

# SLK-R602 Series Industrial 4G/3G Router Usermanual



#### Directory

1 Parameter configuration	4
1.1 Preparation before router configuration	4
1.1.1 Obtain ip address automatically (recommended)	4
1.1.2 Set static ip address	4
1.2 Login configuration page	5
2 Network Setting	6
2.1 Modify static login page address	6
2.1 SIM card 2/3/4G Internet access	7
2.3 DHCP server	9
2.4 WAN port settings	
2.4.1 DHCP client	
2.4.2 PPOE dial	10
2.4.3 Static Address	11
2.4.4 As Lan (convert WAN port to LAN port)	12
2.5 Wireless AP	12
2.5.1 WIFI Access Point	
2.5.1 WIFI Client	13
2.5.3 WIFI repeater	15
①Change the local IP address	15
②Connect to the main wireless AP	15
③Disable DHCP	16
2.6 Time Reboot	17
2.7 Network backup	17
2.8 Watchcat	
2.9 Diagnosis	20
3 Firewall	22
3.1 Firewall on and off	22
3.2 DMZ setting	22
3.3 Port Forwarding	24
3.4 Intranet penetration (frp)	
3.4.1 Add TCP proxy protocol	
3.4.2 Add STCP proxy protocol	
3.4.3 Add UDP proxy protocol	40
3.4.4 Add HTTP proxy protocol	42
4 VPN (Virtual Private Network)	43
4.1 PPTP VPN	44
4.2 L2TP VPN	44
4.3 OPENVPN	45
5 Basic Management (Device Management)	48
5.1 Date Time	48
5.2 Language Setting	49
5.3 Backup File	49



5.4 Upgrade firmware	
5.5 Factory Reset	51
5.6 Device restart	51
5.7 Page Exit	



# **1** Parameter configuration

### **1.1 Preparation before router configuration**

After completing the hardware installation, you need to ensure that the management computer has an Ethernet card installed before logging in to the router's Web setting page.

### 1.1.1 Obtain ip address automatically (recommended)

Please set the management PC to "Obtain IP address automatically" and "Obtain DNS server address automatically" (computer systemDefault configuration), the device automatically assigns an IP address to the management PC.

### 1.1.2 Set static ip address

Please set the IP address of the management PC (for example: 192.168.2.11) and the IP address of the LAN port of the device in the same network segment (the initial IP address of the device's LAN port is 192.168.2.1, and the subnet mask is 255.255.255.0).

Open "Control Panel"-"Network and Internet"-"Network Connections"-"Local Area Connection" and modify as follows:

00-1	・ 控制面板 → 网络和 Internet → 网络连接 →	财络连接
组织 ▼	费用此网络设备 诊断这个连接 重命名此连接 查看此连接的状态 更改此连接的设置	₩ <b>=</b> ▼
VN VN 未 VP VP VV VV VV VV VV VV VV	ware Network Adapter net1 到的网络 N 连接 所行连接 N Miniport (PPTP)	
	♀ 本地连接 雇性 Internet 协议版本 4 (TCP/IPv4) 雇性	8 ×
	注接时使用:     加黑网络支持此功能,则可以禁取自动指派的 IP 设       梁 Realtek PCIe FE Family Controller     如黑网络支持此功能,则可以禁取自动指派的 IP 设	置。否则,
	配置 (C) ◎ 自动获得 IP 地址 (O) 此连接使用下列项目 (O):	_
	● ● Microsoft 网络客户端     ●     IP 地址(I):     192.168.2       ● ● Vilware Bridge Protocol     ●     ●     子网箍码(U):     255.255	. 11
	☑ 圓Microsoft 网络的文件和打印机共享	
	● Litternet 协议服务 4 (UF/IFV) ● 使用下面的 DNS 服务器地址(3): ● 使用下面的 DNS 服务器地址(3):	
	安装 (8)         卸載 (1)         属性 (8)         自送 UNG 加力 (5)            描述	
	的相互连接的网络上的通讯。	高级(V)



# **1.2 Login configuration page**

Open IE or other browsers and enter 192.168.2.1 in the address bar. After the connection is established, log in as the system administrator (admin) in the pop-up login interface, enter the password in the login interface (the default password is admin).

