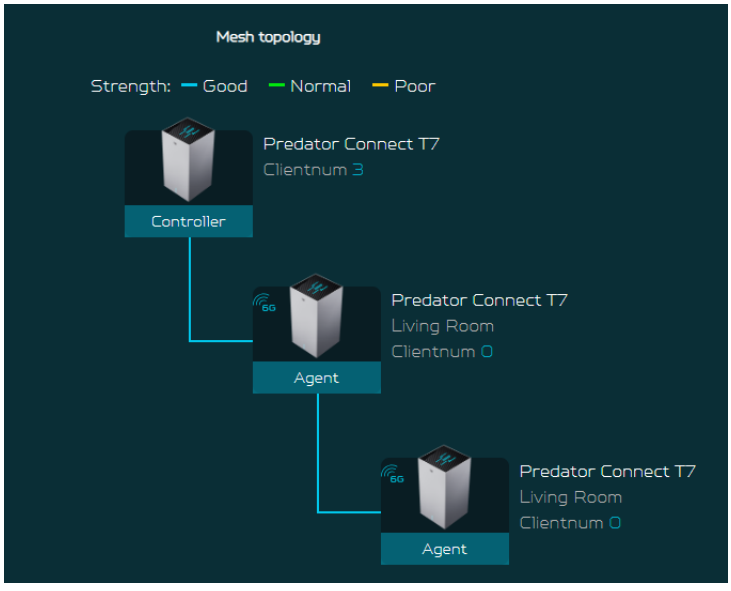
In start topology of 3 agents, a controller is simultaneously connected with three agents, and the medium between a controller and the agents can be wireless or wired connectivity.



Daisy Chain topology – 2 agents

In daisy chain topology of 2 agents, a controller is connected with the agent, and then agent is connected with an another agent, making a chain topology.

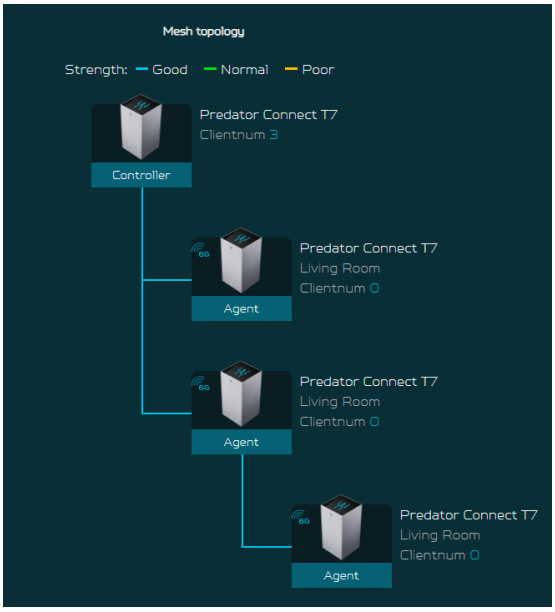
The agent connections in the mesh topology depends on the RSSI strength between the controller and the agent, and it will not connect directly behind the on-boarding device.
Blue color line indicates a good signal strength.



Tree topology – 3 agents

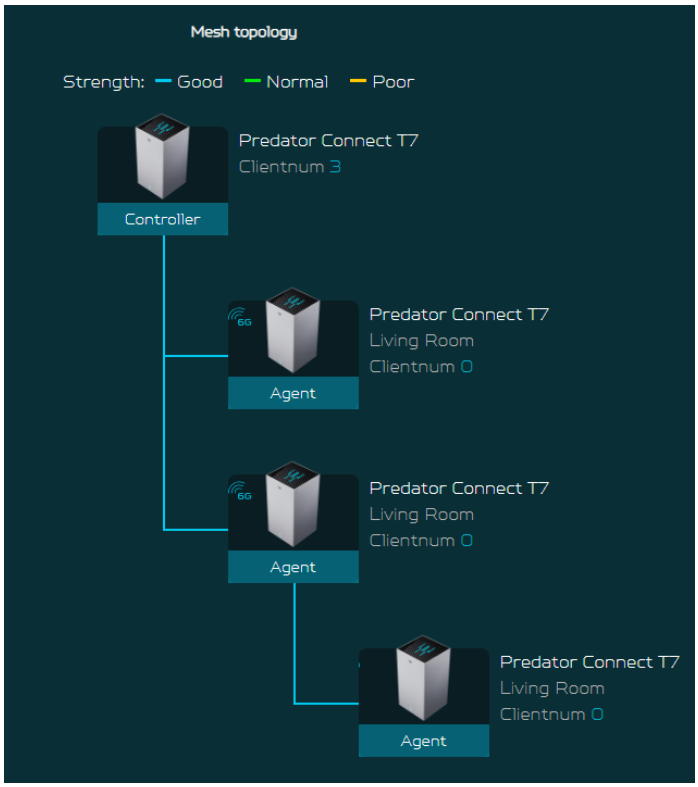
In tree topology of 3 agents, a controller is connected with the two agents; whereas a third agent is connected with the second agent, making a tree topology.

Medium between a controller and the agents can be wireless or wired connectivity.



Agent connected via Wi-Fi

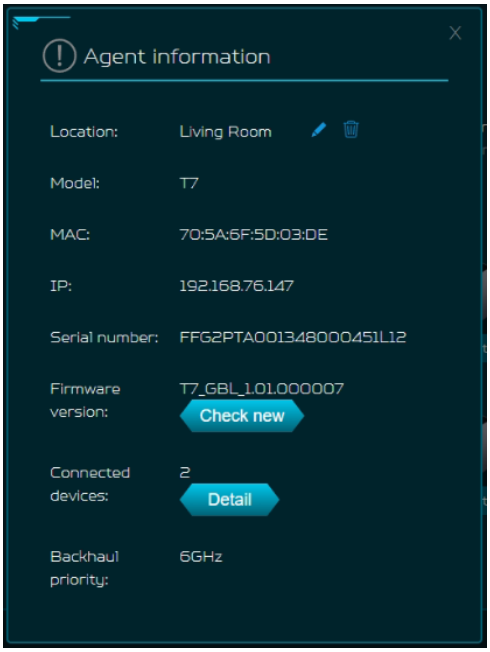
In this topology, a controller is wirelessly connected with the two agents; whereas the third agent is connected with the second agent through wired connectivity.



Agent information

From this tab, you can see the agent's information including:

1) Location
2) Model number
3) IP address
4) Serial number
5) Firmware version
6) Devices connected with the agent
7) Agent backhaul connectivity.



There are some limitations in our mesh which are listed below:

I. Due to the adoption of front-haul and backhaul sharing bandwidth to connect various nodes in the Mesh network, if the Mesh agent is in a daisy-chain configuration, each layer of connected nodes needs to simultaneously handle communication with both upper-layer nodes and lower-level devices. As a result, the available bandwidth speed will be halved and evenly distributed. Based on this limitation, we recommend that users assemble the Mesh network using Ethernet cables to connect the nodes. This will avoid rate loss due to shared bandwidth (achieving lossless conditions). If users must connect the nodes wirelessly, we suggest forming a star topology network to prevent significant rate reduction caused by multi-tiered connections.

II. All devices are factory-defaulted as routers. Users can change the device role (e.g., Mesh controller, Mesh agent) through Quick Setup.

III. Once a device has been set as a Mesh controller or Mesh agent, changing the device role requires restoring the device to its factory settings before the role change can be made. Note: When the current device is a router, it can be changed to other roles such as Mesh controller or agent (using GUI operation mode or Quick Setup).

IV. Mesh supports WPS Onboarding, but in cases where connection is hindered due to environmental interference, it's recommended to move the agent closer to the controller, or restore the device to its factory default settings and follow the Quick Setup process to reconfigure the agent.
Alternatively, you can perform the setup steps via Ethernet connection.

V. If the Mesh Wi-Fi SSID or password is changed in an existing Mesh network, agents will apply the new configuration after the synchronization process is done. If the agent does not apply the new configuration successfully or the agent is in the offline status, it must go through the onboarding process with the controller again. This is necessary for the updated SSID or password to be applied to these agents.

7. WAN

7.1 WAN Status

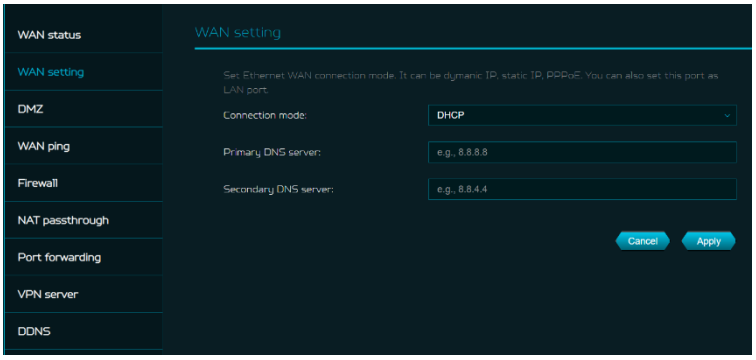
This tab provides information about WAN connectivity status and the following key information:

- Time duration (format HH:MM:SS)
- MAC address
- Connection Mode: DHCP, static IP, PPPoE, etc.
- IP address
- Subnet mask
- Default gateway
- Primary & Secondary DNS server

7.2 WAN Setting:

On this page, you can set up Ethernet WAN connection mode to DHCP, Static IP, PPPoE or switch WAN port to LAN1, depending on your connection usage. Click on drop-down arrow to reveal the options to select your preferred WAN settings.

You can select “Switch WAN port to LAN1 , if you are using the router in repeater mode in which the port is not required. As a result, you can have one more LAN port.



7.3 DMZ

DMZ is physical or logical subnetwork that contains and exposes the firm's facing services to an untrusted, usually larger, network such as the Internet.

If external users can't access certain network services provided by the Local Area Network (LAN), use the DMZ function to set the client that provides the required network services as the DMZ host. The host IP address needs to be entered and then external users will have access to all services.

