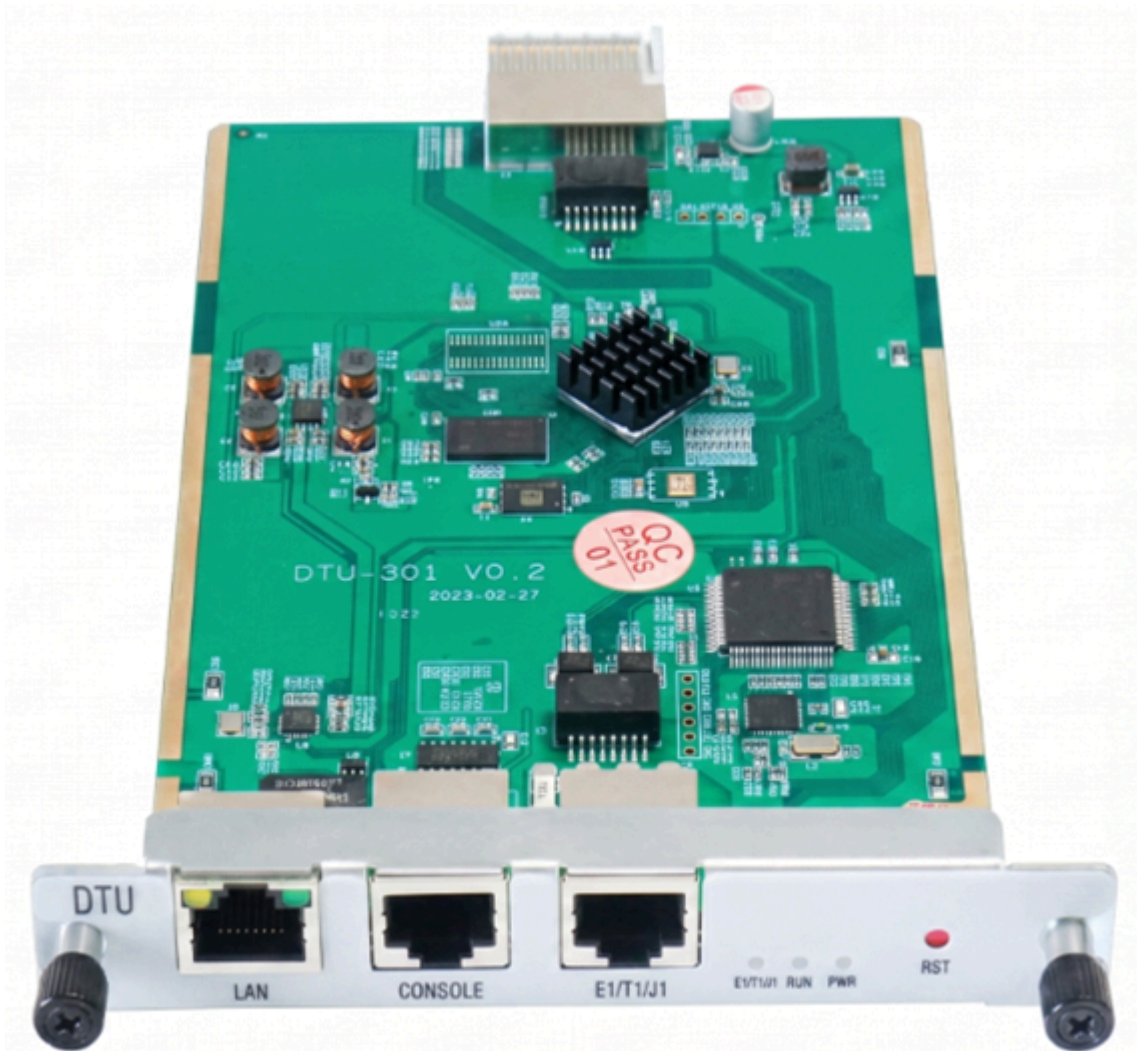


DTU-30X Digital Gateway User Manual



Version 2.0

Address: Room 624, 6/F, Tsinghua Information Port, Shukan Building, Qingxiang Road, Longhua Street, Longhua District, Shenzhen 518109

Tel: +86-755-66630978, 82535461, 82535362

Sales: sales@openvoxtech.com

Technical Support: support@openvoxtech.com

Business Hours: Monday to Friday, 09:00-18:00 (GMT+8), excluding holidays

Thank you for choosing OpenVox products.

Statement

The copyright of this document belongs to Shenzhen OpenVox Communication Co., Ltd. (OpenVox). Without permission, images and text in this document may not be copied or reproduced for commercial use. Shenzhen OpenVox Communication Co., Ltd. reserves all rights of interpretation. For details, contact OpenVox sales or technical support.

Revision History

Version	Release Date	Description
2.0	25/5/2026	

Document Information

- Product: DTU-30X
- Document Type: User Manual
- Interface Type: 1/2/4 E1/T1 port

1. Overview

1.1 Product Introduction

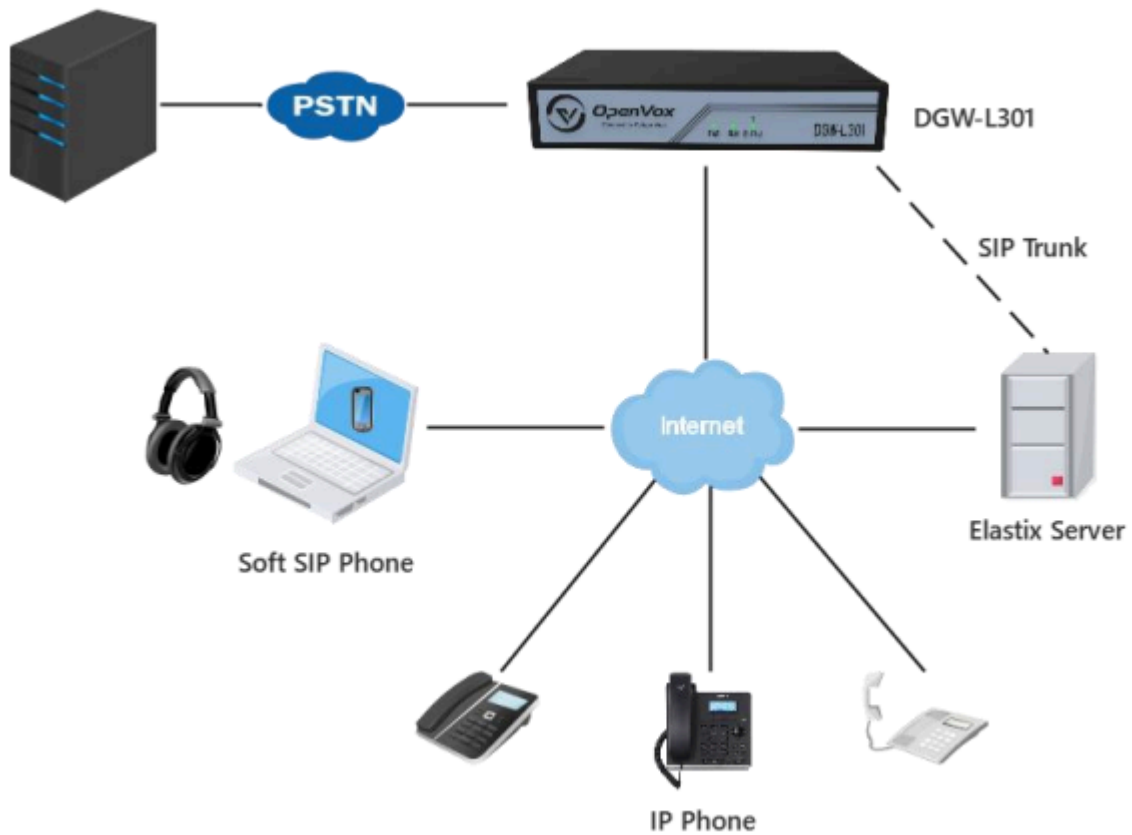
The OpenVox Digital Gateway service board includes DTU-301, DTU-302, and DTU-304, which support 1, 2, and 4 T1/E1/PRI ports, respectively, and support 30, 60, and 120 concurrent calls.

This series of devices is a new generation of converged media gateways, which can realize the perfect integration of traditional TDM communication and VoIP networks, support multiple signaling protocols (PRI, R2, SS7) and multiple codec formats, and can be seamlessly compatible with mainstream IPPBX, soft switching, and IMS platforms. Users can easily complete the configuration through the intuitive web GUI, and support OpenAPI interface development, which is suitable for various scenarios such as operators, enterprise-level call systems, and call centers.

1.2 Typical Applications

DTU-30X series typical applications are shown in the diagram, enabling enterprise branch interconnection, smooth transition from traditional PBX to IP, remote voice access, and other applications.

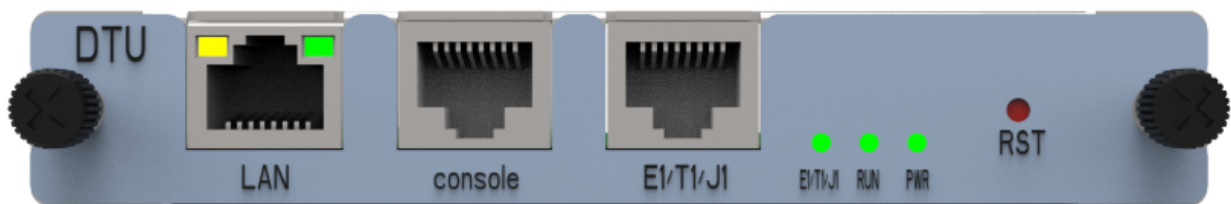
Figure 1-2-1 Application Topology



1.3 Product Appearance

DTU-30X series product front and rear panel design continues the OpenVox industrial style, providing stable and reliable interface layout.

