

User Guide

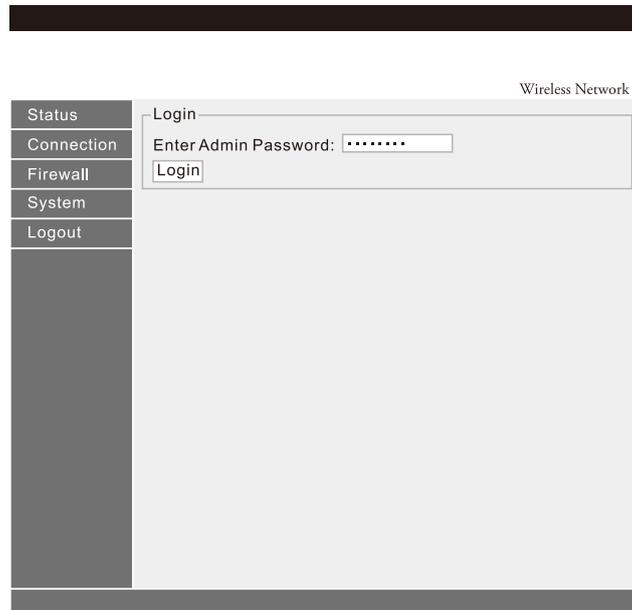
4G Router Manual



4G Router Manual

Chapter 1 Login	2
Chapter 2 Status	2
2.1 Overview.....	3
2.1.1 Hardware status.....	3
2.1.2 Time status.....	3
2.1.3 LAN port.....	3
2.1.4 4G Network.....	3
2.1.5 DNS Server.....	4
2.1.6 WAN Port.....	4
2.2 Connected Hosts.....	4
2.3 Connection List.....	4
Chapter 3 Connection	5
3.1 Basic Settings.....	5
3.1.1 Internet/WAN.....	6
3.1.2 Local Network/LAN.....	7
3.1.3 Wireless.....	7
3.2 DHCP Server.....	8
3.2.1 DHCP&Static IPs.....	8
3.3 APN.....	8
3.4 DDNS setting.....	8
3.5 Ping Watchdog.....	9
Chapter 4 Firewall	10
4.1 Port Forwarding.....	10
4.2 Connection Limits & Restrictions.....	10
4.3 Restrictions.....	11
Chapter 5 System	12
5.1 Router Access.....	12
5.2 Time.....	12
5.3 Restore.....	13
5.4 Update Firmware.....	13
5.5 Reboot.....	14
Chapter 6 Logout	14

Chapter 1 Login



Log in to the computer network to automatically obtain an IP address.
Default IP address: 192.168.110.251, Default login password: password;

Chapter 2 Status

2.1 Overview

Wireless Network

Status

Overview

Connected Hosts

Connection List

Connection

Firewall

System

Logout

Status

Memory Usage: 15.8MB / 122.2MB (12.9%)

Connections: 442/16384

CPU Load Averages: 0.17 / 0.24 / 0.11 (1/5/15 minutes)

Uptime: 0 days, 0 hours, 3 minutes

Current Date & Time: 2019/07/18 14:57 UTC+8

LAN IP Address: 192.168.110.251

LAN Netmask: 255.255.255.0

LAN MAC Address: 74:96:37:09:62:18

4G IP Address: 10.10.174.248

4G Netmask: 255.255.255.240

4G Gateway IP: 10.10.174.249

SIM Card Slot: SIM1

4G Signal Strength: Strong

DNS Server: 211.136.17.107
211.136.20.203

WAN IP Address: -

WAN Netmask: -

WAN MAC Address: 74:96:37:09:62:19

2.1.1 Hardware status

Memory usage, number of connections, and CPU usage (Timeline 1/5/15 minutes respectively).

2.1.2 Time status

System runtime and world time.

2.1.3 LAN port

LAN IP Address, LAN Netmask, LAN MAC Address.

2.1.4 G Network

4G IP Address, Netmask, Gateway IP, SIM Card Slot, Singal Strength.

Note: 4G router reads SIM1 (lower card slot) by default. When the 4G router is started, the Ping watchdog function detects network connectivity. If no response is received within the maximum time limit, 4G router will automatically restart and automatically switch to SIM2 (Upper card slot), continue to detect after reboot, until the network is back to normal. This process takes about 8-9 minutes, please be patient.

2.1.5 DNS Server

DNS Server

2.1.6 WAN Port (WAN port needs to be connected to the external network)

WAN IP Address, Netmask, MAC.