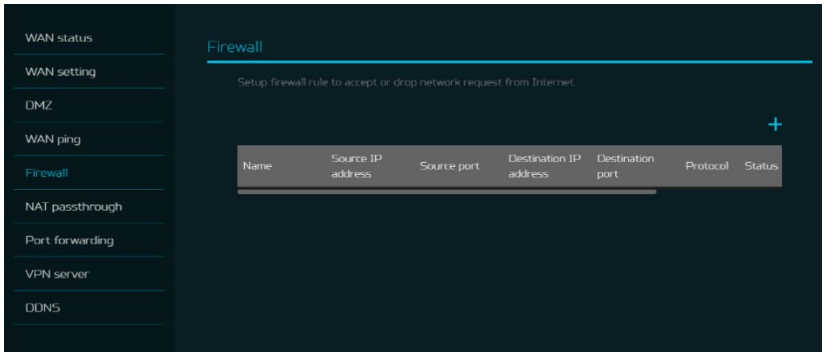
7.4 WAN Ping

By enabling this feature, WAN port of Predator Connect T7 will respond to ping requests that are sent to the WAN IP address from the Internet.

For better security, keep the feature turned OFF, and the device will not respond to a WAN ping.

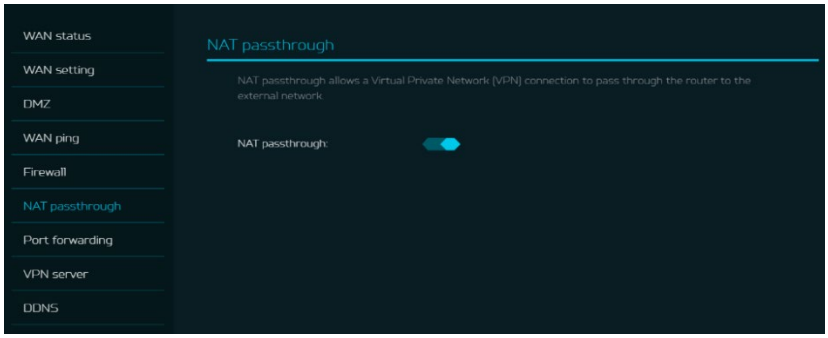
7.5 Firewall

Setup firewall rule to accept or drop network requests from Internet.
To set up a firewall, click on (+) icon and enter the name, source and destination port and IP address, protocol, target and status info.



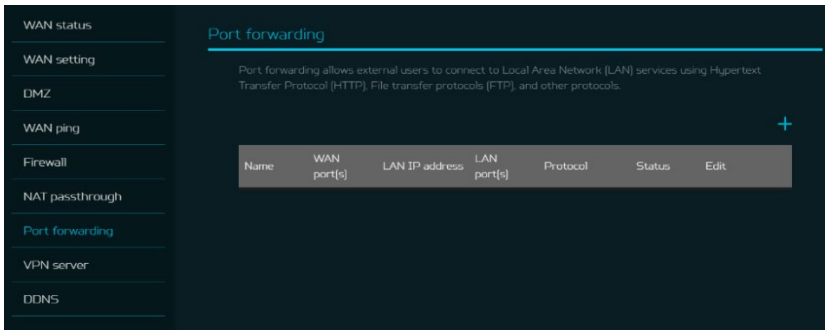
7.6 NAT pass-through

NAT pass-through allows a Virtual Private Network (VPN) connection to pass through the router to the external network.



7.7 Port Forwarding

This feature allows external users to connect to Local Area Network (LAN) services using Hypertext Transfer Protocol (HTTP), File transfer protocols (FTP), and other protocols. To add any application, click on (+) icon and select a required service.

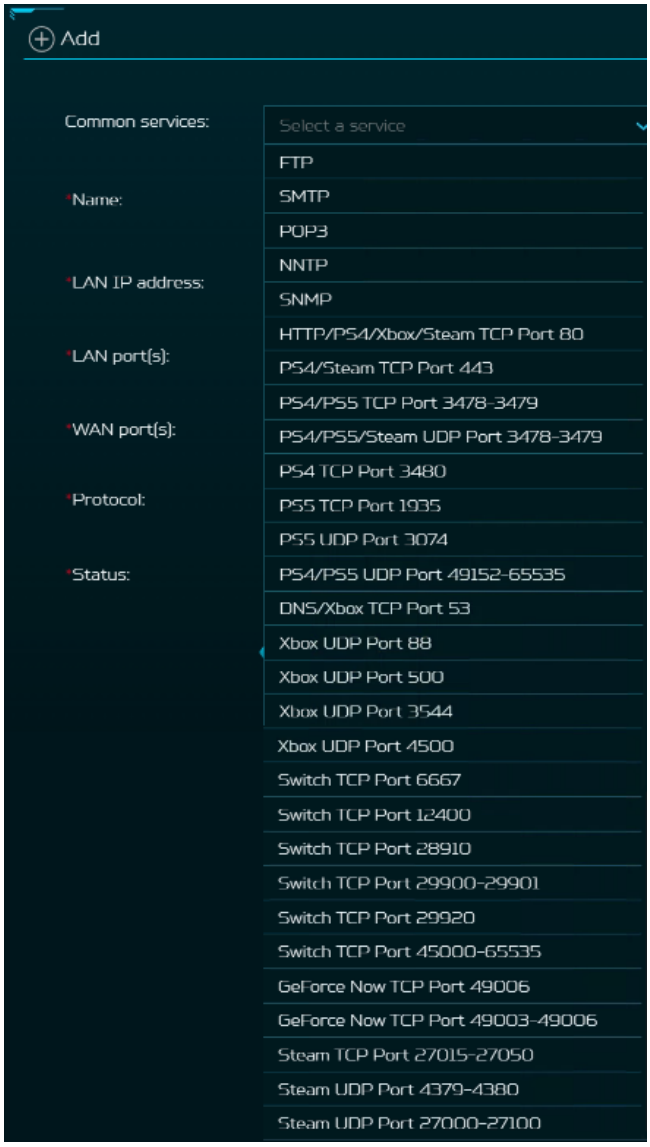


You can select any service profile from common services tab and it will then automatically show its name, the port number and its protocol.

Enter the LAN IP address and select the status ON/OFF and click on the “Apply” button to activate the service.

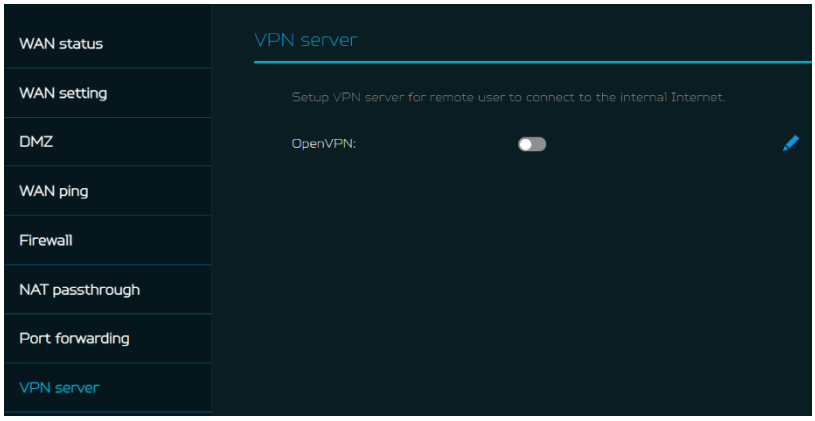
We have added a new game console profile including:

- Xbox network
- Play Station 5
- Play Station 4
- Nintendo SWITCH
- Nvidia GeForce Now
- Steam



7.8 VPN Server

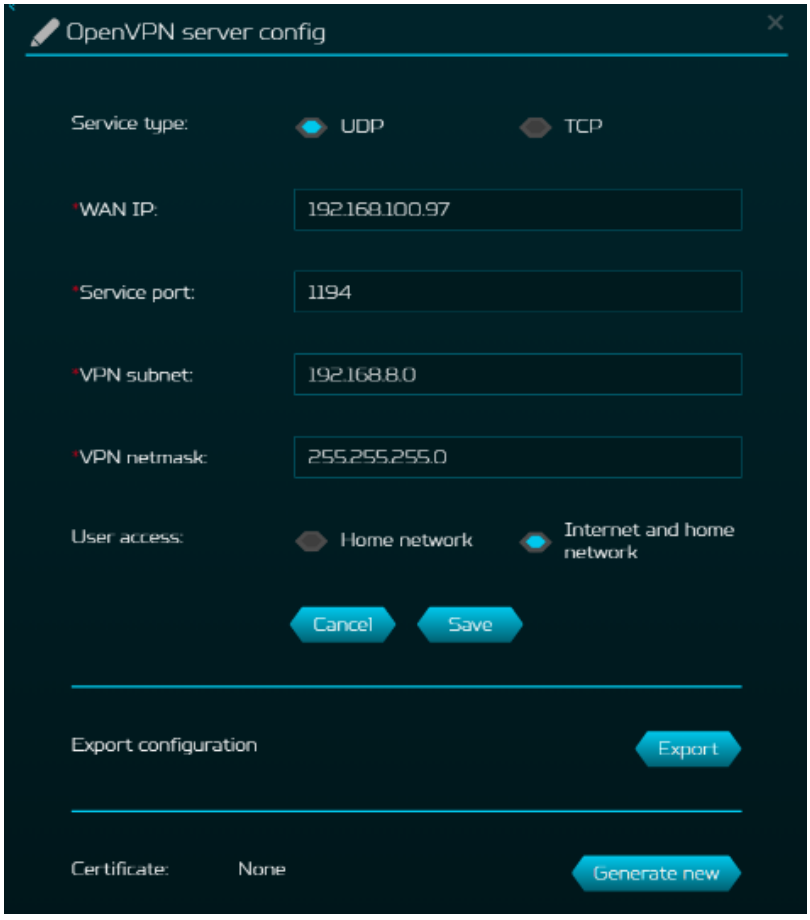
Setup VPN server on Predator Connect T7 for remote VPN connection over the Internet. This router offers following VPN service:



7.8.1 OpenVPN

The user needs to generate a certificate before enabling the VPN server. Once you create a VPN server, the VPN connection link establish, and the status with be shown. It will display the connection type, remote & local IP address, and duration.

