STRONG

Dual Band Wi-Fi 7 Router

ROUTERBE3600

CPU AN7563CT | Wi-Fi 7 BE3600 | 5× 3 dBi antennas | 4-year warranty

User Manual

User Manual | Bedienungsanleitung | Manuale utente | Manual del usuario
Gebruiksaanwijzing | Brugervejledning | Brukerveiledning | Användarhandbok
Manual do utilizador | Korisnički priručnik | Uživatelský manuál | Podręcznik użytkownika

I. Introduction

1. General Overview

Welcome to the comprehensive user guide for the STRONG Dual Band Wi-Fi 7 Router ROUTERBE3600. It guides you from the initial power-on to full mastery of the configuration interface.

The ROUTERBE3600 is a high-performance Wi-Fi 7 router that connects to your existing modem via Ethernet cable. No need to change your Internet box — simply plug it in to instantly benefit from Wi-Fi 7 technology and the Easy Mesh network. Manage your network from the Web UI interface or from the MySTRONG mobile application.

Main features:

- Wi-Fi 7 (IEEE 802.11be) dual band: 688 Mbps @ 2.4 GHz + 2,882 Mbps @ 5 GHz = 3,600 Mbps total
- CPU AN7563CT — 5 external 3 dBi antennas for maximum coverage and reliability
- Multi-Link Operation (MLO): simultaneous aggregation of the 2.4 GHz and 5 GHz bands
- 1 WAN port 2.5 Gbps + 3 Gigabit LAN ports for ultra-fast wired connections
- Band Steering: automatic direction of devices to the most efficient band
- Easy Mesh: extension of the Wi-Fi network in mesh mode with other compatible STRONG devices
- Repeater Mode: extension of the range of an existing Wi-Fi network
- WPA2 / WPA3 Security — Firewall — DoS Protection — ACL
- Management via Web UI interface (192.168.1.1) and MySTRONG mobile application
- Automatic firmware update (OTA) — 4-year warranty

⚠ **IMPORTANT**
The ROUTERBE3600 is a pure Wi-Fi router — it does NOT have a built-in modem or SIM slot. It must be connected to an existing modem or Internet box.

2. Box Contents

Item	Description
ROUTERBE3600 Router × 1	The router with its 5 external antennas.
Cat6 Ethernet Cable × 1	1-meter network cable provided for WAN connection to your modem/box.
DC 12V/1.5A Power Adapter × 1	External power supply.
Quick installation guide × 1	Essential start-up instructions.
Safety instructions and warranty card × 1	Regulatory documentation and 4-year warranty.

3. Physical Overview

Fig. 1 — Front panel: 5 antennas and status LED

Fig. 2 — Rear side: ports and buttons

3.1 Front side

Component	Description
5 external antennas	3 dBi adjustable Wi-Fi antennas. Position them vertically for optimal coverage (3 in the center, 1 on each side).
Status LED (bi-color)	Single operation indicator located on the front panel (see section 3.3).
STRONG logo + Wi-Fi 7	Identification markings on the front panel.

3.2 Rear side (ports and buttons)

Port / Button	Description
LAN1 / LAN2 / LAN3 (yellow ports)	3 Ethernet ports 1 Gbps for wired connection of devices (computers, TV, consoles, NAS…). Yellow connectors for easy identification.
WAN/2.5G (blue port)	2.5 Gbps WAN port for connection to your modem or Internet box. Blue connector. To be connected with the supplied Ethernet cable.
RESET (pinhole button)	Factory reset. Hold down for 5 to 10 seconds with a pin (router powered on) until the LED flashes.
WPS (button)	Wi-Fi Protected Setup — simplified connection of a Wi-Fi device without entering the password.
POWER (DC connector)	DC 12V/1.5A power connector.

3.3 LED Indicator

LED	Meaning
Solid orange	Startup in progress (Power-on process).
Solid green	Normal operation — Internet connection available.
Solid red	No Internet connection available. Please check the WAN connection.
Off	Router powered off.

LED	Meaning
LED disabled	LED intentionally turned off via System Tools > LED Control (router remains operational).

> ⚠ **IMPORTANT**
> If the LED is red after startup, please ensure that the Ethernet cable is properly connected between the WAN/2.5G (blue) port of the router and your modem/box. Please also check the WAN settings (Network > WAN Configuration).

4. Overview of the Web UI

The Web UI allows you to fully configure and manage the router from your browser.

Access address: http://192.168.1.1

Tab	Content
Status	Real-time information: router status, WAN, LAN (Ethernet + WLAN).
Network	WAN and LAN configuration (IPv4/IPv6/DHCP), operating mode, static routes, SNTP, QoS.
WLAN	Wi-Fi settings 2.4 GHz and 5 GHz, multiple SSIDs, MLO, Band Steering, scheduler, access control.
Advanced	NAT (DMZ, ALG, Port Forwarding), IPTV, UPnP, DDNS.
Security	Firewall (level), DoS protection, WAN access, ACL (LAN/WAN access control).
System Tools	Admin password, network diagnostics, reboot (manual + scheduled), backup/restore, firmware, LED.

II. Getting Started — Initial Setup

1. Physical connection

Fig. 3 — Rear panel: connect the WAN (blue) to your modem

1. Unfold the 5 antennas and position them vertically.
2. Connect one end of the supplied Cat6 Ethernet cable to the WAN/2.5G (blue) port of the router.
3. Plug the other end into a LAN port of your modem or Internet box.
4. Plug the DC 12V/1.5A power adapter into the POWER connector of the router, then into the power outlet.
5. Wait approximately 60 seconds. The LED turns orange (startup) then green (operational).

TIP
Never connect the WAN port of the ROUTERBE3600 to another WAN port or to a port identified as Internet on your box. Please use a LAN port on your modem/box.

2. Wi-Fi connection and access to the Web UI

6. On your device, open the Wi-Fi settings and look for the default SSID (STRONG_WiFi7_XXXX — XXXX = last 4 characters of the MAC address).
7. Enter the default Wi-Fi password shown on the label under the router.
8. Open a browser and enter: http://192.168.1.1
9. Enter the administrator password (default on the label or requested during first access).
10. Click on Login — you will access the Web UI.

TIP

You may also connect an Ethernet cable between your PC and one of the router's LAN (yellow) ports to access the Web UI without Wi-Fi.

3. Changing the administrator password

Recommended upon first login: System Tools > User Management. Enter the old password (Old Password), the new one (New Password, max. 16 characters), and confirm (Confirm Password). Click Save & Apply.

4. WAN Configuration (Internet connection)

In most cases, the Internet connection is established automatically after plugging in. If this is not the case, configure the WAN type:

11. Go to Network > WAN Configuration.
12. Click Edit on the existing connection or create a new one.
13. Select the Connection Mode according to your ISP: DHCP (the most common), PPPoE, Static IP, or Bridge.
14. For PPPoE: enter the username and password provided by your ISP.
15. Click Save & Apply.

TIP
If you do not know your connection type, please contact your Internet Service Provider (ISP). DHCP mode works with the vast majority of Internet boxes.

5. Factory reset

Via the Web UI: System Tools > Backup & Restore > Perform Restore Default.

Via the physical button: hold down the RESET button (back panel, pinhole) for 5 to 10 seconds with a pin, with the router powered on. The LED blinks to confirm.

IMPORTANT
The reset will erase ALL your configurations. First, back up via System Tools > Backup & Restore > Backup configuration files.

III. Full description of the Web UI

Access: http://192.168.1.1 from any device connected to the router (Wi-Fi or Ethernet cable).

Navigation: horizontal tabs at the top (Status · Network · WLAN · Advanced · Security · System Tools), sub-menus in the left column.

1. Status — Real-time status

1.1 Device Info

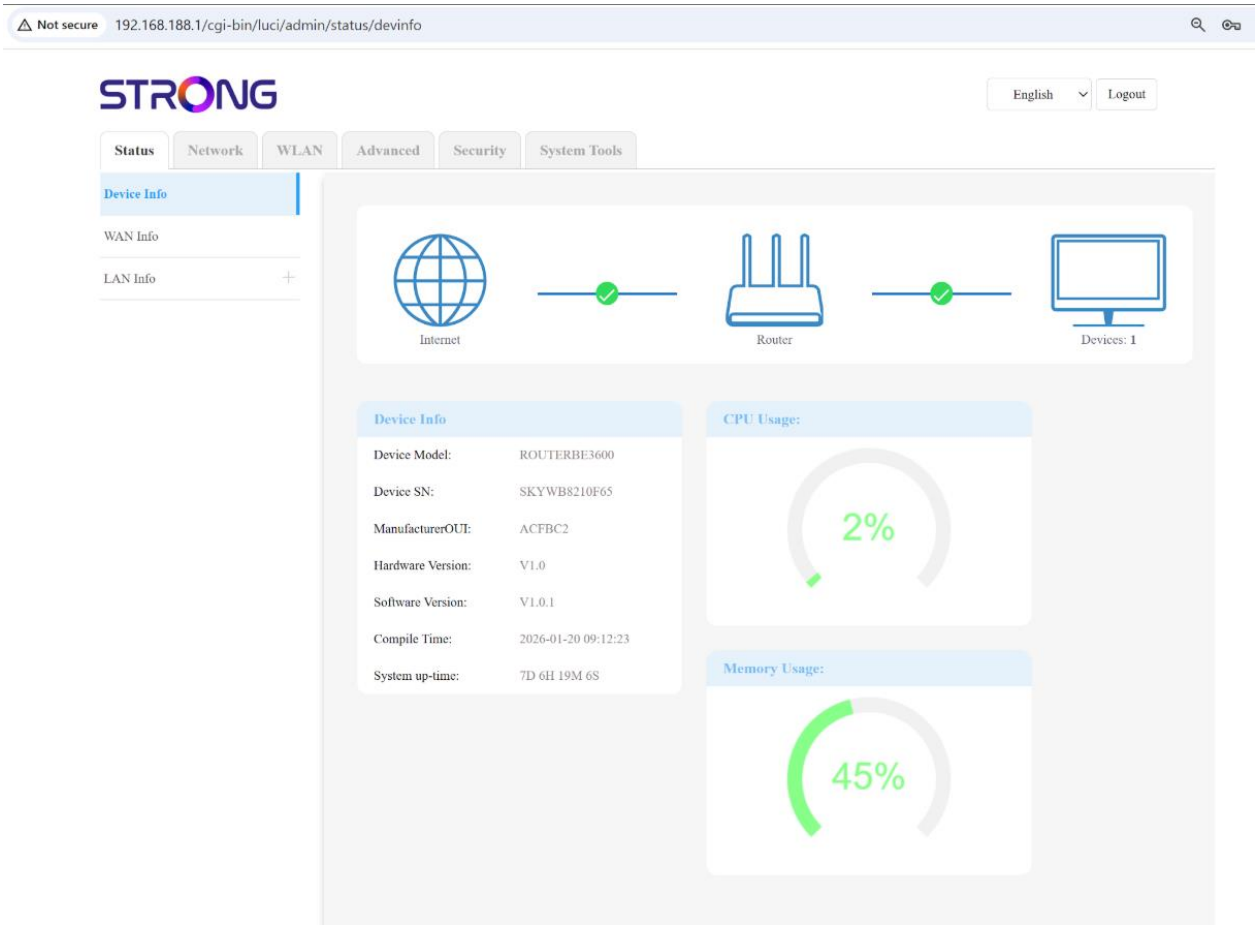

Fig. 4 — Status > Device Info: model, versions, CPU, memory, and connectivity diagram

Web UI home page. Displays a connectivity diagram (Internet → Router → Devices) with green/red indicators according to the status of each link.

Information	Description
Device Model	Router reference: ROUTERBE3600.
Device SN	Unique serial number.
ManufacturOUI	Manufacturer identifier (OUI).
Hardware Version	Hardware version of the router.
Software Version	Installed firmware version. Update via System Tools > Firmware Upgrade or Online Upgrade.

Information	Description
Compile Time	Firmware compile date.
System up-time	Operating time since the last restart.
CPU Usage	Current CPU load (%).
Memory Usage	RAM memory usage (%).

1.2 WAN Info

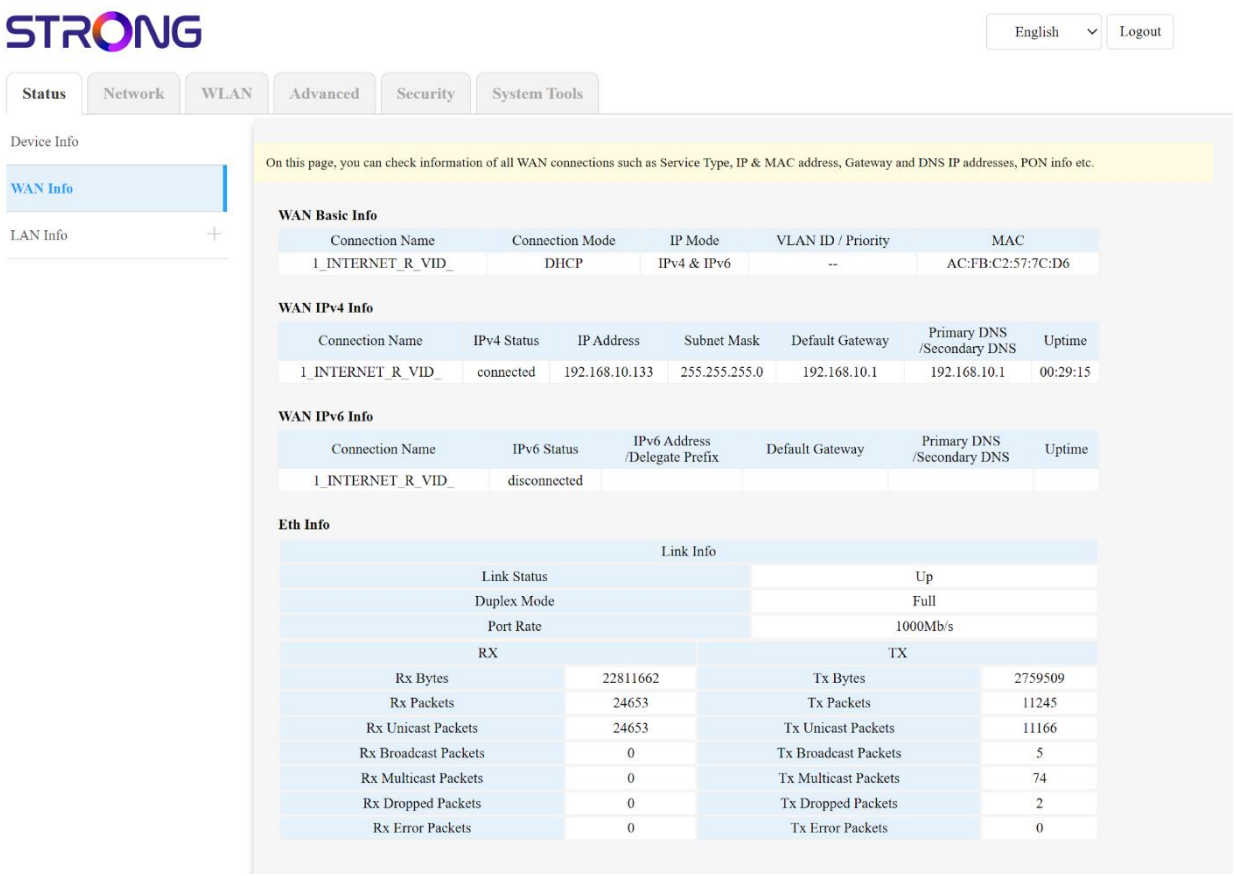

Fig. 5 — Status > WAN Info: WAN connection, IPv4, IPv6, and Ethernet statistics

Displays the complete status of the WAN connection in three blocks:

Section	Content
WAN Basic Info	Connection name, mode (DHCP/PPPoE…), IP mode (IPv4 & IPv6), VLAN ID, MAC address.
WAN IPv4 Info	Connection status, IPv4 address, mask, gateway, primary/secondary DNS, connection duration (Uptime).
WAN IPv6 Info	IPv6 address, delegated prefix, gateway, IPv6 DNS, status.
Eth Info	Status of the physical WAN link (Up/Down), duplex mode, rate (Port Rate), RX/TX statistics (bytes, packets, errors, drops).

