



# **Predator Connect W6 AXE7800 Tri-band Wi-Fi 6E Router**

## **User Guide**

v2.3

All Rights Reserved. © 2023.

Important: This manual contains proprietary information that is protected by copyright laws. The information contained in this manual is subject to change without notice. Some features described in this manual may not be supported depending on the Operating System version. Images provided herein are for reference only and may contain information or features that do not apply to your device. Acer Group shall not be liable for technical or editorial errors or omissions contained in this manual.

Revision Aug, 2023

© 2023. All Rights Reserved.

This revision: Aug 2023

Important: This manual contains proprietary information that is protected by copyright laws. The information contained in this manual is subject to change without notice. Some features described in this manual may not be supported depending on the Operating System version. Images provided herein are for reference only and may contain information or features that do not apply to your device. Acer Group shall not be liable for technical or editorial errors or omissions contained in this manual.

## Contents

1. <a href="#">Overview</a> .....	3
2. <a href="#">Installation and Setup</a> .....	3
3. <a href="#">Initial Configuration</a> .....	6
4. <a href="#">Dashboard</a> .....	7
5. <a href="#">Hybrid QoS</a> .....	9
6. <a href="#">Quick Setup</a> .....	11
6.1 <a href="#">How to create a Mesh network</a> .....	12
6.2 <a href="#">Mesh topologies</a> .....	13
7. <a href="#">WAN</a> .....	18
7.1 <a href="#">WAN status</a> .....	18
7.2 <a href="#">WAN setting</a> .....	18
7.3 <a href="#">DMZ</a> .....	19
7.4 <a href="#">Firewall</a> .....	19
7.5 <a href="#">WAN ping</a> .....	19
7.6 <a href="#">NAT pass-through</a> .....	20
7.7 <a href="#">Port forwarding</a> .....	20
7.8 <a href="#">VPN server</a> .....	21
7.9 <a href="#">DDNS</a> .....	22
8. <a href="#">Wi-Fi</a> .....	22
8.1 <a href="#">Wi-Fi Status</a> .....	22
8.2 <a href="#">Mesh Wi-Fi</a> .....	22
8.3 <a href="#">Basic Settings</a> .....	23
8.4 <a href="#">Advanced Settings</a> .....	23
8.5 <a href="#">Wi-Fi MAC filter</a> .....	24
8.6 <a href="#">WPS</a> .....	24
8.7 <a href="#">Smart Home Wi-Fi</a> .....	24
8.8 <a href="#">Guest Wi-Fi</a> .....	25
8.9 <a href="#">Antenna Calibration</a> .....	25
8.10 <a href="#">ACS</a> .....	26
9. <a href="#">LAN</a> .....	26
10. <a href="#">IPv6</a> .....	27
11. <a href="#">Home Network Security</a> .....	27
11.1 <a href="#">Network Security Setting</a> .....	28
11.2 <a href="#">Parental Control</a> .....	29
12. <a href="#">System</a> .....	30
12.1 <a href="#">Operation mode</a> .....	30
12.2 <a href="#">Login password</a> .....	30
12.3 <a href="#">System time</a> .....	31
12.4 <a href="#">Languages</a> .....	31
12.5 <a href="#">Backup and restore</a> .....	31
12.6 <a href="#">System Information</a> .....	32
12.7 <a href="#">Restart and Reset default</a> .....	32
12.8 <a href="#">Firmware update</a> .....	32
12.9 <a href="#">System log</a> .....	33
12.10 <a href="#">USB storage</a> .....	33
12.11 <a href="#">Main LED</a> .....	34
13. <a href="#">Troubleshooting</a> .....	35
13.1 <a href="#">Quick Tips</a> .....	35
13.2 <a href="#">FAQs (Frequently Asked Questions)</a> .....	35
14. <a href="#">Appendix factory default settings</a> .....	36
15. <a href="#">Router Basic Specification</a> .....	37

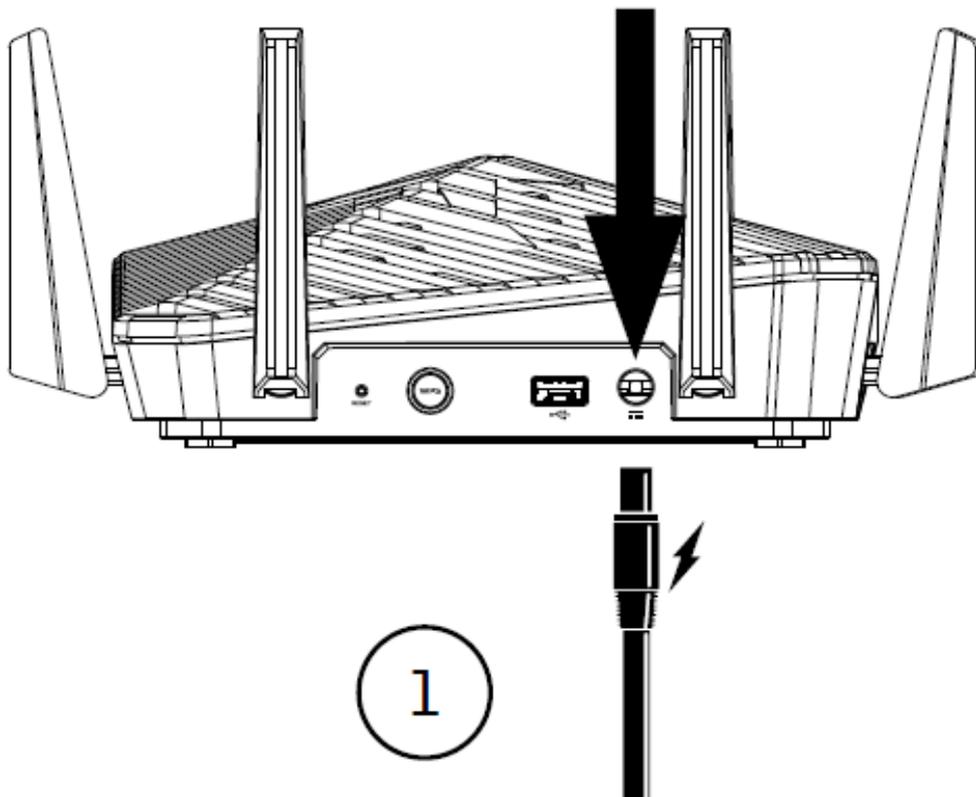
---

# 1. Overview

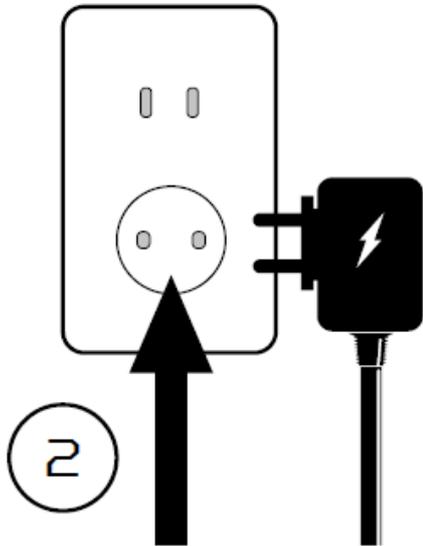
Acer Connect series W6, a whole new Wi-Fi 6E Tri-band AXE7800 wireless router, is optimized for gamers with intensive features and simple setup steps via a 1-2-3 wizard. A new stylish 6-antenna desktop wireless router tuned for optimal gaming experience and for your household. Network Security protection is embedded. Live updates ensure your network is immune from malware and vulnerability threats 24-7. Smart home (IoT) devices can be set up on their Wi-Fi network. ACS (Automatic Channel Selection) dynamically chooses the most suitable channel for the W6 when you experience interference from nearby 5GHz 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. The bridge mode is available for you, extending new Wi-Fi 6GHz coverage for new mobile or laptop devices without replacing your ISP router or MSO DOCSIS modem at home.

## 2. Installation and Setup

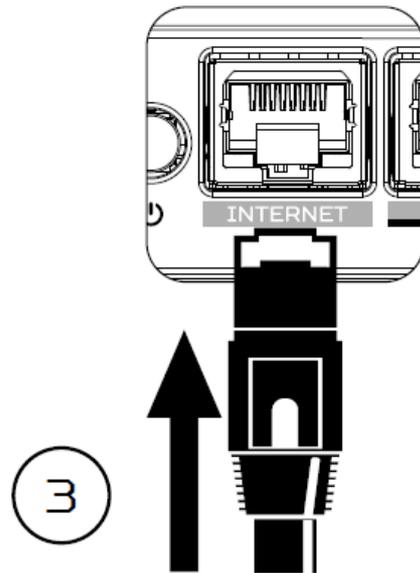
2.1. Plug in the AC adapter.



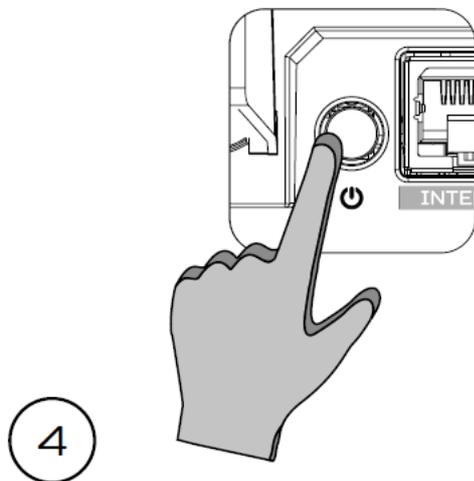
2.2. Plug into an outlet.



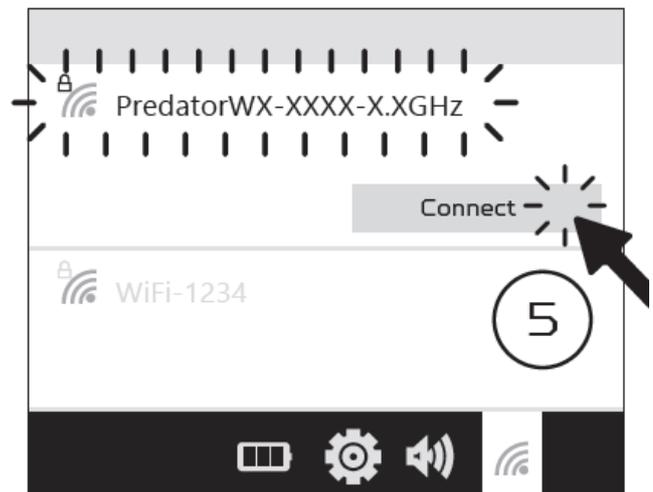
2.3 Plug-in Internet cable.



2.4 Power on the device.



2.5 Connect to PredatorW6 Wi-Fi.



2.6 Important information is at the bottom of the device.



2.7 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.



- 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 bottom label. The default admin and Wi-Fi password will be automatically exported into the mobile app. (SSID: PredatorW6-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 bottom label, and find the router's default SSID (PredatorW6-YYYY) 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.

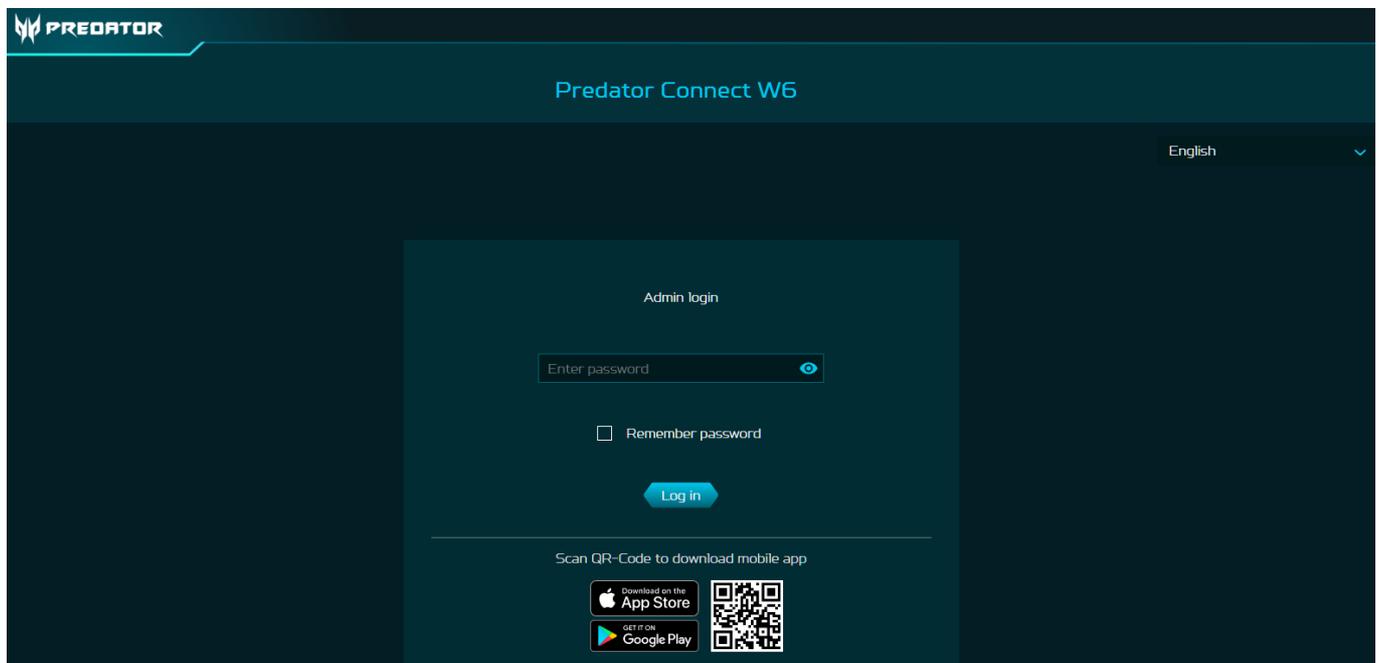
Note: The SSID Wi-Fi password can't be the same as the admin login password.