Open VPN is SSL VPN and uses a chosen UDP or TCP port, allowing for flexible configuration choices. User access comes with two different options; Home network, Internet and home network. Users can also export OpenVPN configuration file (client.ovpn).



Enter the following information to configure Open VPN services.

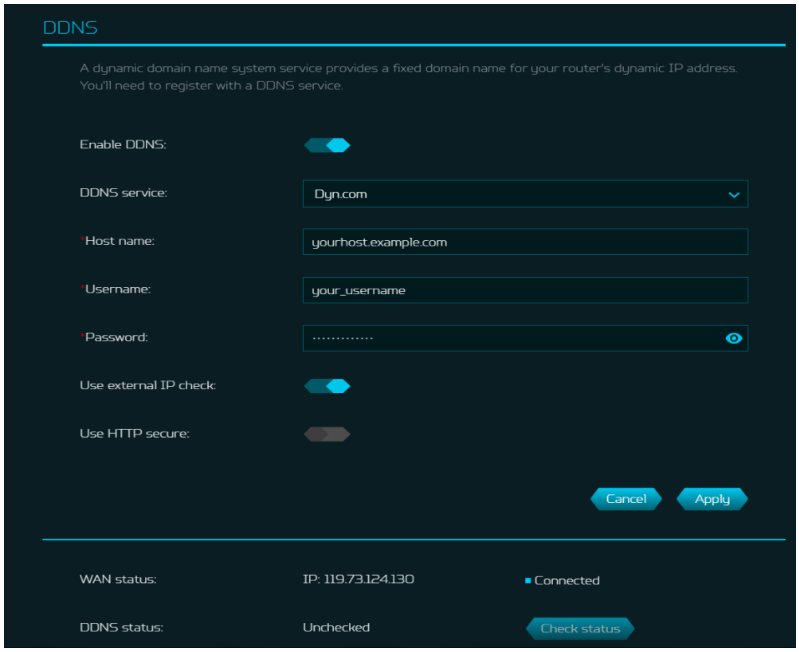
1) WAN IP address
2) Service port
3) VPN subnet
4) VPN netmask

7.9 DDNS

A DDNS service provides a fixed domain name for your router's dynamic IP address. You will need to register with a DDNS service among the following ones.

1. Dyn.com
2. No IP
3. Google domain
4. Cloudflare.com

Once you select the DDNS service, enter the host name, username and password, and click on 'Apply' button to activate DDNS.
DDNS and WAN status will be shown once the DDNS information is entered.



8. Wi-Fi

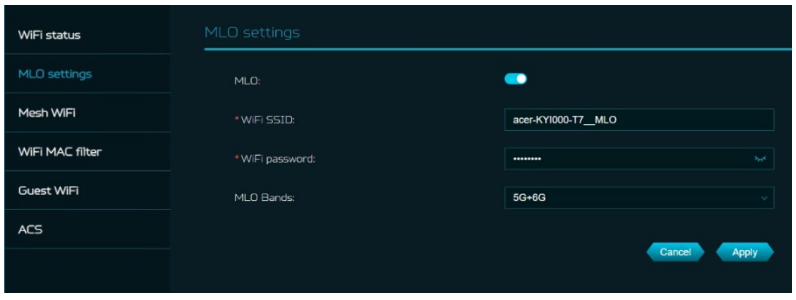
8.1 Wi-Fi Status

Displays key information such as:

- Wi-Fi SSID
- SSID Broadcast
- Security
- Channel
- Connected devices
- Gateway address
- Mac address of 2.4GHz, 5GHz & 6GHz bands

8.2 MLO Settings

Wi-Fi 7's MLO (Multi-Link Operation) is a major technical advancement. It enables devices to simultaneously send and receive data across different frequency bands and channels. It's the reason why the new standard can achieve and maintain 1ms latency, even for the most data-demanding, real time applications. Connecting to MLO network enhances throughput and improves network efficiency.
When the mesh is activated, the backhaul settings between the controller and the agent are set to default MLO's 5+6G.



8.3 Mesh Wi-Fi (In Mesh Mode)

This tab provides information about Mesh Wi-Fi SSID and password.

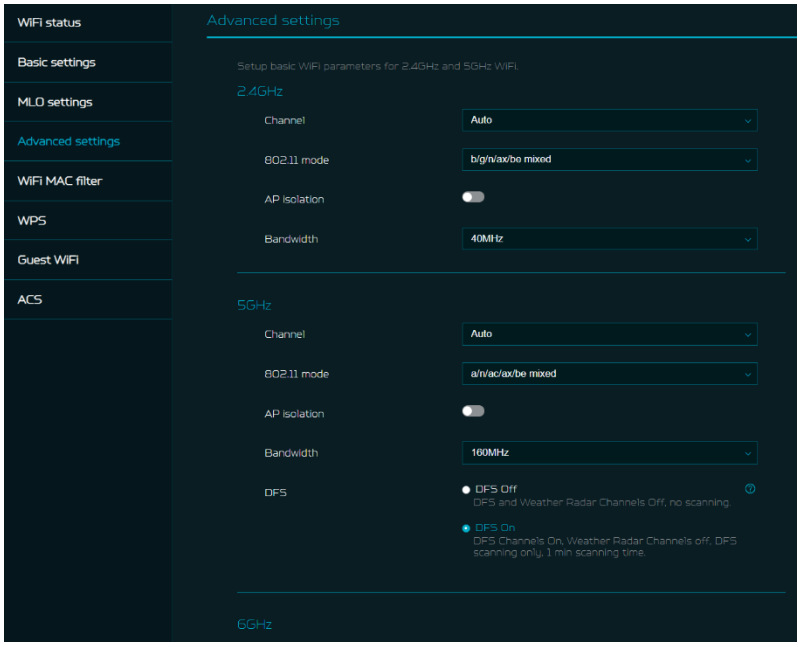
Band steering is ON by default, it automatically connects your devices to the best available Wi-Fi frequency in your surroundings.

8.4 Advanced Settings

This tab will help you to setup advanced Wi-Fi parameters for 2.4GHz, 5GHz & 6GHz band.

AP isolation is a feature that enables you to create a separate virtual network preventing client communicating with each other and preventing unwanted hacking. This feature is disabled by default.

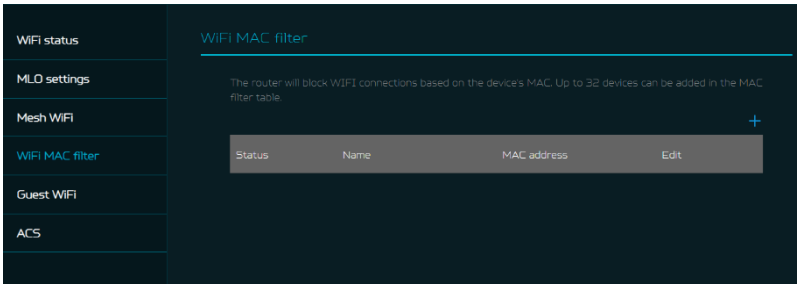
The full list of **PSCs** is:5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213 and 229.
802.11 mode will be “b/g/n/ax/be mixed” by default. 802.11be (Wi-Fi 7) standard aims to implement wireless communications at much faster speeds and larger capacities than the previous 802.11ax.



8.5 Wi-Fi MAC filter

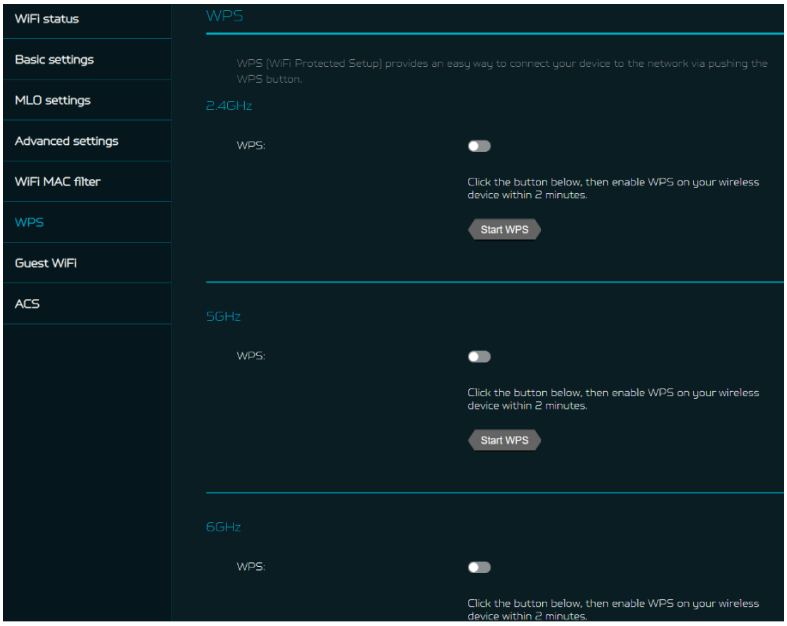
Devices that are added to the Wi-Fi MAC filter will be blocked from accessing the Internet.

Click on the (+) icon to add the device in the filter table by entering its name & MAC address. Up to 32 devices can be added to the MAC filter.



8.6 WPS

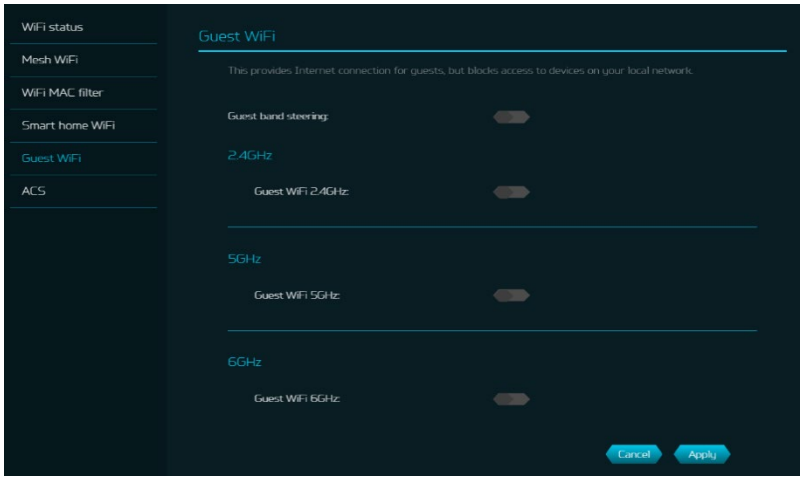
WPS (Wi-Fi Protected Setup) provides an easy way to connect your device to the network by pushing the WPS button or entering a PIN code. On this page, you can configure the WPS settings of 2.4/5/6GHz bands.
Click on “Start WPS”, then enable WPS on your wireless device within two minutes.
WPS will be disabled, if Wi-Fi set to WPA3, WPA, or TKIP mode, or if the SSID broadcast is turned off.