A Not secure 192 168 2 1/cai bin/luci/		
#Seriallink		
	Language : English 🗸	
	Authorization Required	
	Password	
	Login	

The default login password is admin. If the user needs to protect the configuration interface to avoid being modified by others, you can modify the login password, click "Equipment Manager"-"Modify Password", then fill in the password to be modified, and then "SAVE & APPLY", as follows:

▲ Route Status	Router Password
Network Settings	Changes the administrator password for accessing the device
🛱 Route Settings	
A Service Manage	Password
E VPN Service	Confirmation
🛠 System	
Date Time	
Language Setting	
Modify Password	DAVE & APPL
— Backup File	
Update Firmware	Copyright @2013-2022 Seriallink Inc, All Rights Reserved.
Factory Reset	
- Reboot	



# **2 Network Setting**

# 2.1 Modify static login page address

The default static address of the router is 192.168.2.1. You can modify the static ip address in the navigation bar "Network Settings"-"LAN Setting". After the modification, the new ip address will be used to log in to the page.

IP Address:Fill in the ip address to be modified. Netmask:Fill in netmask.

Route Status	letwork Configuratio	n		
Network Settings				
4G Modem	LAN Configuration			
WAN Setting	General Setun			
- LAN Setting	ocherar octup	Untime: 0b 12m 25c		
DHCP Setting Wireless	Status	MAC-Address: 70:B3:D5:E6:00:11 BX: 261.48 KB (2720 Pkts.) br-lan TX: 944.76 KB (2521 Pkts.)		
Time Reboot		IPv4: 192.168.2.2/24 IPv6: fd19:7c82:39dc::1/60		
Network Backup	IP Address	192.168.2.2		
Watchcat	Netmack	255 255 255 0		
Diagnosis	Neuridsk	200.200.200.0		
Load Balancing	Gateway			
Route Settings	DNS		2	
Service Manage				
VPN Service				
System				SAVE & APPI
→ C ① ▲ 不安全 192.168.2.2	cgi-bin/luci			아 Q 년 ☆ 🛛 🌡 🗍
Seriallink®				
	需要打	语言: 中文(Chinese) 受权	v	
		密码		
		登录		



### 2.1 SIM card 2/3/4G Internet access

The router uses SIM card 2/3/4G to surf the Internet by default. You can see the information of the SIM card in the navigation bar "Routing Status"-"Status", and you can check the network is 2/3/4G and the signal of the mobile phone card in the upper right corner.

<b>#</b> Seriallink®			4G1
<ul> <li>Routing Status</li> </ul>	Cellular Status		
Status	SIM CARD	SIM READY	
Routes	COPS	UNICOM	
- Log	Cellular Network	LTE	
Network Setting	Frequency Band	3	
🛱 Routing Setting	CEREG	0,1	
M DDNS/FRP	Signal Quality	28	
E VPN Service	Card Slot	SIM1	
🛠 System	IMEI	862138050326664	
	IMSI	460012238632850	

If you use an ordinary mobile phone data card, you don't need to care about the location of the APN setting, and the default is empty. If you use an APN card, you need to set the APN in "Network Settings"-"4G Modem"-"General Setup", fill in by yourself.

Network Settings			
4G Modem	SIM Settings		
WAN Setting	General Setup Advanced	Settings	
LAN Setting	Enable		
DHCP Setting			
— Wireless	APN		
Time Reboot	Username		
Network Backup	Password		<i>a</i>
Watchcat			
Load Rolonging	Auth Type	none	×
	PIN Code		
Route Settings			
ሻ Service Manage			
E VPN Service	Abnormal Restart		
🛠 System	Network exception handling: check	the network connection in a loop for 5 seconds	If the Ping IP address is not successful, After the network exceeds the abnormal
Eugout	number, restart and search the regi	istered network again.	
	Enable		
	Ping IP address	114.114.114.114	
	Abnormal number	10	~
			SAVE & APF