---

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 W6 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 W6. 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 W6 dashboard.

The screenshot displays the Predator Connect W6 dashboard with a dark teal theme. On the left is a navigation sidebar with the following items: Dashboard, Hybrid QoS, Quick setup, WAN, WiFi, LAN, IPv6, Home network security, System, APP download, and User manual. The main content area is divided into three sections:

- Internet:** Shows WAN connection status as 'Good' with a globe icon. It displays download speed of 2.656 Kbps and upload speed of 3.696 Kbps, along with the IP address 118.163.28.118. A link is provided to check internet speed using SpeedTest.
- Network traffic:** A line graph showing WAN traffic in Kbps over time, with a peak around 10:22:33.
- Mesh topology:** A diagram showing a central 'Controller' node connected to three mesh nodes: 'Wayne offi... W6', 'Agent2 W6', and 'Agent3 W6d'. A legend indicates connection strength: Good (green), Normal (yellow), and Poor (red).
- Predator:** A section for the Predator mesh controller, showing:
  - Mesh WiFi:** Three networks named 'Acer\_W6\_Mesh' with 2.4G and 5G bands. Band steering is 'Enabled'.
  - Guest WiFi:** Three networks: 'W6-Guest-2.4GHz', 'W6-Guest-5GHz', and 'W6-Guest-6GHz'. Band steering is 'Disabled'.
  - Smart home WiFi:** Three networks: 'W6-Smart-home-2.4GHz', 'W6-Smart-home-5GHz', and 'W6-Smart-home-6GHz'. Band steering is 'Disabled'.
  - System up time:** 0 day 00:18:26.
  - Clients:** A row of icons representing connected devices, with a total count of 4.

**Connection Status:** shows the current connection status of Internet.

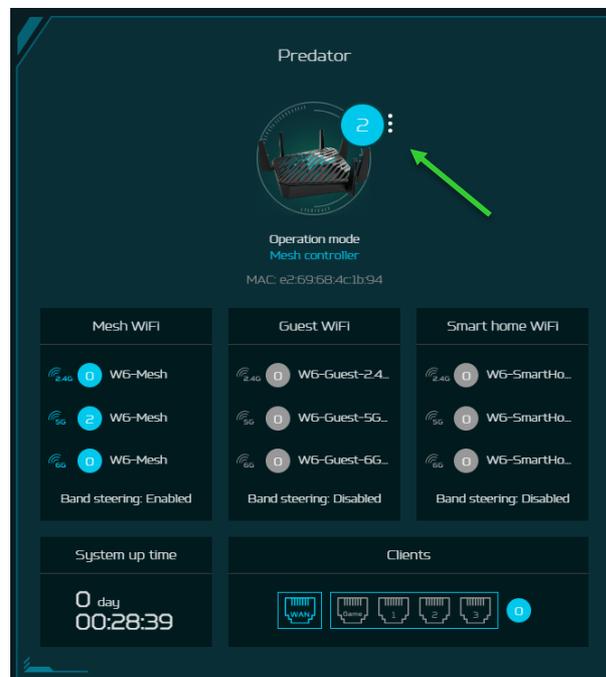
**WAN Status:** shows WAN connectivity and Download/Upload speed and WAN IP.

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

**Wi-Fi Status:** shows the number of wireless client devices connected with 2.4GHz, 5GHz and 6GHz bands.

**LAN Status:** quickly indicates the status of LAN ports. Predator Connect W6 has one WAN port, one Game port and three LAN ports i.e. LAN 1, LAN 2, LAN 3.

The “icon” (at the far right) represents the number of devices connected to the W6 router. Clicking on this icon will display the table shown below.



**Connected Devices:** shows how many client’s devices are connected with your Predator Connect W6 through Wi-Fi or LAN.

You can also modify the device name by clicking on the pencil icon.

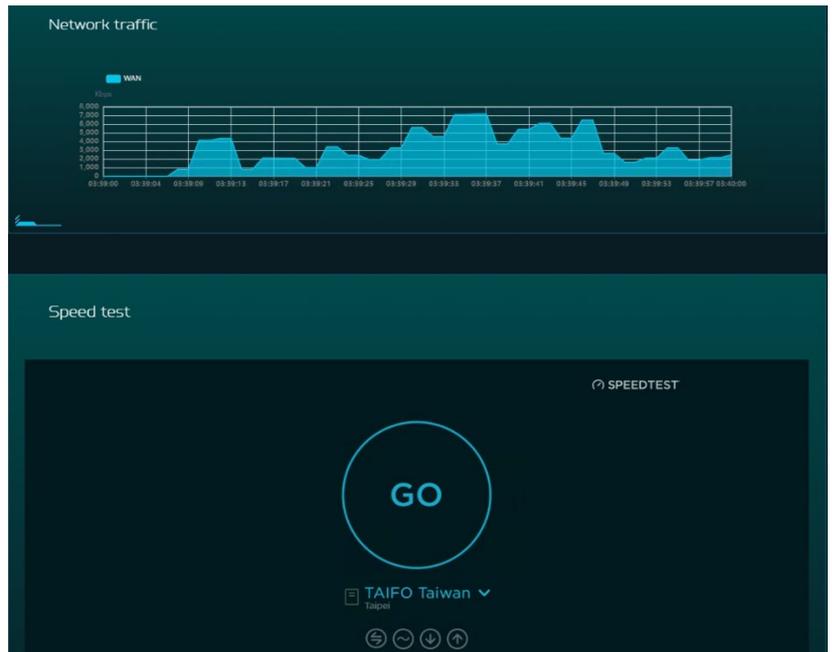
This tab displays the client device name, the IP address allocated by the router, MAC address, mode of connection (whether the device is connected with the router through Ethernet or Wi-Fi), and the duration of device connectivity with the router. You can even block the device from accessing the Internet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

Connected devices					
Connected devices - Host WiFi and others [4]					
Device	IP address	MAC address	Connection	Duration	Edit
Galaxy A10s	192.168.76.194	76:50:e3:07:10:78	Host WiFi-2.4GHz	01:54:30	
Apple iPhone 14	192.168.76.116	7a:69:05:14:79:d1	Host WiFi-2.4GHz	00:32:08	
Apple iPhone 14	192.168.76.250	7a:fd:7e:0cef:d8	Host WiFi-2.4GHz	01:11:09	
SRComputer-PC	192.168.76.168	00:1e:c2:a3:84:07	Host WiFi-5GHz	00:22:48	
Connected devices - Guest WiFi [0]					
Device	IP address	MAC address	Connection	Duration	Edit
Connected devices - Smart home WiFi [0]					
Device	IP address	MAC address	Connection	Duration	Edit
Blocked devices [0]					
Device	MAC address	Edit			

**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 W6 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 W6 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)

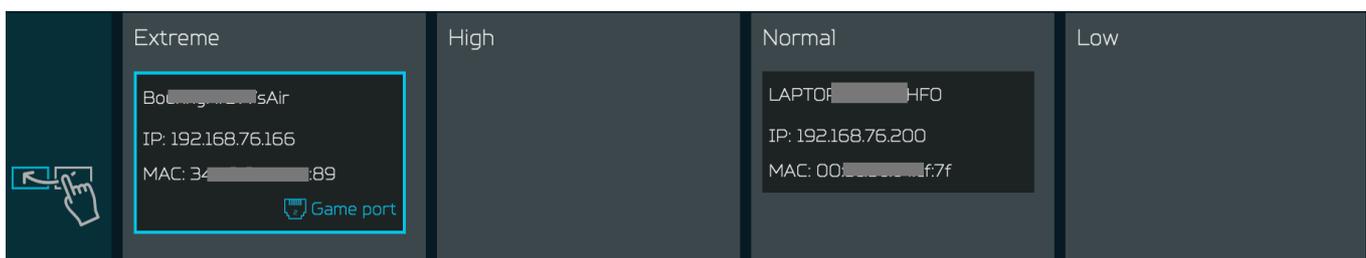
\*Note: Application Priority will use the DSCP value in the IP header for packet classification. Laptop/desktop with Killer™ embedded traffic priorities in four grades by application. I.e. Extreme (Games), High (Streaming), Normal (Browsing), Low (Download).

Priority	Extreme (Games)	High (Streaming)	Normal (Browsing)	Low (Download)
Applications (DSCP) Intel Killer	- 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, GT-Booster	- 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: Game console device is set to default extreme priority whether connected by wired Ethernet or by wireless. The connected device via game port will also get extreme priority.

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.

**Bandwidth**

For the upload and download bandwidth configuration, please contact your ISP to get the exact value of upload and download bandwidth. Or please connect to speedtest website and check the bandwidth result in your network. After the bandwidth is configured, QoS will reserve the bandwidth according to the weighting percentage for each priority queue.

Use default configuration  Setting manually

Upload bandwidth:  Mbps

Download bandwidth:  Mbps

Priority weighting:

Extreme:	High:	Normal:	Low:
<input type="text" value="85"/> %	<input type="text" value="10"/> %	<input type="text" value="3"/> %	<input type="text" value="2"/> %

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.

Hybrid QoS  
Enable Application Priority and Device Priority with bandwidth limitation. Application Priority will use the DSCP value in the IP header for packet classification.

**GeForce NOW**  
Enable optimized performance for GeForce NOW gaming client without bandwidth limitation nor NAT acceleration.  
Note: TrendMicro engine will be stopped.

Max Throughput  
Enable maximum performance for router with NAT acceleration and without bandwidth limitation.

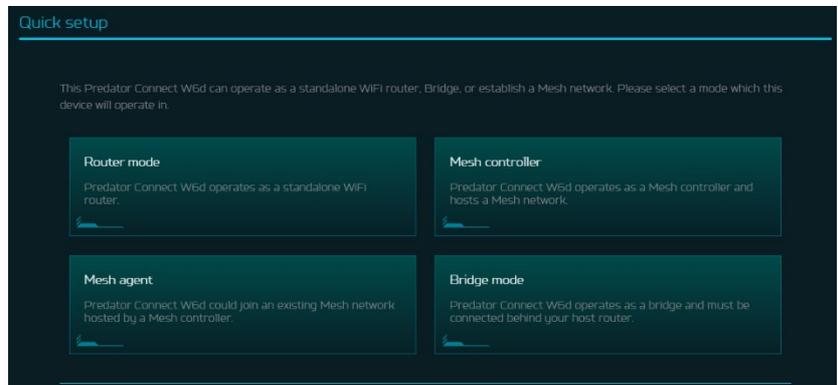
You can select **GeForce NOW** option to enable optimized performance for GeForce NOW gaming clients without bandwidth limitation or NAT acceleration. Note: TrendMicro engine will be stopped.

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

# 6. Quick Setup

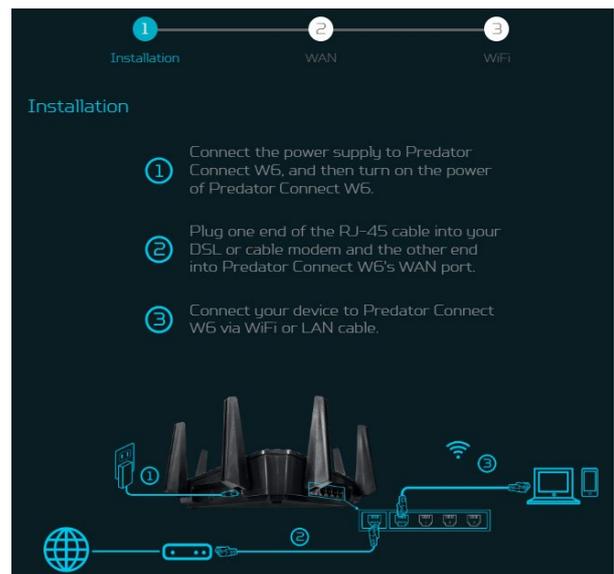
The Predator Connect W6 can operate as a standalone Wi-Fi router, Bridge, or establish a Mesh network. Please select a mode which this device will operate in:

- 1) Router Mode
- 2) Mesh Controller
- 3) Mesh Agent
- 4) Bridge mode



In **Router mode**, plug one end of the RJ-45 cable into your DSL or cable modem and the other end into Predator Connect W6d's WAN port.

Connect your device to Predator Connect W6d 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)

Note: To keep a better performance, please be aware that a controller could only have 3 agents under its network.

For the fourth agent, it will be performed factory reset after connecting to the mesh network and switched back to router mode automatically.

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.

How to create a Mesh network

- 1 Set one router as Mesh controller. (A)
- 2 Set another router as Mesh agent. (B)



Note: To keep a better performance, please be aware that a controller could only have 3 agents under its network. For the fourth agent, it will be performed factory reset after connecting to mesh network and switched back to router mode automatically.