2.2 Connected Hosts

Wireless Network

Status

Overview

Connected Hosts

Connection List

Connection

Firewall

System

Logout

Refresh Rate

10 Seconds ▼

This specifies how frequently data on this page is reloaded

Current DHCP Leases

Hostname	Host IP	Host MAC	Lease Expires
SC-201808131922	192.168.110.182	9C:EB:E8:11:34:3A	11h 54m

Connected Wireless Hosts

Hosts With Active Connections

Hostname	Host IP	Host MAC	Active TCP Cnns	Recent TCP Cnns	UDP Cnns
(unknown)	10.10.174.248	unknown	0	0	12
TD-954G2	127.0.0.1	unknown	0	0	2
SC-201808131922	192.168.110.182	9C:EB:E8:11:34:3A	99	262	16

You can set the page refresh time to display DHCP lease user information, active users.

2.3 Connection List

Wireless Network

Status

Overview

Connected Hosts

Connection List

Connection

Firewall

System

Logout

Current Connections

Refresh Rate: 2 Seconds ▼

Bandwidth Units: Auto (Mixed) ▼

Host Display: Display Hostnames ▼

Proto	WAN Host/LAN Host	Bytes Up/Down	L7 Proto
tcp	10.10.174.248:51609 111.45.68.207:443	224.578 KBytes 7.382 KBytes	
tcp	10.10.174.248:51601 183.240.115.248:443	214.101 KBytes 6.287 KBytes	
tcp	10.10.174.248:51300 183.232.152.223:443	185.267 KBytes 6.095 KBytes	
tcp	10.10.174.248:51538 183.232.152.223:443	174.070 KBytes 4.950 KBytes	

1.You can set the page refresh time, you can modify the traffic data unit, display mode host name / IP.

=====

Chapter 3 Connection

3.1 Basic settings

Wireless Network	
Status	Internet / WAN
Connection	Connect Via: <input type="text" value="DHCP (Wired) ▼"/>
	Current IP: <input type="text" value=""/>
	Current Lease Expires: <input type="button" value="Renew Lease Now"/>
	Use Custom MAC Address: <input type="text" value="74:96:37:09:62:19"/>
	Use Custom MTU: <input type="text" value="1500"/>
Local Network/ LAN	
Router IP: <input type="text" value="192.168.110.251"/>	
Subnet Mask: <input type="text" value="255.255.255.055"/>	
DNS Servers: <input type="text" value="I Default DNS Servers Specified byISP ▼"/>	
	<input type="checkbox"/> Allow NameCoin/OpenNIC Resolution
	<input type="checkbox"/> Force Clients To Use Router DNS Servers
Wireless	
Wireless Mode: <input type="text" value="Access Point (AP) ▼"/>	
Operation Mode: <input type="text" value="N+G+B ▼"/>	
Channel Width: <input type="text" value="40MHz (2nd chan. below) ▼"/>	
Transmit Power: <input type="text" value="Max ▼"/> <input type="text" value="28"/> (0 - 28dBm)	
Wireless MAC Filter: <input type="text" value="Disabled ▼"/>	
Access Point SSID: <input type="text" value="Todaair.4G"/>	
Wireless Channel: <input type="text" value="11 ▼"/>	

3.1.1 Internet/WAN

DHCP (wired) - The WAN port connects to the upper-level route, and automatically obtains the external network resources allocated by the superior route to access the Internet, or dials the Internet using the 4G card*1.

Note : 4G SIM card loading instructions: 1. Make sure the SIM card supports the local operator network. 2.This product provides dual card slots(does not support dual SIM cards at the same time , and supports automatic switching of dial-up SIM after disconnected network). 3.The size of the SIM card is a standard card. When inserting, the oblique opening is inward and the contact is downward.

=====

Wireless Network	
Status	Internet / WAN
Connection	Connect Via: <input type="text" value="Static IP (Wired) ▼"/>
	Static IP: <input type="text" value="10.1.1.10"/>
	Subnet Mask: <input type="text" value="255.255.255.0"/>
	Gateway: <input type="text" value="127.0.0.1"/>
	Use Custom MAC Address: <input type="checkbox"/> <input type="text" value="74:96:37:09:62:19"/>
Use Custom MTU: <input type="checkbox"/> <input type="text" value="1500"/>	
Local Network/ LAN	
Router IP: <input type="text" value="192.168.110.251"/>	
Subnet Mask: <input type="text" value="255.255.255.055"/>	
DNS Servers: <input type="text" value="Default DNS Servers Specified by ISP ▼"/>	
	<input checked="" type="checkbox"/> Allow NameCoin/OpenNIC Resolution
	<input type="checkbox"/> Force Clients To Use Router DNS Servers
Wireless	
Wireless Mode: <input type="text" value="Access Point (AP) ▼"/>	
Operation Mode: <input type="text" value="N+G+B ▼"/>	
Channel Width: <input type="text" value="40MHz (2nd chan. below) ▼"/>	
Transmit Power: <input type="text" value="Max ▼"/> <input type="text" value="28"/> (0 - 28dBm)	
Wireless MAC Filter: <input type="text" value="Disabled ▼"/>	
Access Point SSID: <input type="text" value="Todaair.4G"/>	
Wireless Channel: <input type="text" value="11 ▼"/>	

Static IP(Wired)-Manually fill in the static IP address to obtain the upper-layer routing external network resources.