Network diagnosis: It is to deal with network abnormalities. Ping the set ip address every 5s. After the abnormal number of pings, the network still cannot be pinged, and the network will be re-registered. You can set network diagnostics in both "Basic Settings" and "Advanced Settings", or you don't need to enable network diagnostics, just leave it unchecked.

attinga			
ettings			
SIM Settings			
General Setup	Advanced	l Settings	
Account of Product of Product of	Enable		
	101		
	APN		
	Username		
	Password		8
	Auth Type	none	~
9	PIN Code		
ngs			
nage			
e Abnormal Restart			
e Abnormal Restart	handling: checl	k the network connection in a loop for 5 seconds	. If the Ping IP address is not successful, After the network exceeds the abnormal
Abnormal Restart Network exception number, restart an	n handling: check d search the reg	k the network connection in a loop for 5 seconds istered network again.	. If the Ping IP address is not successful, After the network exceeds the abnormal
Abnormal Restart Network exception number, restart an	handling: checl d search the reg Enable	k the network connection in a loop for 5 seconds istered network again.	. If the Ping IP address is not successful, After the network exceeds the abnormal
e Abnormal Restart Network exception number, restart an	handling: check d search the reg Enable ing IP address	k the network connection in a loop for 5 seconds istered network again.	. If the Ping IP address is not successful, After the network exceeds the abnormal
e Abnormal Restart Network exception number, restart an P	handling: check d search the reg Enable ing IP address tormal number	k the network connection in a loop for 5 seconds istered network again.	. If the Ping IP address is not successful, After the network exceeds the abnormal
e Abnormal Restart Network exception number, restart an P Abr	handling: check d search the reg Enable ing IP address normal number	k the network connection in a loop for 5 seconds istered network again.	. If the Ping IP address is not successful, After the network exceeds the abnormal

"Network Settings"-"4G Network"-"Advanced Settings" can bind 2/3/4G. If the service type is selected as LTE Only, it means that only 4G network is used. If it is not 4G, there will be no network automatically. The default is 2/3/4G. Which one will be used first if the network signal is stronger, and 4G will be used first. Locking the frequency band is forbidden. The frequency band with good signal is preferred. You can also lock the frequency band according to your needs. If the locked frequency band is unsuccessful, the module does not support this frequency band temporarily. Click "SAVE & APPLY".



Route Status	Mobile Network			
Network Settings				
4G Modem	SIM Settings			
WAN Setting	General Setup Advanced	Settings		
LAN Setting	Force Dial			
DHCP Setting	Fore Star			
Wireless	ІР Туре	IPV4V6	~	
Time Reboot	Server Type	Automatically	×	
Network Backup Watchcat	Override MTU	Automatically GSM Only UMTS Only		
Diagnosis	Metric	LTE Only GSM And UMTS		
Load Balancing	· · · · · · · · · · · · · · · · · · ·	LTE And UMTS LTE And GSM		
Route Settings Service Manage	Abnormal Restart	LTE And UMTS And GSM TD-SCDMA CDMA CDMA And EVDO		
VPN Service System	Network exception handling: check number, restart and search the regi	e the network connection in a loop for 5 sec istered network again.	ands. If the Ping IP address is not successful, After the network exceeds the abnormal	
Logout	Enable			
	Ping IP address	114.114.114.114		
	Abnormal number	10	~	

#### Note:

- > Ordinary 4G mobile phone card can go online without worrying about APN settings
- If you use APN dedicated network card, you must fill in the APN address, user name and password
- Different operators have different specifications of APN dedicated network cards, APN address, user name and password (if any, please refer to the chapter of APN setting table) or consult the local operator.

### 2.3 DHCP server

DHCP adopts the client/server communication mode. The client makes a configuration request to the server, and the server returns the corresponding configuration information such as the IP address assigned to the client to realize the dynamic configuration of the IP address and other information.

DHCP client configuration (usually the default): select "Network Settings"-"DHCP Settings" in turn, "SAVE & APPLY".