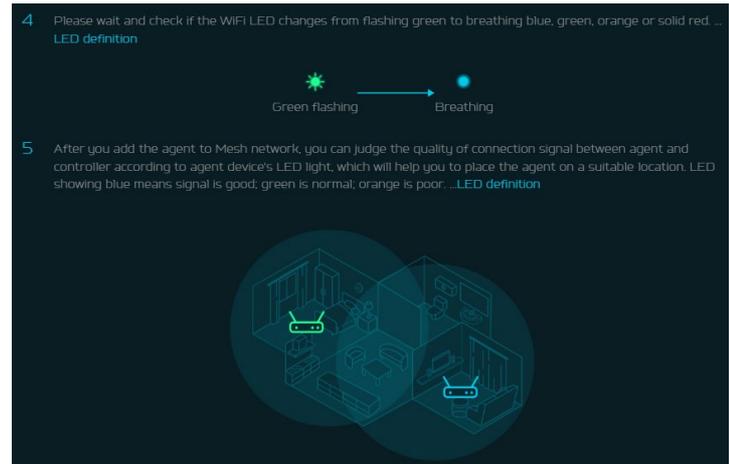
3 There are two ways to onboard an agent to a Mesh network:

- (C) Press the WPS button on both devices for 2 seconds at the same time.
- (D) Connect agent to controller via LAN cable.



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

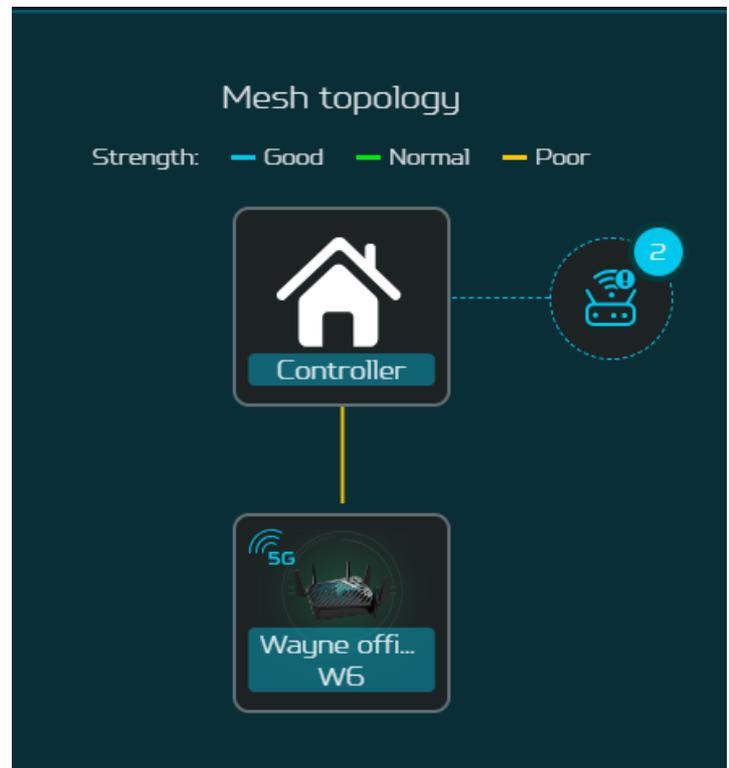
Following are the mesh topologies:

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

#### Topology – One Agent

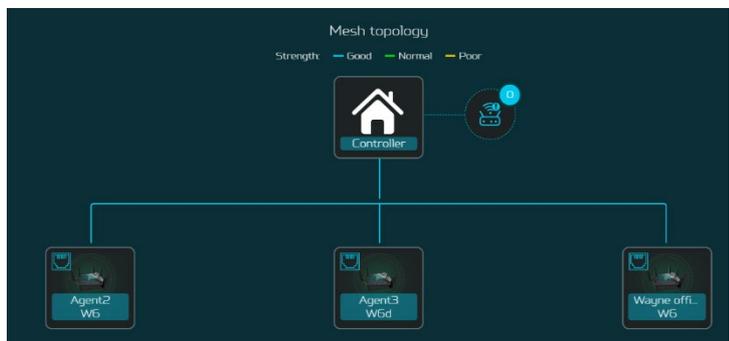
In one agent topology, a controller is connected with one agent, and the medium between a controller and the agent can be wireless or wired connectivity.

Yellow color line indicates the poor signal strength between a controller and the agent, so it is 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.

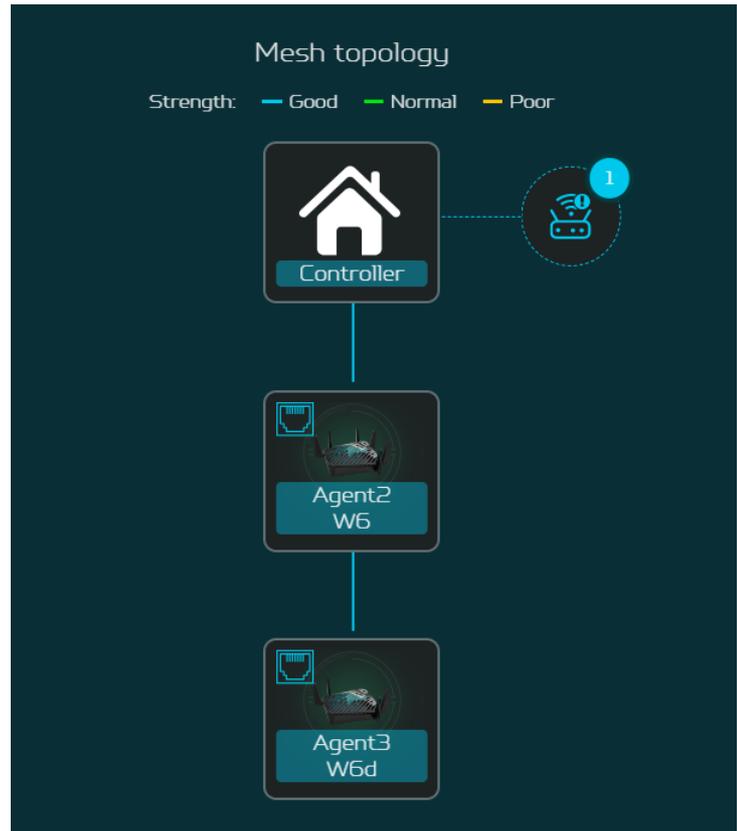


### Daisy Chain topology – 2 agents

In daisy chain topology of 2 agents, a controller is connected with agent 2, and the agent 3 is connected with the agent 2, making a chain topology.

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

Blue color line indicates a good signal strength.

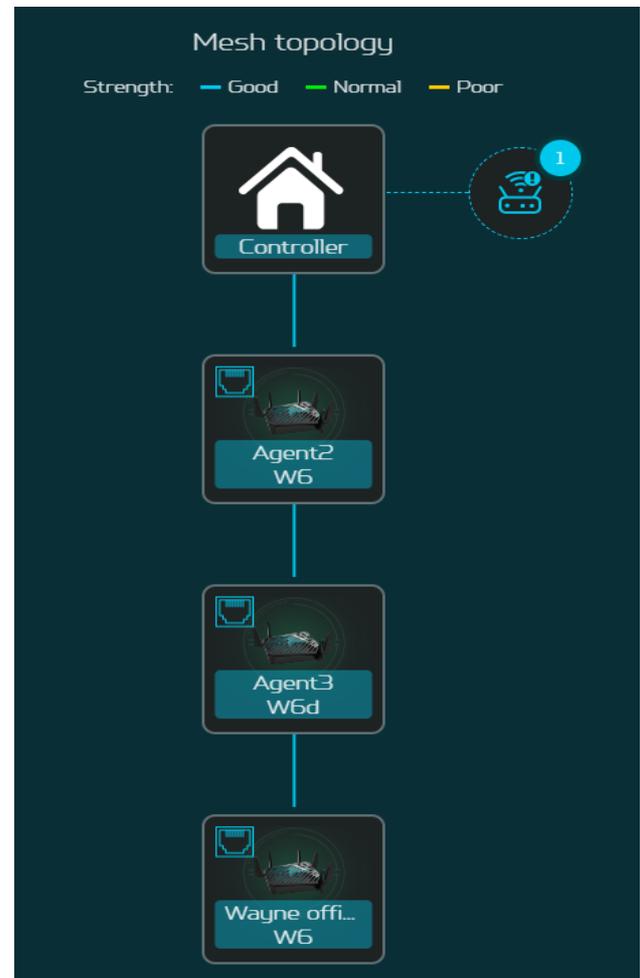


### Daisy Chain topology – 3 agents

In daisy chain topology of 3 agents, a controller is connected with agent 2, agent 3 is connected with agent 2, and last agent is connected with agent 3, making a chain topology of 3 agents.

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

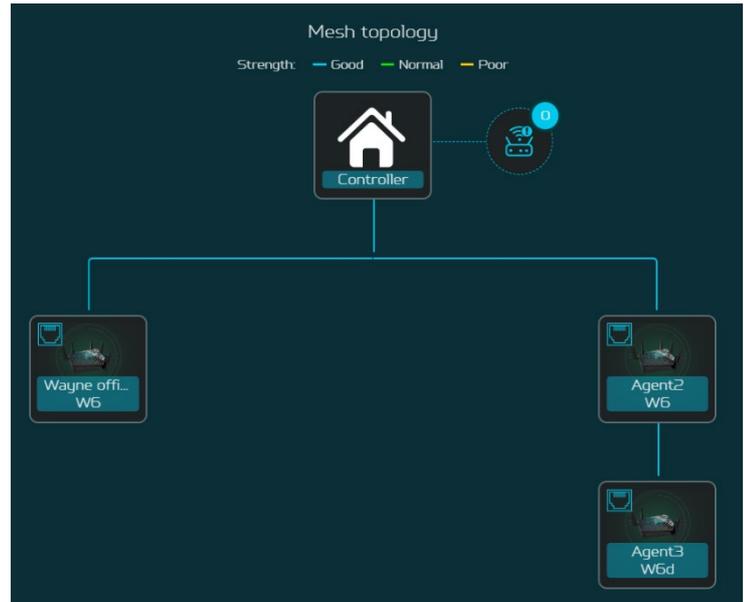
Blue color line indicates a good signal strength.



## Tree topology – 3 agents

In tree topology of 3 agents, a controller is directly connected with two agents; whereas a third agent (Agent 3) is connected with agent 2, making a tree topology.

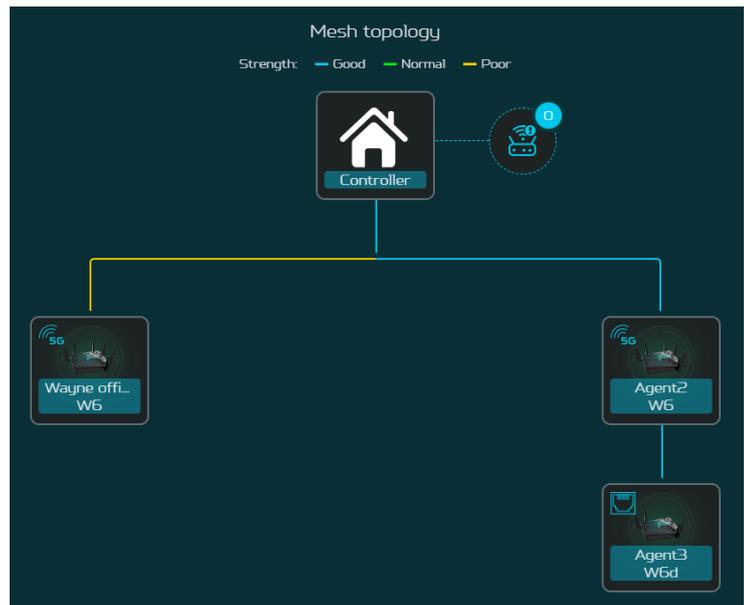
Medium between a controller and the agents can be wireless or wired connectivity.



## Agent connected via Wi-Fi

In this topology, a controller is wirelessly connected with the two agents; whereas the third agent (Agent 3) is connected with agent 2 through wired connectivity.

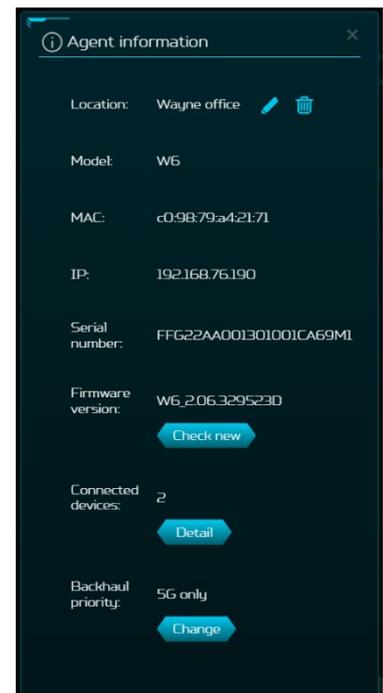
Yellow color line indicates a poor signal strength, and the blue color line indicated a good signal strength.