8.7 Guest Wi-Fi

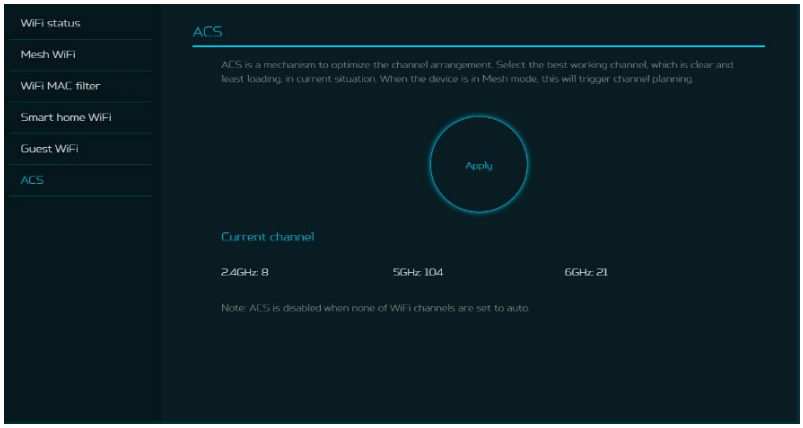
This tab provides information about the Internet connection for guests and their devices accessing your network.

Guest Wi-Fi password is set by the default for all bands, so it is suggested changing the passwords for security reasons.



8.8 ACS (Automatic Channel Selection)

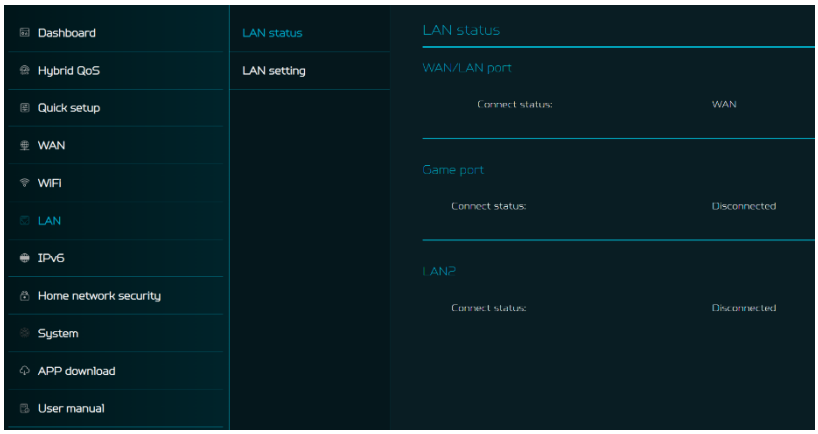
ACS is a mechanism to optimize the channel assignment. It selects the best working channel dynamically. One that is clear and has the least traffic.
Note 1: There will be a small delay, rescanning, and then cycling OFF and ON if the client is associated with the ACS enablement band.
Please check your device’s wireless connection and select the best Wi-Fi T7 router SSID after the ACS process is completed.
Note 2: The ACS is not applicable if all three bands (2.4GHz, 5GHz, and 6GHz) are configured as fixed channels.
ACS also works in a Mesh mode and when the device is in mesh mode, this will trigger channel planning.



9. LAN

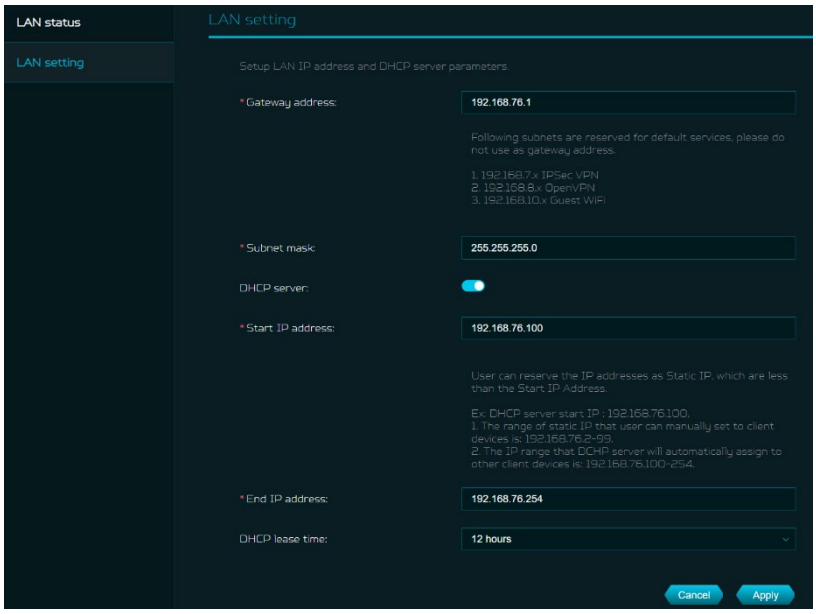
LAN status

On this page, you can view each LAN port status including its associated IP address, MAC address and DHCP server. The Predator Connect T7 has one Game port and two LAN ports, with one port as WAN/LAN port.



LAN Setting

This tab allows you to set up LAN IP gateway address with an option to enable or disable the DHCP server feature. You can enter the gateway address and subnet mask. DHCP provides and assigns IP addresses, default gateways, and other network parameters to client devices. DHCP server can be enabled or disabled as per the network requirement.

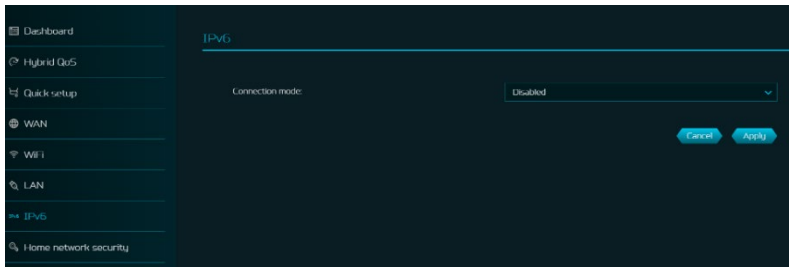


The following subnets are reserved for default services. Please do not use it as a gateway address.

1. 192.168.7.x (IPsec VPN)
2. 192.168.8.x (Open VPN)
3. 192.168.10.x (Guest Wi-Fi)

10. IPv6

You can setup IPv6 settings from this tab. The Predator Connect T7 supports IPv6 mode below: DHCPv6, static IPv6, PPPoE, 464xlat, 6rd, DS-Lite. Connection mode will be disabled by default.

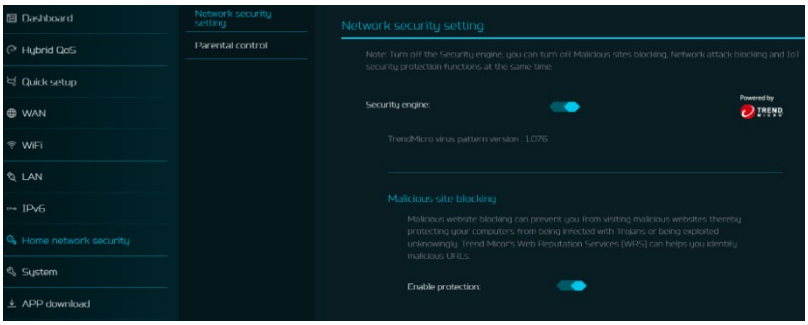


Please consult local Internet Service Provider before enabling and configuring the option.

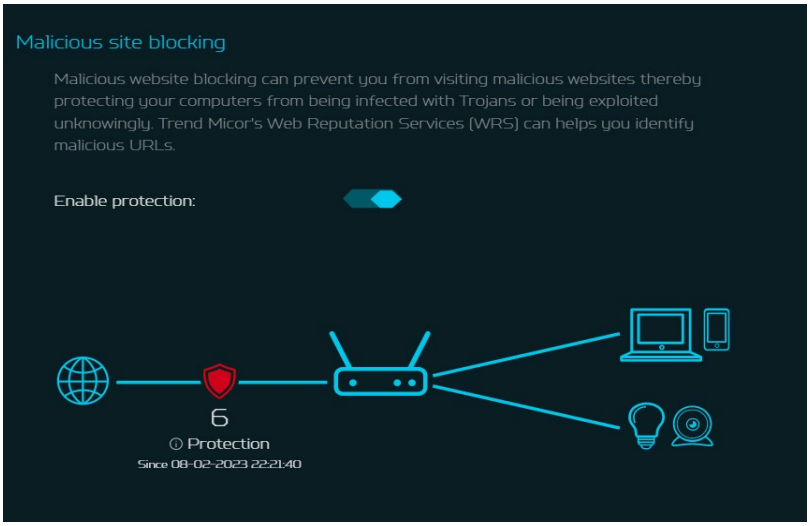
11. Home Network Security

The home network security tab includes network security settings and web and app
controller within the parental control feature. These two features must accept the Trend Micro license agreement before enablement.