The new RS232 (RJ45) console port makes engineering-level debugging and maintenance easier.



1.4 Software Features

	L301	L302	L304
Telephony Ports (E1/T1)	1	2	4
Concurrent Calls	30	60	120
Signaling Support	PRI, R2, SS7, multi-country standards compatible		
Voice Codecs	Supports G.711A/U, G.723.1, G.729A/B, iLBC, OPUS, ARM, ARM-WB		
Fax Support	T.38 and G.711 pass-through, compatible with V.17./V.21./V.27./V.29		
SIP Standard	RFC3261 compliant, supports TLS/SRTP encryption		
QoS Policy	Supports ToS/DiffServe/802.1p priority tagging		
Network Protocols	IPv4/IPv6, TCP/UDP, RTP/RTCP, HTTP/HTTPS, DHCP, NTP, PPPoE, STUN		
Security	HTTPS, SIPS, 802.1x authentication, whitelist access control		
System Management	Supports SNMP, cloud management, OpenAPI, SSH remote CLI, scheduled reboot		
	Compatible platforms: Asterisk, Issabel, 3CX, FreeSWITCH, VOS, BroadSoft		

1.5 Hardware Features

	L301	L302	L304
Console Port	RS232(RJ45)		
Network Interface	2 * 10/100Mbps ports	2 * 1000Mbps ports	
Weight	1.2Kg	1.3Kg	1.4Kg
Dimensions	232mm* 152mm*45mm		
Max Power	12W		
Power Supply	12V 1A		
Operating Temperature	0°C~50°C		
Storage Temperature	-20°C~70°C		
Environmental Humidity	10%~90% non-condensing		

1.6 System Login and Initial Configuration

Default IP Address: 192.168.6.65

Username: admin

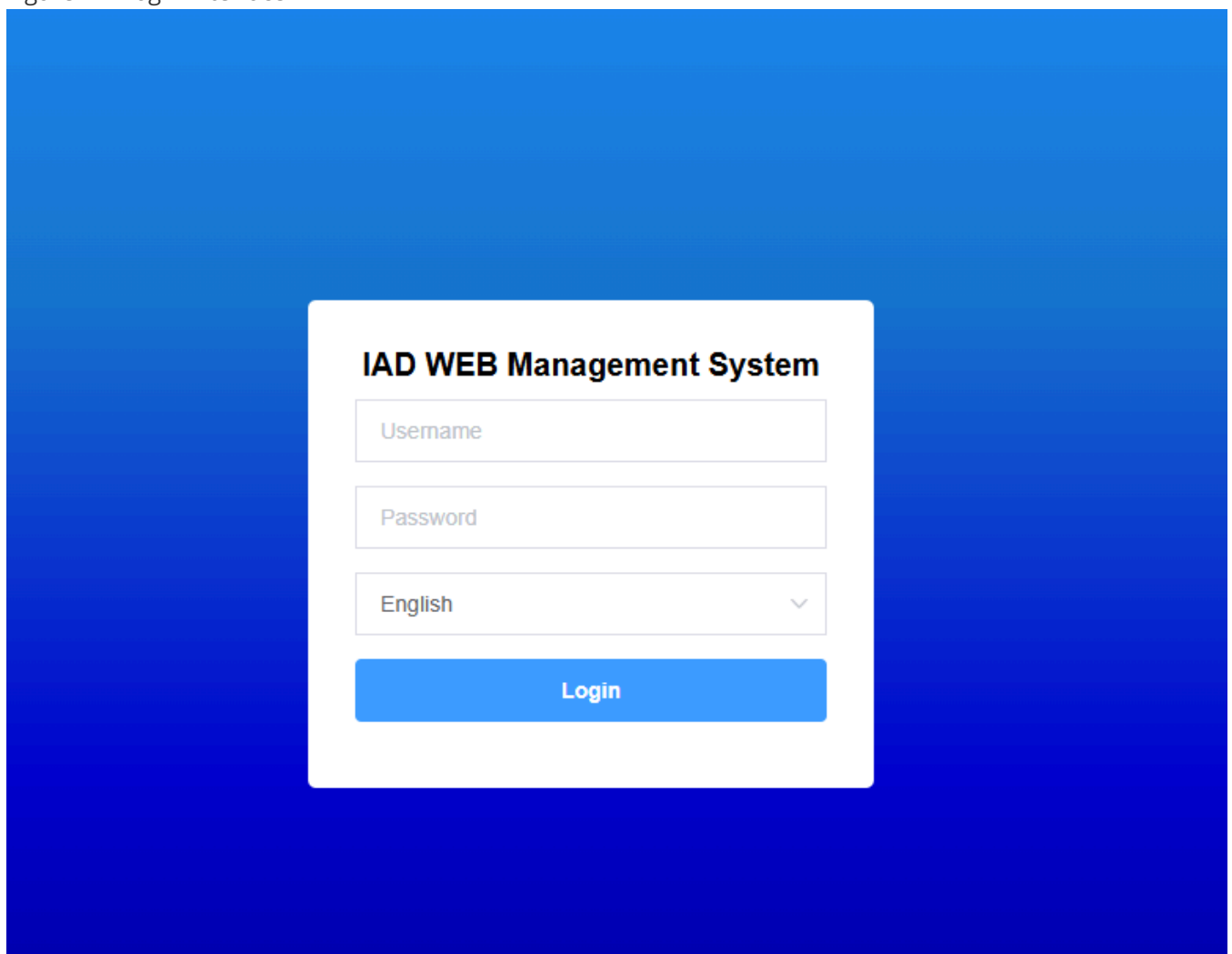
Password: admin

Connect the network cable to LAN1/LAN2, enter the default IP in the browser, and access the gateway for configuration.

Note: The default network mode of this product is bridge mode. Whether the network cable is connected to the WAN port or LAN port, the IP address is the same.

Open the browser, enter the default IP, and access the gateway login interface.

Figure 4-1 Login Interface



The default network mode is bridge mode, and the management page can be accessed from any interface (WAN/LAN).

2. Status

2.1 System Status

On the "System Status" page, product information, firmware information, system time, and resource usage are displayed.

Figure 2-1-1 System Status Display

System Information

Product Information

Product Name: OpenVox IAD Series

Product Model: DGW-L304

Serial Number: 88888888

Manufacturer: OpenVox

Manufacturer Website: www.openvoxtech.com

Firmware Information

Firmware Version: 2.2.8

Build Number: r0-5ba9490e

MAC Address: A0:98:05:02:D1:1D

System Time

Uptime: 0 Days 2 Hours 22 Minutes 40 Seconds

System Time: 2025/10/24 17:08:40

Resource Usage

2.2 Network Status

On the "Network Status" page, network status and VPN connection status are displayed.

Network configuration interface is as follows:

Network Status

WAN

Network Type:	Static IP
IP Address:	172.16.5.194
Subnet Mask:	255.255.255.0
Gateway:	172.16.5.1
DNS:	172.16.188.5
MAC Address:	a0:98:05:02:d1:1d

MGT

Network Status:	Disable
------------------------	---------

VPN

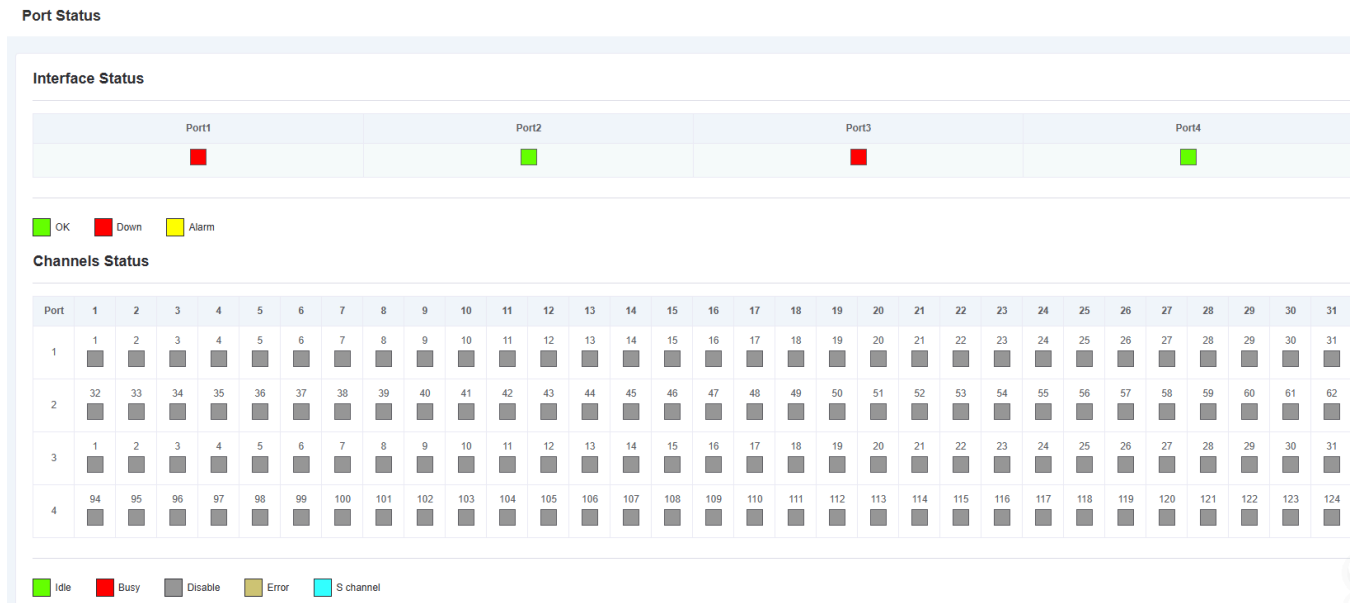
Connection State:	Disable
Connection Address:	
Connection Mask:	

2.3 Port Status

On the "Port Status" page, port status and channel status are displayed.