## 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:

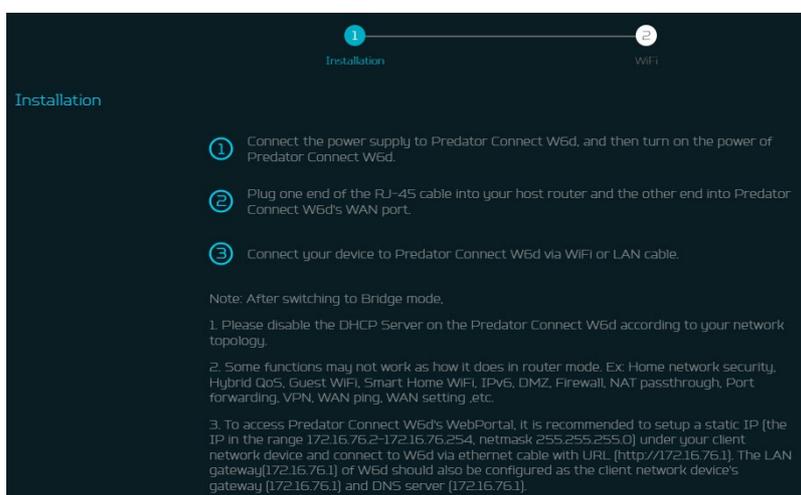
- I. Due to the adoption of front-haul and backhaul sharing bandwidth to connect various nodes in the Mesh network, if the Mesh agent is in a daisy-chain configuration, each layer of connected nodes needs to simultaneously handle communication with both upper-layer nodes and lower-level devices. As a 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 client devices connect to the Mesh network through the front-haul interface of each node, while the connection between nodes relies on the backhaul bandwidth to reach the controller and then access the Internet. In other words, the speed at which clients connect to the Internet cannot exceed the backhaul bandwidth. Users can configure their preferred band for the backhaul using the GUI. Here are the maximum rates achievable when using each band as backhaul:
  - 6GHz with 160MHz bandwidth: DL1201Mbps/UL1201Mbps (default using the maximum available 6GHz bandwidth).
  - 5GHz with 80MHz bandwidth: DL1201Mbps/UL1201Mbps (default using 5GHz bandwidth to avoid DFS radar interference or CAC connection wait).
  - 2.4GHz with 20MHz bandwidth: DL286Mbps/UL286Mbps (default using 2.4GHz bandwidth to avoid interference from neighboring 40MHz bandwidth signals)
- III. Limitations of the W6 series Mesh: A maximum of one controller + three agents are allowed. Products that can act as controllers: Predator Connect X5/W6/W6d, Acer Connect Vero W6m. Products that can act as agents: Predator Connect W6/W6d, Acer Connect Vero W6m. Users will be reminded to avoid adding a fourth agent. When a user attempts to add a fourth agent, the fourth agent will be forcibly factory reset to the router state. The more agent nodes connected, the more devices share the bandwidth. Particularly in daisy-chain topology networks, we recommend keeping the number of agents connected to three or fewer.
- IV. All devices are factory-defaulted as routers. Users can change the device role (e.g., Mesh controller, Mesh agent, or bridge) through Quick Setup.
- V. Once a device has been set as a Mesh controller, Mesh agent, or bridge, 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, agent, or bridge (using GUI operation mode or Quick Setup).
- VI. Currently, only the controller supports Guest & Smart Home Wi-Fi, while it cannot be used in agent nodes. Agent nodes will not have any Guest & Smart Home Wi-Fi options.

- VII. 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.
- VIII. 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.

In **bridge mode**, plug one end of the RJ-45 cable into your host router and the other end into Predator Connect W6's WAN port.

Please note that after switching to bridge mode, disable the DHCP server. Some functions like Home network priority, Hybrid QoS, Guest Wi-Fi, Smart Home Wi-Fi, IPv6, DMZ, Firewall, NAT, pass-through, port forwarding, VPN, WAN ping, WAN setting etc. may not work.

To access Predator Connect W6's web portal in a bridge mode, it is recommended using a static IP.

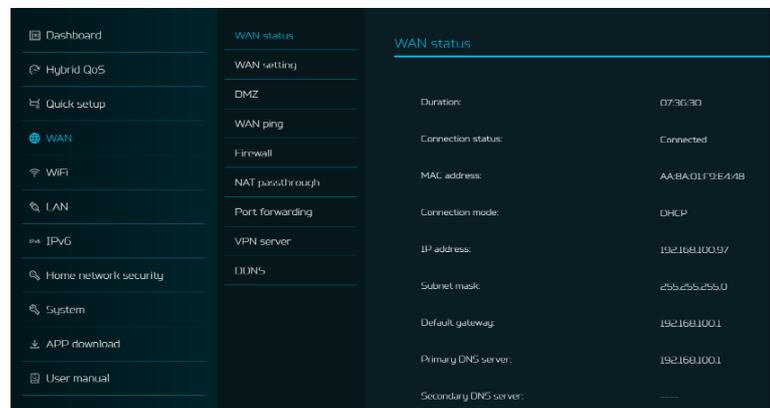



# 7. WAN

## 7.1 WAN Status

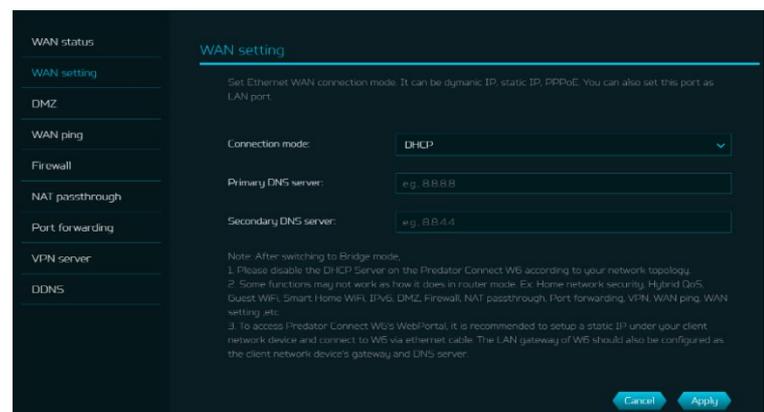
This tab provides information about WAN connectivity status and the following key information:

- 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 LAN, depending on your connection usage. Click on down arrow to reveal the drop-down the menu to select your preferred WAN settings.



You can select “Switch WAN port to LAN (Switch/Bridge mode)”, if you are using the router in bridge mode in which the port is not required. As a result, you can have one more LAN port.

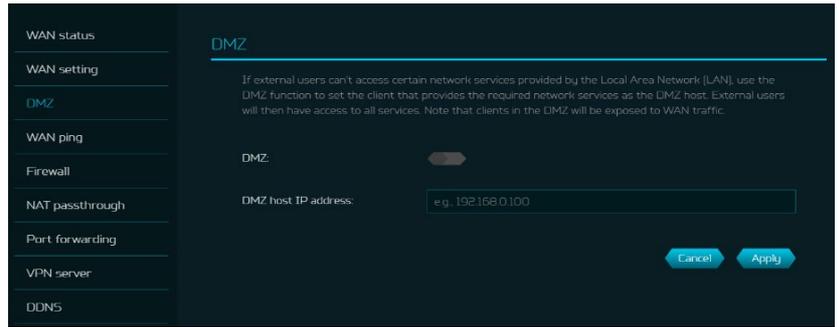
Note: After switching to Bridge mode,

- 1) Please disable the DHCP Server on the Predator Connect W6 according to your network topology.
- 2) Some functions may not work as how it does in router mode. E.g. Home network security, Hybrid QoS, Guest Wi-Fi, Smart Home Wi-Fi, IPv6, DMZ, Firewall, NAT pass-through, Port forwarding, VPN, WAN ping, WAN setting.
- 3) To access Predator Connect W6’s web portal, it is recommended to set up IP under your client network device and connect to W6 via Ethernet cable. The LAN gateway of W6 should also be configured as the client network device’s gateway and DNS server.

### 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.

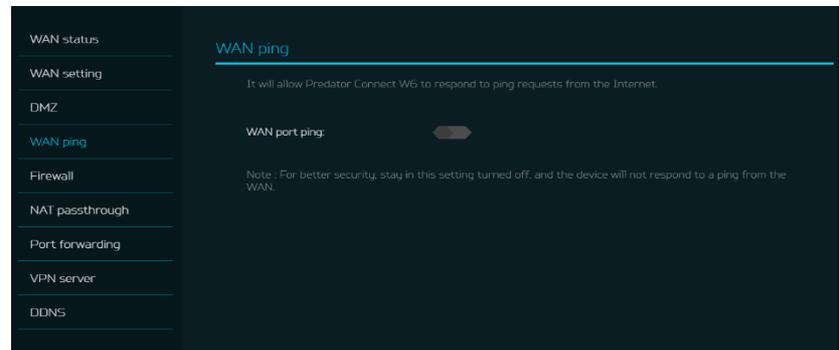
If external users can't access certain network services provided by the Local Area Network (LAN), use the DMZ function to set the client that provides the required network services as the DMZ host. The host IP address needs to be entered and then external users will have access to all services.



### 7.4 WAN Ping

By enabling this feature, WAN port of Predator Connect W6 will respond to ping requests that are sent to the WAN IP address from the Internet.

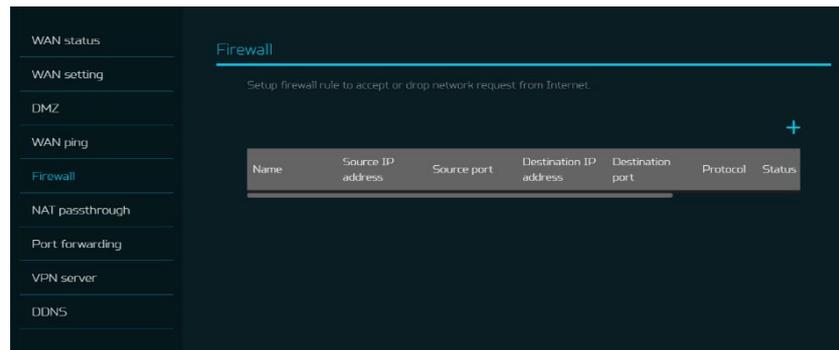
For better security, keep the feature turned OFF, and the device will not respond to a WAN ping.



### 7.5 Firewall

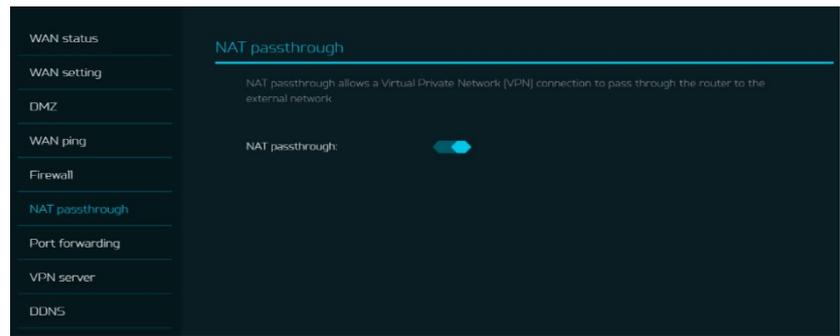
Setup firewall rule to accept or drop network requests from Internet.

To set up a firewall, click on (+) icon and enter the name, source and destination port and IP address, protocol, target and status info.



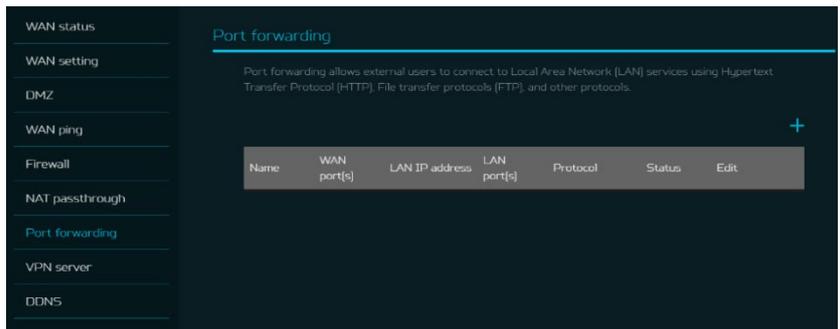
## 7.6 NAT pass-through

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 W6 for remote VPN connection over the Internet. This router offers two VPN services:

- 7.8.1 OpenVPN
- 7.8.2 IPsec VPN

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).