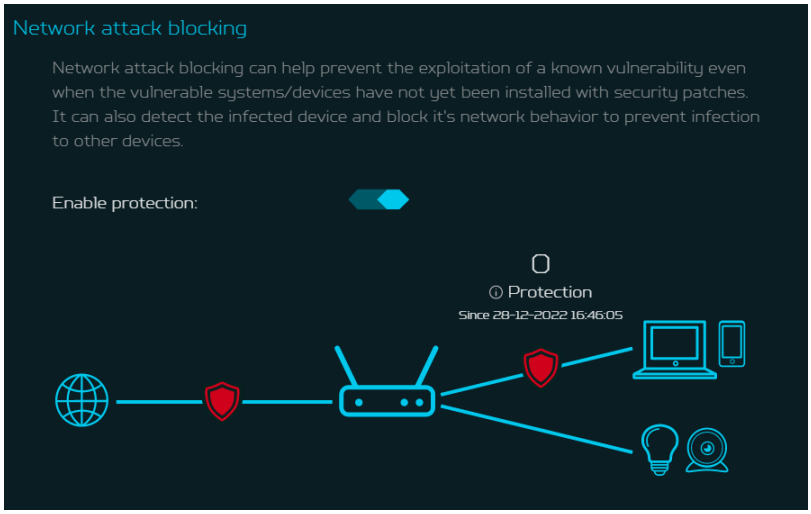
11.1 Network Security Setting
This tab contains the network security-related information, powered by Trend Micro, where you can turn on/off the security engine and enable protection against malicious sites, network attacks and harmful connections coming from IoT devices.



Malicious site blocking prevents unwanted sites to open and hence protecting your computer from being infected with Trojans. There is a feature called “Trend Micro’s Web Reputation Service (WRS) that identifies malicious URLs and allow you to take action against infected URLs.

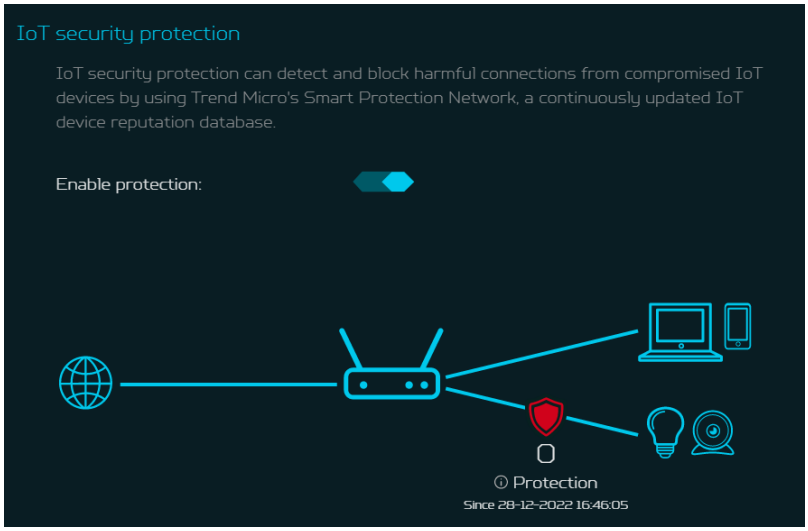


By enabling **Network attack blocking** feature, the router detects the infected devices and block its network behavior to prevent infection in other devices.



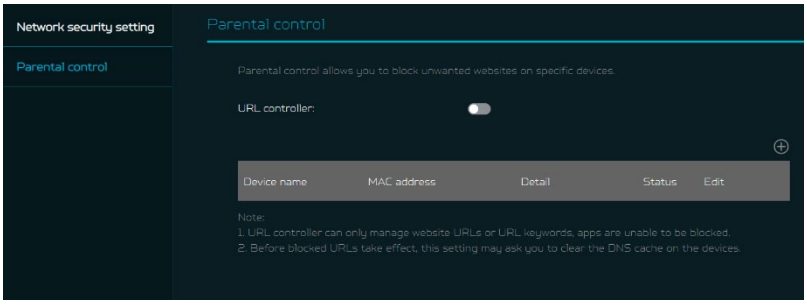
Enabling **IoT security protection** feature detects and blocks harmful connections from compromised IoT devices by using Trend Micro's smart protection network.

It's a continuously updated IoT device reputation database that prevents the network from false connections.



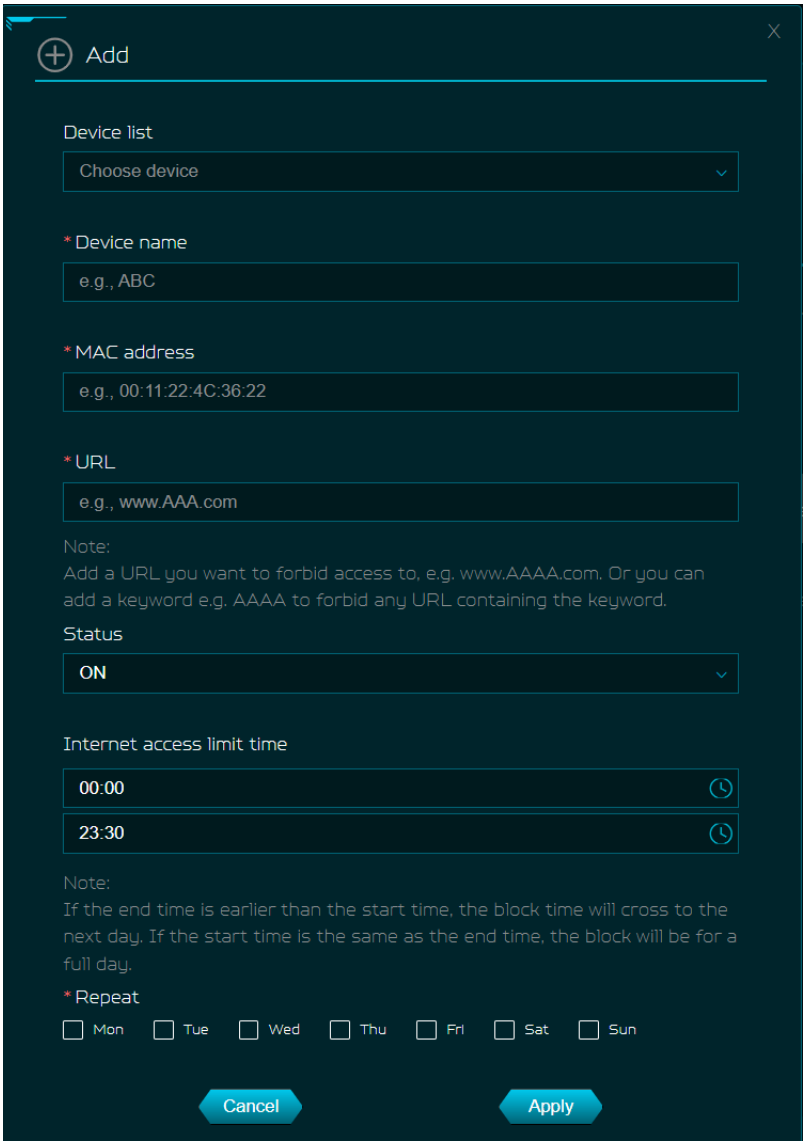
11.2 Parental Control

This feature allows you to control and block unwanted sites on specific devices.
You can enable/disable URL controller.



Once you click on (+) icon, the following window will appear and here you can enter the device list, device name, its MAC address, URL, status and Internet access limit time.

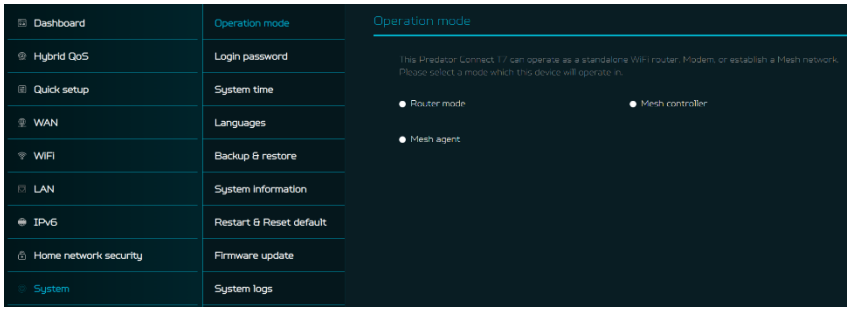
Note: If the end time is earlier than the start time, the block time will cross to the next day. If the start time is the same as the end time, the block will be for a full day.



12. SYSTEM

12.1 Operation Mode

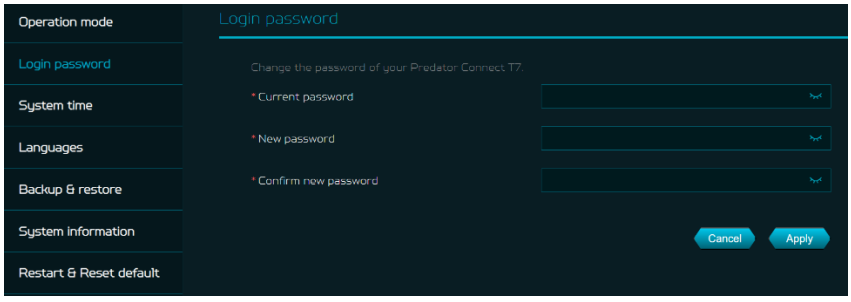
In this tab, you can view the different operation modes of the router.



12.2 Login Password

You can change the password of your Predator Connect T7 from this page.

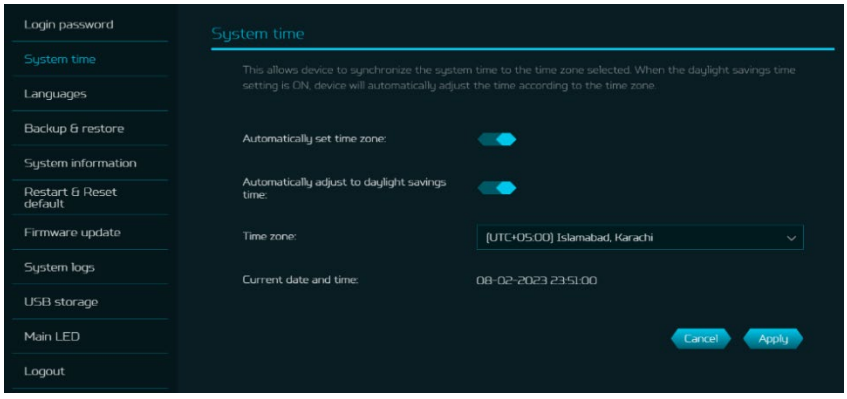
To make a new password, you need to enter your current password first. Please use a strong password to keep it secure.