Figure 2-3-1 Port Status

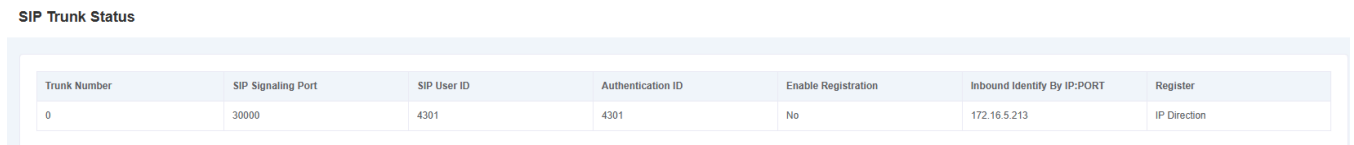
On the "Network Status" page, network status and VPN connection status are displayed.



2.4 SIP Trunk Status

On the SIP trunk status page, you can view the SIP trunk number, SIP signaling port, SIP user ID, authentication ID, registration status, IP direct sending table, and whether registered.

Figure 2-4-1 SIP Trunk Status Page



2.5 CDR

On the CDR page, users can configure CDR and query CDR

Figure 2-5-1 CDR

CDR

CDR Settings

Enable CDR: No Yes

Call Status:

Save Quantity:

CDR Query

Quantity:

Port:

Caller:

Callee:

Status:

Total 0 < 1 >

Incoming Trunk	Calling Number	Outgoing Trunk	Called Number	Call Status	Invoke Start Time	Call Start Time	End Call Time	Call Duration
----------------	----------------	----------------	---------------	-------------	-------------------	-----------------	---------------	---------------

Note: Local CDR will only be saved in memory and will be cleared by rebooting

Note: CDR is only saved in memory and will be cleared upon reboot.

Table 2-5-1 CDR Options

Option	Description
Enable CDR	This option selects whether to enable CDR
Call Status	Select the call status saved by CDR
Save Quantity	Set the number of CDR entries saved
Quantity	Select the number of CDR queries
Port	Select the port for CDR query
Caller	Filter CDR query items by caller number
Callee	Filter CDR query items by callee number

3. Network Configuration

3.1 Local Network

Figure 3-1-1 Local Network Interface

Local Network

Local Network MGT Settings Local DNS

WAN Settings

Enable IPv6 Address: No Yes

Network Type: Static IP

IP Address: 172.16.5.194

Subnet Mask: 255.255.255.0

Default Gateway: 172.16.5.1

Primary DNS: 172.16.188.5

Secondary DNS:

Manage Access: Both WAN And MGT Interfaces

Set OPT 60:

MTU: 1500

Table 3-1-1 WAN Settings Interface Parameter Description

Option	Description
Network Mode	Select device network mode
Network Type	Select network type: DHCP, Static IP, PPPoE
IP Address	Set the device's IP address
Subnet Mask	Set the device's subnet mask
Default Gateway	Set the device's default gateway
Primary DNS	Set the device's primary DNS

Option	Description
Gateway	Set the device's gateway
Remote DNS	Select whether to allow remote DNS
DNS	Set the device's DNS

Figure 3-1-3 VLAN Settings Interface

Table 3-1-3 VLAN Settings Interface Parameter Description

Option	Description
WAN Port Layer 2 QoS 802.1Q./VLAN Tag	Set WAN port tag
Layer 2 SIP Signaling QoS 802.1p Priority	Set SIP signaling priority
Layer 2 Voice QoS 802.1p Priority	Set voice priority
Management Port Layer 2 QoS 802.1Q./VLAN Tag	Set management port tag
Management Port Layer 2 QoS 802.1p Priority	Set management port priority

Figure 3-1-4 Local DNS Settings Interface

Figure 3-1-5 Add Local DNS Settings Interface

Table 3-1-4 Local DNS Interface Parameter Description

Option	Description
Domain Name	Set device domain name
Resolution IP	Set the IP to be resolved

3.2 Static Routes

On the "Static Routes" page, the network interface, destination IP address, subnet mask, gateway, hop count, and operations of static routes are displayed. Static routes can be added here. Click the Add button to add static routes.

Figure 3-2-1 Static Routes Interface

Network Interface	Destination IP Address	Subnet Mask	Via Gateway	Jump Point	Action
No Data Available					

Figure 3-2-2 Add Static Route Interface

Static Routing

Network Interface: WAN

Destination IP Address:

Subnet Mask:

Via Gateway:

Jump Point: 0

3.3 Firewall

On the "Firewall" page, the firewall rule name, protocol, source network domain, source IP, source port, destination network domain, destination IP, destination port, and rule action are displayed. Firewall rules can be added here to ensure device security. Click the Delete button to delete firewall rules, and click the Add button to add firewall rules.

Figure 3-3-1 Firewall Interface

Rule Name	Protocol	Source Network Domain	Source IP	Source Port	Destination Network Domain	Destination IP	Destination Port	Rule Action	Enable Rule	Action
Allow-Ping	ICMP	WAN						ACCEPT	Enabled	Edit Delete ↑ ↓
Allow-SSH	TCP	WAN					3505	ACCEPT	Disabled	Edit Delete ↑ ↓
Allow-Http	TCP	WAN					80	ACCEPT	Disabled	Edit Delete ↑ ↓
Allow-Https	TCP	WAN					443	ACCEPT	Disabled	Edit Delete ↑ ↓
Allow-SNMP	UDP	WAN					161	ACCEPT	Disabled	Edit Delete ↑ ↓
Allow-uPnP	TCP	WAN					5000	ACCEPT	Disabled	Edit Delete ↑ ↓

Figure 3-3-2 Add Firewall Rule Interface

The screenshot shows a web-based configuration interface for adding a firewall rule. The interface is titled 'Firewall' and has 'Back' and 'Save' buttons in the top right corner. The configuration fields are as follows:

- Rule Name:** An empty text input field.
- Protocol:** A dropdown menu with 'TCP' selected.
- Source Network Domain:** A dropdown menu with 'None' selected.
- Source IP:** An empty text input field.
- Source Port:** A text input field containing '1-65536'.
- Destination Network Domain:** A dropdown menu with 'None' selected.
- Destination IP:** An empty text input field.
- Destination Port:** A text input field containing '1-65536'.
- Rule Action:** A dropdown menu with 'ACCEPT' selected.
- Enable Rule:** A dropdown menu with 'Enabled' selected.
- ICMP Type:** A dropdown menu with 'Select' selected.

Table 3-3-1 Add Firewall Rule Parameter Description

Option	Description
Name	Firewall rule name
Protocol	Protocol restricted by the firewall rule
Source Network Domain	Source network domain of the firewall rule
Option	Description
Source IP	Source IP defined by the firewall rule, leave empty for all IPs
Source Port	Define source port, range is 1-65535
Destination Network Domain	Destination network domain of the firewall rule
Destination IP	Destination IP defined by the firewall rule, leave empty for all IPs
Destination Port	Define destination port, range is 1-65535
Rule Action	Define rule action, options are ACCEPT, REJECT, DROP

3.4 IP Alias

DTU-30X supports setting multiple IP addresses, which can be set in the IP Alias interface.

Figure 3-4-1 IP Alias Interface

The screenshot shows a web interface for configuring IP aliases. At the top, there is a header 'IP Alias' with 'Save' and 'Undo' buttons. Below the header, the interface is organized into two sections: 'IP Alias 1' and 'IP Alias 2'. Each section contains two input fields: 'IP Address' and 'Subnet Mask'.

3.5 VPN Settings

Figure 3-5-1 OpenVPN Settings Interface

The screenshot shows a web interface for configuring OpenVPN settings. At the top, there is a header 'VPN Settings' with 'Save' and 'Undo' buttons. Below the header, there are two tabs: 'Settings' (active) and 'Log'. The main configuration area includes:

- VPN Type:** A dropdown menu currently set to 'OPENVPN'.
- Account Authentication Name:** An empty text input field.
- Account Authentication Password:** An empty text input field.
- Certification Authentication Password:** An empty text input field.
- OpenVPN Configuration Content:** A text input field with a 'Choose File' button next to it.
- Connection State:** A status indicator showing 'Disconnected' in red text.

Table 3-5-1 VPN Settings Description

Option	Description
VPN Type	Can select to close VPN or use OpenVPN/SoftEther VPN
Account Authentication Name	Authentication name used by OpenVPN
Account Authentication Password	Authentication password used by OpenVPN
Cert Authentication Password	Cert authentication password
ovpn Configuration Content	Upload OpenVPN configuration file
Connection Status	Display VPN connection status

On the log page, you can select the number of log lines to display, then click the Query button. The log will be displayed in the "Log Result" box.