3.5 Ping Watchdog

The screenshot shows the 'Ping Watchdog' configuration page. The left sidebar contains a menu with 'Ping Watchdog' selected. The main content area has a title 'Ping Watchdog' and a sub-header 'Wireless Network'. Below this, there are fields for 'Address' (containing 'qq.com') and 'Interval' (set to '2 Minutes'). At the bottom, there are 'Save Changes' and 'Reset' buttons.

The “Ping Watchdog” function is a function of 4G router detection network connectivity. It sends a Ping packet to a specified address periodically. If the reply is received normally, the network is unobstructed. If no response is received within the maximum time limit, the 4G route will automatically restart. After the restart, the detection will continue until the network returns to normal.

3.6 Cloud Management

Add the cloud code to the binding code, and you can view the router's online status and device status on the platform. For detailed, please refer to the cloud platform instruction manual.

The screenshot shows the 'Cloud' configuration page. The left sidebar contains a menu with 'Remote Management' selected. The main content area has a title 'Cloud' and a sub-header 'Wireless Network'. Below this, there are fields for 'Binding code' and a 'Show/Hide' checkbox. A link 'Access the cloud management platform!' is displayed. At the bottom, there are 'Save Changes' and 'Reset' buttons.

Chapter 4 Firewall

4.1 Port Forwarding

It is support individual port forwarding, port range forwarding, DMZ, UPnP and NAT-PMP functions.

The screenshot shows the 'Firewall' configuration page. The left sidebar contains a menu with 'Firewall' selected. The main content area has a title 'Firewall' and a sub-header 'Wireless Network'. Below this, there are sections for 'Individual Port Forwarding', 'Port Range Forwarding', 'DMZ', and 'UPnP /NAT-PMP'. The 'Individual Port Forwarding' section has a table with columns 'Description (optional)', 'Protocol', 'From Port', 'To IP', and 'To Port (Optional)'. The 'DMZ' section has a checkbox 'Use DMZ (De-Mitarized Zone)' and a field for 'DMZ IP:' containing '192.168.110.252'. The 'UPnP /NAT-PMP' section has a checkbox 'Enable UPnP & NAT-PMP serice' and a table with columns 'Proto', 'LANHost', and 'Port'. At the bottom, there is a field 'Upload speed to report:' set to '1250 Kbytes / second'.

The user can set the port functions according to actual needs.

4.2 Connection Limits & Restrictions

Set up TCP/UDP timeout in the router

Status	Connection Limist	
Connection	Max connections:	<input type="text" value="16384"/> (max 16384)
Firewall	TCP Timeout:	<input type="text" value="7440"/> seconds(max 3600)
	UDP Timeout:	<input type="text" value="180"/> seconds(max 3600)
<input type="button" value="Save Changes"/> <input type="button" value="Reset"/>		
System		
Logout		

4.3 Restrictions

Wireless Network		
Status	Access Restrictions	
Connection	New Restriction Rule:	
Firewall	Rule Description:	<input type="text"/>
	Rule Applies To:	<input type="text" value="All Hosts"/>
	Schedule:	<input checked="" type="checkbox"/> All Day <input checked="" type="checkbox"/> Every Day
	Restricted Resources:	<input checked="" type="checkbox"/> All Network Access
<input type="button" value="Add New Rule"/>		
System	Current Restrictions:	
Logout	Exceptions (White List)	
New Exception:		
Exception Description:		<input type="text"/>
Exception Applies To:		<input type="text" value="All Hosts"/>
Schedule:		<input checked="" type="checkbox"/> All Day <input checked="" type="checkbox"/> Every Day
Permitted Resources:		<input checked="" type="checkbox"/> All Network Access
<input type="button" value="Add New Rule"/>		
Current Exceptions:		
<input type="button" value="Save Changes"/> <input type="button" value="Reset"/>		

Users can set connection restrictions and access rules according to actual needs.