1.3 LAN Info — LAN Ethernet Info

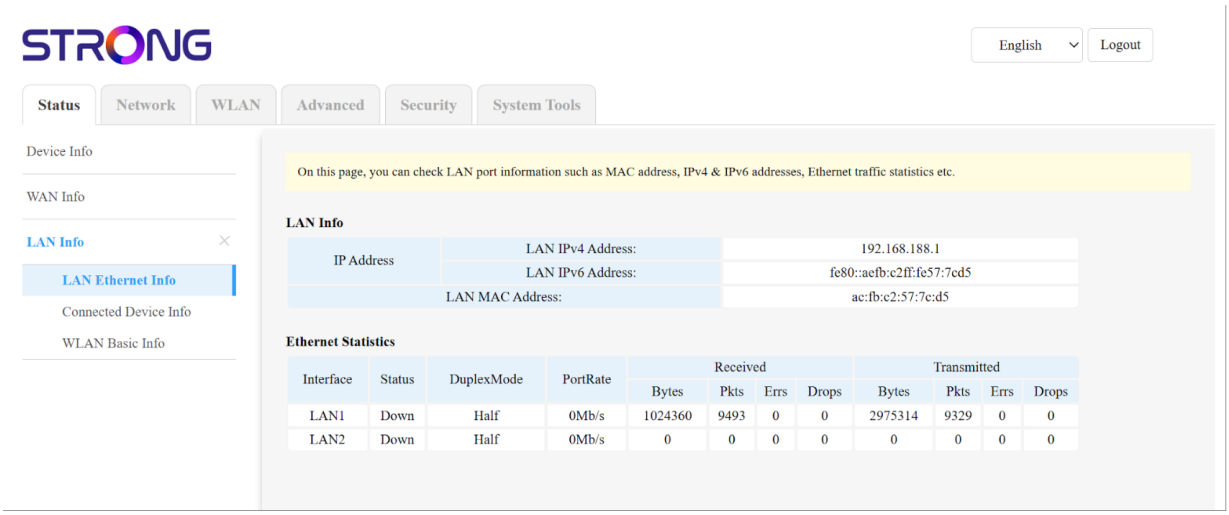

Fig. 6 — Status > LAN Info > LAN Ethernet Info: LAN addresses and statistics

Field	Description
IP Address — LAN IPv4	IPv4 address of the router on the local network (default: 192.168.1.1).
IP Address — LAN IPv6	Local IPv6 address of the router.
LAN MAC Address	MAC address of the router's LAN interface.
Ethernet Statistics	Table per LAN interface (LAN1, LAN2…) : link status, duplex mode, rate, RX/TX Bytes, Packets, Errors, Drops.

NOTE
The LAN Info submenu also contains Connected Device Info (list of devices connected via DHCP) and WLAN Basic Info (summary of active Wi-Fi settings).

2. Network — Network Configuration

2.1 WAN Configuration

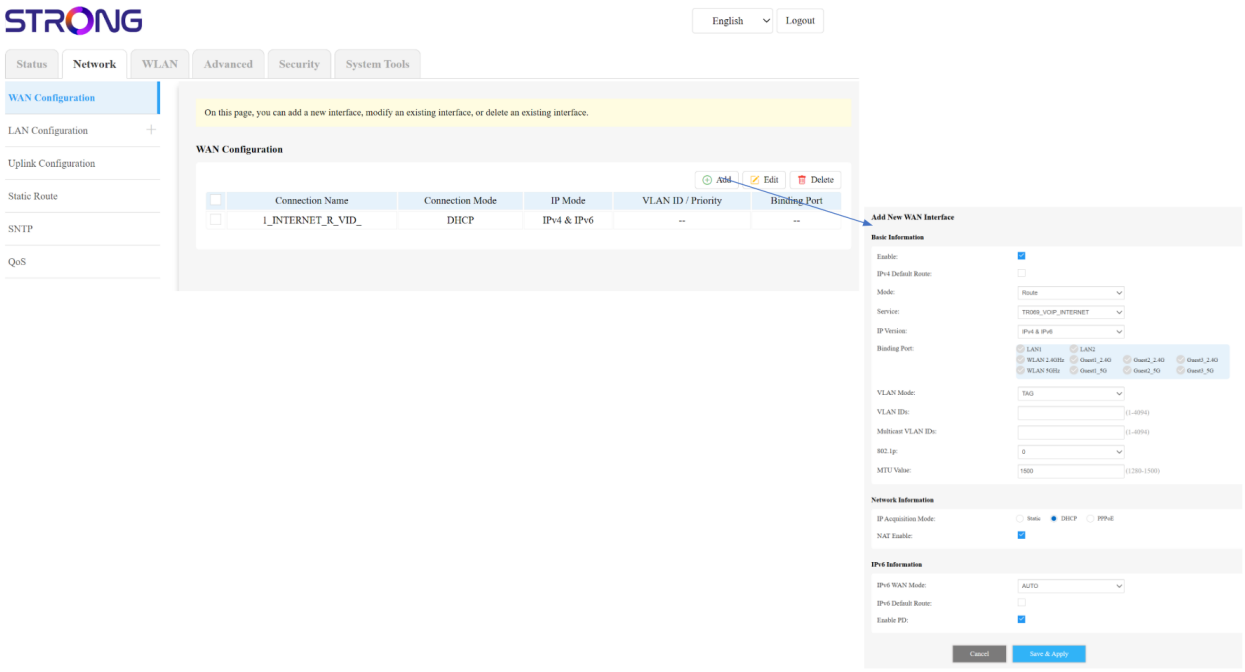

Fig. 7 — Network > WAN Configuration with the window for adding a WAN interface

Configures the WAN interfaces (Internet connection). An interface is created by default (1_INTERNET_R_VID_). You may modify it or create a new one.

Field	Description
Connection Name	Name of the WAN interface for identification.
Enable	Enables/disables this WAN interface.
Name	Name of the network interface (e.g.: pppoe).
Service	Type of WAN service: INTERNET, VOIP, IPTV, INTERNET+VOIP, etc.
IP Version	IPv4 only, IPv6 only, or IPv4 & IPv6 (dual stack — recommended).
Binding Port	Physical WAN port associated with this interface.
VLAN Mode	Enables or disables VLAN on this interface.
VLAN ID	VLAN identifier (if your ISP requires one, e.g.: 100, 835…).
MTU	Maximum packet size (default: 1480 for PPPoE, 1500 for DHCP).
PPPOE VID	Specific VLAN ID for PPPoE.
IP Acquisition Mode	IP acquisition mode: Auto (DHCP) · Static (fixed IP).
IPv6 WAN Mode	IPv6 assignment modes: auto, DHCPv6, SLAAC, static, etc.
Enable PD	Enable IPv6 prefix delegation.

TIP

For a standard DHCP connection (the most common): Connection Mode = DHCP, IP Version = IPv4 & IPv6. For a PPPoE connection (fiber with some ISPs): add the PPPoE username and password.

2.2 LAN Configuration — IPv4

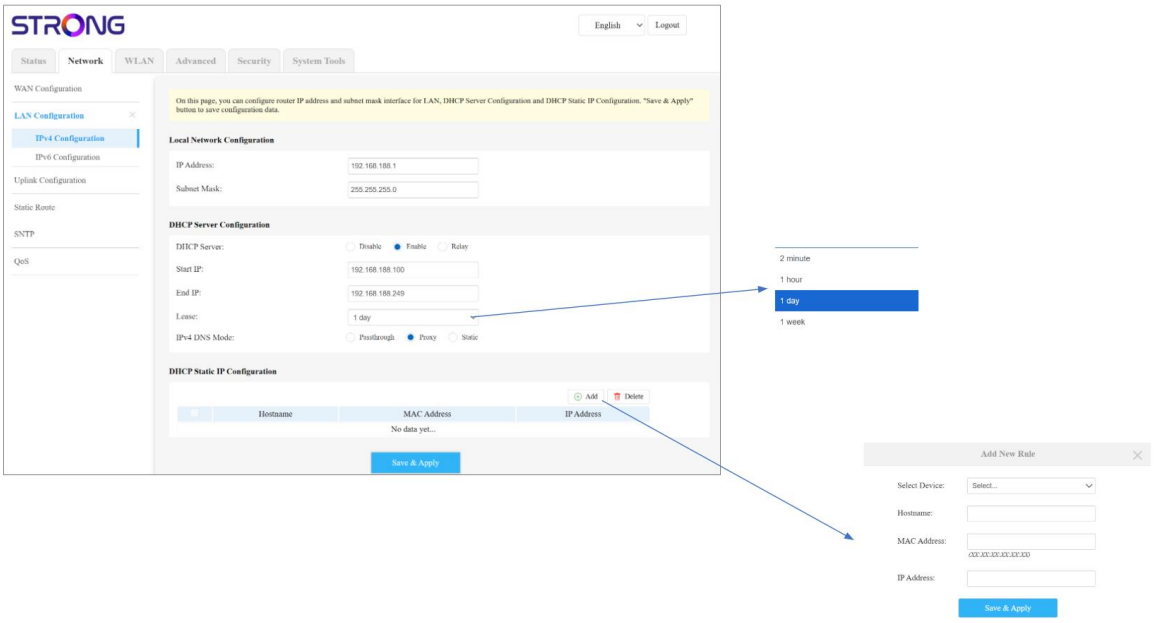

Fig. 8 — Network > LAN Configuration > IPv4 Configuration with DHCP and Static DHCP

Setting	Description
IP Address	IP address of the router on the local network (default: 192.168.1.1).
Subnet Mask	Subnet mask (default: 255.255.255.0).
DHCP Server	Enable (active by default) / Disable / Relay.
Start IP / End IP	Range of IP addresses assigned to devices. By default: 192.168.1.100 to 192.168.1.200.
Lease	DHCP lease duration (default: 1 day).
IPv4 DNS Mode	Passthrough (uses the operator's DNS) or Proxy (local DNS resolution).
DHCP Static IP	Table of fixed IP associations by MAC address. Add button to create: select the device or manually enter the host name, MAC address, and desired IP.

2.3 LAN Configuration — IPv6

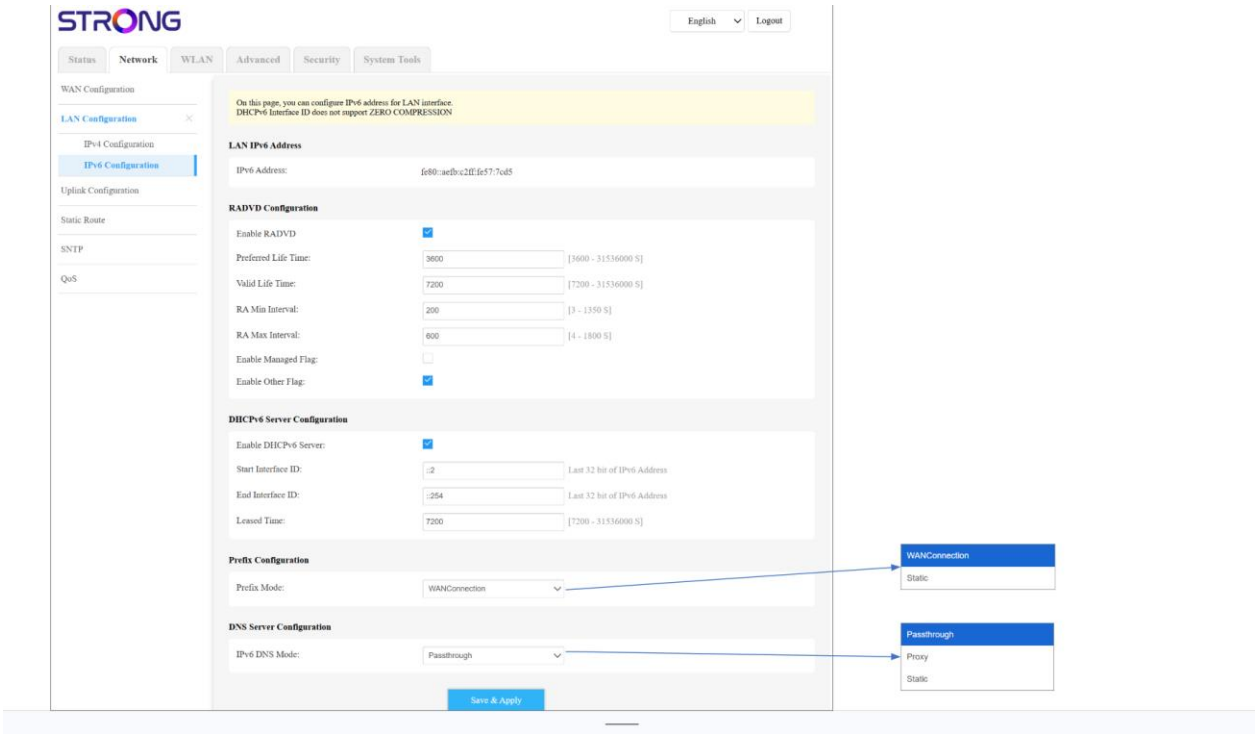

Fig. 9 — Network > LAN Configuration > IPv6 Configuration: RA, DHCPv6, prefixes

Setting	Description
LAN IPv6 Address	Local IPv6 address of the router.
Enable RADVD	Enables the router advertisement daemon (Router Advertisement) for automatic IPv6 configuration.
Preferred/Valid Lifetime	Lifetime of IPv6 advertisements.
RA Max/Min Interval	Intervals between RA advertisements (seconds).
Enable DHCP IPv6 Server	Enables the DHCPv6 server to assign IPv6 addresses to devices.
Prefix Mode	WAN Connector (uses the delegated WAN prefix) / Static (manually defined fixed prefix).
IPv6 DNS Mode	Passthrough or Proxy.

2.4 Uplink Configuration — Operating Mode

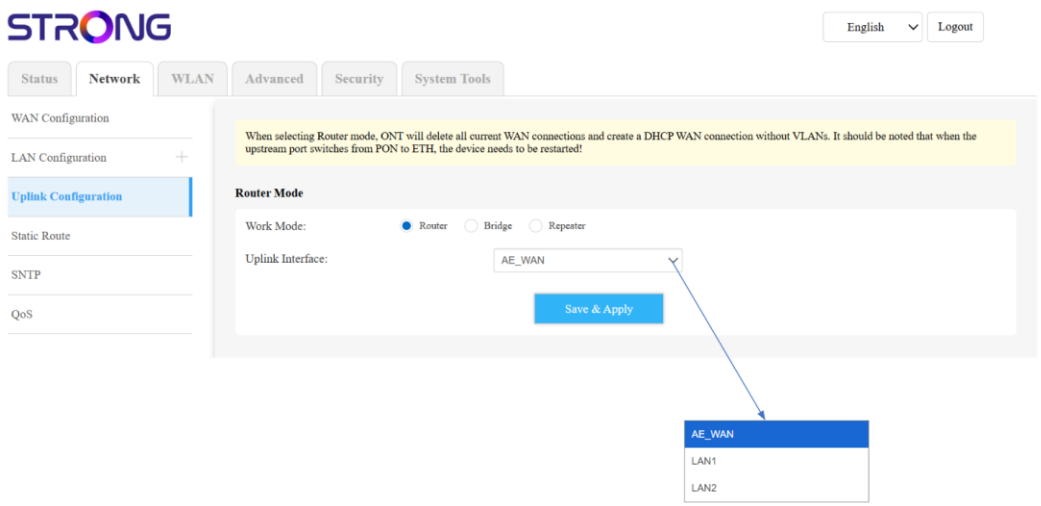

Fig. 10 — Network > Uplink Configuration: Router, Bridge or Repeater

Mode	Description
Router (default mode)	The router operates in standard NAT mode — connection via the WAN port to your modem/box. Recommended mode for typical home use.
Bridge	Bridge mode: the router forwards packets without NAT. Useful if you already have an upstream router and wish to extend your network.
Repeater	Wi-Fi repeater mode: the router connects to an existing Wi-Fi network and extends it. Select the uplink interface (AE_WAN, LAN1, LAN2).

NOTE
In Repeater mode, the router connects to a source Wi-Fi network and retransmits the signal. A restart may be required when changing modes.