Figure 3-5-2 SoftEther VPN Settings Interface

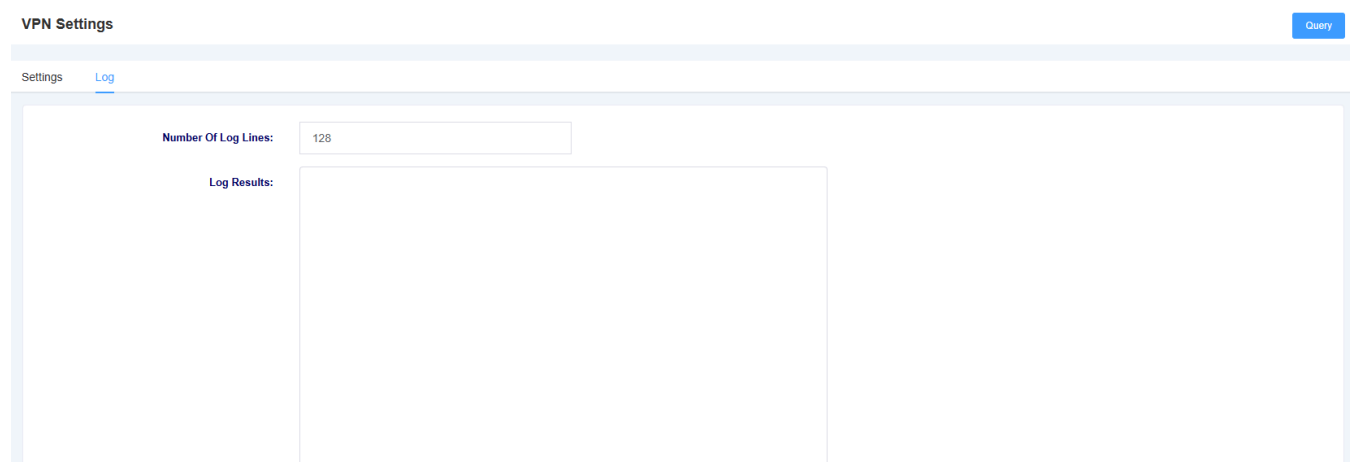
The screenshot displays the 'VPN Settings' configuration page. At the top right, there are 'Save' and 'Undo' buttons. Below the title bar, there are 'Settings' and 'Log' tabs. The main configuration area includes the following fields:

- VPN Type:** A dropdown menu currently showing 'SOFTETHERVPN'.
- Server Address:** An empty text input field with a red warning icon to its right.
- Server Port:** A text input field containing the value '443'.
- HUB:** An empty text input field.
- Account Authentication Name:** An empty text input field.
- Interface Type:** A dropdown menu showing 'Standard Password'.
- Account Authentication Password:** An empty text input field.
- Line Type:** A dropdown menu showing 'DHCP'.
- IP Address:** An empty text input field.
- Subnet Mask:** An empty text input field.
- Connection State:** An empty text input field.

Table 3-5-2 SoftEther VPN Settings Description

Option	Description
VPN Type	Can select to close VPN or use OpenVPN/SoftEther VPN
Server Address	Server address used by SoftEther VPN
Server Port	Server port used by SoftEther VPN
Hub	Hub name
Interface Type	Select standard password or signature certificate
Account Authentication Password	Enter password
Certificate Cert	Authentication file
Certificate Key	Certificate Key
Connection Type	Select DHCP or Static IP
IP Address	Configure IP
Subnet Mask	Configure subnet mask
Connection Status	Display VPN connection status

Figure 3-5-3 VPN Log Interface



4. Template

DTU-30X provides a convenient SIP registration method. Users can conveniently apply preset templates to SIP trunks. A total of four templates are available for setting.

4.1 SIP Settings

Figure 4-1-1 SIP Settings

The screenshot shows the 'SIP Settings' configuration page for 'Profile 1'. At the top right, there are 'Save' and 'Undo' buttons. Below the profile name, there are navigation tabs: 'SIP Settings', 'VOIP Settings', 'IP->Tel Route', 'Tel->IP Route', and 'IP->IP Route'. The 'SIP Settings' tab is active. The main content area is titled 'Basic Settings' and contains the following fields:

- SIP Primary Server: 172.16.5.213
- SIP Primary Server Port: 5060
- SIP Backup Server: (empty)
- SIP Backup Server Port: 5060
- SIP Address Selection: Default (dropdown)
- DNS Mode: Auto Identification (dropdown)
- Outgoing Proxy Server: (empty)
- Backup Outgoing Proxy Server: (empty)
- From Domain: (empty)

At the bottom, there is a 'Stun' section with radio buttons for 'No' (selected) and 'Yes'.

Table 4-1-1 SIP Settings Parameter Description

Option	Description
SIP Primary Server	Set SIP primary server
SIP Primary Server Port	Set SIP primary server port
SIP Backup Server	Set SIP backup server
Option	Description
SIP Backup Server Port	Set SIP backup server port
SIP Address Selection	Select which network port SIP registers on
DNS Mode	Set DNS mode, can select automatic or use DNSSRV
Outbound Proxy Server	Set outbound proxy server, the gateway will send signaling to this external proxy instead of directly to the peer.
From Domain	Set the domain name used to authenticate the peer
STUN	Select whether to enable STUN service

Option	Description
Compatibility Mode	Select whether to enable compatibility mode
Figure 4-1-2 SIP Settings	

Registration Settings

SIP Transmission Mode:

Authentication Domain:

Registration Validity Period (s):

Registration Failure Retry Interval (s):

Registration Failure Retry Times:

Heartbeat Settings

Disable Quality Verification: No Yes

SIP Heartbeat Sending Frequency (s):

SIP Heartbeat Timeout (s):

RTP Encryption

RTP Encryption Mode:

Table 4-1-2 SIP Settings Parameter Description

Option	Description
SIP Transport Method	Set SIP transport method, can select UDP, TCP, and TLS
Authentication Domain	Set SIP registration authentication domain
Option	Description
Registration Validity Period	Set registration validity period, default value is 3600 seconds
Registration Failure Retry Interval	Set registration failure retry interval, default value is 30 seconds
Registration Failure Retry Times	Set registration failure retry times, default value is 10 times
Qualify Verification	Whether to enable qualify verification
SIP Heartbeat Send Frequency	Set SIP heartbeat packet send frequency
SIP Heartbeat Timeout	Set SIP heartbeat packet timeout
RTP Encryption Mode	Whether to enable RTP encryption

Figure 4-1-3 SIP Settings

Certificate Settings

Version:

URI Pattern:

Select The PEM Certificate:

Select The CA Certificate Chain: No Yes

UAC Verifies Paired-end Certificate: No Yes

UAS Verifies Paired-end Certificate: No Yes

Option	Description
Version	Select the certificate version, the device supports different versions of TLS, SSL, SS certificates
URI Mode	Select URI mode, supports SIP and SIPS
Select Device PEM Certificate	Select device PEM certificate
Select CA Certificate Chain	Select whether to enable CA certificate chain
Option	Description
UAC Verify Peer Certificate	As the calling party, select UAC to use the phone as the refresher. Or select UAS to use the called party or proxy server as the refresher.
UAS Verify Peer Certificate	As the called party, select UAC to use the called party or proxy server as the refresher, or select UAS to use the phone as the refresher.

4.2 VOIP Settings

On this interface, users can set VOIP related parameters.

Figure 4-2-1 VOIP Settings

SIP Settings **VOIP Settings** IP->Tel Route Tel->IP Route IP->IP Route

Call Settings

RTP Keepalive Transmission Interval (s):

Call RTP Timeout Duration (s):

Call Hold RTP Timeout (s):

DTMF Settings

DTMF Mode:

Table 4-2-1 VOIP Settings Parameter Description

Option	Description
Allow Call Transfer	Select whether to enable call transfer
RTP Keepalive Send Interval	Set RTP keepalive send interval
Call RTP Timeout	Set call RTP timeout
Call Hold RTP Timeout	Set call hold RTP timeout
DTMF Mode	Set DTMF mode, can select RFC4733, inband, info, auto, and auto_info
Figure 4-2-2 VOIP Settings	

Encoding Settings

Duration When Using Encoding: No Yes

Voice Frames Per TX:

Encoding Priority1:

Encoding Priority2:

Encoding Priority3:

Encoding Priority4:

Encoding Priority5:

Encoding Priority6:

Encoding Priority7:

Encoding Priority8:

Encoding Priority9:

Encoding Priority10:

Table 4-2-2 VOIP Settings Parameter Description

Option	Description
Use Codec Packing Time	Select whether to use codec packing time for more efficient use of bandwidth and resources in transmission, storage, and processing
Codec Priority	Set codec priority
Enable UDPTL	Select whether to enable UDPTL
UDPTL Error Correction	Select UDPTL error correction method

4.3 IP->Tel Routing

Related routing can be set on this page.

Figure 4-3-1 IP->TEL Routing

SIP Settings VOIP Settings IP->Tel Route Tel->IP Route IP->IP Route

Routing Failed Call Destination Type:

Routing Failed Call Destination:

Call Source Type	Call Source	Call Destination Type	Call Destination	Routing Action	Calling Number Prefix	Callee Number Prefix	Delete Caller Prefix Len	Delete Caller Suffix Len	Add Caller Prefix	Add Caller Suffix	Delete Callee Prefix Len	Delete Callee Suffix Len	Add Callee Prefix	Add Callee Suffix	Action
No Data Available															

Table 4-3-1 IP->TEL Routing Parameter Description

Option	Description
Failure Backup Line	Send to this destination when call fails
Call Source Type	Call source device type
Call Source	Call source device
Call Destination Type	Destination type
Call Destination	Call destination
Routing Action	Reject or permit
Caller Number Prefix	Set caller number prefix type
Callee Number Prefix	Set callee number prefix type
Delete Caller Prefix	Delete caller number prefix
Delete Callee Prefix	Delete callee number prefix
Add Caller Prefix	Add caller number prefix
Add Caller Suffix	Add caller number suffix
Delete Callee Prefix	Delete callee number prefix
Delete Callee Suffix	Delete callee number suffix
Add Callee Prefix	Add callee number prefix
Add Callee Suffix	Add callee number suffix

4.4 TEL->IP Routing

Related routing can be set on this page.