12.3 System Time

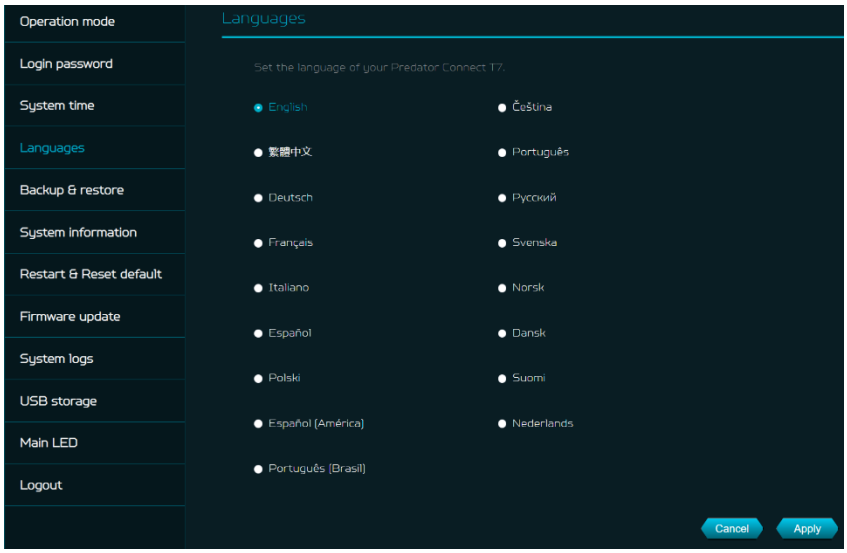
This tab allows you to synchronize the device time with the system time by enabling “Automatically set time zone”.

By enabling “daylight savings time”, the device will automatically adjust the time according to the time zone.



2.4 languages

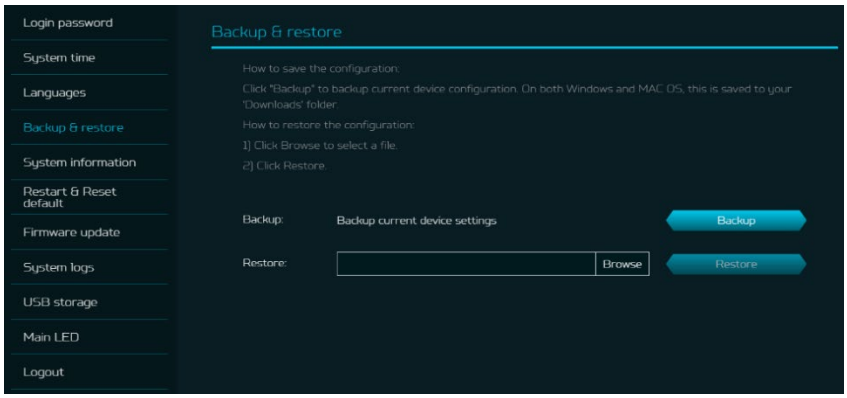
You can select the language of your Predator Connect T7 from this tab.



12.5 Backup and Restore

In this tab, you can check how to save the configuration:
Click on "Backup" to backup current device configuration. On both Windows and MAC OS, this is saved to your 'Downloads' folder.

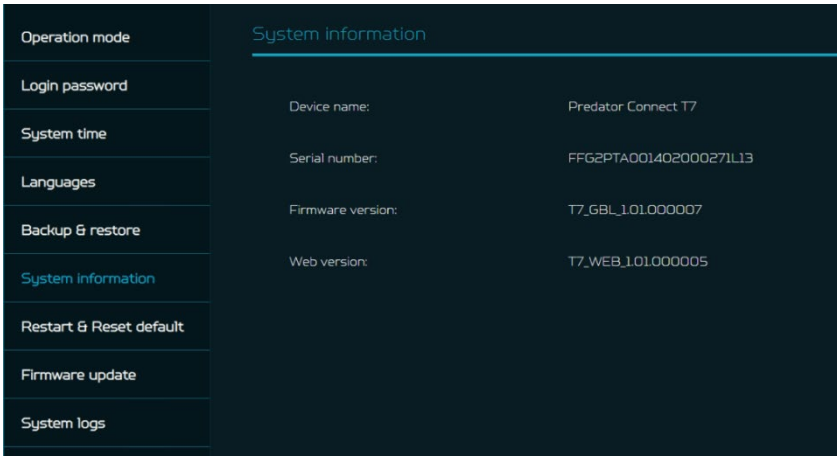
How to restore the configuration:
1) Click Browse to select a file
2) Click Restore



12.6 System Information

It shows key device information of Predator Connect T7, such as:

- Device name
- Serial number
- Firmware version
- Web version

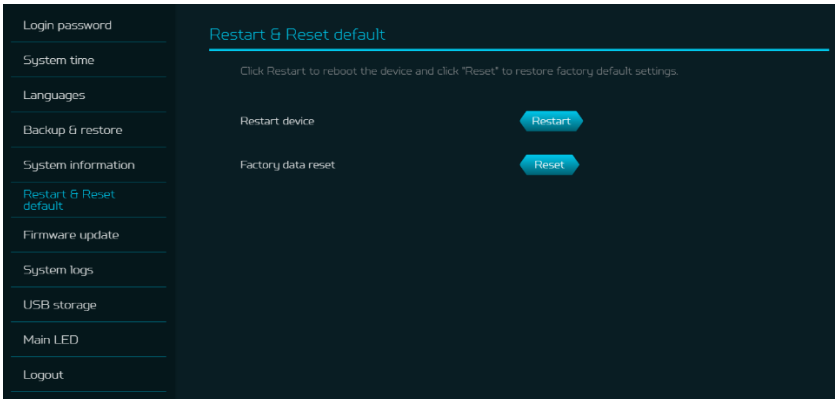


12.7 Restart and Reset Default

From this tab, you can click on “Restart device” to reboot the router and click on “Factory data reset” to restore the factory default settings.

Please check if you bind your device with Predator Connect Mobile App.

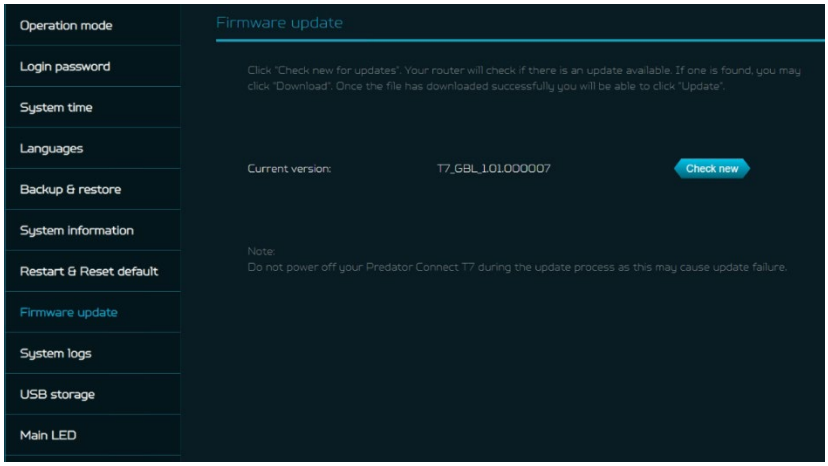
After the factory reset, please don’t forget to unbind the device from the mobile app.



12.8 Firmware Update

In this tab, you can check the existing firmware version and also, click on “check new”, to see if there is an update available.

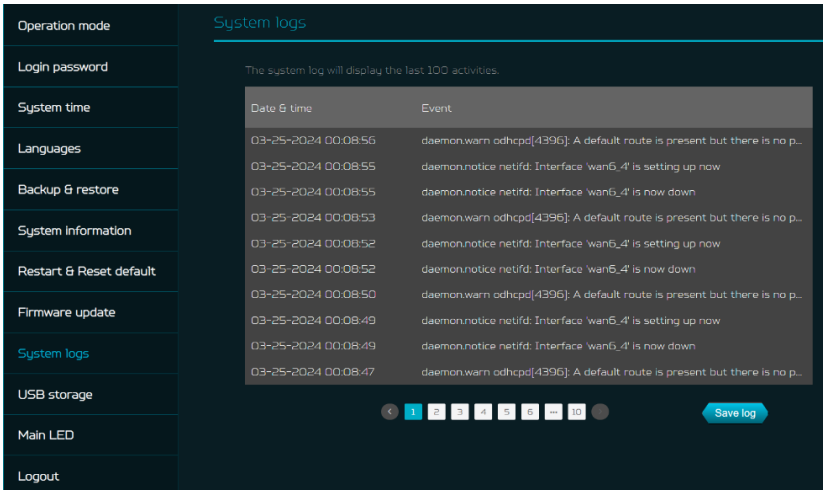
You may click on the top right icon “New firmware available” to upgrade the Predator Connect T7 with the latest firmware.



12.9 System Log

The System logs consists of general logs and Wi-Fi logs. It will display here all the recent 100 activities you have done with the router.

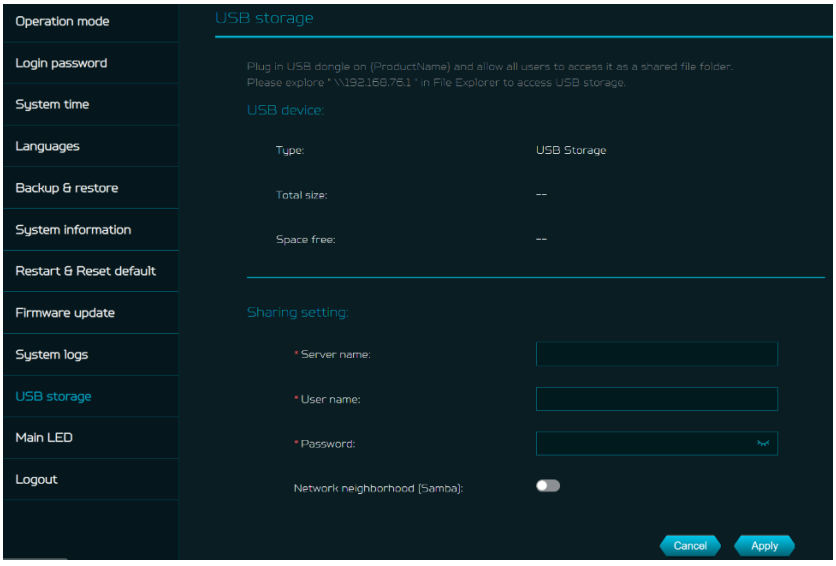
You can save the system logs by clicking the “Save log” button at the bottom of the page. The main purpose of savings logs is to allow the logs to be saved and sent back to Acer for analysis, if there are issues encountered.