2.5 Static Route — Static Routes

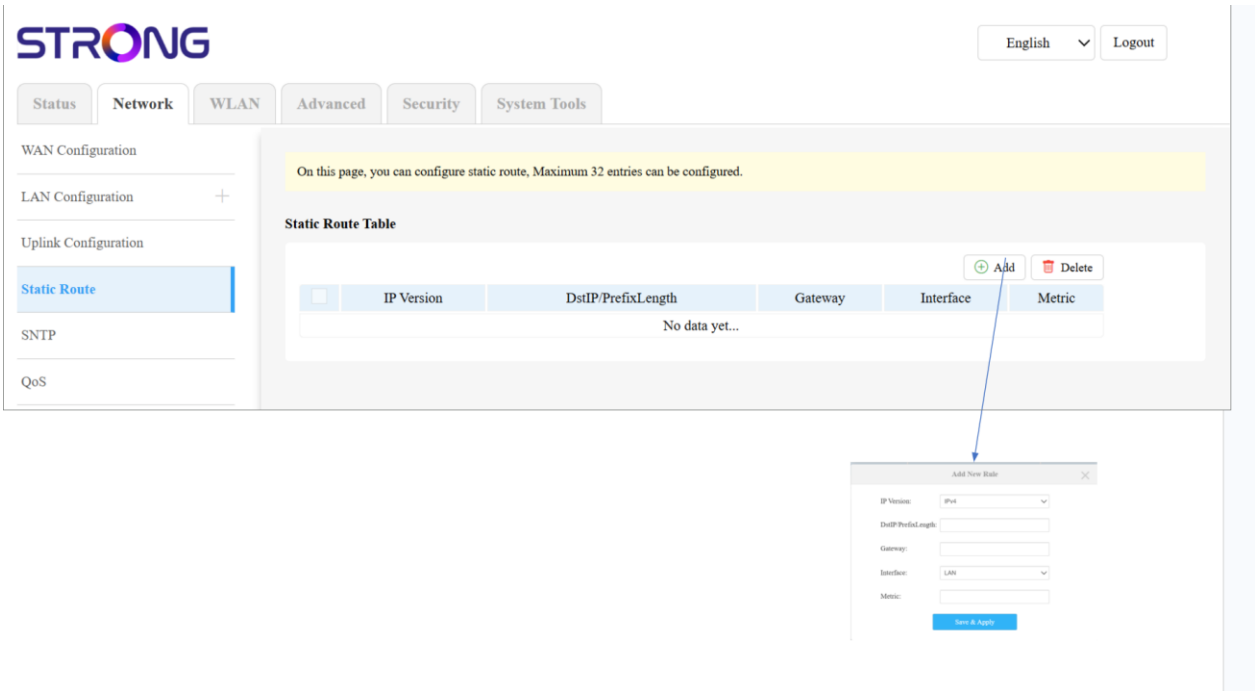

Fig. 11 — Network > Static Route: configuration of static routes (max. 32)

Allows you to define static IP routes to direct traffic to specific networks via a specified gateway. Maximum 32 entries. To add: click Add, enter IP Version, DstIP/PrefixLength, Gateway, Interface, and Metric, then Save & Apply.

2.6 SNTP — Time synchronization

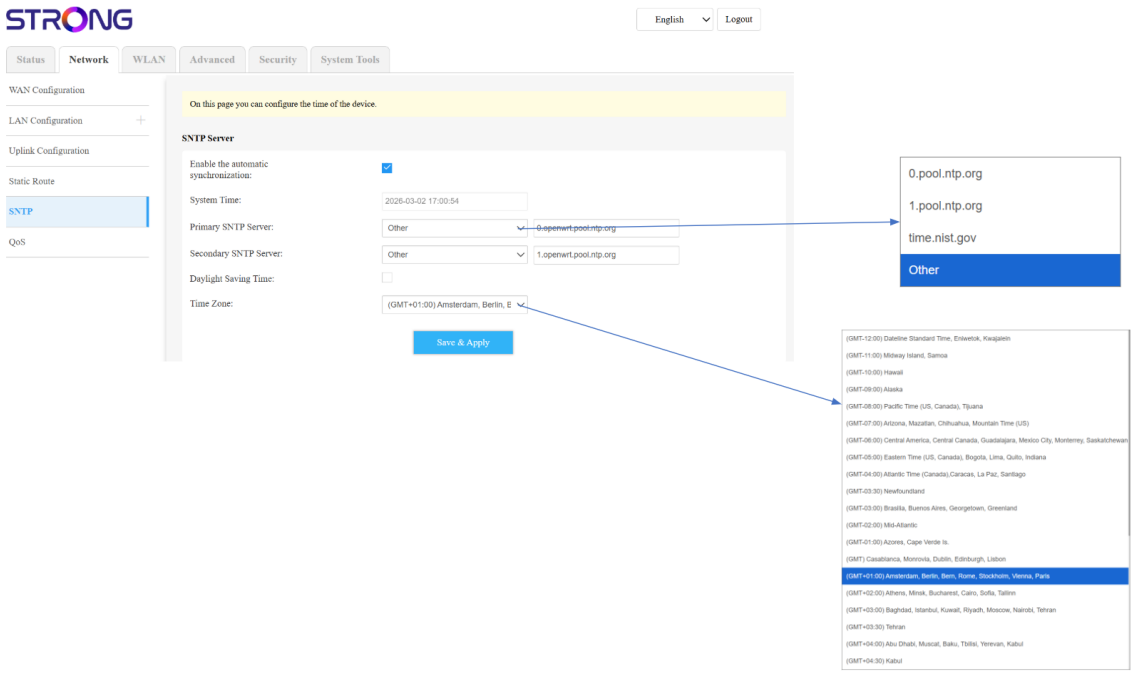

Fig. 12 — Network > SNTP: NTP servers and time zone

Setting	Description
Enable the automatic synchronization	Check to enable automatic NTP synchronization.
System Time	Current time of the router.
Primary SNTP Server	Main NTP server (default: pool.ntp.org — or custom).
Secondary SNTP Server	Backup NTP server.
Time Zone	Time zone (e.g.: GMT+01:00 Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna). Full list available in the drop-down menu.

2.7 QoS — Quality of Service

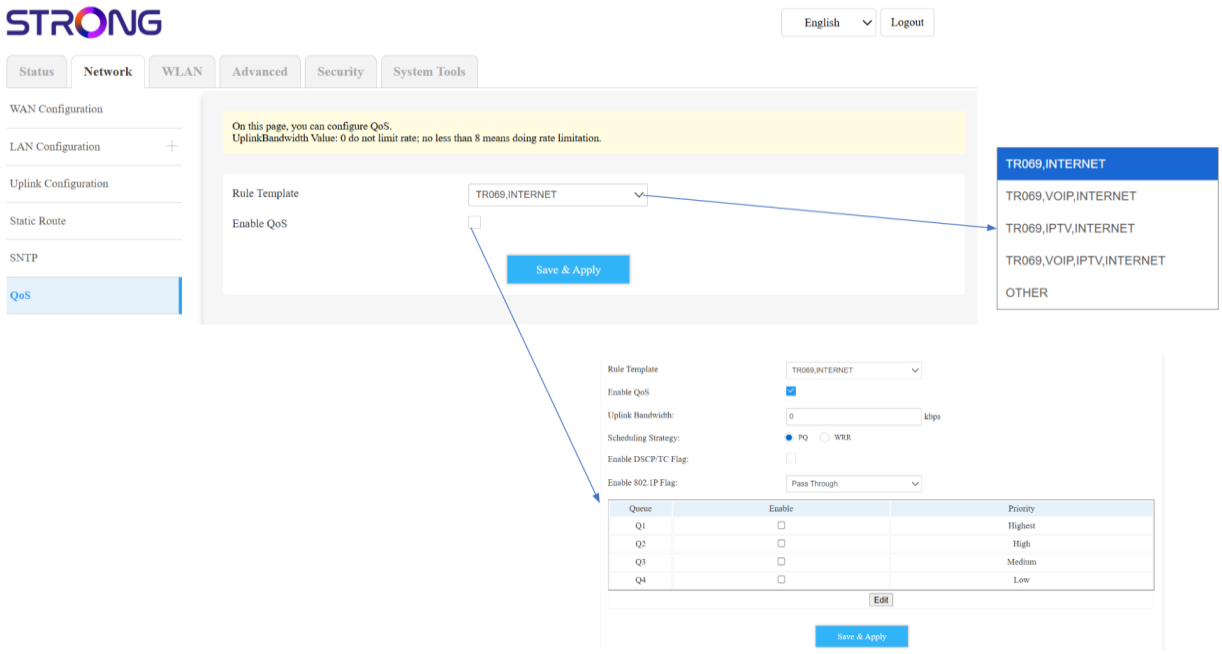

Fig. 13 — Network > QoS: network traffic prioritization

Setting	Description
Role Template	Select the predefined QoS profile: TR069.INTERNET (default), TR069.VOIP.INTERNET, TR069.IPTV.INTERNET, TR069.VOIP.IPTV.INTERNET, OTHER.
Enable QoS	Enable/disable quality of service management.
Uplink Bandwidth	Maximum uplink bandwidth in Kbps (0 = no limit). Enter the value provided by your ISP.
Scheduling Strategy	Scheduling strategy: SP (Strict Priority) or WRR (Weighted Round Robin).
Enable DSCP IP flag	Enables DSCP marking on IP packets.
Enable 802.1P Flag	Enables 802.1p priority marking (Pass Through or fixed value).
Queue (Q1 to Q4)	Traffic queues with priorities: Q1 = Highest, Q2 = High, Q3 = Medium, Q4 = Low. Check Enable to activate each queue.

3. WLAN — Wi-Fi Configuration

3.1 WLAN 2.4G — Basic Settings

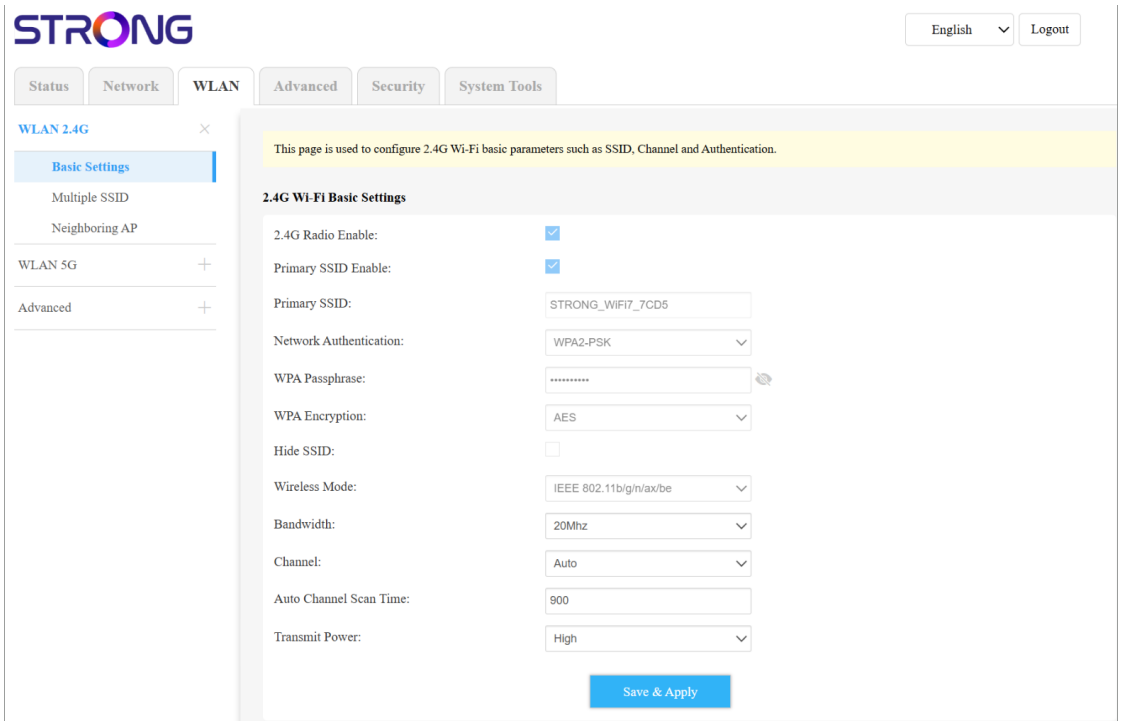

Fig. 14 — WLAN > WLAN 2.4G > Basic Settings: 2.4 GHz Wi-Fi settings

Setting	Description
2.4G Radio Enable	Completely enables/disables the 2.4 GHz Wi-Fi radio.
Primary SSID Enable	Enables/disables the broadcast of the primary SSID on the 2.4 GHz band.
Primary SSID	Name of the main 2.4 GHz Wi-Fi network (default: STRONG_WiFi7_XXXX).
Network Authentication	Security mode: WPA2-PSK, WPA/WPA2-PSK, WPA3-SAE, WPA2-PSK/WPA3-SAE (recommended), Open System.
WPA Passphrase	Wi-Fi network password (minimum 8 characters).
WPA Encryption	Encryption: AES (recommended) or TKIP.
Hide SSID	Check to hide SSID broadcast (hidden network).
Wireless Mode	Wi-Fi standard: IEEE 802.11b/g/n/ax/be (Wi-Fi 7 — recommended).
Bandwidth	Channel width: 20 MHz, 40 MHz (default 20 MHz on 2.4 GHz).
Channel	Radio channel (Auto recommended). Available channels: 1 to 13.
Auto Channel Scan Time	Time in seconds between two automatic channel scans (default: 900 s).
Transmit Power	Transmission power: Low, Medium, High (default: High).

3.2 WLAN 2.4G — Multiple SSID (Additional SSIDs)

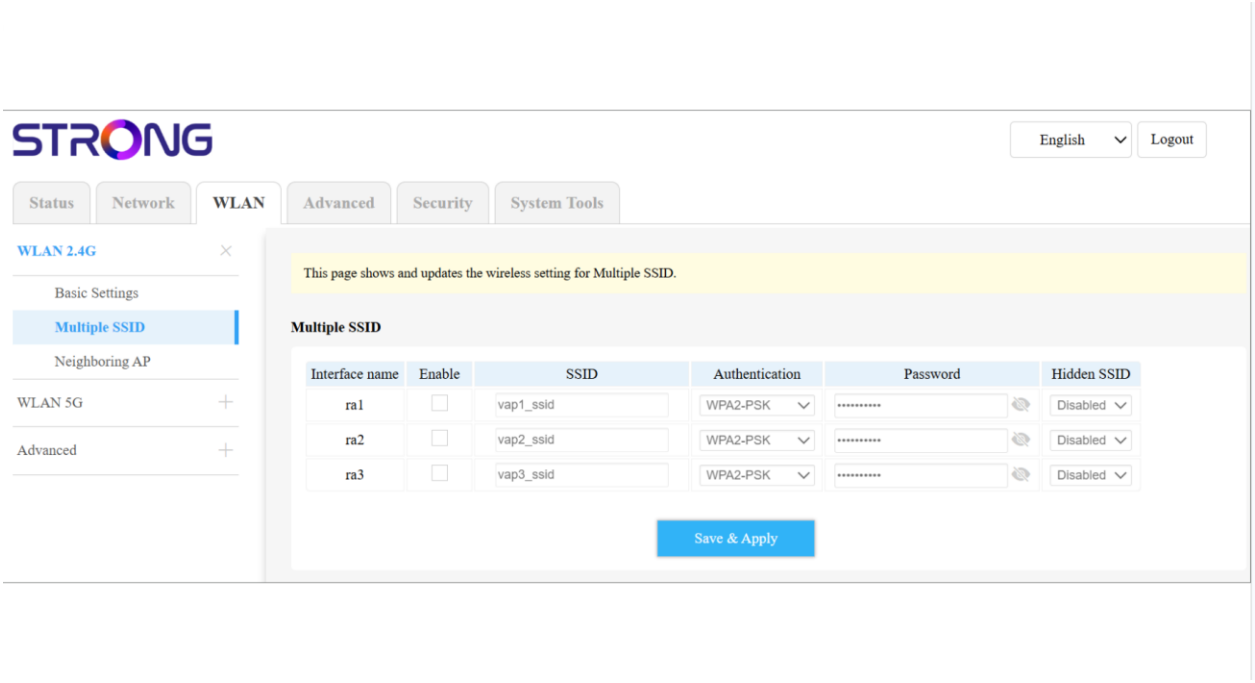

Fig. 15 — WLAN > WLAN 2.4G > Multiple SSID: Virtual SSIDs ra1, ra2, ra3

Allows you to create up to 3 additional virtual Wi-Fi networks on the 2.4 GHz band (interfaces ra1, ra2, ra3), in addition to the main SSID. Useful for creating guest networks or isolated networks.

Column	Description
Interface name	Virtual interface identifier: ra1, ra2, ra3.
Enable	Check to enable this virtual SSID.
SSID	Name of the virtual Wi-Fi network.
Authentication	Security mode: WPA2-PSK, etc.
Password	Password for the virtual network.
Hidden SSID	Hide or display this SSID.