Chapter 5 System

5.1 Router Access

Status	Web Access	
Connection	Web Admin Protocol:	<input type="text" value="HTTP & HTTPS"/>
Firewall	Local HTTP Port:	<input type="text" value="80"/>
	Local HTTPS Port:	<input type="text" value="443"/>
	Remote Web Admin Access:	<input type="text" value="Disabled"/>
	Web Login Session Length:	<input type="text" value="15 minutes"/>
<input type="checkbox"/> Disable password protection of web interface(Not Recommended!!)		
System	SSH Access	
Router Access	LocalSSH Port:	<input type="text" value="22"/>
Time	<input type="checkbox"/> Enable Remote SSH Access	
Restore	Remote SSH Port:	<input type="text" value="22"/>
Update Firmware	Max Remote Login Attempts:	<input type="text" value="10 Attempts Every Five Minutes"/>
Reboot		
Logout	Change Administrator Password	
New Password:		<input type="text"/>
Confirm Password:		<input type="text"/>
<input type="button" value="Save Changes"/> <input type="button" value="Reset"/>		

Users can modify the Web access rule settings, SSH access settings, and modify the login password.

5.2 Time

Status	Time	
Connection	Current Date & Time: 2019/07/18 15:00 UTC+8	
Firewall	Time Zone:	<input type="text" value="UTC+08:00 China, Hong Kong, Singapore, Taiwan, Russia"/>
	Date Format:	<input type="text" value="yyyy/mm/dd"/>
	NTP Servers:	<input type="text" value="2.asia.pool.ntp.org"/> <input type="text" value="1.asia.pool.ntp.org"/>
	Asia	<input type="text" value="0.asia.pool.ntp.org"/>
System	Logout	
Router Access	<input type="button" value="Save Changes"/> <input type="button" value="Reset"/>	
Time		
Restore		
Update Firmware		
Reboot		

Set the corresponding time zone, date format and NTP (time) server. After the external network connection is successful, it will be calibrated according to the settings.

5.3 Restore

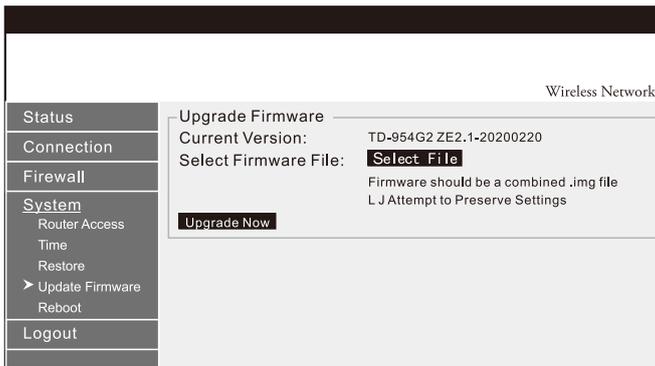


Web interface control to restore settings

Hardware control to restore settings, long press the reset button for 8-10 seconds.

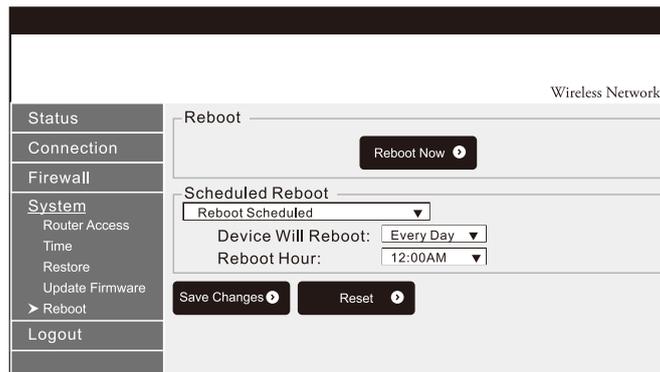
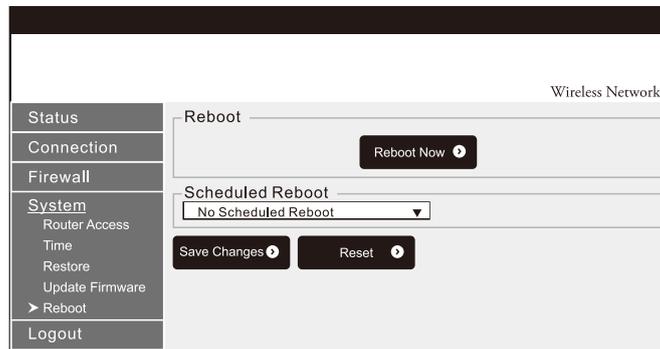
=====

5.4 Update Firmware



Choose the firmware provided by the company to upgrade.

5.5 Reboot



Reboot now or schedule automatic reboot time.

=====

Chapter 6 Logout

Execute to exit the current login status.