Figure 4-4-1 TEL->IP Routing

SIP Settings VOIP Settings IP->Tel Route **Tel->IP Route** IP->IP Route

Routing Failed Call Destination Type:

Routing Failed Call Destination:

Call Source Type	Call Source	Call Destination Type	Call Destination	Routing Action	Calling Number Prefix	Callee Number Prefix	Delete Caller Prefix Len	Delete Caller Suffix Len	Add Caller Prefix	Add Caller Suffix	Delete Callee Prefix Len	Delete Callee Suffix Len	Add Callee Prefix	Add Callee Suffix	Action
SS7	1	SIP	0 (4301)	Accept	Ignore	Any	0	0			0	0			<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="↑"/> <input type="button" value="↓"/>

Table 4-4-1 TEL->IP Routing Parameter Description

Option	Description
Failure Backup Line	Send to this destination when call fails
Call Source Type	Call source device type
Call Source	Call source device
Call Destination Type	Destination type
Call Destination	Call destination
Routing Action	Reject or permit
Caller Number Prefix	Set caller number prefix type
Callee Number Prefix	Set callee number prefix type
Delete Caller Prefix	Delete caller number prefix
Delete Callee Prefix	Delete callee number prefix
Add Caller Prefix	Add caller number prefix
Add Caller Suffix	Add caller number suffix
Delete Callee Prefix	Delete callee number prefix
Delete Callee Suffix	Delete callee number suffix
Add Callee Prefix	Add callee number prefix
Add Callee Suffix	Add callee number suffix

4.5 IP->IP Routing

Related routing can be set on this page.

Figure 4-5-1 IP->IP Routing

SIP Settings VOIP Settings IP->Tel Route Tel->IP Route **IP->IP Route**

Routing Failed Call Destination Type:

Routing Failed Call Destination:

Call Source Type	Call Source	Call Destination Type	Call Destination	Routing Action	Calling Number Prefix	Callee Number Prefix	Delete Caller Prefix Len	Delete Caller Suffix Len	Add Caller Prefix	Add Caller Suffix	Delete Callee Prefix Len	Delete Callee Suffix Len	Add Callee Prefix	Add Callee Suffix	Action
No Data Available															

Table 4-5-1 IP->IP Routing Parameter Description

Option	Description
Failure Backup Line	Send to this destination when call fails
Call Source Type	Call source device type
Call Source	Call source device
Call Destination Type	Destination type
Call Destination	Call destination
Routing Action	Reject or permit
Caller Number Prefix	Set caller number prefix type
Callee Number Prefix	Set callee number prefix type
Delete Caller Prefix	Delete caller number prefix
Delete Callee Prefix	Delete callee number prefix
Add Caller Prefix	Add caller number prefix
Add Caller Suffix	Add caller number suffix
Delete Callee Prefix	Delete callee number prefix
Delete Callee Suffix	Delete callee number suffix
Add Callee Prefix	Add callee number prefix
Add Callee Suffix	Add callee number suffix

5. Trunk Settings

On this page, trunk types can be configured.

5.1 SIP Trunk

Figure 5-1-1 Add SIP Trunk Page

Table 5-1-1 SIP Trunk Page Parameter Description

Option	Description
Trunk Number	Custom trunk number
Template	Select the template setting to use
Enable Registration	Select whether to enable registration settings
SIP User ID	Trunk name setting
FROM Force Account	Set FROM force account
Authentication ID	Authentication ID corresponding to this SIP user ID
Password	Password corresponding to the authentication ID
IP Direct Sending Table	Set caller display name

5.2 Port Settings

Figure 5-2-1 Port Settings

Port Settings
Save

General

Line Region: China

Interface Type: E1 T1

Port

Port	Timing Source	PCM Encoding	Framing	Coding	Line Build-out	CRC4	Signaling	D Channel
1	Remote	Default	CCS	HDB3	0 db (CSU) / 0-133 feet (DSX-1)	No	SS7	0
2	Remote	Default	CCS	HDB3	0 db (CSU) / 0-133 feet (DSX-1)	No	SS7	0
3	Remote	Default	CCS	HDB3	0 db (CSU) / 0-133 feet (DSX-1)	No	SS7	0
4	Remote	Default	CCS	HDB3	0 db (CSU) / 0-133 feet (DSX-1)	No	SS7	0

Table 5-2-1 Call Settings Parameter Description

Option	Description
Line Area	Set line area
Interface Type	E1 or T1 type
Clock Source	Select clock source
PCM Coding	Select coding format
Frame Structure	Frame structure type
Line Coding	Select line coding
Line Compensation	External line represents the cable length from this gateway port to the next device.
CRC4	Set verification
Signaling	Set signaling type
D Channel	Set D channel position

5.3 PRI Settings

Figure 5-3-1 PRI Settings

PRI Settings

Port	Enabled	Signaling Type	Switch Type	Group	Profiles	Echo Cancel (ms)	RX Gain (dB)	TX Gain (dB)	Action
1	No	User Side	EuroISDN	4	1	Disabled	0.0	0.0	Edit
2	No	User Side	EuroISDN	4	1	Disabled	0.0	0.0	Edit
3	No	User Side	EuroISDN	4	1	Disabled	0.0	0.0	Edit
4	No	User Side	EuroISDN	4	1	Disabled	0.0	0.0	Edit

PRI Settings

[Back](#) [Save](#)

Port:

Enabled: No Yes

Signaling Type:

Switch Type:

Group:

Profiles:

Echo Cancel (ms):

RX Gain (dB):

TX Gain (dB):

Network Specific Facility(NSF):

Service Message Support: No Yes

ISDN Facility Enable: No Yes

Dialing Plan:

Local Dialing Plan:

PRI Settings

Back Save

never
 No Yes
 No Yes
 No
 No Yes
 No Yes
 No Yes
 Text
 Text

 Update
 Inband
 Physical
 Retain
 Retain
 No

Table 5-3-1 Call Settings Parameter Description

Option	Description
Port	Select port
Enable	Whether to enable
Signaling Type	Set signaling type
Switch Type	Digital signaling switch type
Group	Set group number
Template	Select the template to use
Echo Cancellation	Echo cancellation length
RX Gain	Receiving audio energy gain
TX Gain	Transmitting audio energy gain
ATT Carrier	ATT carrier network special parameters
Enable Message Service	Enable message service support

Option	Description
Dialing Plan	Dialing plan
Local Dialing Plan	Local dialing plan
Peer Dialing Plan	Peer dialing plan
Number Prefix International	Number prefix International
Number Prefix National	Number prefix National
Number Prefix Local	Number prefix Local
Number Prefix Private	Number prefix Private
Number Prefix Unknown	Number prefix Unknown
Unused B Channel Restart Cycle	Unused B channel restart cycle
SETUP ACK Receive Inband Audio	Receive inband audio at SETUP ACK (Q.SIG must be enabled if overlap is enabled)
PROCEEDING Receive Inband Audio	Receive inband audio at PROCEEDING
Overlap Dialing	Overlap dialing
Send ISDN Request	Send ISDN Malicious Caller ID request on SPAN
Auto Restart Unavailable Channels	Whether to automatically restart unavailable channels
Hide Caller Number	Whether to hide caller number
Hide Caller Name	Whether to hide caller name
Send Display	Send display Note: only NET side supports, CPE and Q.SIG do not support
Receive Display	Receive display Note: only NET side supports, CPE and Q.SIG do not support
Send Information	Whether to send connect number information when sending connect
Busy and Congestion Indication Method	PRI busy and congestion indication method
Q.SIG Channel Mapping Method	Set Q.SIG channel mapping method Note: T1 forces physical
Q.SIG Calling Signaling Link	Set Q.SIG calling signaling link
Q.SIG Responding Signaling Link	Set Q.SIG responding signaling link
NET Side Send Datetime to CPE Side	Set NET side send datetime to CPE side

5.4 R2 Settings

Figure 5-4-1 R2 Settings

R2 Settings

Port	Enabled	Variant	Group	Profiles	Echo Cancel (ms)	RX Gain (dB)	TX Gain (dB)	Action
1	No	China	4	1	Disabled	0.0	0.0	Edit
2	No	China	4	1	Disabled	0.0	0.0	Edit
3	No	China	4	1	Disabled	0.0	0.0	Edit
4	No	China	4	1	Disabled	0.0	0.0	Edit

R2 Settings [Back](#) [Save](#)

Port:

Enabled: No Yes

Variant:

Group:

Profiles:

Echo Cancel (ms):

RX Gain (dB):

TX Gain (dB):

Get ANI First: No Yes

Max ANI:

Max DNIS:

Category:

MF Timeout (ms):

Metering Pulse Timeout (ms):

Parameter	Description
Port	Select port
Enable	Whether to enable port
Protocol Type	Select protocol type
Group	Set group
Template	Select the template to use
Echo Cancellation	Whether to enable echo cancellation
RX Gain	Set receive gain
TX Gain	Set transmit gain
Get ANI	Get ANI before obtaining DNIS
Max ANI Requested	Maximum ANI digits requested
Max DNIS Requested	Maximum DNIS digits requested

Parameter	Description
Incoming Subscription	Incoming subscription category
MF Timeout	MF timeout
Pulse Timeout	Pulse timeout
Skip Request Caller Category and ANI	Skip request caller category and ANI
Support Double Answer	Whether to support double answer

5.5 SS7 Settings

Figure 5-5-1 SS7 Settings

SS7 Settings Save

Linkset Settings

Link Set	Profiles	Variant	OPC	DPC	Enabled ST	Use Connect	Hunting Policy	Protocol Type	Action
1	1	14Bit	0x6	0x5	No	ACM/ANM	Linear from low to	ISUP	Edit
2	1	14Bit	0x6	0x5	No	ACM/ANM	Linear from low to	ISUP	Edit
3	1	14Bit	0x6	0x5	No	ACM/ANM	Even numbers fro	ISUP	Edit
4	1	14Bit	0x6	0x5	No	ACM/ANM	Even numbers fro	ISUP	Edit

Link Settings

Port	Enabled	Link Set	Signaling SChannel	Voice Channel	First CIC	Echo Cancel	Echo Cancel Train	Echo Cancel Taps	RX Gain (dB)	TX Gain (dB)	Interface Type
1	Yes	1	16	1-15,17-31	1	allways	300	128	0.0	0.0	E1
2	Yes	1	0	1-31	32	allways	300	128	0.0	0.0	E1
3	Yes	1	0	1-31	63	allways	300	128	0.0	0.0	E1
4	Yes	1	0	1-31	94	allways	300	128	0.0	0.0	E1

Table 5-5-1 SS7 Parameter Description

Parameter	Description
Enable	Whether to enable
Link Group	Select link group
Signaling Channel	Signaling channel
Voice Channel	Audio channel
Starting Circuit Identification Code	CIC starting position
Echo Cancellation	Echo cancellation switch
Echo Cancellation Training	Echo training period
Echo Cancellation Taps	Echo cancellation TAPS(ms=taps/8)
RX Gain	Receiving audio energy gain

Parameter	Description
TX Gain	Transmitting audio energy gain

6. Advanced Configuration

6.1 Fax Parameters

On this page, fax-related parameters can be configured.