3.3 WLAN 2.4G — Neighboring AP

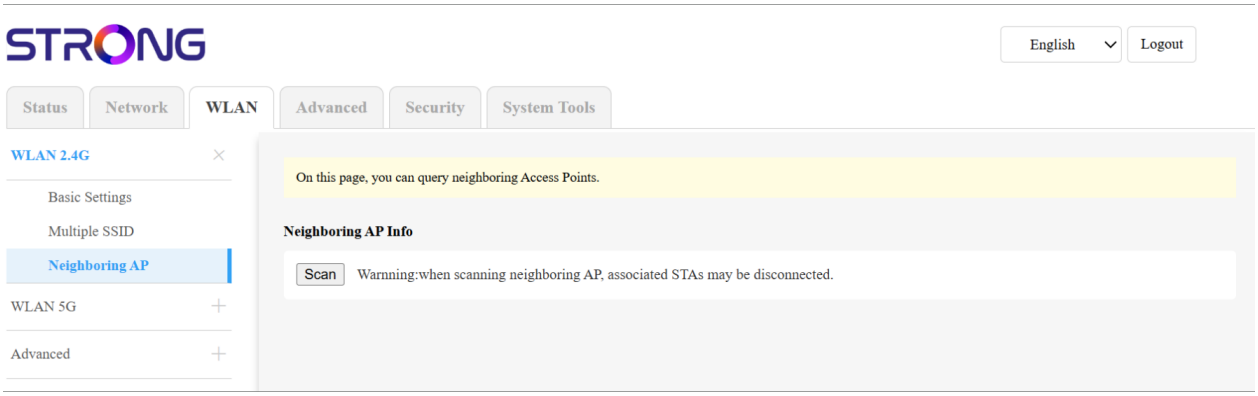

Fig. 16 — WLAN > WLAN 2.4G > Neighboring AP: scan of neighboring access points

Displays the Wi-Fi access points detected in the environment. Click on Scan to start the search.

> ⚠ **IMPORTANT**
> Warning: scanning neighboring APs may temporarily disconnect associated Wi-Fi devices.

3.4 WLAN 5G — Basic Settings

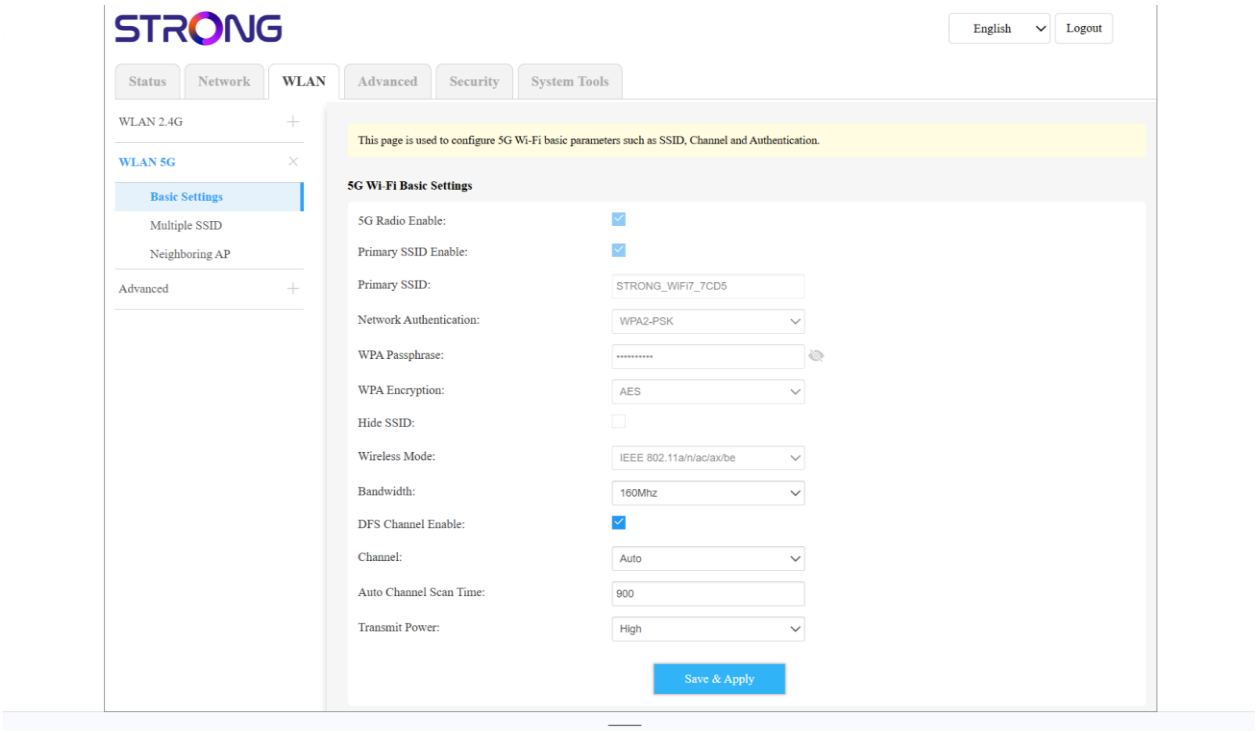

Fig. 17 — WLAN > WLAN 5G > Basic Settings: 5 GHz Wi-Fi settings

Setting	Description
5G Radio Enable	Enables/disables the 5 GHz Wi-Fi radio.
Primary SSID Enable	Enables/disables the main 5 GHz SSID.
Primary SSID	Name of the 5 GHz Wi-Fi network (default: STRONG_WiFi7_XXXX, identical to 2.4 GHz if Band Steering is active).
Network Authentication	Security mode (same options as 2.4 GHz).
WPA Passphrase	5 GHz Wi-Fi password.
WPA Encryption	AES recommended.
Hide SSID	Hide the 5 GHz network.
Wireless Mode	IEEE 802.11a/n/ac/ax/be (Wi-Fi 7 — recommended for maximum performance).
Bandwidth	Channel width: 20 MHz, 40 MHz, 80 MHz, 160 MHz (160 MHz = maximum Wi-Fi 7 performance).
DFS Channel Enable	Enables DFS channels (Dynamic Frequency Selection) for more available 5 GHz channels.
Channel	Radio channel (Auto recommended). Available channels: 36-161.
Auto Channel Scan Time	Automatic scan interval (default: 900 s).
Transmit Power	Low, Medium, High (default: High).

3.5 WLAN 5G — Multiple SSID

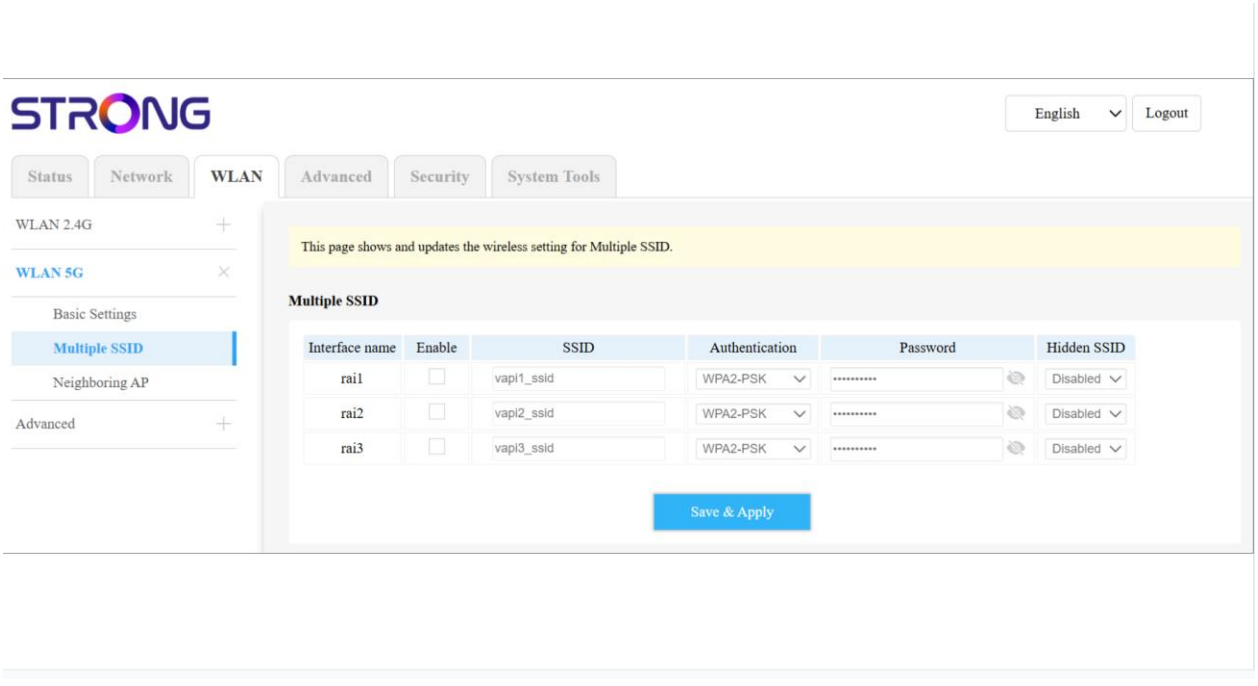

Fig. 18 — WLAN > WLAN 5G > Multiple SSID: Virtual SSIDs rai1, rai2, rai3

Identical to the multiple SSIDs for 2.4 GHz. Up to 3 additional virtual networks on the 5 GHz band (interfaces rai1, rai2, rai3).

3.6 WLAN 5G — Neighboring AP

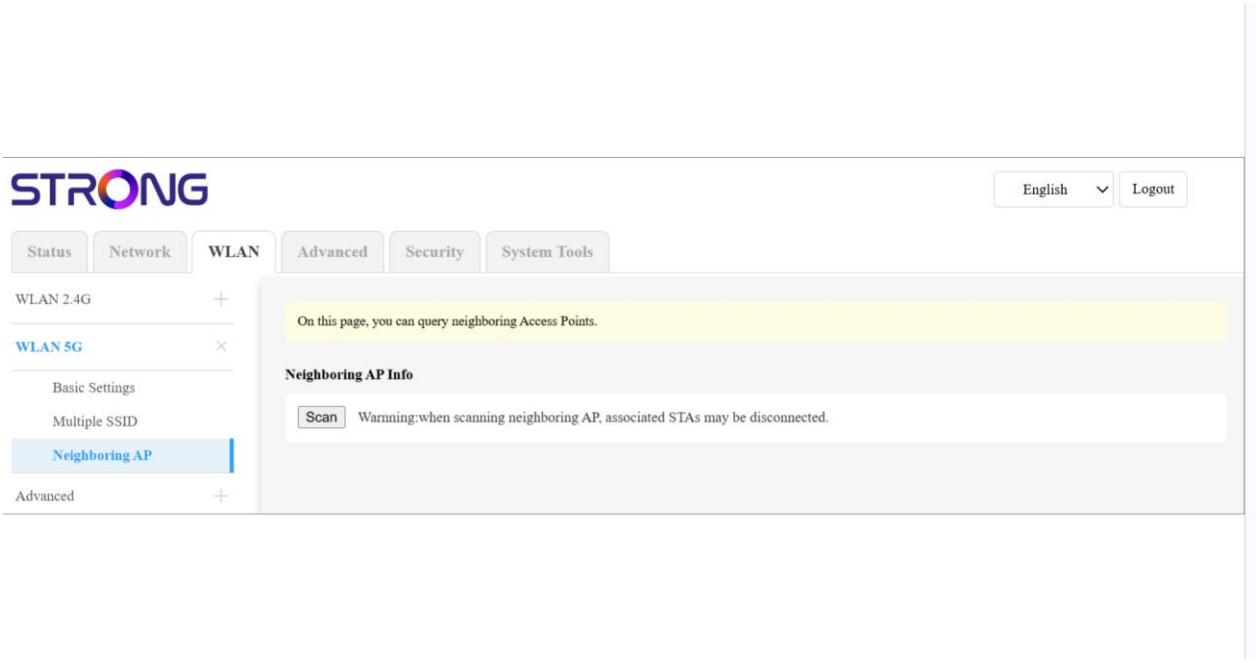

Fig. 19 — WLAN > WLAN 5G > Neighboring AP: scan of neighboring APs on 5 GHz

Same operation as for the 2.4 GHz band. Scan of surrounding 5 GHz Wi-Fi networks.

3.7 WLAN Advanced — Scheduler (Wi-Fi Scheduler)

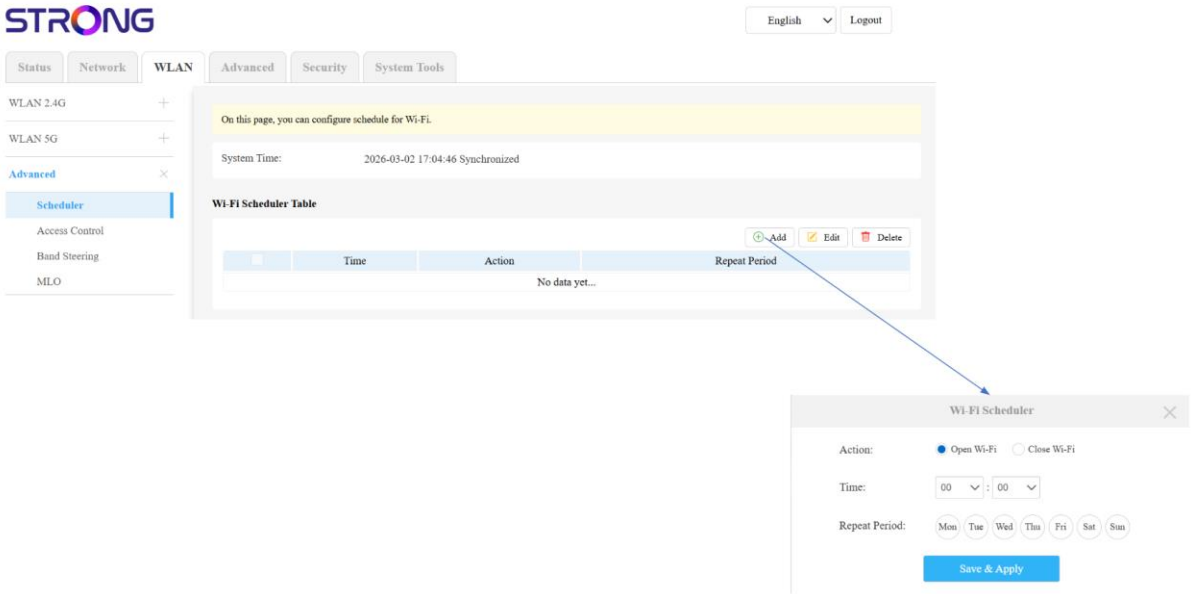

Fig. 20 — WLAN > Advanced > Scheduler: Wi-Fi scheduling

Allows you to schedule time slots for automatic Wi-Fi activation/deactivation. Ideal for turning off Wi-Fi at night or during defined periods.

Item	Description
Wi-Fi Scheduler Table	List of scheduled rules (Time, Action, Repeat Period).
Add	Create a new rule. A window opens with: Action (Open Wi-Fi / Close Wi-Fi), Time (HH:MM), Repeat Period (days of the week: Mon to Sun).
Edit	Edit an existing rule.
Delete	Delete a rule.

3.8 WLAN Advanced — Access Control

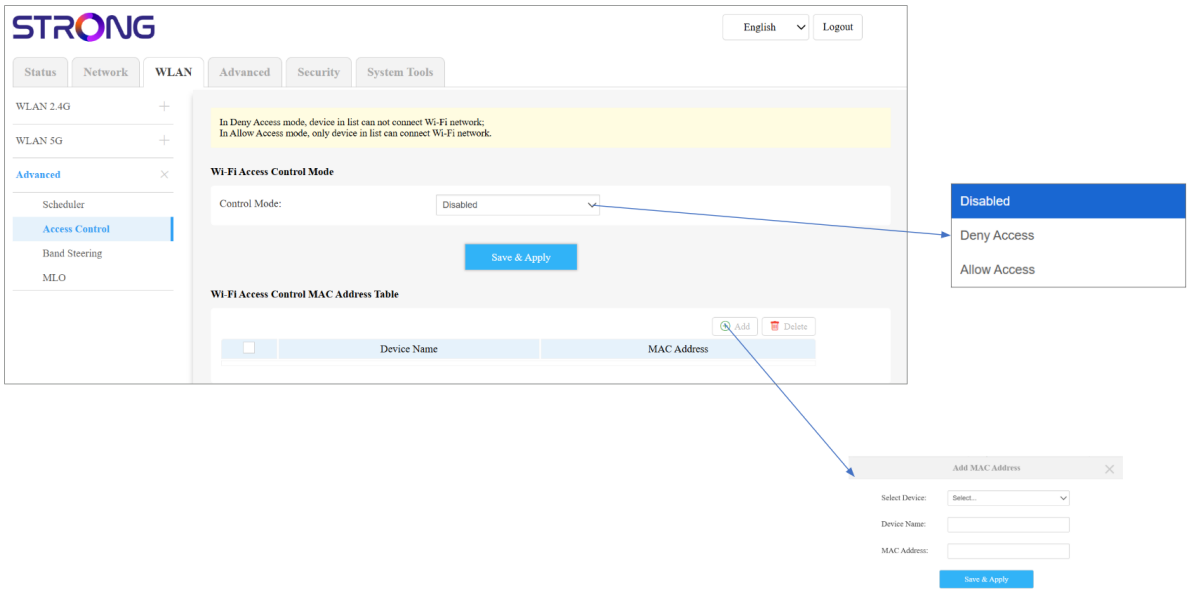

Fig. 21 — WLAN > Advanced > Access Control: Wi-Fi access control by MAC

Mode	Description
Disabled	No filtering — all devices can connect to Wi-Fi.
Deny Access	Blocks devices whose MAC address is in the list. All others are allowed.
Allow Access	Only allows devices whose MAC address is in the list.