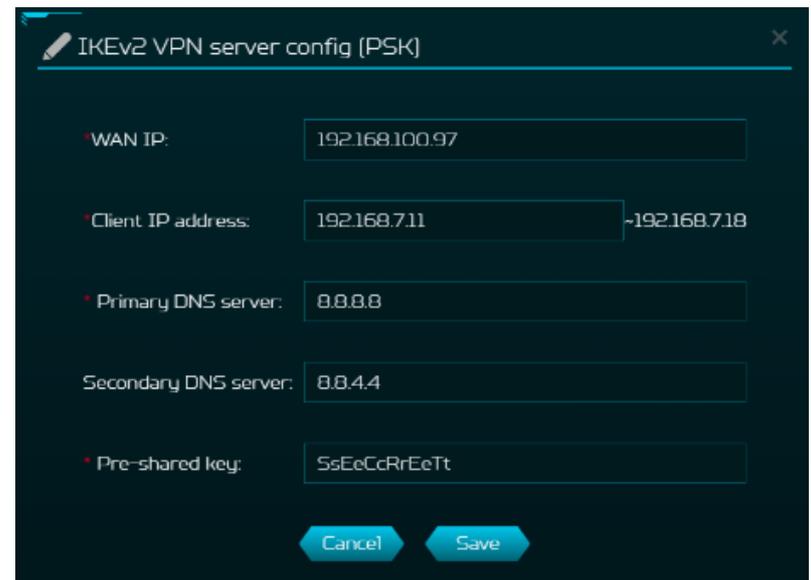
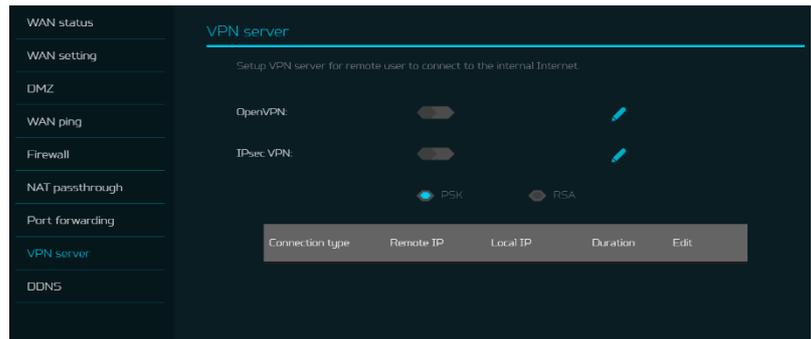
Enter the following information to configure Open VPN services.

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

**IPsec VPN** uses predefined communication channels, UDP 500 and UDP 4500, to establish the encrypted tunnel and ESP for the transmission of encrypted data.

Enter the following information to configure IPsec VPN services.

- 1) WAN IP address
- 2) Client IP address
- 3) Primary DNS server
- 4) Secondary DNS server
- 5) Pre-shared key



## 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.

The screenshot shows the DDNS configuration page. At the top, there is a title 'DDNS' and a brief explanation: 'A dynamic domain name system service provides a fixed domain name for your router's dynamic IP address. You'll need to register with a DDNS service.' Below this, there are several configuration options:

- Enable DDNS:** A toggle switch that is currently turned on (blue).
- DDNS service:** A dropdown menu with 'Dyn.com' selected.
- Host name:** A text input field containing 'yourhost.example.com'.
- Username:** A text input field containing 'your\_username'.
- Password:** A text input field with a masked password '.....' and an eye icon to toggle visibility.
- Use external IP check:** A toggle switch that is currently turned on (blue).
- Use HTTP secure:** A toggle switch that is currently turned off (grey).

At the bottom right, there are 'Cancel' and 'Apply' buttons. Below the configuration fields, there is a status section:

- WAN status:** IP: 119.73.124.130, Connected (indicated by a blue square).
- DDNS status:** Unchecked, with a 'Check status' button.

# 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

The screenshot shows the 'Wi-Fi status' page. On the left, there is a navigation menu with options: Dashboard, Hybrid QoS, Quick setup, WAN (selected), WiFi, LAN, IPv6, Home network security, System, APP download, and User manual. The main content area is divided into two columns:

- Left Column (WIFI status):** Contains links for Mesh WiFi, WiFi MAC filter, Smart home WiFi, Guest WiFi, and ACS.
- Right Column (WiFi status):** Displays details for two frequency bands: 2.4GHz and 5GHz. For each band, it shows: WiFi SSID (W6-Mesh), SSID broadcast (Enabled), Security (WPA2), Channel (Auto[Channel 10]), Connected devices (0), Gateway address (192.168.76.1), and MAC address (00:0c:43:25:60:00).

## 8.2 Mesh Wi-Fi (In Mesh Mode)

This tab provides information about Mesh Wi-Fi SSID, security settings, encryption and Wi-Fi password.

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

The screenshot shows the 'Mesh WiFi' configuration page. On the left, there is a navigation menu with options: WiFi status, Mesh WiFi (selected), WiFi MAC filter, Smart home WiFi, Guest WiFi, and ACS. The main content area displays configuration options for Mesh WiFi:

- WiFi SSID:** A text input field containing 'Acer\_W6\_Mesh'.
- Security:** A dropdown menu with 'WPA2' selected.
- Encryption:** A dropdown menu with 'AES' selected.
- WiFi password:** A text input field with a masked password '.....' and an eye icon to toggle visibility.

At the bottom right, there are 'Cancel' and 'Apply' buttons.

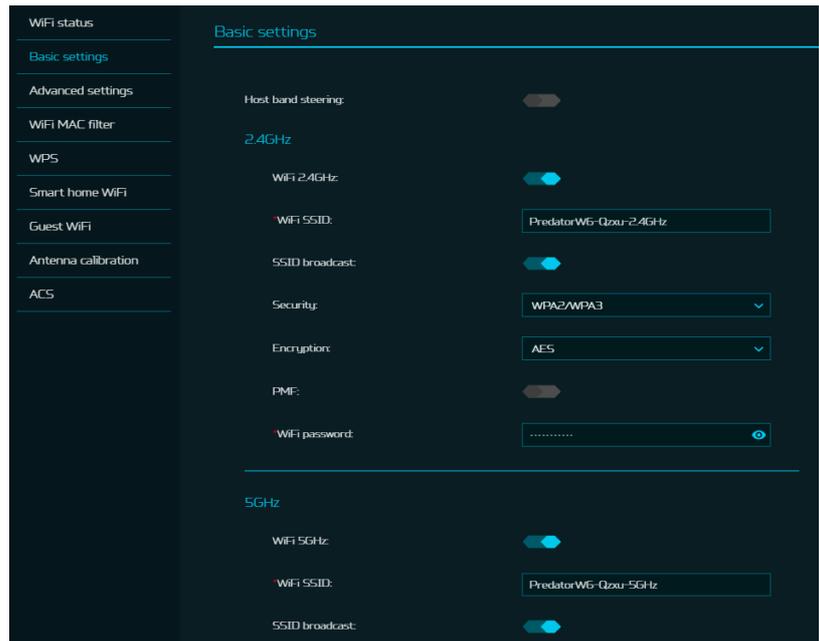
### 8.3 Basic Settings (Router Mode)

This tab shows only when the W6 is configured in router mode.

In this page, you can edit Wi-Fi SSID and enable or disable SSID broadcast and use the following security parameters for 2.4GHz, 5GHz & 6GHz bands

WPA, WPA2, WPA/WPA2, WPA3 personal, WPA2/WPA3, Enhanced open;  
Encryption option: AES, Auto, TKIP. Auto and TKIP are available only, when WPA, WPA/WPA2 security option applied.

The Wi-Fi band steering must be ON in the mesh mode; whereas, in the router mode, user can switch ON/OFF for band steering in the host Wi-Fi.



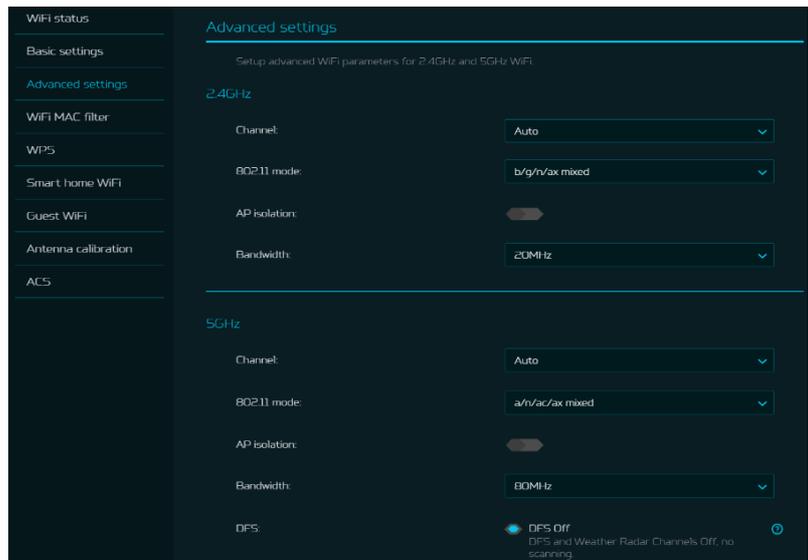
### 8.4 Advanced Settings

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.

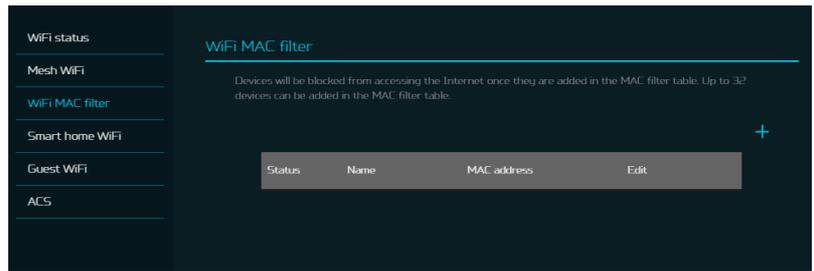
802.11 mode will be “ax only”, as it is the latest Wi-Fi standard and is the highest performing. Bandwidth will be 160MHz by default and you can choose to select in between 20MHz to 160MHz.



## 8.5 Wi-Fi MAC filter

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

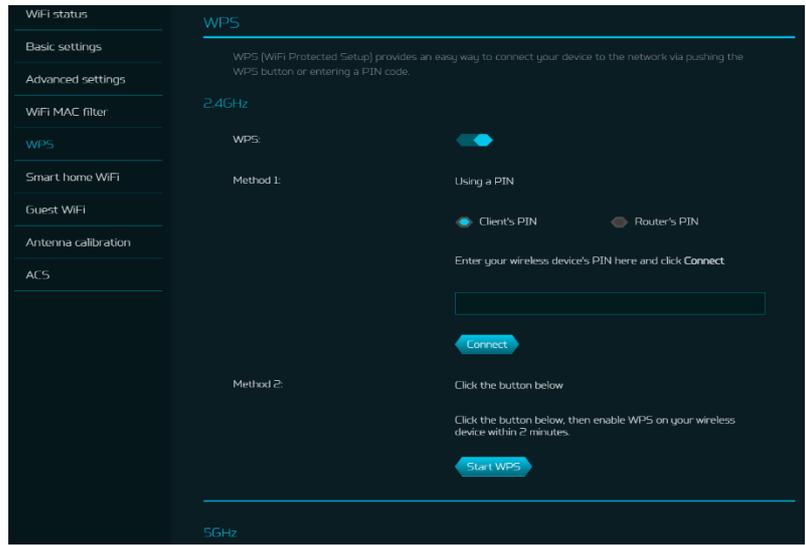
Click on the (+) icon to add the device in the filter table by entering its name & MAC address. Up to 32 devices can be added to the MAC filter.



## 8.6 WPS

WPS (Wi-Fi Protected Setup) provides an easy way to connect your device to the network by pushing the WPS button (next to the USB port) or entering a PIN code.

On this page, you can configure the WPS settings of 2.4GHz and 5GHz bands. There are two methods to configure WPS i.e. using a PIN (client's pin or Router's pin) or you can choose a second method, in which you need to 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.

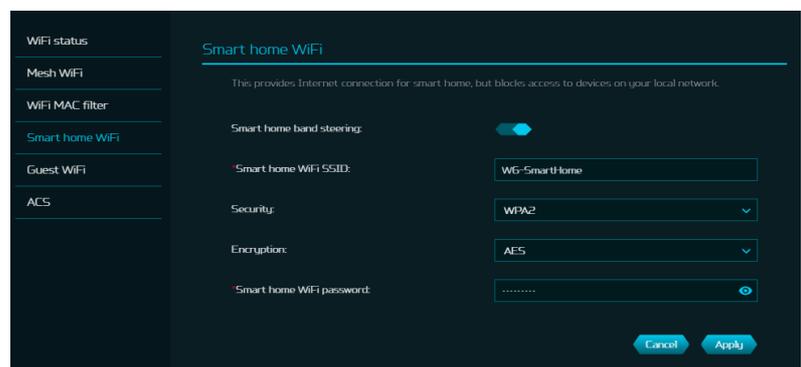


## 8.7 Smart Home Wi-Fi

This tab provides Internet connection for smart home Wi-Fi, but blocks access to devices on your local network.

With the band steering feature enabled, it automatically connects your devices to the best available Wi-Fi frequency in your surroundings.

Smart home Wi-Fi password is set by default, so it is suggested to change the passwords for security reasons.

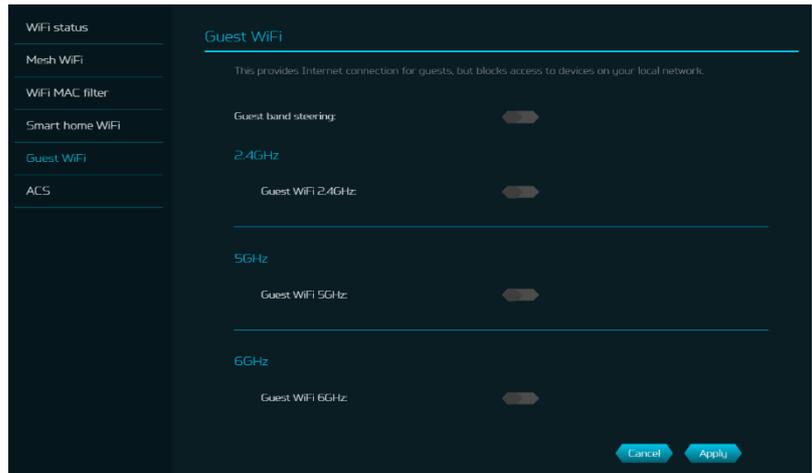


## 8.8 Guest Wi-Fi

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

Guest Wi-Fi and Smart home Wi-Fi only works on controller mode. It means that the client can't connect to guest/smart home Wi-Fi via mesh agents.