12.10 USB Storage

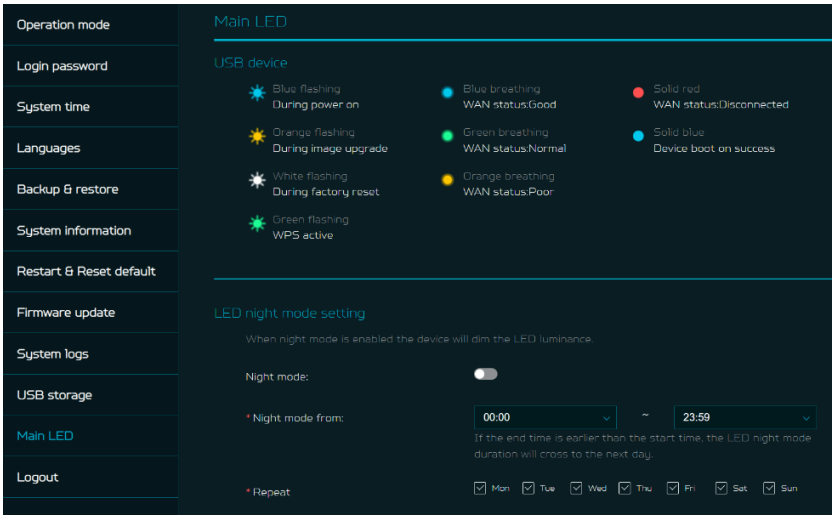
This router has a USB type-c port where you can plug in a USB drive and allow all authorized users to access the files on your USB drive. Once you plug in a USB drive, it will display device type, size and free space available.

Enter the server name and login credentials for shared access to USB drive. In sharing setting, there is an option to enable/disable Network neighborhood (Samba).



12.11 Main LED

This tab displays information about LED colors and its indication. These LED indicators will help you to know and understand router behavior.



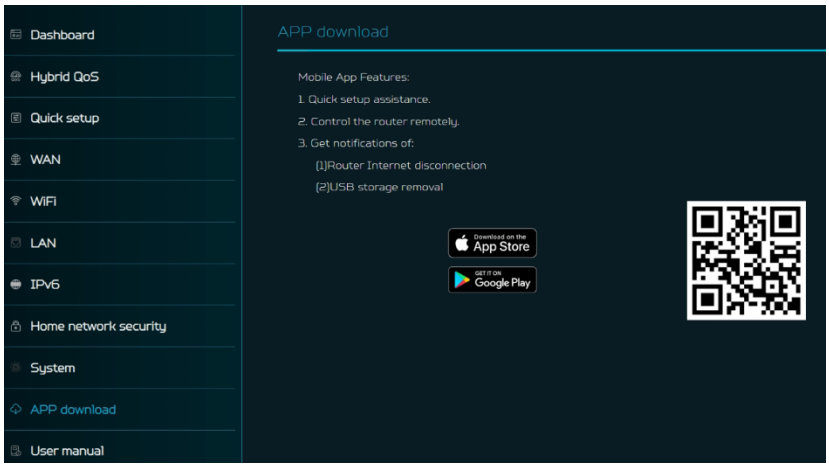
Enabling **LED night mode**, only dims the device's luminance. Please check if you have already setup the correct time zone (auto/manual), before enabling this option. You can set up the daily schedule as needed. Please refer to following light definitions, as the T7 has two LEDs; mask and front.

T7	Mask LED	Blue flashing LED	The router is powering on.
	Mask LED	Solid Blue LED	The router is powered on.
	Mask LED	Blue breathing LED	WAN status is good.
	Mask LED	Green breathing LED	WAN status is normal.
	Mask LED	Orange breathing LED	WAN status is poor.
	Mask LED	Solid Red LED	WAN is disconnected. (No internet)
	Mask LED	Green flashing LED	WPS is active. Mesh on-borading
	Mask LED	Orange flashing LED	The firmware is being upgraded.
	Mask LED	White flashing LED	The router is performing a factory reset.
	Mask LED	PING Server	PING site: (default is Google server, user can add and edit PING Server) if 8.8.8.8 cannot be accessed then access the second one 8.8.4.4 …and so on 1.8.8.8.8 (default) 2.8.8.4.4 3.4.2.2.2 4.1.1.1.1 5.1.0.0.1 or Ping 2001:4860:4860::8888 (IPv6)
	Mask LED	LED status of internet	Blue : connection is good Green: connection is normal Orange: connection is Poor Red : disconnect
	Mask LED	PING Rule	send out 4 PING requests with interval 1 sec, in every 60 secs, If packet loss =0, the condition is good (LED flashing Blue); If packet loss <= 25%, the condition is not good(LED flashing Green) If packet loss > 25%, the condition is bad(LED flashing Orange)
	Front LED(Wi-Fi)	Blue flashing LED	The device is powering on.
	Front LED(Wi-Fi)	Solid Blue LED	The device is powered on and Wi-Fi AP is ready. (2.4GHz band or 5GHz band or 6GHz band)
	Front LED(Wi-Fi)	Solid Red LED	The device is powered on and Wi-Fi APs have a problem. (2.4GHz band and 5GHz band and 6GHz band)

13. APP Download

User can download the mobile App by scanning the QR code, available in “App download” tab, to control the following features:

1. Quick setup assistance
2. Control the router remotely
3. Get notifications of:
   1) Router Internet disconnection
   2) USB storage removal



14. Troubleshooting

14.1 Quick Tips

This section describes common issues which you can encounter.

Sequence to restart the device and network:

1. Turn off and unplug the modem power plug.
2. Plug in the modem power plug and then turn it on. Wait for two minutes till the modem LED is steady as before.
3. Wait for the device's upper deck main LED to steady breathing.

14. 2 Frequently Asked Questions (FAQs)

14.2.1 What can I do if I forget my wireless password?

- Connect to the T7 router via Ethernet cable LAN.
- Visit device portal http://acer-connect.com and login admin.
- Go to Wi-Fi -> Basic settings/Retrieve or reset the Wi-Fi passwords.

14.2.2 What can I do if I forget the router's web portal admin password?

Reset the device by pressing and holding the reset key until the LED starts blinking white. After the device restores to factory default, please login web admin portal with admin PWD,
label printed on the bottom of the device.

Note 1: The device web admin will be locked after 5 wrong password attempts. The user is required to reboot the device to disable the web admin.
Note 2: Remember to set up the device's internet connection after resetting. Remember to also change the admin password.
Note 3: If you ever bind the device via Predator Connect mobile app; remember to unbind it after the factory data reset.

14.2.3 What can I do if I can't log into the router's web admin portal?

Please follow the steps below to check on your client's device.

- Check whether the client-allocated IP and DNS server IPs both are with the same subnet and gateway.
- Clean the browser cookies or use private/Incognito mode to access the router admin.

14.2.4 What can I do if I can't surf the internet even though the configuration is finished?

Please follow the step below to check on your T7 router:

- Login to the web admin portal dashboard to check Internet status.
- Continuingly, if the Internet status is up and connect. Go to the WAN setting, manually configure the DNS server using the below IP and apply:
  Primary DNS server: 8.8.8.8
  Secondary DNS server: 8.8.4.4
- If the issue is still there, please restart the modem and router accordingly.

15. Factory Default Settings

Router web admin	
URL	http://acer-connect.com or http://192.168.76.1
Login Password (case-sensitive)	AcerXXXX (XXXX is randomized variables. Please check the device's bottom label)
Local Network (LAN)	
Gateway address	192.168.76.1
Subnet mask	255.255.255.0
DHCP server	192.168.76.1
DHCP range	192.168.76.100 to 192.168.76.254
Time zone	Depends on the country or region you bought the router.
DHCP starting IP address	192.168.76.100
DHCP ending IP address	192.168.76.254
Time adjusted for daylight save time	Enabled.
Wireless LAN (WLAN)	
Wi-Fi SSID (case-sensitive)	2.4GHz: T7_YYYY_2.4GHz 5GHz: T7_YYYY_5GHz 6GHz: T7_YYYY_6GHz (YYYY is randomized variables. Please check the device's bottom label)
Security	2.4GHz : WPA2/WPA3 5GHz : WPA2/WPA3 6GHz : WPA3
SSID Broadcast	Enabled.
RF channel	2.4GHz : Auto 5GHz : Auto 6GHz : Auto
Default operation mode (with AX enabled)	2.4GHz: 2x2 MIMO streams, 1024 QAM, 40MHz, 574MBps 5GHz: 4x4 MIMO streams, 4096 QAM, 80MHz, 4804Mbps 6GHz: 2x2 MIMO streams, 4096 QAM, 80MHz, 2402Mbps
Guest Wi-Fi	Disabled.
Home Network Security	Disabled.