To add: click Add, select the device from the list of connected devices (Select Device) or manually enter the Device Name and MAC address, then Save & Apply.

3.9 WLAN Advanced — Band Steering

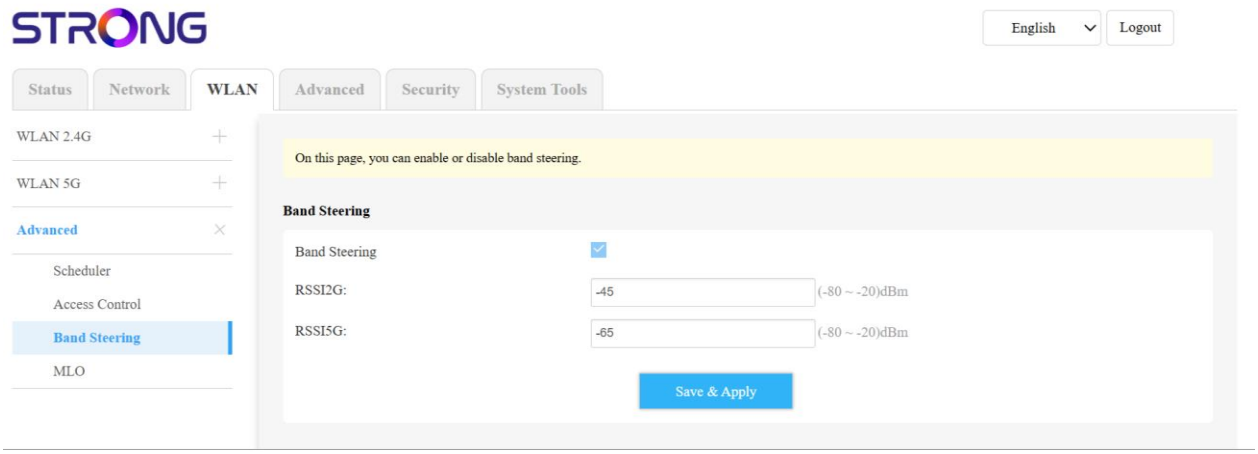

Fig. 22 — WLAN > Advanced > Band Steering: automatic orientation to the optimal band

Band Steering analyzes the signal quality of each device and automatically directs it to the most efficient band (5 GHz by priority). RSSI thresholds configure the switching behavior.

Setting	Description
Band Steering	Enables (checked) or disables Band Steering.
RSSI2G	2.4 GHz signal threshold in dBm (-80 to -20 dBm). Default: -45 dBm. Below this threshold, the router tries to migrate the device to 5 GHz.
RSSI5G	5 GHz signal threshold in dBm (-80 to -20 dBm). Default: -65 dBm. Below this, the device remains on 2.4 GHz.

3.10 WLAN Advanced — MLO (Multi-Link Operation)

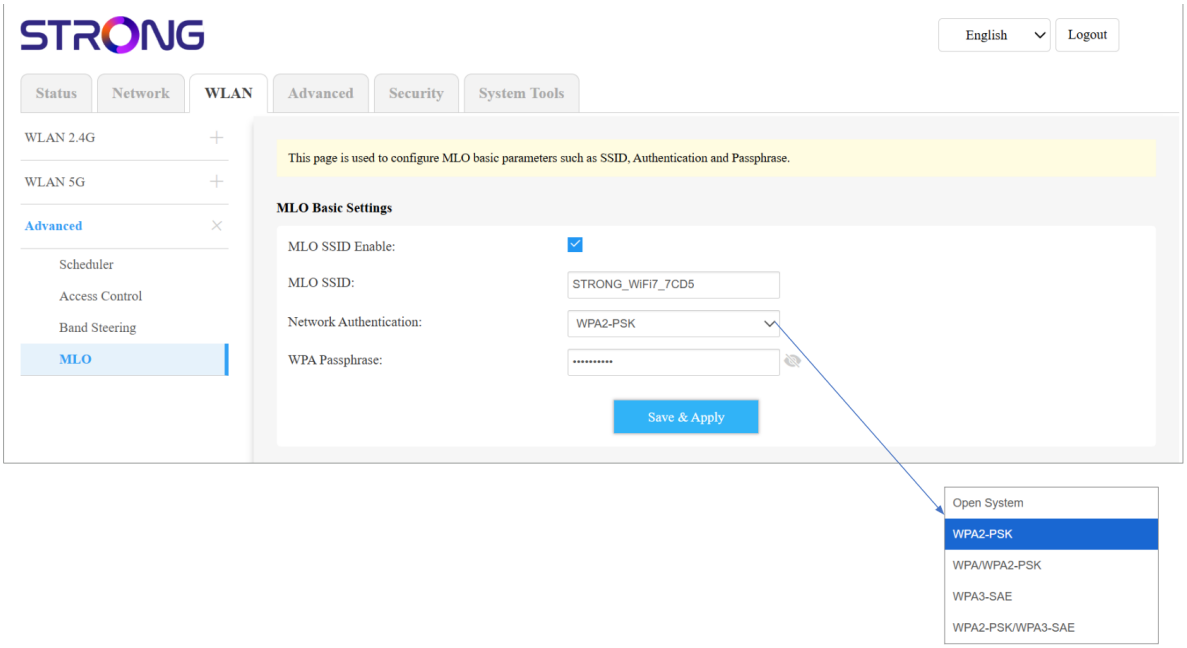

Fig. 23 — WLAN > Advanced > MLO: Wi-Fi 7 multi-band aggregation

MLO (Multi-Link Operation) is the flagship technology of Wi-Fi 7: the router and compatible devices simultaneously use the 2.4 GHz and 5 GHz bands on a single connection, multiplying speed and reducing latency.

Setting	Description
MLO SSID Enable	Enables/disables the MLO network.
MLO SSID	Name of the MLO network shared between both bands (default: STRONG_WiFi7_XXXX).
Network Authentication	Security: Open System, WPA2-PSK (default), WPA/WPA2-PSK, WPA3-SAE, WPA2-PSK/WPA3-SAE.
WPA Passphrase	MLO network password.

> **NOTE**
> MLO requires client devices compatible with Wi-Fi 7 (IEEE 802.11be). On non-compatible devices, the connection is established normally via the individual SSID of each band.

4. Advanced — Advanced Functions

4.1 NAT — DMZ

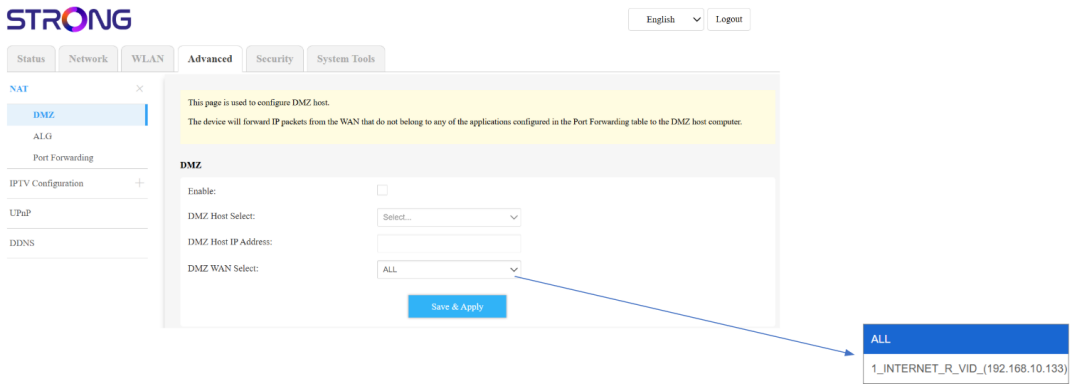

Fig. 24 — Advanced > NAT > DMZ: exposing a LAN host to the Internet

The DMZ exposes a LAN device directly to the Internet — all WAN packets not matching a Port Forwarding rule are redirected to the DMZ host.

Field	Description
Enable	Enables/disables the DMZ.

Field	Description
DMZ Host Select	Select the LAN device to expose in the DMZ (dropdown list of connected devices).
DMZ Host IP Address	LAN IP address of the DMZ host (manual entry or automatic selection).
DMZ WAN Select	WAN interface used for the DMZ (ALL or specific interface).

> ⚠ **IMPORTANT**
> The DMZ exposes the selected host to ALL incoming Internet connections. Use this function only for servers that have their own protection.

4.2 NAT — ALG (Application Layer Gateway)

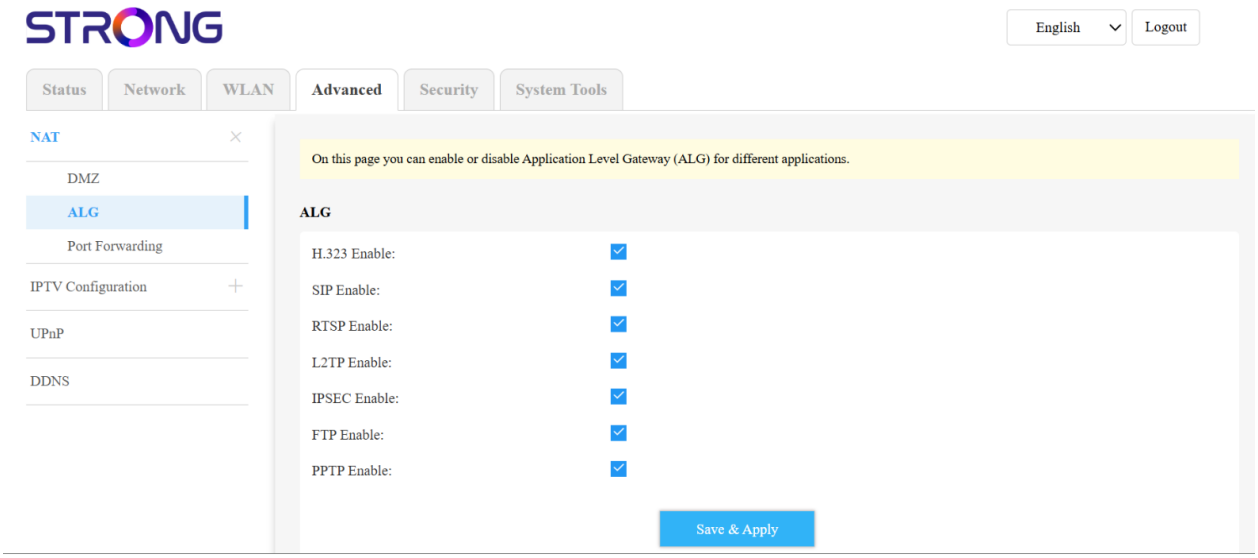

Fig. 25 — Advanced > NAT > ALG: enabling ALG protocols

The ALG (Application Layer Gateway) allows certain application protocols to properly traverse the router's NAT. Enable only the necessary protocols.

Protocol	Description
H.323 Enable	ALG for H.323 video/voice calls (classic Skype, Cisco…).
SIP Enable	ALG for SIP VoIP telephony. Enable if you are using a VoIP service.
RTSP Enable	ALG for RTSP streaming (camera feeds, media…).
L2TP Enable	ALG for L2TP VPN tunnels.
IPSEC Enable	ALG for IPSec VPN connections.
FTP Enable	ALG for the FTP file transfer protocol (passive mode).
PPTP Enable	ALG for PPTP VPNs.

4.3 NAT — Port Forwarding

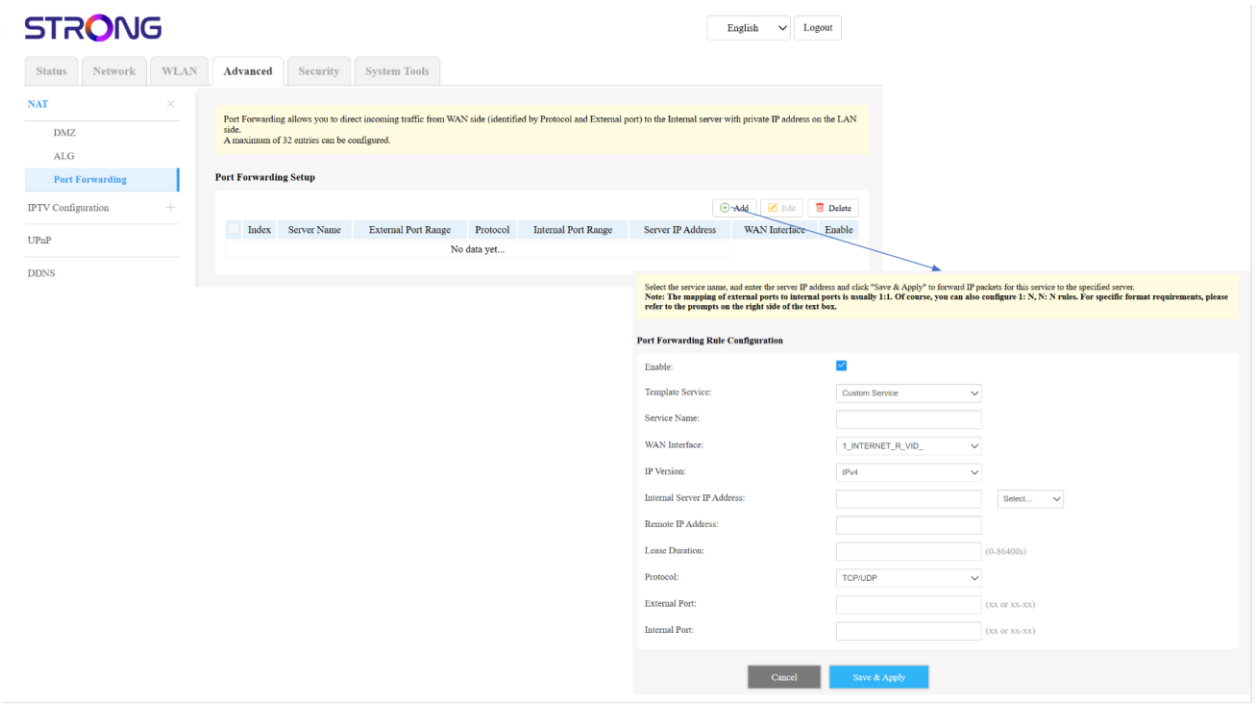

Fig. 26 — Advanced > NAT > Port Forwarding with the rule configuration window

Redirects incoming connections on specific WAN ports to specific devices on the local network. Maximum 32 rules.

Field	Description
Enable	Enable/disable this rule.
Template Service	Predefined service (HTTP, HTTPS, FTP, SSH, RDP…) or Custom Service.
Service Name	Descriptive name of the rule.
WAN Interface	WAN interface to which the rule applies.
IP Version	IPv4 or IPv6.
Internal Server IP Address	LAN IP of the destination device.
Remote IP Address	Allowed source WAN IP (optional, blank = all).
Protocol	TCP, UDP or TCP/UDP.
External Port	Incoming WAN port (e.g.: 8080 or 8080-8090 for a range).
Internal Port	Destination LAN port (e.g.: 80 or 80-90).

NOTE
External/internal mapping is generally 1:1. The on-screen note reminds you that you can also configure 1:N or N:N rules according to the indicated syntax.

4.4 IPTV Configuration — Proxy and Snooping

Subsection	Description
Proxy (slide 26)	Enables the IPTV proxy on a specific WAN interface. Interface: select the WAN interface dedicated to IPTV (e.g.: 1_INTERNET_R_VID_). Enable Proxy: check to activate.
Snooping (slide 27)	Enables IGMP Snooping to optimize IPTV multicast traffic on the LAN network. IPTV Snooping Enable: check to activate.