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



## 8.9 Antenna Calibration

In general, we suggest putting all six router antennas up (90 degrees vertically with the surface) toward the ceiling when positioned on a flat desk. However, if you want a specific client to benefit from lower latency for a better gaming experience, you can follow the steps below to adjust the antenna angle accordingly.

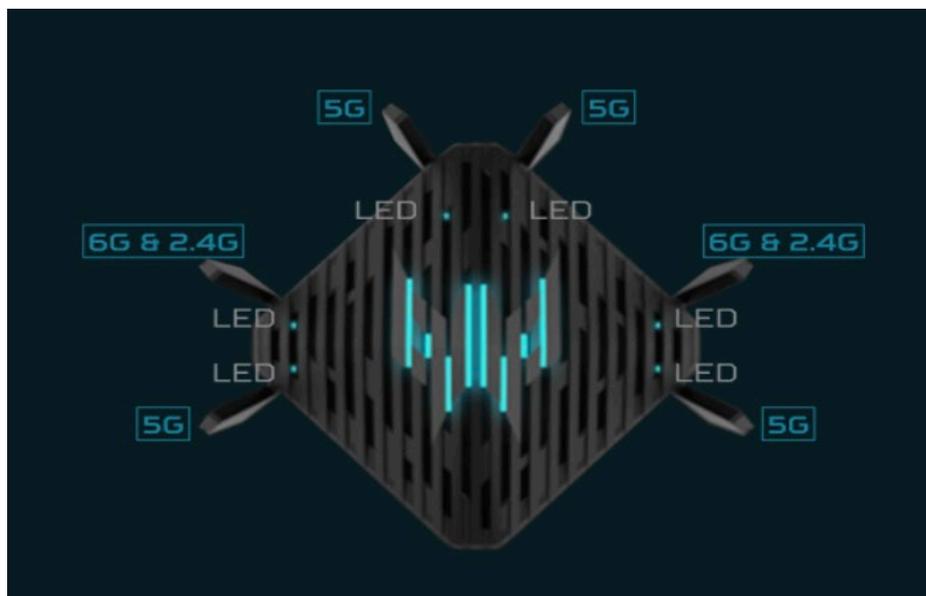
### Step 1:

Put the mobile or laptop in a position where you want the best coverage, and then enable the calibration option.

Note: Walls and floors affect the signal between the router and your device. For an optimal signal, it is recommended to put your device in the line of sight with the router.

### Step 2:

LED indicators adjacent to the router antenna use color to reflect the signal strength: blue is good; green is normal; red is weak.



Note 1: Please make sure that your mobile device or computer is wirelessly connected to the router. The feature is not applicable when connected via Ethernet LAN.

Note 2: Four signal strength LEDs will be ON when the client is associated with 5GHz and calibrated. If the client is associated with 2.4GHz or 6GHz, only two signal-strength LEDs will be ON.

### Step 3:

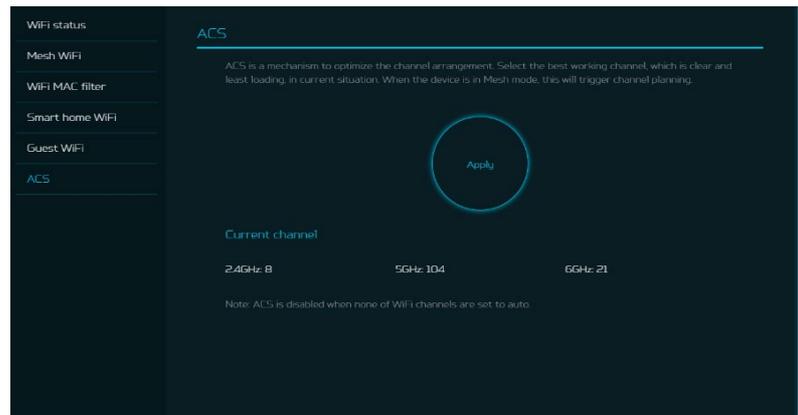
Adjust each antenna direction to get better performance.

## 8.10 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 W6 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.

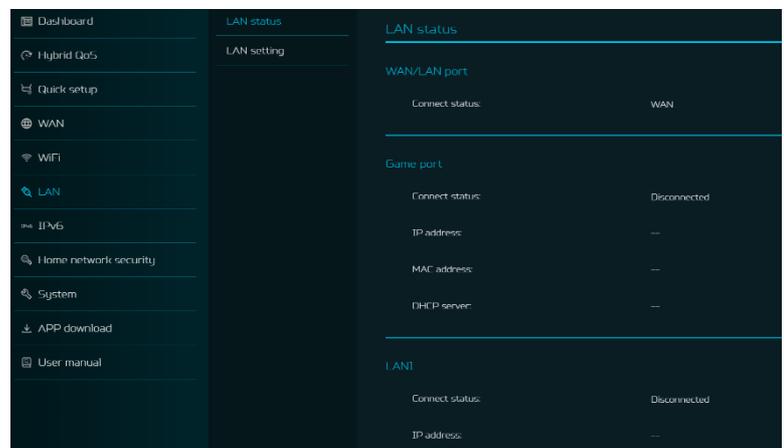


# 9. LAN

## 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 W6 has one Game port and three LAN ports.

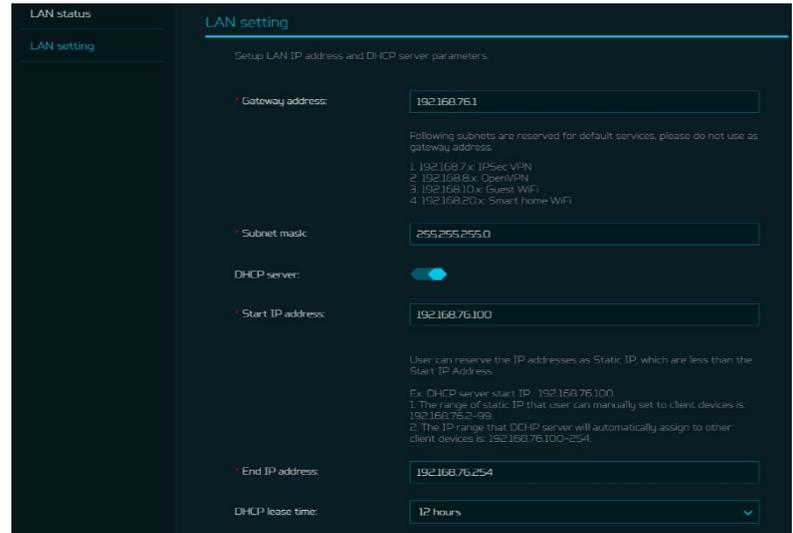


## LAN Setting

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)
4. 192.168.20.x (Smart Home Wi-Fi)



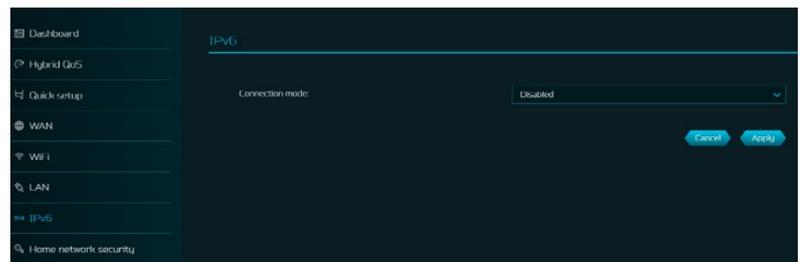
## 10. IPv6

You can setup IPv6 settings from this tab.

The Predator Connect W6 supports IPv6 mode below: DHCPv6, static IPv6, PPPoE, 4G4xlat, 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

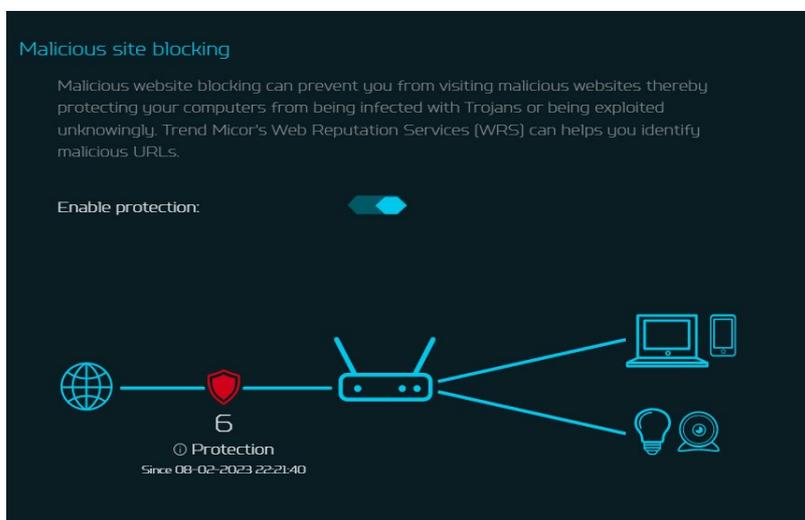
The home network security tab includes network security settings and web and app controller within the parental control feature. These two features must accept the Trend Micro license agreement before enablement.

## 11.1 Network Security

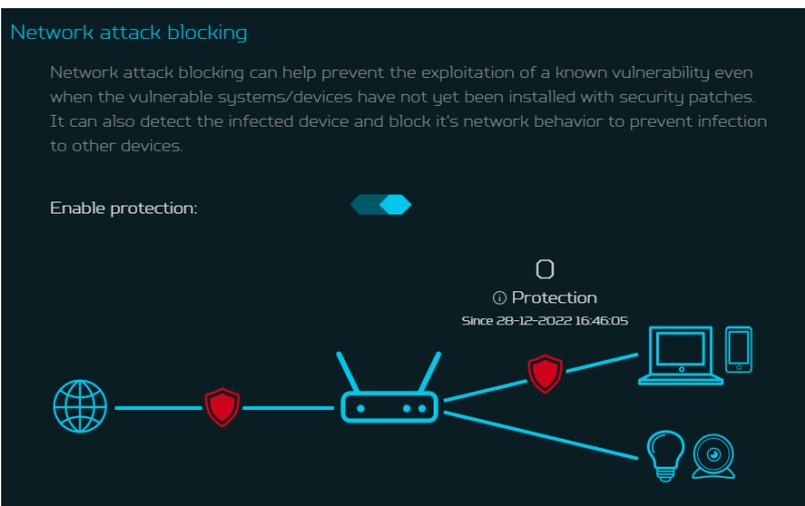
This tab contains the network security-related information, powered by Trend Micro, where you can turn on/off the security engine and enable protection against malicious sites, network attacks and harmful connections coming from IoT devices.



**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.

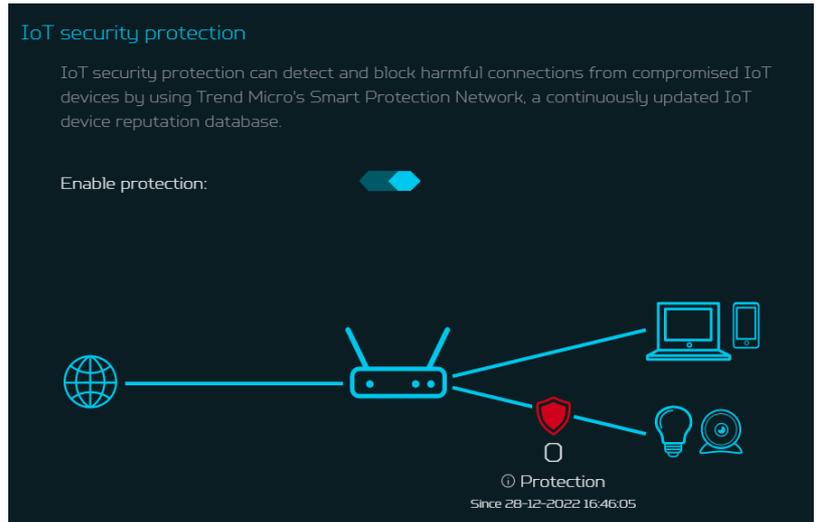


By enabling **Network attack blocking** feature, the router detects the infected devices and block its network behavior to prevent infection in other devices.



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

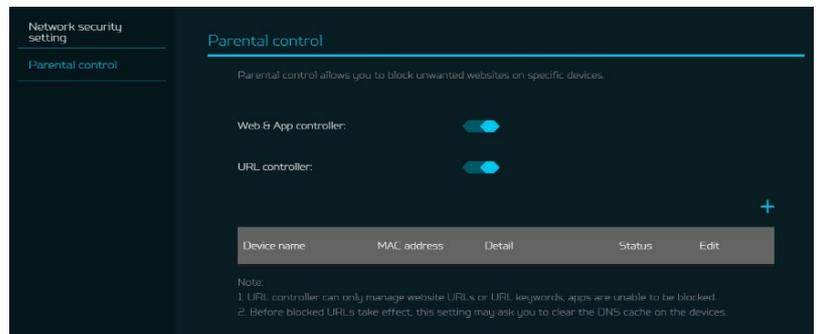
It's a continuously updated IoT device reputation database that prevents the network from false connections.