Figure 6-1-1 Fax Parameters

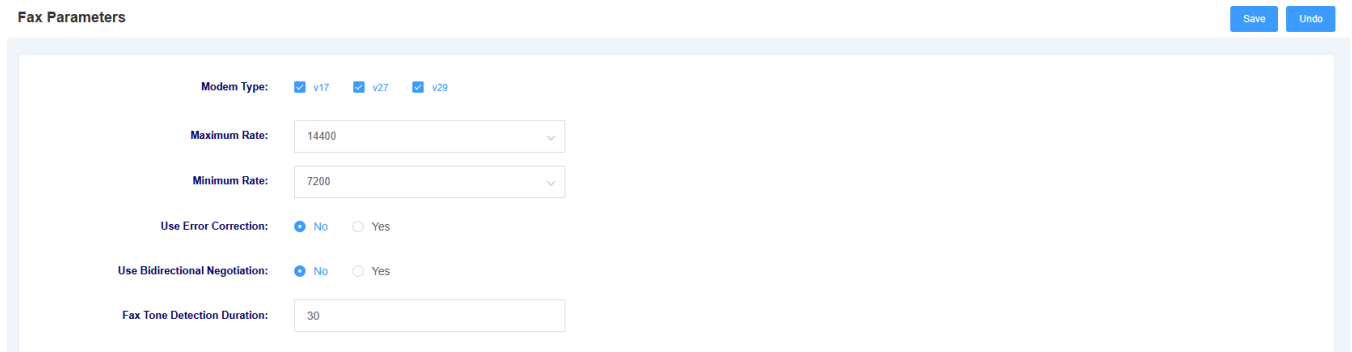


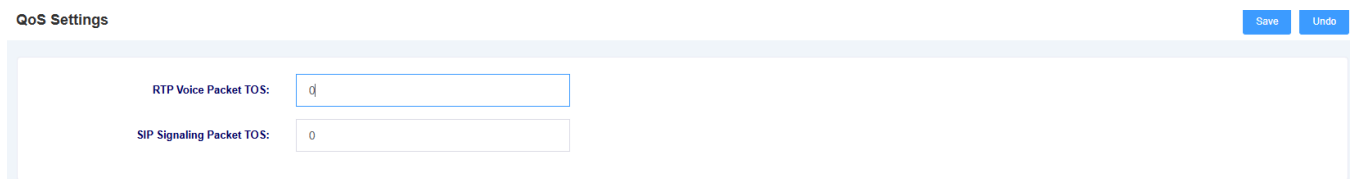
Table 6-1-1 Network Settings Description

Option	Description
Modem Type	Set supported modem types
Max Rate	Select the maximum rate supported by fax
Min Rate	Select the minimum rate supported by fax
Error Verification	Select whether to enable error verification
Bidirectional Negotiation	Select whether to enable bidirectional negotiation
Fax Tone Detection Duration	Set fax tone detection duration

6.2 QoS Settings

On this interface, RTP voice packet TOS and SIP signaling packet TOS can be set.

Figure 6-2-1 QoS Settings Interface



6.3 E1/T1 Settings

On this interface, digital line related parameters can be set, such as DTMF and jitter buffer.

Figure 6-3-1 E1/T1 Settings Interface

E1/T1 Settings

General

Line Region:

Audio Language:

Indication of Busy / Congestion:

Call In Waiting Time (s):

DTMF

DTMF To Total Energy:

DTMF Gsize:

DTMF Threshold:

Table 6-3-1 E1/T1 Parameter Description

Option	Description
Line Area	Select the area where the line is located
Audio Language	Select the language for voice prompts
Busy and Congestion Indication Method	Method to generate BUSY and CONGESTION notifications
Total Energy Ratio Coefficient	Adjust energy ratio coefficient
Sampling Points per Detection Segment	Set sampling points
Energy Threshold	Set energy threshold

Figure 6-3-2 E1/T1 Settings Interface

JitterBuffer

Enable Jitter Buffer: No Yes

Jitter Max Buffer (ms):

Jitter Buffer Sync Threshold (ms):

Jitter Buffer Method :

MFCR2

Save Logs: No Yes

Logs Level:

Table 6-3-2 E1/T1 Settings Parameter Description

Option	Description
Jitter Buffer	Select whether to enable jitter buffer
Jitter Buffer Method	Select jitter buffer method
Jitter Sync Timestamp	Set jitter sync timestamp
Jitter Max Buffer	Set jitter max buffer
Save Log	Whether to save log
Log Level	Set log level

6.4 VOIP Settings

On this page, VoIP-related settings can be made, such as call settings and session settings.

Figure 6-4-1 VoIP Settings

VOIP Settings

Basic Settings

Listening Mode:

SIP Start Port:

RTP Start Port:

Unregister Upon Reboot: No Yes

Stun: No Yes

Stun Server Address:

Minimum DTMF Duration:

Table 6-4-1 VoIP Settings Parameter Description

Option	Description
Listening Mode	Select listening mode, can select multi-port and single-port
SIP Starting Port	Set SIP starting port
RTP Starting Port	Set RTP starting port
Unregister on Restart	Select whether to unregister on restart
STUN	Select whether to enable STUN
STUN Server Address	Set STUN server address
Min DTMF Duration	Set minimum DTMF duration

Figure 6-4-2 VoIP Settings

Call Settings

T1 Timeout (ms):

T2 Timeout (ms):

Incoming Call Wait Timeout (s):

Outgoing Call Wait Timeout (s):

Maximum Call Time Limit (ms):

Outgoing Caller ID Priority:

User Agent:

Do Not Escape The "#" Number: No Yes

Enable Early Media: No Yes

Table 6-4-2 VoIP Settings Parameter Description

Option	Description
T1 Timeout	Set T1 timeout time
T2 Timeout	Set T2 timeout time
Incoming Wait Timeout	Set incoming wait timeout time
Outgoing Wait Timeout	Set outgoing wait timeout time
Call Max Duration	Set call maximum duration, call will be hung up after exceeding
Caller Number Display Priority	Select caller number priority from FROM field or P-Asserted-Identity field
User Agent	Set User Agent
Do Not Escape "#"	Whether not to escape #

Figure 6-4-3 VoIP Settings

Session Settings

Session Timer Mode:	Yes
Min-SE (ms):	90
Session Timeout (ms):	1800
G723 Rate:	6.3kbps Encoding Rate
iLBC Frame Size:	30ms

Table 6-4-3 VoIP Settings Parameter Description

Option	Description
Session Timer Mode	Select session timer mode
Min-SE	Set minimum session timeout duration
Session Timeout	Set session timeout time
G723 Rate	Set G723 rate
iLBC Frame Duration	Set iLBC frame duration

6.5 Security Settings

On this page, certificates can be uploaded.

Figure 6-5-1 Security Settings Interface

Security Settings Save Undo

Certificate 1:	<input type="text"/>
Certificate 2:	<input type="text"/>
Certificate 3:	<input type="text"/>
Certificate 4:	<input type="text"/>
CA Certificate Chain:	<input type="text"/>

7 Maintenance

7.1 Auto Restart

On this page, the auto restart function can be set, and the device can restart according to the set time.

Figure 7-1-1 Restart Page

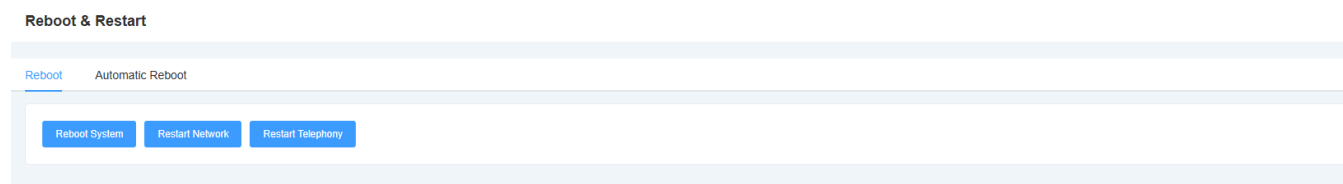


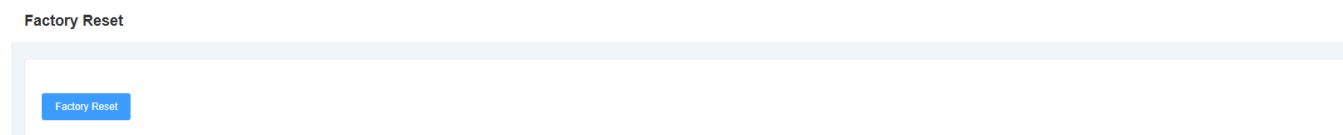
Figure 7-2-1 Auto Restart Page



7.2 Factory Reset

After clicking the factory reset button, the device will automatically restart and restore factory settings.

Figure 7-2-1 Factory Reset Interface



7.3 Auto Deployment

DTU-30X configuration file and upgrade file function can be set on this page.