4.5 UPnP

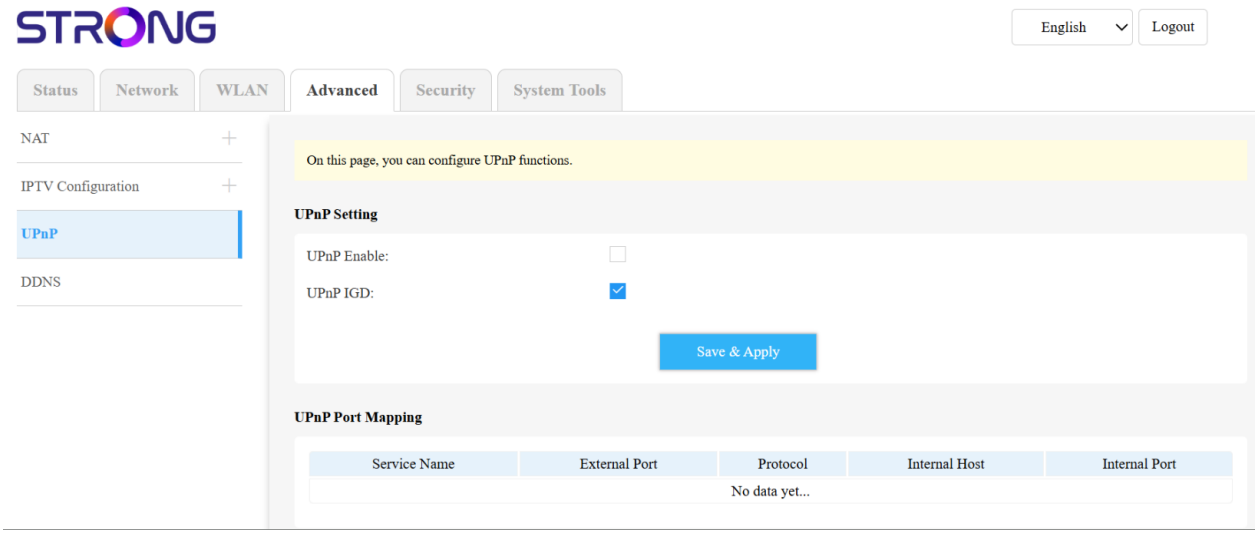

Fig. 27 — Advanced > UPnP: Universal Plug and Play

Setting	Description
UPnP Enable	Enables/disables UPnP. When enabled, applications (games, file sharing, VoIP) can automatically open ports.
UPnP IGD	Enables the Internet Gateway Device — the Internet gateway device detection function via UPnP.
UPnP Port Mapping	Table of port forwarding rules automatically created by UPnP (read-only).

4.6 DDNS — Dynamic DNS

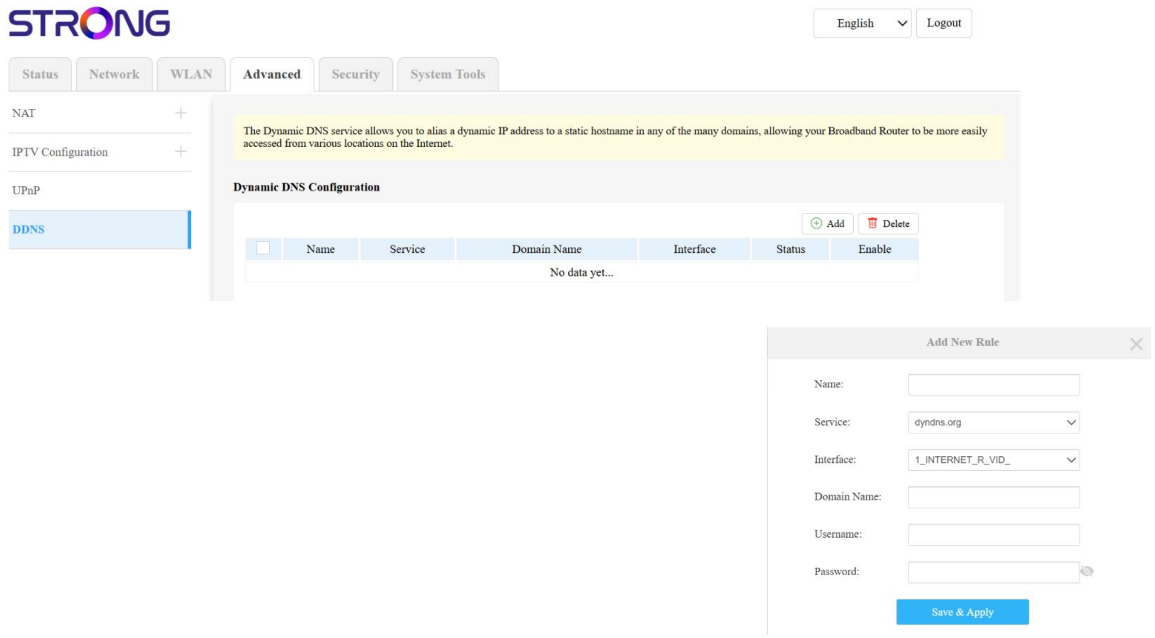

Fig. 28 — Advanced > DDNS with the rule addition window

DDNS allows you to associate a fixed domain name with your dynamic public IP address. Useful for remotely accessing your devices (server, NAS, cameras…) via a stable domain name.

Field	Description
Name	Name of the DDNS rule.
Service	DDNS provider: dyndns.org, noip.com, etc.
Interface	WAN interface to monitor for IP changes.
Domain Name	DDNS domain name registered with the provider.
Username	DDNS account username.
Password	DDNS account password.

5. Security — Security

5.1 Firewall — Firewall Level

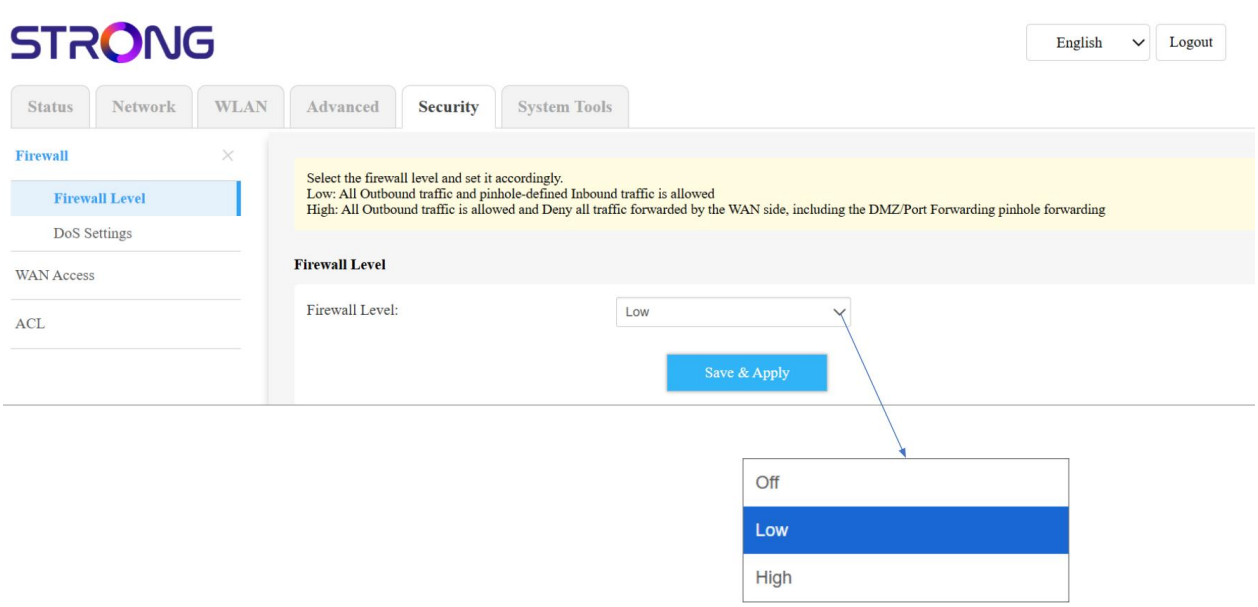

Fig. 29 — Security > Firewall > Firewall Level: Off, Low or High

Level	Description
Off	Firewall disabled. All incoming WAN traffic is allowed (including unsolicited traffic). Not recommended.
Low	Default level. All outgoing traffic is allowed. Incoming WAN traffic is only allowed if it matches the configured Port Forwarding or DMZ rules.
High	Strict level. All outgoing traffic is allowed. All incoming WAN traffic is blocked, including Port Forwarding and DMZ rules.

> ⚠ **IMPORTANT**
> In High mode, Port Forwarding and DMZ rules no longer function. Use this mode only if you do not require incoming access from the Internet.

5.2 Firewall — DoS Settings

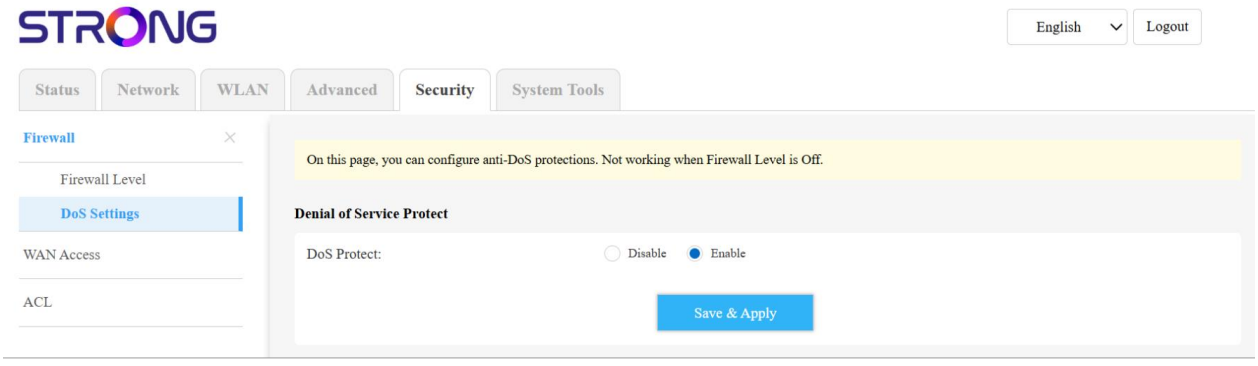

Fig. 30 — Security > Firewall > DoS Settings: anti-DoS protection

Enables protection against denial of service (DoS) attacks. Works only when the firewall level is set to something other than Off.

Option	Description
DoS Protect — Enable	Enables DoS protection (default: Enable). The router detects and blocks typical attack patterns (SYN flood, ping flood, port scan…).
DoS Protect — Disable	Disables protection. Not recommended except for very specific use cases.

5.3 WAN Access — Access to the Web UI from the Internet

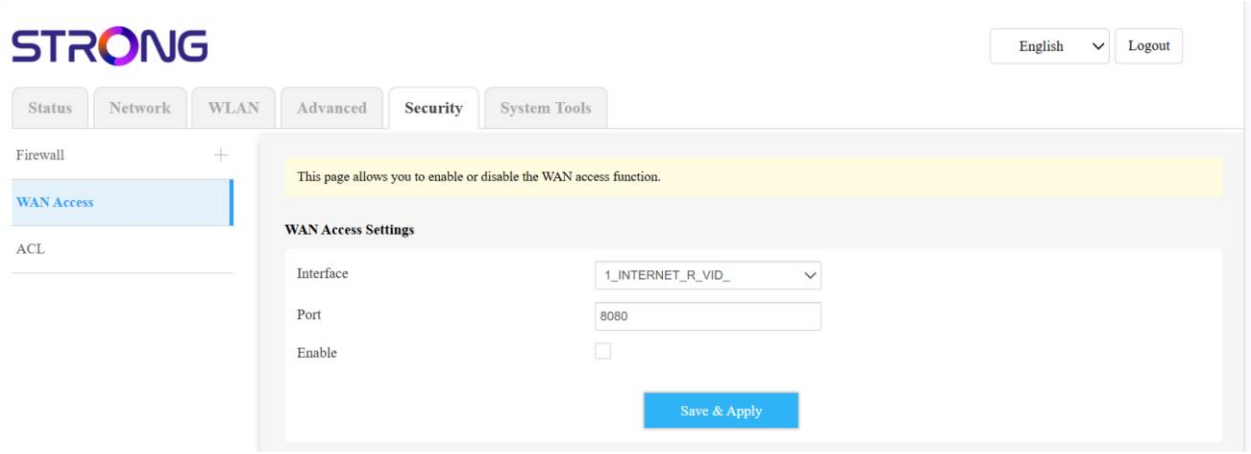

Fig. 31 — Security > WAN Access: administrative access from the WAN

Allows access to the router's configuration interface from the Internet (from the WAN), useful for remote administration.

Setting	Description
Interface	WAN interface on which remote access is allowed.
Port	Listening port for remote access (default: 8080). Enter the port of your choice (1-65535).
Enable	Check to enable WAN access to the Web UI.

> ⚠ **IMPORTANT**
> Enabling WAN access exposes your administration interface to the Internet. Ensure that you use a strong password and only enable this option if necessary.

5.4 ACL — Access control for services (IPv4 and IPv6)

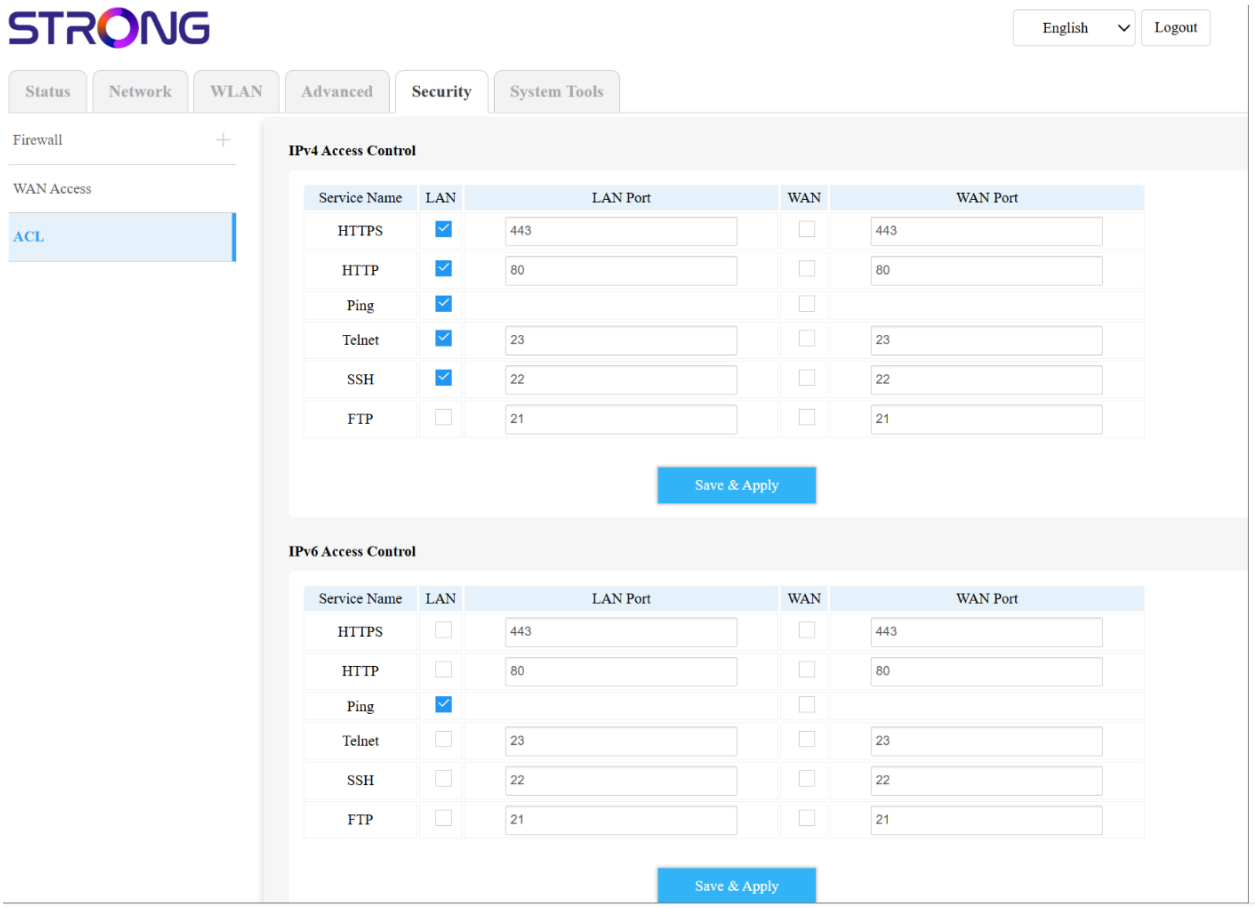

Fig. 32 — Security > ACL: LAN/WAN authorization by service

The ACL (Access Control List) controls access to the router's system services (Web UI, Ping, SSH, Telnet, FTP) from the local network (LAN) and/or from the Internet (WAN).

Service	Default access
HTTPS (port 443)	Access to the Web UI via HTTPS. LAN enabled by default. WAN disabled by default.
HTTP (port 80)	Access to the Web UI via HTTP. LAN enabled by default. WAN disabled.
Ping	Response to ping requests. LAN enabled. WAN disabled to prevent scans.
Telnet (port 23)	Telnet access. LAN enabled. WAN disabled.
SSH (port 22)	Secure SSH access. LAN enabled. WAN disabled.
FTP (port 21)	FTP access. LAN and WAN disabled by default.

NOTE
The IPv4 and IPv6 tables are identical. Check the LAN and/or WAN box for each service, modify the ports if necessary, then click Save & Apply.