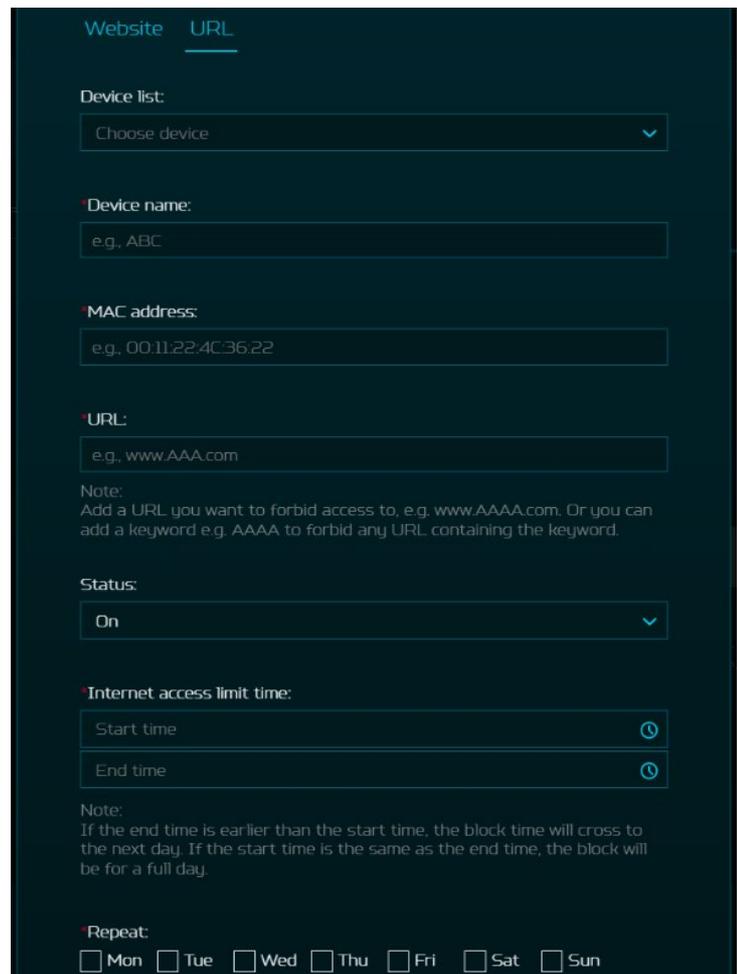
## 11.2 Parental Control

This feature allows you to control and block unwanted sites on specific devices. You can enable/disable Web & App controller & 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, status and select the following categories for blocking websites.



- **Adult**  
Block websites and Apps which include Adult, Mature, Illegal, Prohibited, Alcohol, Tobacco, Gambling, Violence, Hate, Racism, Weapons, Illegal Drugs related content.
- **Instant Messaging and Communication**  
Block websites and Apps related to Social Networking and Instant Messaging like Facebook, Instagram, Twitter etc.
- **P2P and File Transfer**  
Block websites and Apps which include P2P or File transfer.

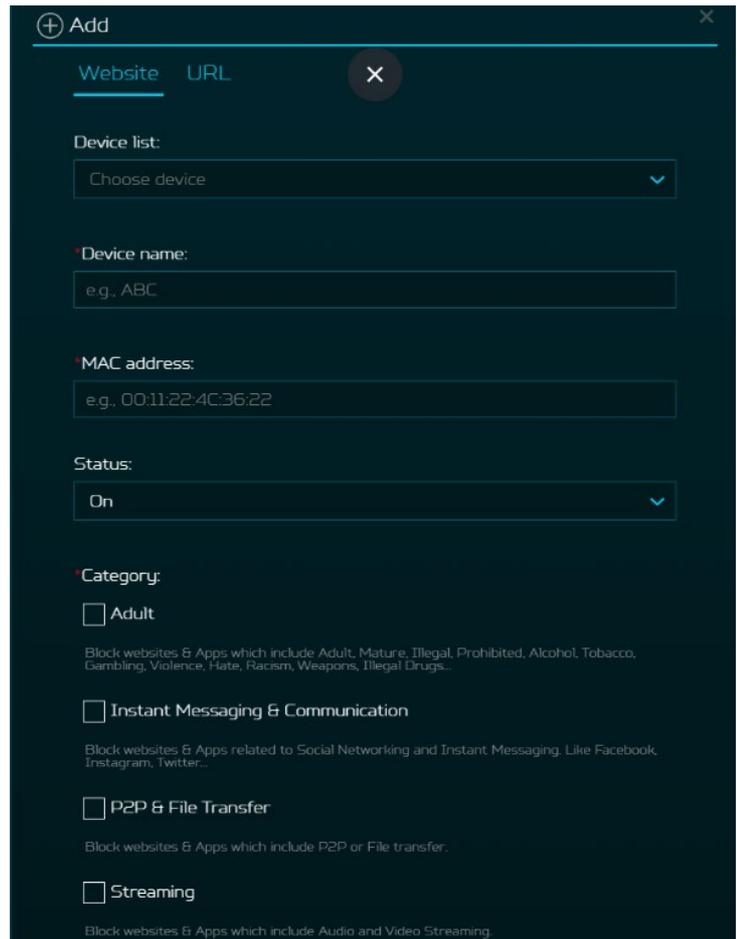


- **Streaming**

Block websites and Apps which include Audio and Video streaming. Under the URL tab (see adjacent image) you can enter the device list, device name, its MAC address and URL, which you want to forbid access to e.g. www.aaaa.com. Or you can add a keyword e.g. AAAA to forbid any URL containing the keyword.

You can also enter the Internet access time limit by setting the start time and end 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.

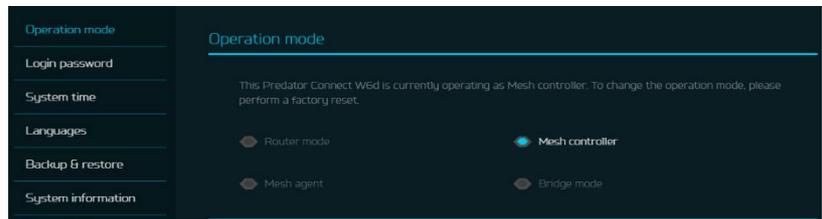


## 12. SYSTEM

### 12.1 Operation Mode

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

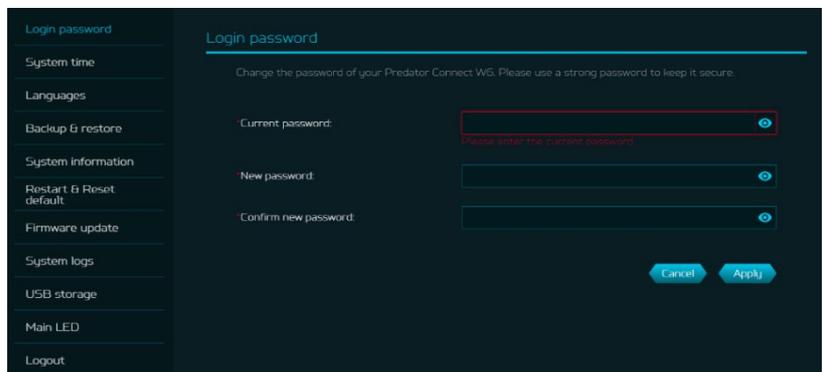
Currently, the Predator Connect W6d is operating as Mesh controller.



### 12.2 Login Password

You can change the password of your Predator Connect W6 from this page.

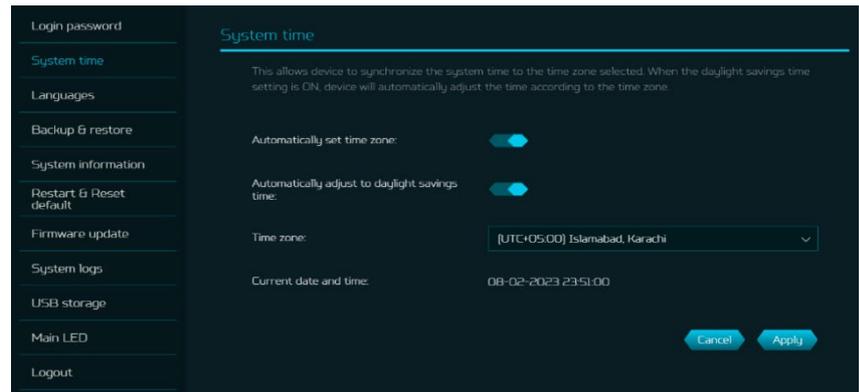
To make a new password, you need to enter your current password first. Please use a strong password to keep it secure.



## 12.3 System Time

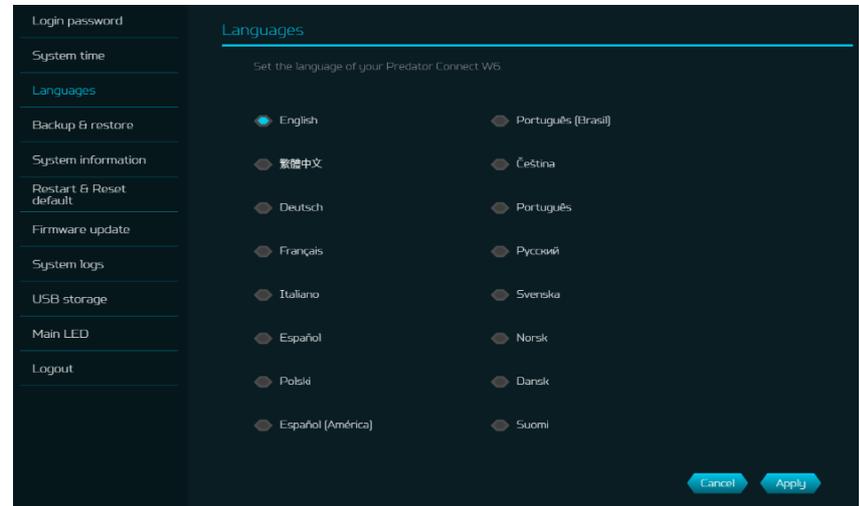
This tab allows you to synchronize the device time with the system time by enabling “Automatically set time zone”.

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



## 12.4 languages

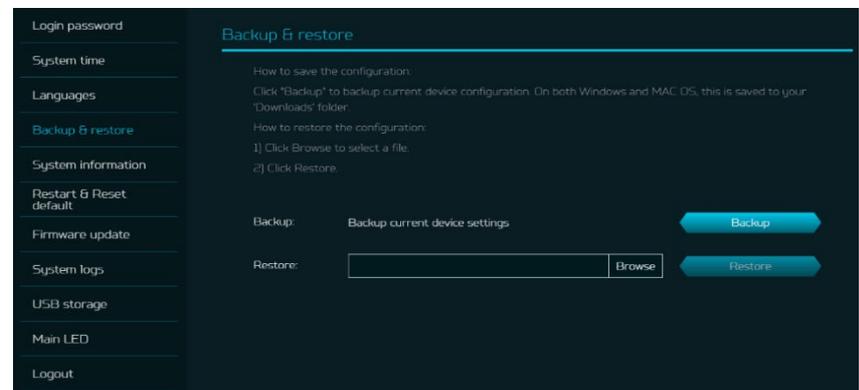
You can select the language of your Predator Connect W6 from this tab.



## 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.

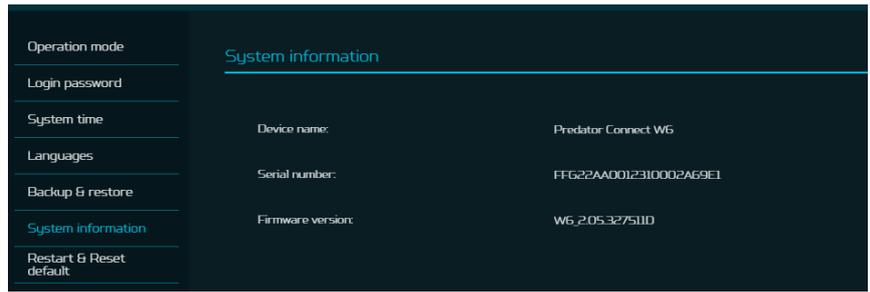
How to restore the configuration:  
1) Click Browse to select a file  
2) Click Restore



## 12.6 System Information

It shows key device information of Predator Connect W6, such as:

- Device name
- Serial number
- Firmware version

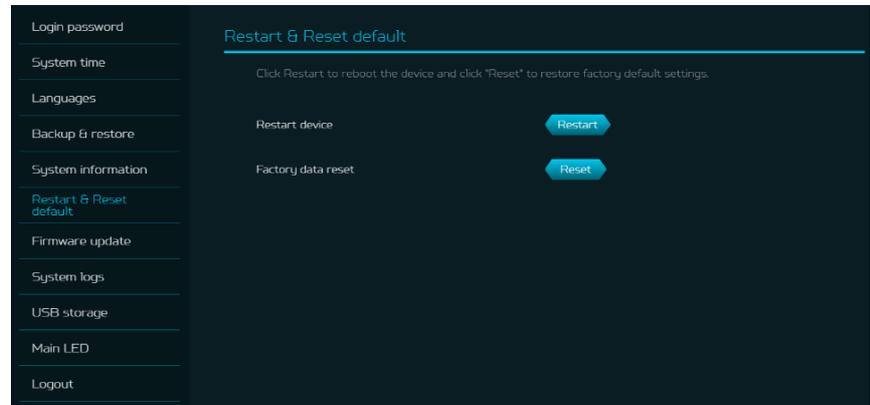


## 12.7 Restart and Reset Default

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.