Figure 7-3-1 Auto Deployment Interface

Auto Provision

Save
Run Provision
Undo

Auto Provision:

Auto Provision Hour:

Auto Provision Week:

Auto Provision Scope:

Upgrade Method:

Disable DHCP Option66: No Yes

Firmware Upgrade Address:

Firmware File Prefix:

Firmware File Suffix:

Configuration Upgrade Address:

Configuration File Prefix:

Configuration File Suffix:

Configuration File Name:

Uploading A Configuration File

Upload Configuration:

Restore

Download The Configuration File

Download Configuration: Download

Table 7-3-1 Auto Deployment Parameter Description

Option	Description
Auto Deployment	Set auto deployment mechanism, can select auto deployment after each power-on or deploy at set time intervals
Auto Deployment Hour	Set at what time to deploy
Auto Deployment Week	Set on which day of the week to deploy
Auto Deployment Scope	Select the scope of auto deployment, can select configuration file and upgrade firmware
Upgrade Method	Select auto deployment upgrade method, supports TFTP, HTTP, HTTPS
Disable DHCP Option 66	Select whether to enable DHCP option 66 to obtain files
Option	Description

Option	Description
Firmware Upgrade Address	Set firmware upgrade path
Firmware File Prefix	Set firmware file prefix
Firmware File Suffix	Set firmware file suffix
Configuration Upgrade Address	Set configuration upgrade path
Configuration File Prefix	Set configuration file prefix
Configuration File Suffix	Set configuration file suffix
Upload Configuration	Upload configuration file
Download Configuration	Download device current configuration file

The file name needs to be modified according to the rules. The main control firmware file name rule is (pre)(firmware model).img(post), the interface board firmware file name rule is (pre)ixu(mac).img(post), the configuration file name rule is (pre)cfg(mac)(post), pre is prefix, post is suffix, prefix and suffix can be left blank.

7.4 Firmware Upgrade

On this page, firmware upgrade can be performed. Select the corresponding firmware type and upload the file to upgrade. You can choose whether to retain the system configuration. If the system configuration is not retained, the device will clear the system configuration after upgrading.

Figure 7-4-1 Firmware Upgrade

Firmware Upgrade

The screenshot shows the 'Firmware Upgrade' interface. It is divided into two main sections by a horizontal line. The top section is for upgrading from a file. It includes a 'Keep System Configuration' label with radio buttons for 'No' and 'Yes' (selected). Below this is a 'Choose File' label with a text input field containing a folder icon and the text 'Choose File'. A blue button labeled 'Upgrade from File' is positioned below the input field. The bottom section is for upgrading from a server. It also includes a 'Keep System Configuration' label with radio buttons for 'No' and 'Yes' (selected). Below this is an 'Upgrade Server' label with a text input field. A blue button labeled 'Upgrade from Server' is positioned below the input field.

7.5 Time Settings

On this page, the device time settings can be made. Users can set the time zone and set the NTP server address to automatically synchronize time.

Figure 7-5-1 Time Settings

Time Settings Save Undo

Time Zone: UTC+8:00 (Beijing, Taipei, Kuala Lumpur, Irkutsk) ▾

System Time: 2025/10/24 17:41:25

Disable NTP Time Synchronization: No Yes

NTP Server Address1: pool.ntp.org

NTP Server Address2: time.nist.gov

NTP Server Address3:

Table 7-5-1 Time Settings Parameter Description

Option	Description
Time Zone	Set device time zone
System Time	Display system time
Enable NTP Time Sync	Select whether to enable NTP time sync
NTP Server Address	Set NTP server address

7.6 User Management

DTU-30X supports different user roles for login, with different permissions. On the user management page, passwords can be changed for different roles, SSH function can be switched on and off, and HTTP settings can be made.

Figure 7-6-1 User Management

User Management Save

WEB Account CLI Account SSH Settings HTTP Settings

Viewer

New Password:

Confirm New Password:

User

New Password:

Confirm New Password:

Admin

New Password:

Confirm New Password:

User Management Save

WEB Account CLI Account SSH Settings HTTP Settings

New Password:

Confirm New Password:

User Management Save Undo

WEB Account [CLI Account](#) [SSH Settings](#) [HTTP Settings](#)

Disable SSH Service: No Yes

SSH Service Port:

User Management Save Undo

WEB Account [CLI Account](#) [SSH Settings](#) [HTTP Settings](#)

HTTP Web Port:

HTTPS Web Port:

Web Page Access Mode: HTTP HTTPS Disabled

HTTPS Service Certificate:

Web Session Timeout (s):

7.7 Network Capture

DTU-30X can facilitate network problem location. Users can define the capture interface on this interface and select protocol type, address, and port.

Figure 7-7-1 Network Capture

Network Capture Start Stop

Interface Name:

Filter Protocol Type:

Filter Address:

Filter Port:

Packet Capture State:

7.8 Signaling Capture

DTU-30X can perform signaling capture.

Figure 7-8-1 Signaling Capture

Signal Packet Capture Start Stop

Signaling Type:

Packet Capture State:

7.9 Log Management

On the log management interface, the log server address and port can be set, and the kernel log level can be selected to facilitate viewing device logs for technical analysis.

Figure 7-9-1 Log Management

The screenshot shows a web interface titled "Log Management". At the top right, there are "Save" and "Undo" buttons. Below the title, there are two tabs: "System Log" and "Support Log". The "Support Log" tab is selected. The main content area contains two input fields: "Log Server Address:" followed by an empty text box, and "Log Server Port:" followed by a text box containing the number "0".

Figure 7-9-2 Log Support Interface

The screenshot shows a web interface titled "Log Management". At the top right, there is a "Save" button. Below the title, there are two tabs: "System Log" and "Support Log". The "Support Log" tab is selected. The main content area contains three dropdown menus: "Message Level:" with "Off" selected, "PRI Log:" with "Off" selected, and "Automatic Refresh Rate:" with "Off" selected. At the bottom left, there are three buttons: "Manual Refresh", "Clear", and "Download".

Syslog is often called system log or system record, and is a standard used to transfer record information in Internet Protocol (TCP/IP) networks. This term is often used to refer to the actual syslog protocol, or applications or databases that send syslog messages. The syslog protocol is a client-server protocol: the syslog sender will send a small text message (less than 1024 bytes) to the syslog receiver. The receiver is usually named "syslogd", "syslog daemon", or syslog server. System log messages can be transferred using UDP protocol and/or TCP protocol.

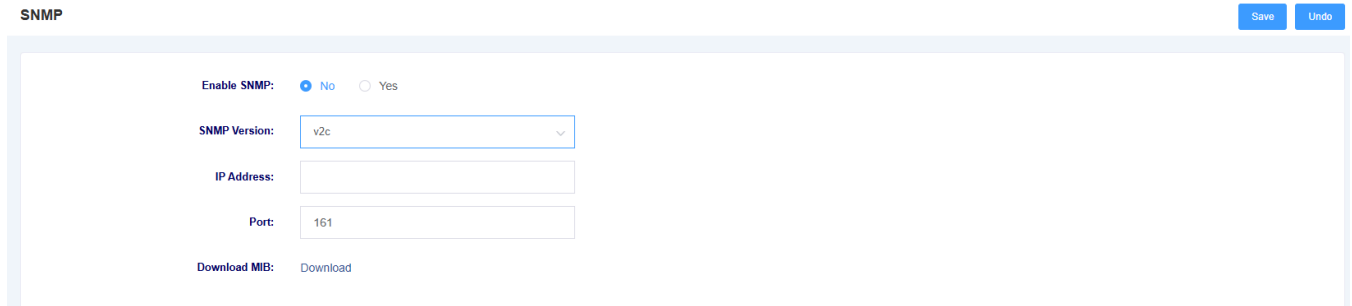
Syslog Level Introduction:

- EMERG Failure
- ALERT Warning
- CRIT Needs to be resolved promptly
- ERROR Error conditions that prevent tools or certain subsystems from achieving some functionality
- WARNING Early warning information
- NOTICE Important common conditions
- INFO Information
- DEBUG Other information that does not contain function conditions or problems

7.10 SNMP

On this page, SNMP service related information can be set. DTU-30X supports SNMPv1, v2c.

Figure 7-10-1 SNMP



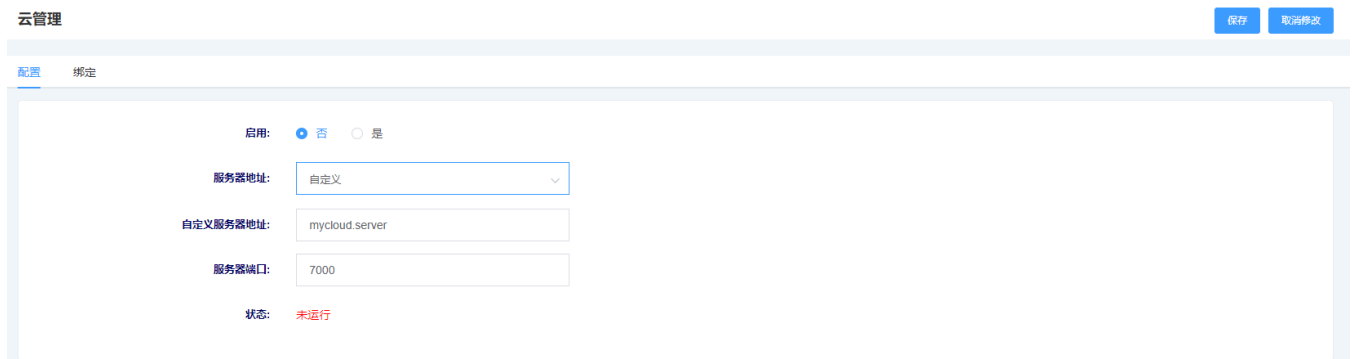
The screenshot shows the SNMP configuration page. At the top left is the title "SNMP" and at the top right are "Save" and "Undo" buttons. The main content area contains the following settings:

- Enable SNMP:** Radio buttons for "No" (selected) and "Yes".
- SNMP Version:** A dropdown menu currently set to "v2c".
- IP Address:** An empty text input field.
- Port:** A text input field containing "161".
- Download MIB:** A "Download" button.