6. System Tools — System Tools

6.1 User Management — Admin password

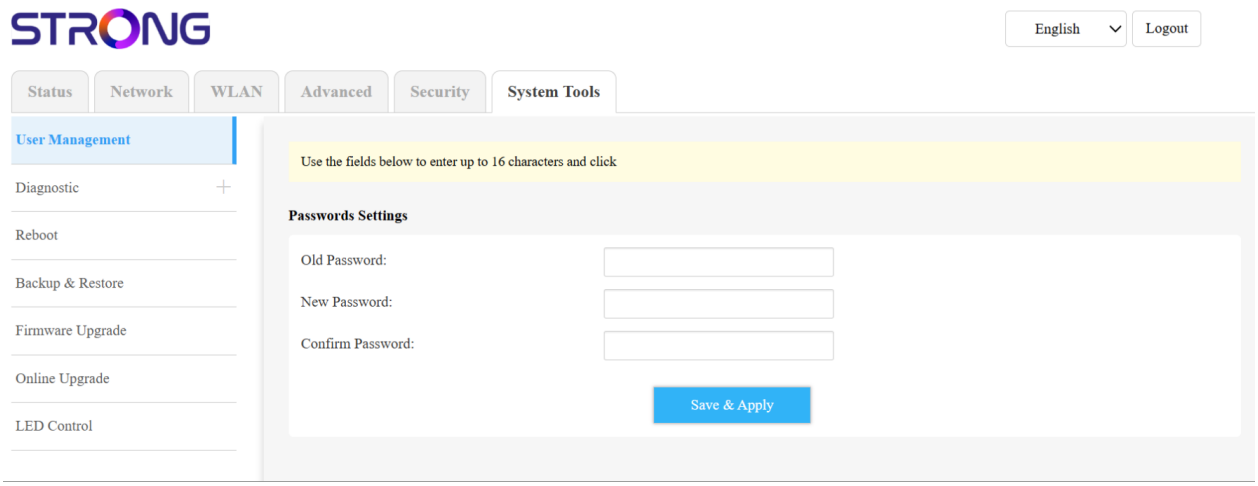

Fig. 33 — System Tools > User Management: password change

Changes the password for accessing the Web UI. Enter the old password (Old Password), the new one (New Password, max. 16 characters), and confirm (Confirm Password). Click Save & Apply.

> ⚠ **IMPORTANT**
> If the password is forgotten, the only solution is a factory reset (RESET button).

6.2 Diagnostic — Ping Test

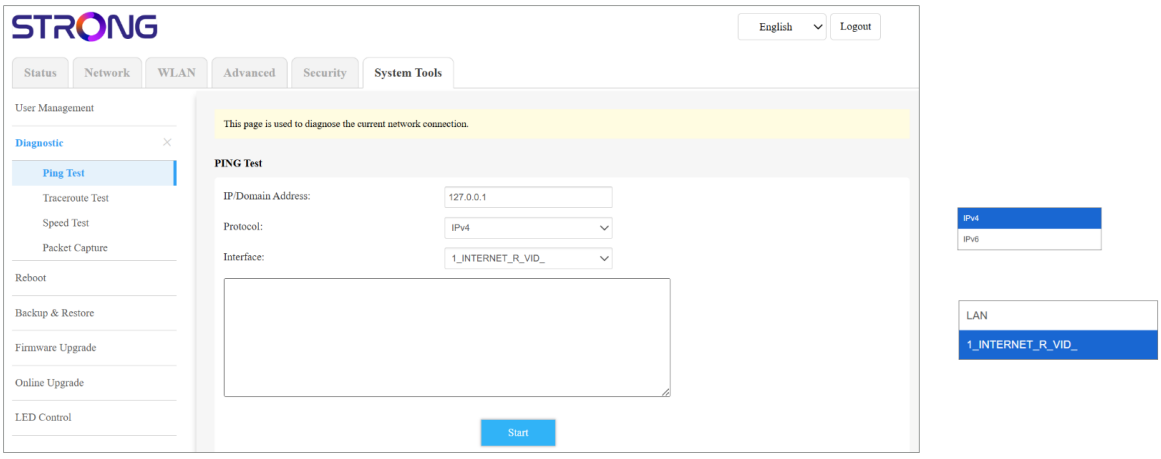

Fig. 34 — System Tools > Diagnostic > Ping Test: network connectivity test

Field	Description
IP/Domain Address	IP address or domain name targeted by the Ping test (default: 127.0.0.1).
Protocol	IPv4 or IPv6.
Interface	Network interface used for the test: LAN or WAN interface (1_INTERNET_R_VID_).
Start	Starts the Ping test. The results are displayed in the text area.

6.3 Diagnostic — Traceroute Test

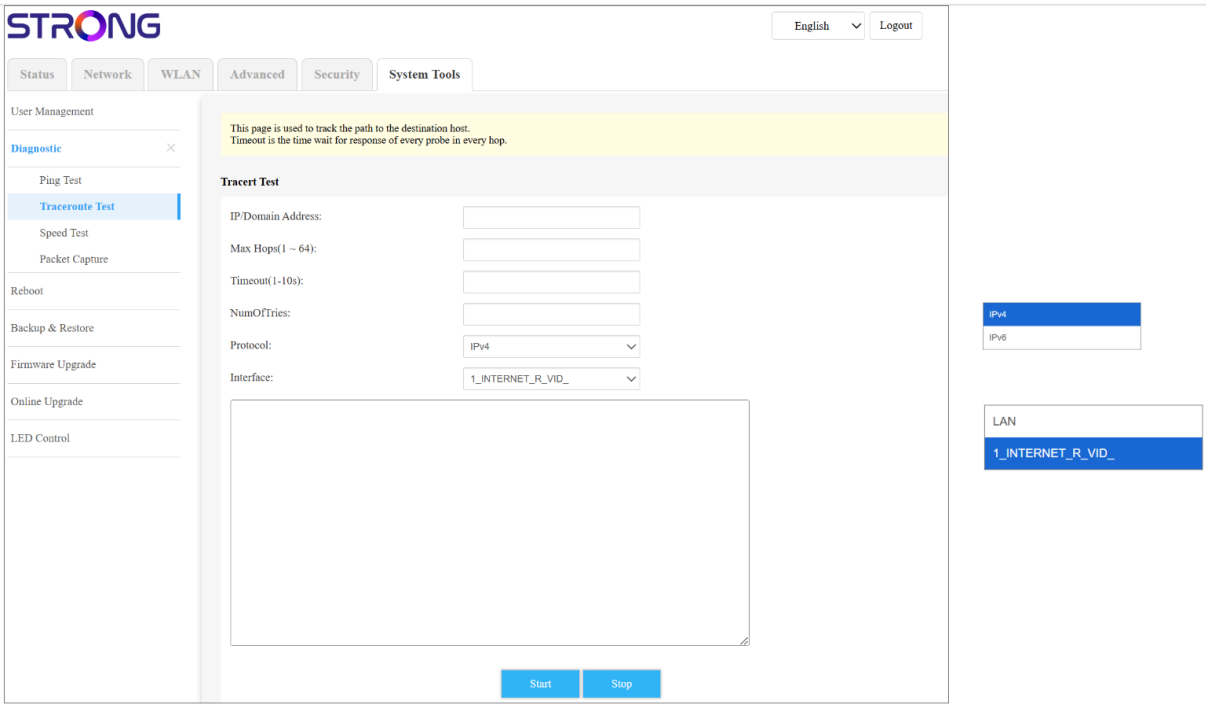

Fig. 35 — System Tools > Diagnostic > Traceroute Test: network route tracing

Field	Description
IP/Domain Address	Traceroute destination.
Max Hops	Maximum number of network hops (1–64).
Timeout	Timeout per hop in seconds (1–10 s).
NumOfTries	Number of probes per hop.
Protocol	IPv4 or IPv6.
Interface	Source network interface.
Start / Stop	Starts or stops the traceroute. Results in the text area.

6.4 Diagnostic — Speed Test

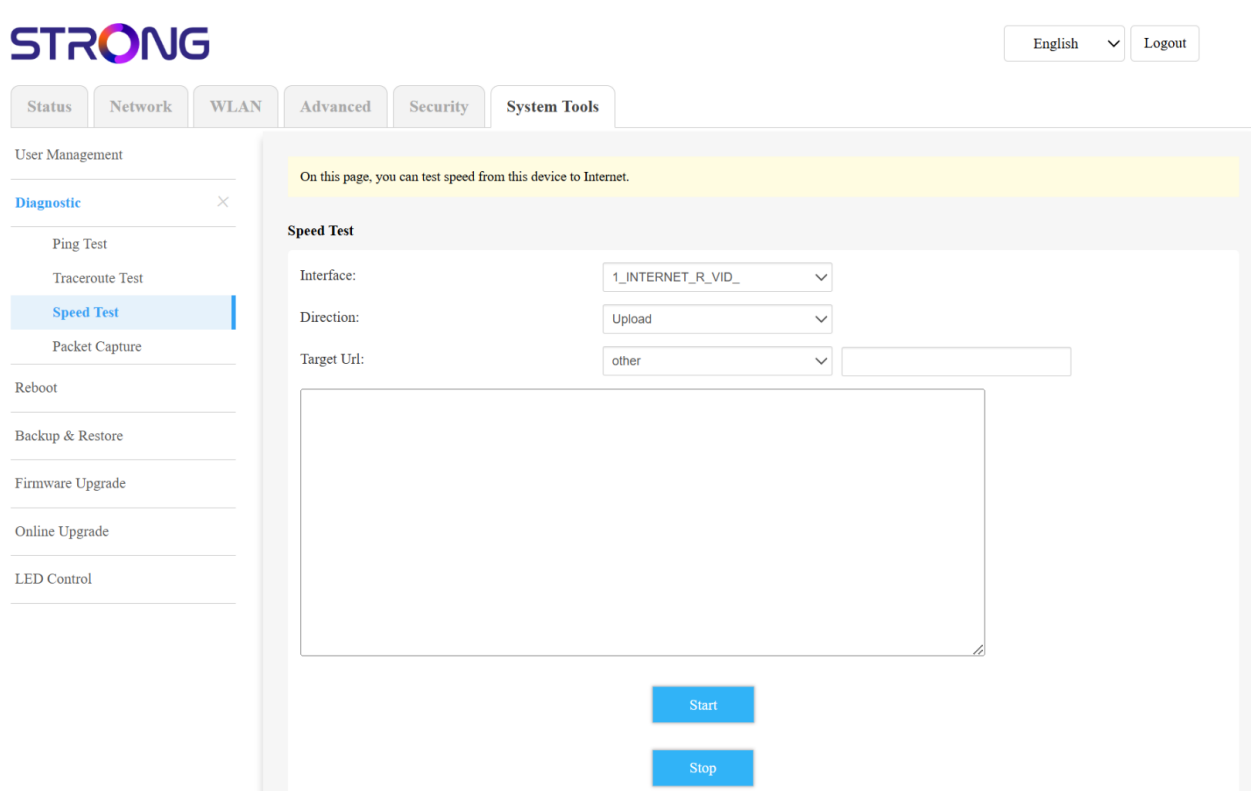

Fig. 36 — System Tools > Diagnostic > Speed Test: throughput test from the router

Measures the actual throughput between the router and the Internet (or a target server).

Field	Description
Interface	Tested WAN interface.
Department	Upload (upstream) or Download (downstream).
Target URL	Test server URL (predefined or 'other' to enter a custom URL).
Start / Stop	Starts or stops the test. Results in the text area.

6.5 Diagnostic — Packet Capture

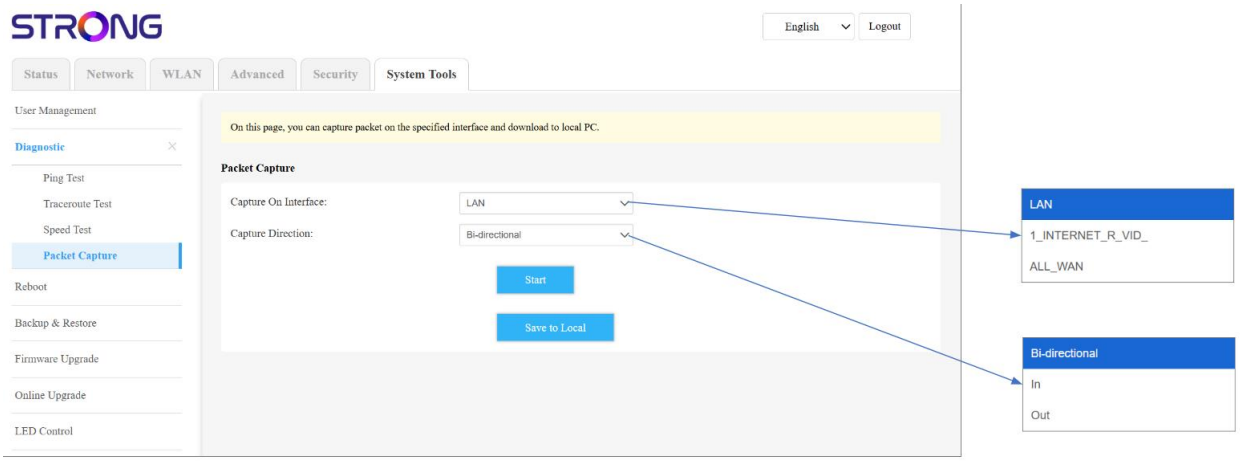

Fig. 37 — System Tools > Diagnostic > Packet Capture: network packet capture

Captures network packets on a specific interface for analysis. Useful for advanced diagnostics.

Field	Description
Capture On Interface	Interface to capture: LAN, 1_INTERNET_R_VID_, ALL_WAN.
Capture Direction	Packet direction: Bi-directional (incoming and outgoing), In (incoming only), Out (outgoing only).
Start	Starts the capture.
Save to Local	Downloads the capture file (.pcap) to your computer for analysis (Wireshark, etc.).

6.6 Reboot — Restart

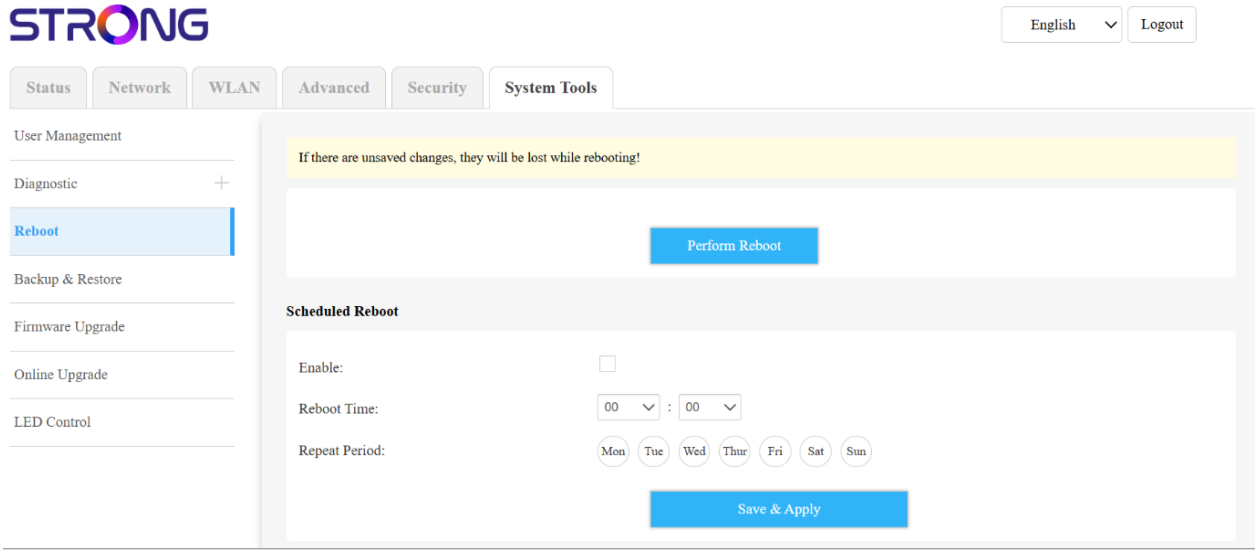

Fig. 38 — System Tools > Reboot: manual and scheduled restart

Option	Description
Perform Reboot	Restarts the router immediately. Unsaved changes will be lost. Duration: approximately 60 seconds.
Scheduled Reboot — Enable	Enables scheduled automatic restart.
Reboot Time	Time of automatic restart (format HH:MM).
Repeat Period	Days of the week on which automatic restart applies (Mon, Tue, Wed, Thu, Fri, Sat, Sun).