16. Router Basic Specification

Processor	CPU	Qualcomm IPQ5322 + QCN6274
Memory	RAM	1GB
	Storage	512MB
Wireless LAN	IEEE standard	802.11 a/b/g/n/ac/ax/be
	Band	Tri-band, 2.4/5/6GHz
	Throughput	BE11000Mbps
Ethernet	WAN	1 x 2.5GbE
	LAN	2 x 1GbE
Interface	Ethernet	Ethernet WAN
Antennas	Antennas	Internal
Software Update	Firmware Upgrade	FOTA
USB	Port	USB 2.0 Type-C
	Storage	FTP, Samba
Button	Power, Reset, WPS	Yes
Material	Main body	ABS
LED	LED	Mask LED and Front LED
Form factor	Dimension	109mm_109mm_212mm
	Weight	915g
Temperature	Operating Temp.	0°C to 40°C
	Operating Humidity	20% - 80%
	Storage Temperature	-10°C to + 70°C
	Storage Humidity	5% - 95%
DC Power Jack	Power Adaptor	12V 3A
Additional Accessories	Accessories	12V 3A Adaptor and network cable

17. Regulatory Information

17.1 Important Safety Precaution

Your Predator Connect T7 Wi-Fi 7 Mesh Router device is manufactured to comply with European safety standards. This section outlines the safety precautions associated with using the device. Please read the safety and operation instructions before using your device and other accessories. Keep these instructions safe for future reference.

17.2 Condition of Use

- The device is not water-resistant. Please protect the device from water or moisture and do not touch the device with wet hands. Otherwise short-circuit and malfunction of the product or electric shock may occur.
- Keep the device and accessories in a cool, well- ventilated area and away from direct sunlight. Do not place the device in a container with poor heat dissipation. Do not enclose or cover your device with clothes, towels, or other objects.
- Put your device in places beyond the reach of children. Do not allow children to use the wireless device without guidance.
- Do not use your device at places for medical treatment (in an operating room, intensive care unit, or coronary care unit, etc.) where wireless device use is prohibited.
- To reduce the risk of accidents, do not use your device while driving.
- RF signals may affect the electronic systems of motor vehicles. For more information, consult the vehicle manufacturer.
- EE recommends using the charger supplied with your device. Use of another type of charger may result in malfunction and/or danger.

17.3 Cleaning and Maintenance

- Do not attempt to dry your device with an external heat source, such as a microwave oven or hair dryer.
- Use a clean, soft, and dry cloth to clean the device and accessories.

17.4 Disposal Instructions

Do not throw this electronic device into the trash when discarding. To minimize pollution and ensure utmost protection of the global environment, please recycle. For more information on the Waste from Electrical and

Electronics Equipment (WEEE) regulations,

visit www.acer-group.com/public/Sustainability

17.5 Ethernet Cable Line Safety

- Disconnect all Ethernet cable lines from the equipment when not in use and/or before servicing.
- To avoid the remote risk of electric shock from lightning, do not connect the Ethernet cable line to this equipment during lightning or thunderstorms.

17.6 Medical Devices

Operation of any radio transmitting equipment, including wireless phones, may interfere with the functionality of inadequately protected medical devices.
Consult a physician or the manufacturer of the medical device to determine if they are adequately shielded from external RF energy or if you have any questions. Switch off your device in health care facilities when any regulations posted in these areas instruct you to do so. Hospitals or health care facilities may be using equipment that could be sensitive to external RF transmissions.

Pacemakers. Pacemaker manufacturers recommend that a minimum separation of 15.3 centimeters (6 inches) be maintained between wireless devices and a pacemaker to avoid potential interference with the pacemaker. These recommendations are consistent with the independent research by and recommendations of Wireless Technology Research. Persons with pacemakers should do the following:

- Always keep the device more than 15.3 centimeters (6 inches) from the pacemaker
- Not carry the device near you pacemaker when the device is switched on. If you suspect interference, switch off your device, and move it.

Hearing aids. Some digital wireless devices may interfere with some hearing aids. If interference occurs, consult your service provider.

17.7 Vehicles

RF signals may affect improperly installed or inadequately shielded electronic systems in motor vehicles such as electronic fuel injection systems, electronic antiskid (anti-lock) braking systems, electronic speed control systems, and air bag systems. For more information, check with the manufacturer, or its representative, of your vehicle or any equipment that has been added. Only qualified personnel should service the device or install the device in a vehicle. Faulty installation or service may be dangerous and may invalidate any warranty that may apply to the device. Check regularly that all wireless equipment in your vehicle is mounted and operating properly. Do not store or carry flammable liquids, gases, or explosive materials in the same compartment as the device, its parts, or enhancements. For vehicles equipped with an air bag, remember that air bags inflate with great force. Do not place objects, including installed or portable wireless equipment in the area over the air bag or in the air bag deployment area. If in-vehicle wireless equipment is improperly installed, and the air bag inflates, serious injury could result. Using your device while flying in aircraft is prohibited. Switch off your device before boarding an aircraft. The use of wireless devices in an aircraft may be dangerous to the operation of the aircraft, disrupt the wireless telephone network, and may be illegal.

17.8 Warning

- Do not attempt to open the device by yourself. Disassembling may result in damage to the device. Small parts may also present a choking hazard.
- When this device is switched on, it should be kept at least 15 cm from any medical device such as a pacemaker, a hearing aid or insulin pump, etc.
- Switch this device off when you are near gas or flammable liquids. Strictly obey all signs and instructions posted in any potentially explosive atmosphere.

17.9 Explosive Device Proximity Warning

Switch off your device when in any area with a potentially explosive atmosphere and obey all signs and instructions. Potentially explosive atmospheres include areas where you would normally be advised to turn off your vehicle engine. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death. Switch off the device at refueling points such as near gas pumps at service stations. Observe restrictions on the use of radio equipment in fuel depots, storage, and distribution areas; chemical plants; or where blasting operations are in progress. Areas with a potentially explosive atmosphere are often, but not always, clearly marked.
They include below deck on boats, chemical transfer or storage facilities, vehicles using liquefied petroleum gas (such as propane or butane), and areas where the air contains chemicals or particles such as grain, dust or metal powders. Do not switch the notebook on when wireless phone use is prohibited or when it may cause interference or danger.

- Warning: Do not operate a portable transmitter (including this wireless adapter device) near unshielded blasting caps or in an explosive environment unless the transmitter has been modified to be qualifies for such use.
- Warning: The wireless adapter is not designed for use with high-gain directional antennas

17.10 Wireless adapter regulatory information

- Warning: For safety reasons, turn off all wireless or radio transmitting devices when using your device under the following conditions.

Remember to follow any special regulations in force in any area, and always switch off your device when its use is prohibited or when it may cause interference or danger. Use the device only in its normal operating positions. This device meets RF exposure guidelines when used normally. To successfully transmit data files or messages, this device requires a good quality connection to the network. In some cases, transmission of data files or messages may be delayed until such a connection is available. Parts of the device are magnetic. Metallic materials may be attracted to the device, and persons with hearing aids should not hold the device to the ear with the hearing aid. Do not place credit cards or other magnetic storage media near the device, because information stored on them may be erased.

Aircraft

Warning FCC and FAA regulations may prohibit airborne operation of radio-frequency wireless devices (wireless adapters) because their signals could interfere with critical aircraft instruments. Ask the airport staff and cabin crew before turning on your device's wireless adapter whilst on board.

The wireless adapter and your health

The wireless adapter, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by the wireless adapter, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The wireless adapter operates within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of the wireless adapter may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations may include:

- Using the wireless adapter on board airplanes, or
- Using the wireless adapter in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful.

If you are uncertain of the policy that applies to the use of wireless adapters in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the adapter before you turn it on.

17.11 Statement

[USA]

- FCC regulations restrict the operation of this device to indoor use only.
- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.
- Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help.
Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

- This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and a human body.

[Canada — Industry Canada (IC)]
This device complies with RSS247 of Industry Canada.

- This device contains licence-exempt transmitter(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) this device may not cause interference,
(2) this device must accept any interference, including interference that may cause undesired operation of the device.

- L'émetteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) L'appareil ne doit pas produire de brouillage;
(2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

- This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and a human body.

- Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et un corps humain.

[NCC]

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

應避免影響附近雷達系統之操作。

高增益指向性天線只得應用於固定式點對點系統。

17.12 EU Regulatory Conformance

List of applicable countries

This product must be used in strict accordance with the regulations and constraints in the country of use. For further information, contact the local office in the country of use. Please see https://europa.eu/ european- union/about-eu/countries_en for the latest country list.

Specific absorption rate information

This device meets the EU requirements on the limitation of exposure of the general public to electromagnetic fields by way of health protection. The limits are part of extensive recommendations for the protection of the general public. These recommendations have been developed and checked by independent scientific organizations through regular and thorough evaluations of scientific studies. The unit of measurement for the European Council's recommended limit for mobile devices is the "Specific Absorption Rate" (SAR), and the SAR limit is 2.0 W/kg averaged over 10 grams of body tissue. It meets the requirements of the International Commission on Non-Ionizing Radiation Protection (ICNIRP).

For body worn operation, this device has been tested and meets the ICNIRP exposure guidelines and the European Standard, for use with dedicated accessories. Use of other accessories which contain metals may not ensure compliance with ICNIRP exposure guidelines.

Hereby, Acer Incorporated declares that the radio equipment type T7 is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available: Please search for Predator Connect T7 Wi-Fi 7 Mesh Router at www.acer.com

17.13 Restrictions

Restriction or Requirement in the CE: 5150 to 5350 MHz indoor-use only.

	AT	BE	BG	CH	CY	CZ	DE
	DK	EE	EL	ES	FI	FR	HR
	HU	IE	IS	IT	LI	LT	LU
	LV	MT	NL	PL	PT	RO	SE
	SI	SK	TR	NO	UK(NI)		

WLAN 5GHz Band: For indoor use only.

	UK

17.14 EU Regulatory Compliance -- Radio

e.i.r.p power limit											
2.4G		5G(U-NII-1)		5G(U-NII-2a)		5G(U-NII-2b)		5G(U-NII-3)		6E(U-NII-5)	
2400 MHz ~	2483.5 MHz	5150 MHz ~	5250 MHz	5250 MHz ~	5350 MHz	5470 MHz ~	5725 MHz	5725 MHz ~	5850 MHz	5945 MHz ~	6425 MHz
e.i.r.p 20dBm		e.i.r.p 23dBm		e.i.r.p 20dBm		e.i.r.p 27dBm		e.i.r.p 13.98dBm		e.i.r.p 23dBm	