Turn off DHCP: Click to turn off the DHCP server

Start: the starting address of the assigned dhcp server, such as 100, which means the assignment starts from 192.168.2.100

Number of customers: the number of IP addresses that can be allocated, ensure that the starting number plus the number of customers cannot exceed 150

Lease time: the length of time of the assigned IP.



oute Status	DHCP Server Settings				
twork Settings	Configurable DHCP Server.				
Nodem					
Setting	General Setup IPv6 Settings				
Setting R Setting	lanore	interface			
SS		O Disable <u>DHCP</u> for this interface.			
leboot		Start 100			
rk Backup		Lowest leased address as offset from	the network address.		
cat		Limit 150			
osis		Maximum number of leased addresse	S.		
Balancing	L	easetime 12h			
e Settings		Expiry time of leased addresses, mining	num is 2 minutes (2m).		
ice Manage					
Service	Static Leases				
em	Static leases are used to assign fixed IP a	ddresses and symbolic hostnames to DHCP clients	They are also required for non-dynamic interface co	onfigurations where only hosts with a corresponding lease are served.	
ut	Use the Add Button to add a new lease en	try. The MAC-Address indentifies the host, the IPv4	Address specifies to the fixed address to use and th	e Hostname is assigned as symbolic name to the requesting host.	
	Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)	
		т	his section contains no values yet		
	ADD				
				SAVE & APPL	LY

# 2.4 WAN port settings

### 2.4.1 DHCP client

Navigation bar "Network Settings"-"wan Settings", Switch protocol of the WAN port to a DHCP address (DHCP client), and the upper-level device needs to be able to assign an IP to the wan port.

<ul> <li>Route Status</li> </ul>	Network Conf	iguration	
Network Settings		J	
4G Modem	WAN Configuration		
WAN Setting	General Setup	Advanced Settings	
LAN Setting		Status Uptime: 0h 0m 0s	
DHCP Setting		MAC-Address: 70:B3:D5:E6:00:12	
Wireless		TX: 227.60 KB (684 Pkts.)	
Time Reboot		Protocol DHCP address	
Network Backup			
Watchcat			
Diagnosis			
Load Balancing		s	AVE & APPLY

### 2.4.2 PPOE dial

If the wan port needs to dial-up to access the Internet, you need to select ppoe dial-up, and fill in the user name and password according to the actual situation.



♠ Route Status	Network Configurat	tion	
Network Settings			
4G Modem	WAN Configuration		
WAN Setting	General Setup Advan	nced Settings	
LAN Setting	Stat	tus Uptime: 0h 0m 0s	
DHCP Setting		etho.2 RX:0 B (0 Pkts.)	
Wireless		TX: 240.42 KB (722 PKts.)	
Network Baskup	Protoc	Col DHCP address	
Watchcat		DHCP address	
Diannosis		As Jan	
Load Balancing		Disable SAVE & APPL	
Concentration			
▲ Route Status	Network Configuration	on	
Network Settings	nethont configuration		
4G Modem	WAN Configuration		
WAN Setting	Canaral Catura Advance	ad Cattings	
LAN Setting	General Setup Advance	Lindings	
DHCP Setting	Status	S MAC-Address: 70:B3:05:E6:00:12	
Wireless		eth0.2 HX: 0 B (0 PKIS.) TX: 243.32 KB (731 Pkts.)	
Time Reboot	Protocol		
Network Backup			
Watchcat	Username		
Diagnosis	Password	d a state of the s	
Load Balancing	Access Concentrator	f auto	
🛱 Route Settings		Leave empty to autodetect	
n Service Manage	Service Name	e auto	
■ VPN Service		Leave empty to autodetect	
<b>%</b> System			
-			
⊖ Logout		SAVE & APPLY	

### 2.4.3 Static Address

The wan port can also choose to set the ip address manually.

Protocol: Static address

IP Address: It can be in the same network segment as the upper-level route, but the upper-level route cannot be the same as the address of the LAN port of your own device, otherwise conflicts will occur. For example, the superior route is 192.168.1.1, so write 192.168.1.xxx here.

Netmask: generally 255.255.255.0.

Gateway: such as 114.114.114.114, 8.8.8.8, etc.

DNS: such as 114.114.114.114, 8.8.8.8, etc.