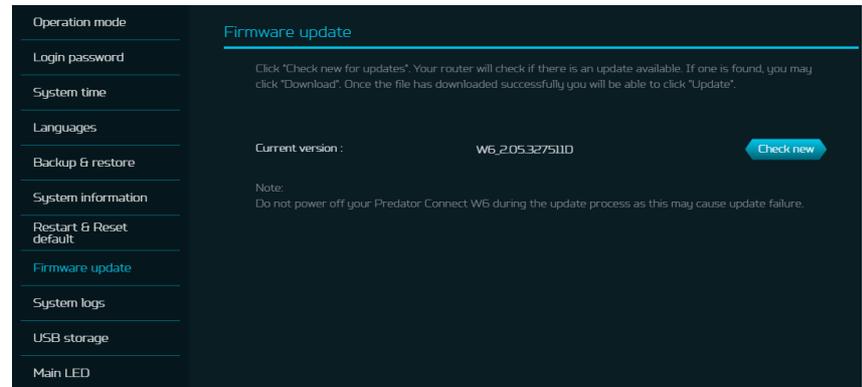
After the factory reset, please don't forget to unbind the device from the mobile app.



## 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.

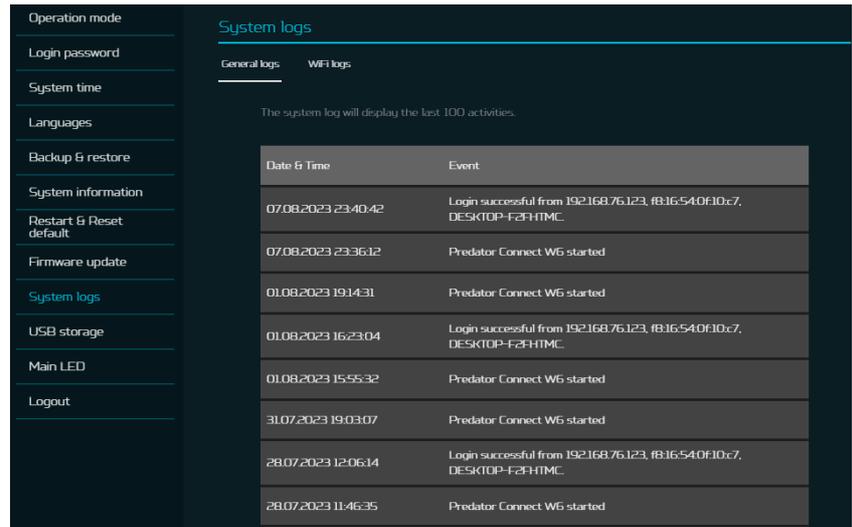
You may click on the top right icon “New firmware available” to upgrade the Predator Connect W6 with the latest firmware.



## 12.9 System Log

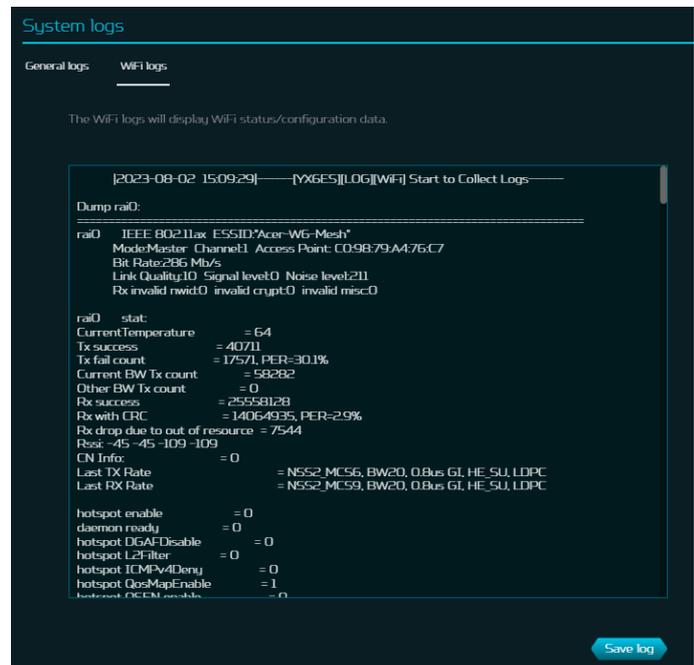
The System logs consists of general logs and Wi-Fi logs. It will display here all the recent 100 activities you have done with the router.

You can save the system logs by clicking the “Save log” button at the bottom of the page.



Click on Wi-Fi logs to see all the Wi-Fi related logs.

You can save the Wi-Fi logs by clicking the “Save log” button at the bottom of the page.



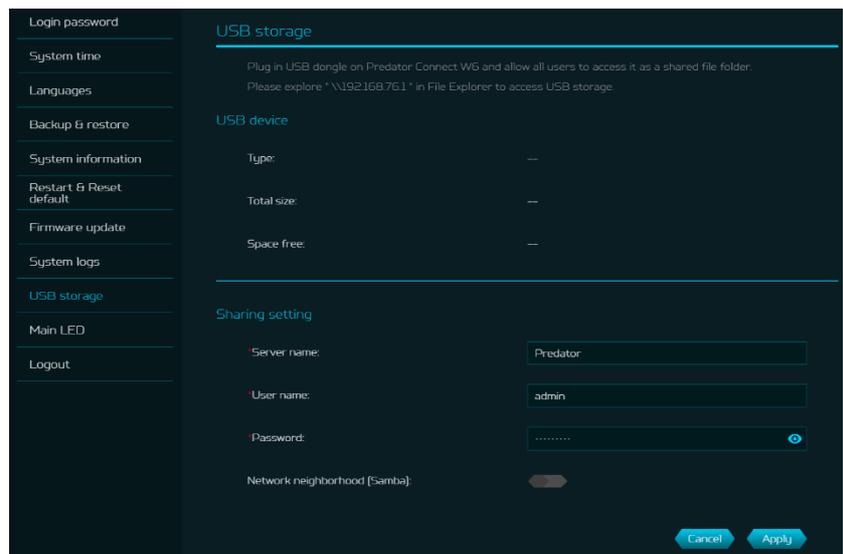
## 12.10 USB Storage

This router has a USB 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

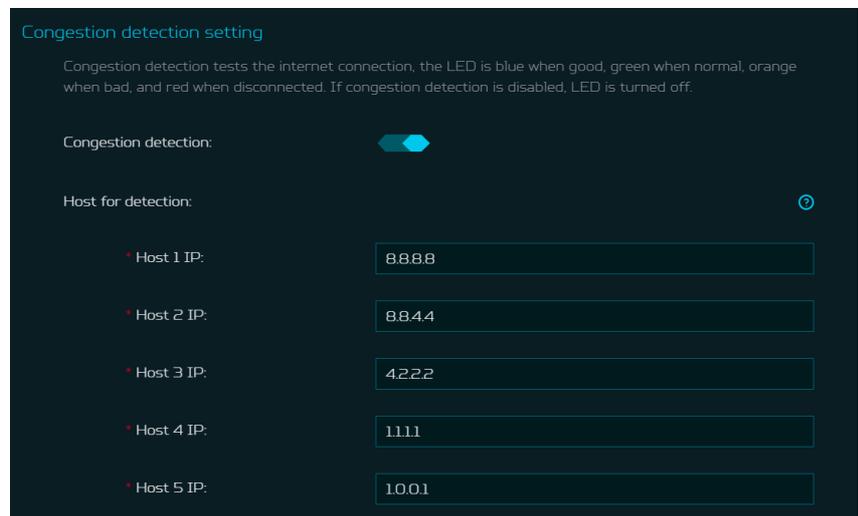
This tab displays information about LED colors and its indication. These LED indicators will help you to know and understand router behavior.



**Congestion Detection** tests helps you to identify the Internet connection status; whether it is good, normal, or poor. Different LED lights will indicate differently statuses.

LED is OFF if congestion detection is disabled.

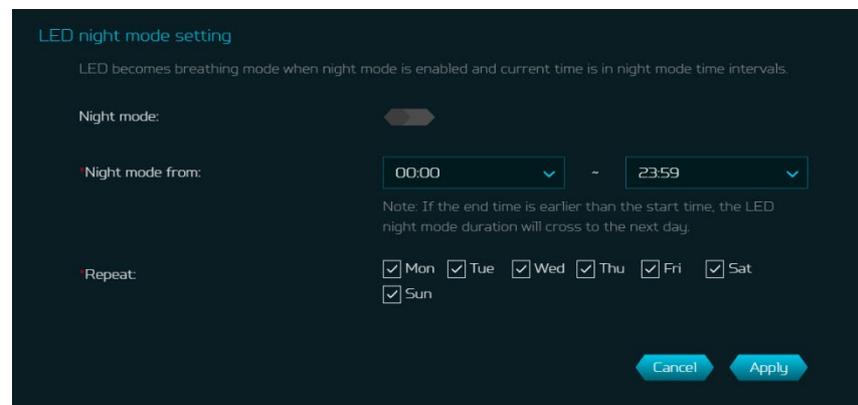
Enter the host IP addresses for detection.



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.



---

# 13. Troubleshooting

## 13.1 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. Turn off the W6 router.
3. Plug in the modem power plug and then turn it on. Wait for two minutes till the modem LED is steady as before.
4. Turn on the W6 router and wait for the device's upper deck main LED to steady breathing.

## 13.2 Frequently Asked Questions (FAQs)

### 13.2.1 What can I do if I forget my wireless password?

- Connect to the W6 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.

### 13.2.2 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.

### 13.2.3 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.

### 13.2.4 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 W6 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.

# 14. Factory Default Settings

<b>Router web admin</b>	
<b>URL</b>	http://acer-connect.com or http://192.168.76.1
<b>Login Password (case-sensitive)</b>	AcerXXXX (XXXX is randomized variables. Please check the device's bottom label)
<b>Local Network (LAN)</b>	
<b>Gateway address</b>	192.168.76.1
<b>Subnet mask</b>	255.255.255.0
<b>DHCP server</b>	192.168.76.1
<b>DHCP range</b>	192.168.76.100 to 192.168.76.254
<b>Time zone</b>	Depends on the country or region you bought the router.
<b>DHCP starting IP address</b>	192.168.76.100
<b>DHCP ending IP address</b>	192.168.76.254
<b>Time adjusted for daylight save time</b>	Enabled.
<b>Wireless LAN (WLAN)</b>	
<b>Wi-Fi SSID (case-sensitive)</b>	2.4GHz: PredatorW6-YYYY-2.4GHz 5GHz: PredatorW6-YYYY-5GHz 6GHz: PredatorW6-YYYY-6GHz (YYYY is randomized variables. Please check the device's bottom label)
<b>Security</b>	2.4GHz : WPA2/WPA3 5GHz : WPA2/WPA3 6GHz : WPA3
<b>SSID Broadcast</b>	Enabled.
<b>RF channel</b>	2.4GHz : Auto 5GHz : Auto 6GHz : Auto
<b>Default operation mode (with AX enabled)</b>	2.4GHz: 2x2 MIMO streams, 1024 QAM, 40MHz, 574Mbps 5GHz: 4x4 MIMO streams, 1024 QAM, 80MHz, 4804Mbps 6GHz: 2x2 MIMO streams, 1024 QAM, 80MHz, 2402Mbps
<b>Guest Wi-Fi</b>	Disabled.
<b>Smart Home Wi-Fi</b>	Disabled.
<b>Home Network Security</b>	Disabled.

# 15. Router Basic Specification

<b>Processor</b>	System	MT7986
	CPU	Quad A53 2.0GHz
<b>Memory</b>	LPDDR	1GB
	Storage	4GB
<b>Wireless LAN</b>	IEEE standard	802.11 a/b/g/n/ac/ax
	Band	Tri-band, 2.4/5/6GHz
	Throughput	AXE7800
	MU-MIMO	2+4+2 streams 2.4GHz: 2x2 MIMO streams, 1024/256 QAM, 20/40MHz, 574Mbps 5GHz: 4x4 MIMO streams, 1024/256 QAM, 20/40/80/160MHz, 4804Mbps 6GHz: 2x2 MIMO streams, 1024/256 QAM, 20/40/80/160MHz, 2402Mbps
	Max Connected Devices	2.4/5/6GHz total: 512 devices
<b>Ethernet</b>	WAN	1 x 2.5Gbps
	LAN	4 x 1Gbps with 1 Game port
<b>USB</b>	Port	USB 3.0 Type-A
	Storage	Samba
<b>Button</b>	Power	Power-ON/OFF
	WPS	Yes
<b>Form factor</b>	Dimension	265 x 260 x 111 mm (with antenna) 255 x 256 x 77 mm (without antenna) 10.42 x 10.20 x 4.30 inch (with antenna) 10.03 x 10.09 x 2.983 inches (without Antenna)
	Wall mount	Yes
	Weight	880g, 1.94 pound
<b>DC Power Jack</b>	Input Voltage	AC 100-240V, 50-60Hz, 1.6A
	Power Adapter	12V/3A 36W