7.11 Cloud Management

On this page, cloud management related information can be set. DTU-30X supports OpenVox cloud management function. After entering the server address, port, and binding code, the device can be managed on the cloud management platform.

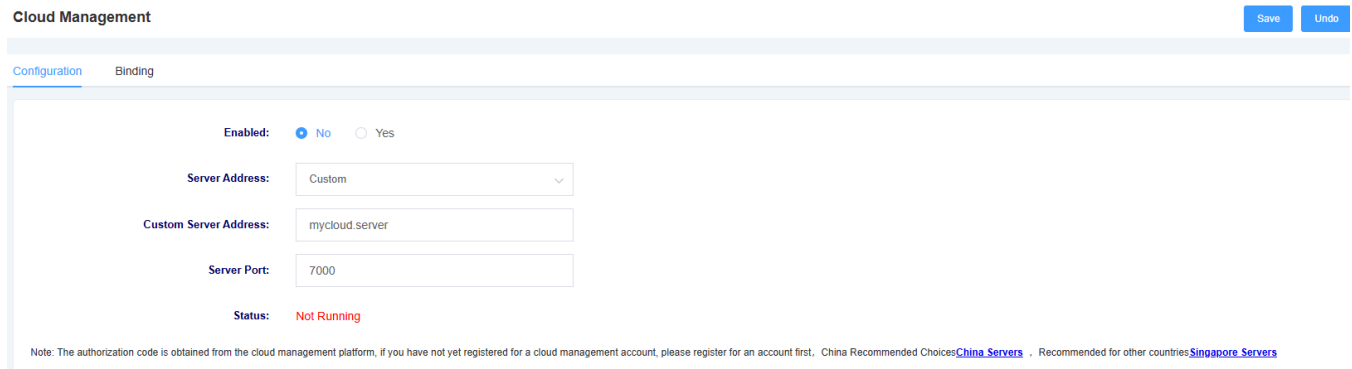
Figure 7-11-1 Cloud Management Settings



The screenshot shows the Cloud Management Settings page. At the top left is the title "云管理" and at the top right are "保存" and "取消修改" buttons. Below the title are tabs for "配置" and "绑定". The main content area contains the following settings:

- 启用:** Radio buttons for "否" (selected) and "是".
- 服务器地址:** A dropdown menu currently set to "自定义".
- 自定义服务器地址:** A text input field containing "mycloud.server".
- 服务器端口:** A text input field containing "7000".
- 状态:** A status indicator showing "未运行" in red text.

Figure 7-11-2 Cloud Management Binding



The screenshot shows the Cloud Management Binding page. At the top left is the title "Cloud Management" and at the top right are "Save" and "Undo" buttons. Below the title are tabs for "Configuration" and "Binding". The main content area contains the following settings:

- Enabled:** Radio buttons for "No" (selected) and "Yes".
- Server Address:** A dropdown menu currently set to "Custom".
- Custom Server Address:** A text input field containing "mycloud.server".
- Server Port:** A text input field containing "7000".
- Status:** A status indicator showing "Not Running" in red text.

Note: The authorization code is obtained from the cloud management platform, if you have not yet registered for a cloud management account, please register for an account first. China Recommended Choices: [China Servers](#) . Recommended for other countries: [Singapore Servers](#)

7.12 UPnP

On this page, you can select whether to enable the UPnP function. After enabling, the local device can be automatically searched on the server for management.

Figure 7-12-1 UPnP Settings

UPnP Save Undo

Switch: Off Enabled

Server Port:

Network Interface:

7.13 Whitelist

On this page, whitelist related information can be set. After setting, only IPs in the whitelist can access the device.

Figure 7-13-1 Whitelist Settings

Whitelist Add Clear Save

Start Address	End Address	Action
No Data Available		

7.14 Ping Test

On this page, the ping command can be used to test network connectivity.

Figure 7-14-1 Ping Test

Ping Test Start

Destination Address:

Number Of Tests:

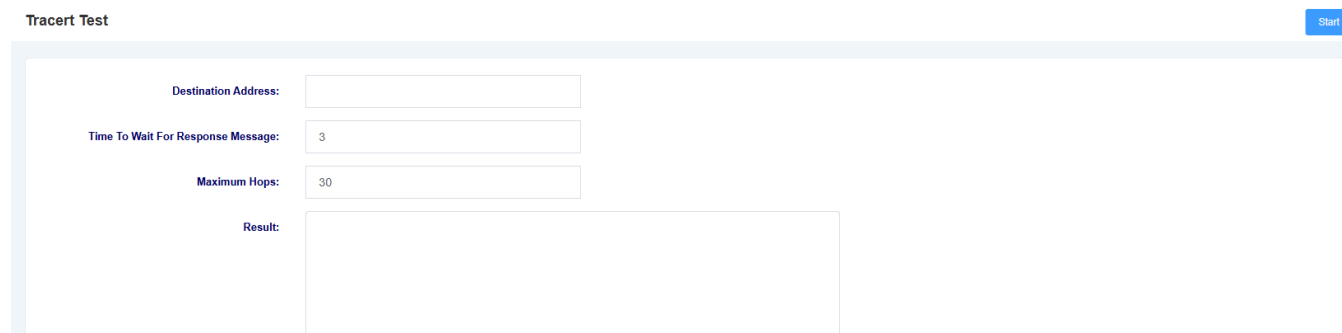
Packet Length:

Result:

7.15 Tracert Test

On this page, the tracert command can be used to test network connectivity.

Figure 7-15-1 Tracert Test

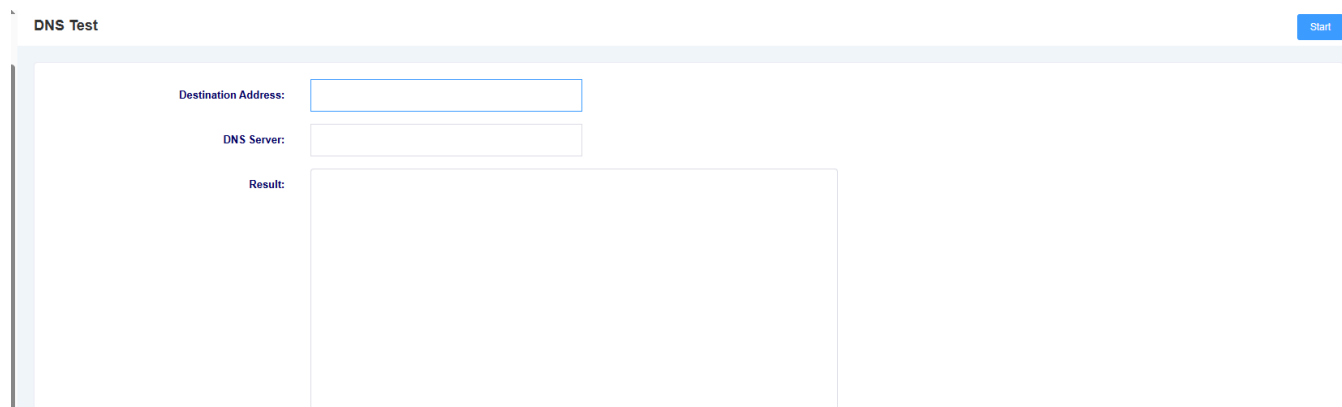


The screenshot shows a web interface titled "Tracert Test" with a "Start" button in the top right corner. The interface contains three input fields: "Destination Address:" (empty), "Time To Wait For Response Message:" (set to 3), and "Maximum Hops:" (set to 30). Below these fields is a large, empty "Result:" box.

7.16 DNS Test

On this page, the specified DNS can be tested.

Figure 7-16-1 DNS Test

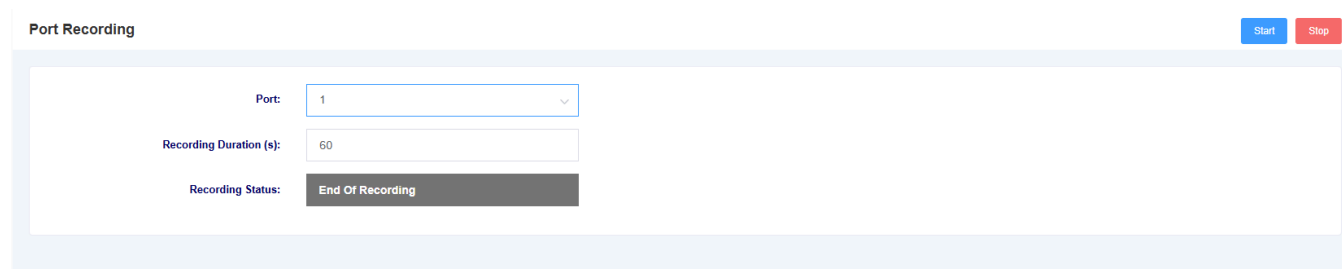


The screenshot shows a web interface titled "DNS Test" with a "Start" button in the top right corner. The interface contains two input fields: "Destination Address:" (empty) and "DNS Server:" (empty). Below these fields is a large, empty "Result:" box.

7.17 Port Recording

On this page, you can select a specified port for recording to troubleshoot problems.

Figure 7-17-1 Port Recording



The screenshot shows a web interface titled "Port Recording" with "Start" and "Stop" buttons in the top right corner. The interface contains three elements: a "Port:" dropdown menu set to "1", a "Recording Duration (s):" input field set to "60", and a "Recording Status:" label with a dark grey button that says "End Of Recording".