♠ Route Status	Network Configuration
Network Settings	· · · · · · · · · · · · · · · · · · ·
4G Modem	WAN Configuration
WAN Setting	General Setup Advanced Settings
LAN Setting	Statue Uptime: 0h 0m 0s
DHCP Setting	MAC-Address: 70:B3:D5:E6:00:12 eth:0 2 RX: 0 B (0 Pkts.)
Wireless	TX: 248.45 KB (746 Pkts.)
Time Reboot	Protocol Static address
Network Backup	Ont Loar son
Watchcat	
Diagnosis	Netmask 255.255.255.0
Load Balancing	Gateway
🛱 Route Settings	DNP
Service Manage	
VPN Service	
& System	
X System	SAVE & APPLY
E Logout	

### 2.4.4 As Lan (convert WAN port to LAN port)

If you need to convert the WAN port to a LAN port, change the wan setting protocol to "As lan", click "SAVE & APPLY", you can convert the wan port to a lan port.

▲ Route Status	Network Configuration	
Network Settings		
4G Modem	WAN Configuration	
···· WAN Setting	General Setup	
LAN Setting	Status Uptime: 0h 0m 0s	
DHCP Setting	# MAC-Address 70 83 05:6:00-12 eth 0: 28X 0 8 10 91x1.	
Wireless	TX: 250.16 KB (751 Pkts.)	
Time Reboot	Protocol As Ian	
Network Backup		
Watchcat		
Diagnosis		_
Load Balancing	SAVE & AP	PLY

# 2.5 Wireless AP

### 2.5.1 WIFI Access Point

The router supports both the wireless AP and the client to be turned on at the same time. It can open a wifi for other devices to connect and connect to other wifi. This function can realize wireless relay.

The router generally defaults wireless AP to be turned on, there is a wifi name of SLK-Routers\_XXX, the default password is slk100200.

Click DISABLE to close router's AP for your needs.

Modify ESSID to rename the WiFi.

We suggest a Mixed Mode for the AP Encryption and also the Key should be modified too.

Channel and Width have an impact on wireless quality, change them according to the actual use environment.

After the configuration is complete, click "Save & Apply" to make it effective.



n	Route Status	WIFI Access Point	WIFI Client						
G	Network Settings								
	4G Modern								
	- WAN Setting		Status	Mode: Master   SSID: SI BSSID: 72:B3:D5:E6:00:	LK-Router_E60011 11   Encryption: WPA2 P	SK (CCMP)			
	LAN Setting			0% Channel: 11 (2.462 GHz Signal: 0 dBm   Noise: 0	z)   <b>Tx-Power.</b> 0 dBm 0 dBm				
	DHCP Setting			Bitrate: 0.0 Mbit/s   Cou	untry: CN				
	- Wireless		Wireless network is enabled	DISABLE					
	Time Reboot		ESSID	SLK-Router_E60011					
	Network Backup			2					
	Watchcat		Hide <u>ESSID</u> (	_					
	Diagnosis		Encryption	WPA2-PSK	~				
	Load Balancing		Key			2			
Ĕ	Route Settings								
a	Service Manage		Channel	11	~				
=	VPN Service		Width	HT20	~				
×	System		WDS (	כ					
G	Logout								
								SAVE & APPLY	

### 2.5.1 WIFI Client

The WIFI Client is not enabled by default, you need to check to enable it in the navigation bar "WIFI Client".

Route Status	WIFLACCESS Point WIFLClient
Network Settings	
4G Modem	Join Wireless
WAN Setting	Status
LAN Setting	Interface not present or not connected yet.
DHCP Setting	Enable
- Wireless	
Time Reboot	

Then select the client wifi interface: select WIFI in the SSID list, change the security option according to whether there is a password,No Encryption、WPA-PSK、WPA-2PSK、WPA-PSK/WPA2-PSK Mixed Mode, WDS is not checked by default.