6.7 Backup & Restore — Backup and Restore

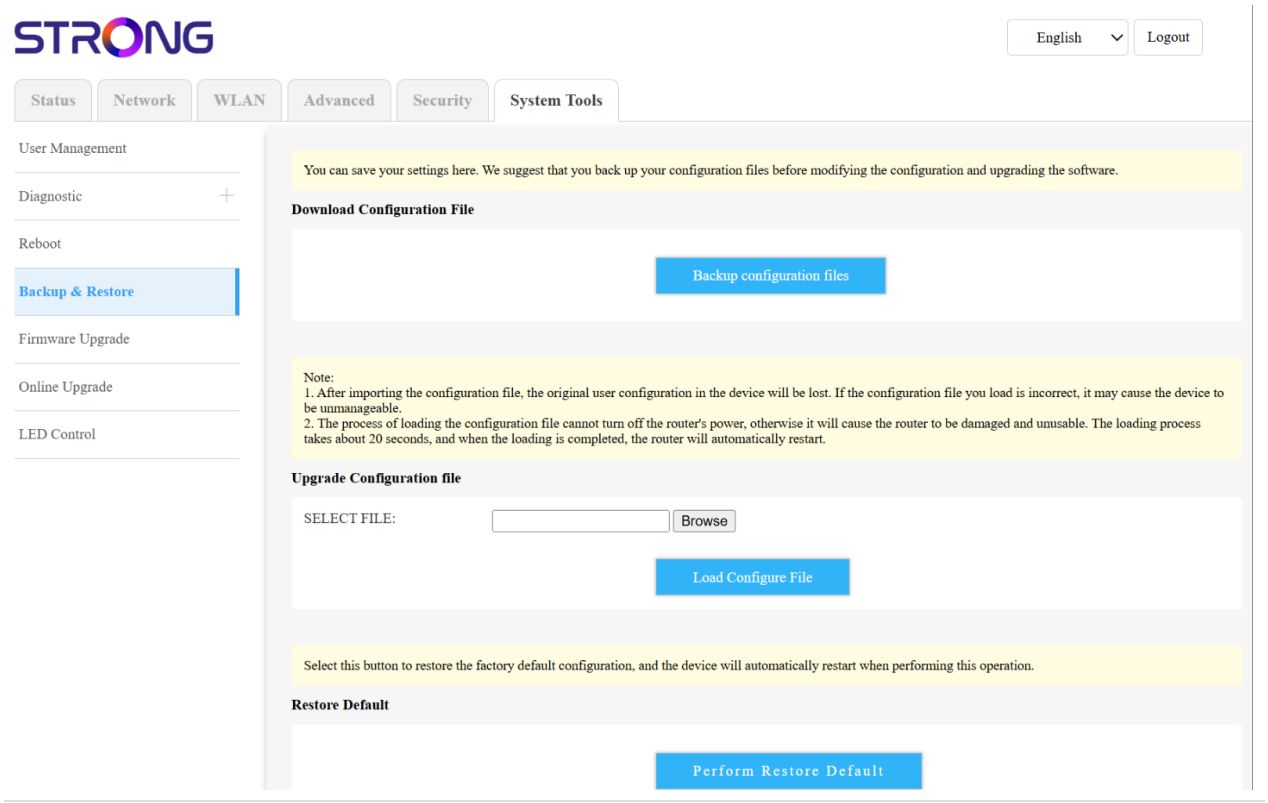

Fig. 39 — System Tools > Backup & Restore: backup, restore, and reset

Action	Description
Backup configuration files	Downloads a complete backup file of the configuration. To be kept in a safe place.
Upgrade Configuration file — Browse + Load Configure File	Select a previously created backup file and click Load Configure File to restore. The router restarts automatically (approximately 20 seconds).
Restore Default — Perform Restore Default	Resets the router to factory settings. IRREVERSIBLE — all custom configurations will be erased.

> ⚠ **IMPORTANT**
> Never disconnect the power during configuration loading or a reset. The process takes approximately 20 seconds.

6.8 Firmware Upgrade — Manual Update

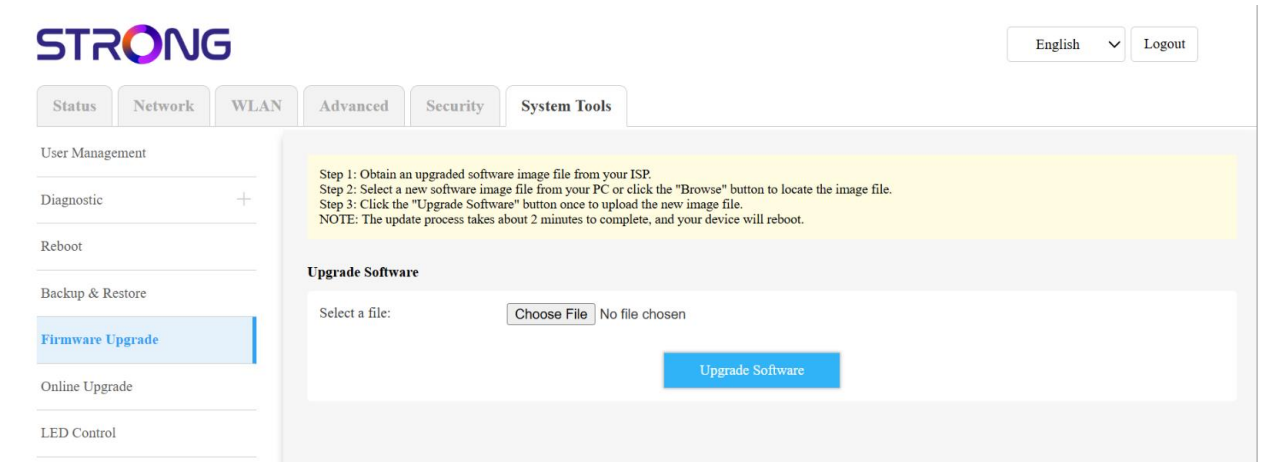

Fig. 40 — System Tools > Firmware Upgrade: manual firmware update

Manual firmware update procedure:

16. Obtain the firmware file from your ISP or from the STRONG support website (strong.tv / strong-eu.com).
17. Click on Choose File and select the downloaded firmware file.
18. Click on Upgrade Software. The update takes approximately 2 minutes.
19. The router will restart automatically at the end.

> ⚠ **IMPORTANT**
> Never turn off the router during a firmware update. This could render the device unusable.

6.9 Online Upgrade — Automatic Update

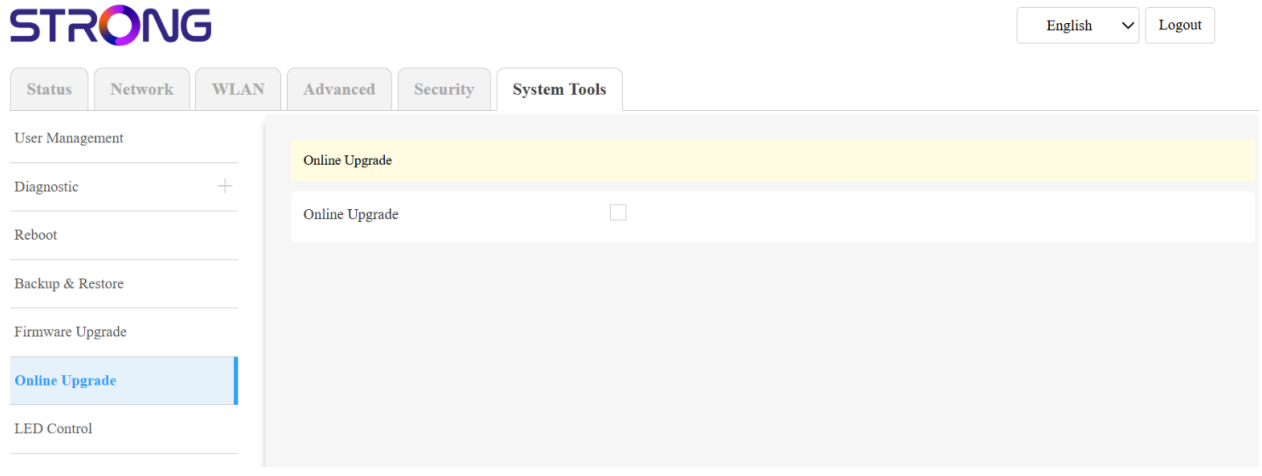

Fig. 41 — System Tools > Online Upgrade: automatic update (OTA)

Check the Online Upgrade box to enable automatic firmware updates via the Internet. When a new version is available on the STRONG servers, the router downloads and installs it automatically.

6.10 LED Control

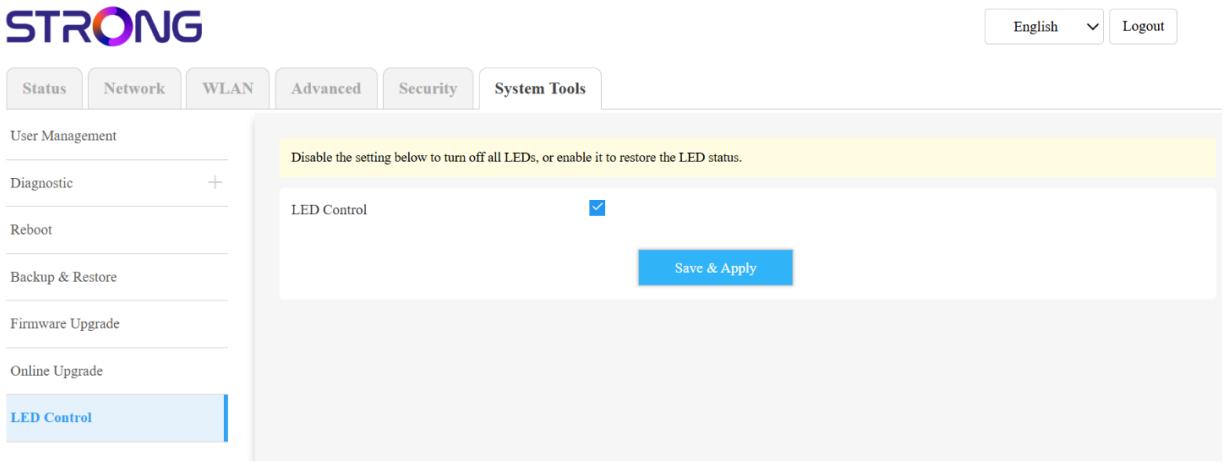

Fig. 42 — System Tools > LED Control: enable/disable the LED

Check LED Control to activate the status LED (normal behavior). Uncheck to turn off the LED (the router will continue to operate normally). Click Save & Apply.

TIP

Disabling the LED is useful if the router is placed in a bedroom and the light disturbs sleep.

IV. Common operations

1. Change the Wi-Fi name and password

20. WLAN > WLAN 2.4G > Basic Settings: change the Primary SSID and WPA Passphrase. Click Save & Apply.
21. WLAN > WLAN 5G > Basic Settings: do the same for the 5 GHz band.

> **TIP**
> If Band Steering is enabled, both bands share the same SSID. Change it in WLAN > Advanced > MLO.

2. Create a guest Wi-Fi network

22. WLAN > WLAN 2.4G > Multiple SSID: check Enable on ra1 (or ra2/ra3).
23. Enter an SSID and a password for the guest network.
24. Click Save & Apply.

3. Enable Wi-Fi 7 MLO

25. WLAN > Advanced > MLO: check MLO SSID Enable.
26. Set the MLO SSID and password.
27. Select Network Authentication (WPA2-PSK/WPA3-SAE recommended).
28. Click Save & Apply.

4. Use in Repeater mode

29. Network > Uplink Configuration: select Repeater.
30. Choose the connection interface (AE_WAN recommended).
31. Click Save & Apply. The router connects to the source Wi-Fi network.

> **NOTE**
> In Repeater mode, the router extends the range of an existing Wi-Fi network. Managing the Web UI may require reconnecting with a static IP.

5. Port forwarding (server hosting)

32. Advanced > NAT > Port Forwarding: click Add.
33. Select the service (or Custom Service), enter the external and internal ports, the device's LAN IP, and the protocol.
34. Check Enable and click Save & Apply.

6. Backup and restore configuration

35. System Tools > Backup & Restore > Backup configuration files: download the backup file.
36. To restore: Browse, select the file, then Load Configure File.

V. Troubleshooting

Symptom	Probable cause	Solution
Router does not start	Faulty power supply	Check the DC 12V/1.5A adapter and the power outlet.
Solid red LED	No Internet access	Check the cable between the WAN/2.5G port (blue) and your modem. Check Network > WAN Configuration.
Web UI inaccessible (192.168.1.1)	Not connected to the router's network	Connect to the router's Wi-Fi or via LAN cable. Enter http://192.168.1.1 (without 's').
Web UI password forgotten	Password lost	Reset using the physical RESET button (back panel, 5–10 seconds with a pin).
Wi-Fi not visible	Hidden SSID or radio disabled	Ensure that 2.4G/5G Radio Enable is checked and Hide SSID is unchecked in WLAN > Basic Settings.
Low Wi-Fi speed	MLO disabled or 2.4 GHz band	Enable MLO in WLAN > Advanced > MLO. Enable Band Steering to migrate to 5 GHz.
Devices on 2.4 GHz only	Band Steering misconfigured	Adjust the RSSI2G and RSSI5G thresholds in WLAN > Advanced > Band Steering.
Port Forwarding does not work	Firewall in High mode	Security > Firewall: set the level to Low. Ensure that the device's LAN IP is fixed (Static DHCP).
IPTV does not work	IPTV Proxy not enabled	Advanced > IPTV Configuration > Proxy: enable and select the correct WAN interface.
Firmware update failed	Incorrect file or connection lost	Ensure that the file is for the ROUTERBE3600 model. Do not disconnect the power during the update.
Repeater Mode does not connect	Incorrect source SSID	Network > Uplink Configuration: verify that the selected interface is correct.
Slow connection despite Wi-Fi 7	MLO not supported by the client device	MLO requires a Wi-Fi 7 client device. Wi-Fi 6/5 devices connect normally but without MLO.

TIP

If none of the solutions resolve your issue, please visit www.strong-eu.com or contact STRONG support. Prepare the serial number (Status > Device Info).

VI. Technical Specifications

General characteristics

Characteristic	Value
Product reference	ROUTERBE3600
CPU	AN7563CT
Dimensions (W×D×H)	235 × 148 × 40 mm
Weight	0,925 kg
Operating temperature	0°C to +45°C
Storage temperature	-20°C to +60°C
Operating humidity	0% – 95% non-condensing
Power supply	External — DC 12V / 1.5A
Warranty	4 years
EAN	9120072379727
Certification	CE

Wi-Fi

Characteristic	Value
Wi-Fi standard	IEEE 802.11 a/b/g/n/ac/ax/be (Wi-Fi 7)
Bands	Simultaneous Dual-Band 2.4 GHz + 5 GHz
Total Wi-Fi speed	3,600 Mbps
2.4 GHz speed	688 Mbps (802.11be)
5 GHz speed	2,882 Mbps (802.11be)
Wi-Fi 7 MLO	Yes — Multi-Link Operation
Antennas	5 × external antennas 3 dBi
Transmission power	< 20 dBm (2.4 GHz) · < 23 dBm (5 GHz) — Europe
2.4 GHz channels	1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 9 / 10 / 11 / 12 / 13
5 GHz channels	36 / 40 / 44 / 48 / 52 / 56 / 60 / 64 / 149 / 153 / 157 / 161
Wi-Fi security	WPA / WPA2 / WPA3
Wi-Fi functions	MLO · Band Steering · Multiple SSIDs · Scheduler · ACL · WPS · Easy Mesh · Repeater Mode

Wired connectivity

Interface	Description
WAN port	1 × RJ-45 — 2.5 Gbps (blue)
LAN ports	3 × RJ-45 — 1 Gbps (yellow)
Buttons	1 × WPS (rear panel) · 1 × Reset (pinhole rear panel)

Software and network functions

Function	Support
WAN types	DHCP · PPPoE · Bridge · Static IP · DHCPv6 · SLAAC
DHCP	DHCP Server · Address Reservation · Client List
NAT / Forwarding	DMZ · Port Forwarding · UPnP
IPTV	IGMP Proxy · IGMP Snooping · Bridge · VLAN Tag
Security	Firewall · DoS protection · Port scan protection
Management	Web UI interface · MySTRONG application · OTA update
Others	NTP · LED control · Backup & Restore · Diagnostics (Ping, Traceroute, Speed Test, Packet Capture) · Scheduled reboot · DDNS · QoS
Required configuration	Windows 7 and later versions · All modern browsers

Legal Notice

This product complies with the applicable European directives. The CE mark certifies its compliance. STRONG is a registered trademark, a subsidiary of Skyworth.

Actual performance may vary depending on the network environment, building materials, and electromagnetic interference. STRONG reserves the right to modify specifications without prior notice.