Status	Interface not present or not connec	sted yet.
Enable	<b>7</b>	
Scan	SCAN	
SSID	_TEST_AP	~
Encryption Key WDS	TEST_AP telunche SLK-Router_2G-0DC8 SLK-Router_2G-0009 SLK-Router_2G-0015 SLK-Router_2G-0398 hbps3 SLK-Router_2G-1234 ChinaNet-qEQX Labpano 赛诺联克 DIRECT-74-HP M283 LaserJet onlywon_Wi-Fi5 Bik=発日	
Interface Configuration	onlywon custom	
Protocol	DHCP address	×



Enable 🗹				
Scan	CAN			
SSID g	度诺联克	~		
Encryption V	VPA-2PSK	~		
Key			]#	
WDS 🗆 Ø E	nable WDS if Bridge Lan is se	elected.		
E	Scan S SSID 3 ncryption V Key WDS 0 9 E	Enable C Scan SCAN SSID 赛诺联克 ncryption WPA-2PSK Key	Enable C Scan SCAN SSID 赛诺联克 ~ ncryption WPA-2PSK ~ Key	Enable C Scan SCAN SSID 赛诺联克 ~ ncryption WPA-2PSK ~ Key

After successfully connecting to WIFI, the WIFI status will be displayed.



WIFI wireless client advanced settings protocol selection:

- A.DHCP address (default): The WiFi client automatically obtains the IP address assigned by the superior route.
- B.Static address: The WiFi client uses the user-configured IP address, subnet mask, gateway, and DNS.
- C.Bridge Lan: Use the LAN port configuration IP address, subnet mask, gateway, DNS, Lan port configuration reference WIFI wireless client advanced settings static address (relay mode select this item).

Pro	tocol Static address	×		
IP Ad	lress 192.168.16.65			
Net	nask 255.255.255.0	¥		
Ga	away 192.168.16.1			
	DNS 192.168.16.1		1	
Sta	tus 愛 Client "赛	Uptime: 0h 0m 2 MAC-Address: 7 RX: 49.93 KB (1 诺联克 TY - 2.38 KB (14	25s 70:B3:D5:E6:00:11 67 Pkts.) Pkts.)	



#### 2.5.3 WIFI repeater

This section describes how to extend the wireless signal length by means of relays. In this configuration mode, the computer terminal connected to the SLK-R602 is in the same IP address segment as the main wireless network.

### **①Change the local IP address**

It is necessary to modify the local IP address of SLK-R602 to be in the same network segment as the main wireless AP. For example, the IP address of the main wireless AP to be connected is 192.168.16.1, then modify the IP address of SLK-R602 to 192.168.16.65. It should be noted that the LAN port gateway is empty by default. After using the relay mode setting, if you need to connect to the Internet through the WAN port in the future, you need to delete the gateway information in the LAN settings to avoid the situation of being unable to access the Internet.



### ②Connect to the main wireless AP

In the navigation bar "Network Setting" - "WIFI Client", check to enable the WIFI wireless client, and configure the connection to the main wireless AP. For example, the SSID of the main wireless AP to be connected here is 赛诺联克, and the password is slk100200,Search and select the SSID as shown in the figure below, fill in the password, select "Bridge Lan" from "Protocol", and click "SAVE & APPLY".



♠ Route Status	WIFI Access Point WIFI Client	
Network Settings		
4G Modem	Tain Wireland	
WAN Setting	Juli Mileles	
LAN Setting	Status Uptme: 0.0 m 0s Mac-Address: 70:03:D5:E6:00:11	
DHCP Setting	Client "雲海穂克" RX: 60.99 KB (596 Pkts.) The Cr2.71 KB (297 Pkts.)	
Wireless	Enable 🗹	
Time Reboot	Seen CCAN	
Network Backup		
Watchcat	SSID 赛诺联克	
— Diagnosis	Encryption WPA-2PSK V	
Load Balancing		
🗂 Route Settings	Key	
A Service Manage	WDS Z © Enable WDS if Bridge Lan is selected.	
VPN Service		
🛠 System		
🕒 Logout	Interface Configuration Protocol DHCP address	
	SAVE & APPLY	

It should be noted that in this mode, the main wireless AP no longer assigns an IP address to this SLK-R602. Therefore, the obtained IP address will not be updated in "Status", and you can confirm whether the connection is successful through the icon color and MAC address. The picture below is successful.

Section Transferred Section 1	MAC-Address: 70:B3:D5:E6:00:11 " RX: 162.64 KB (862 Pkts.) TX: 742.51 KB (1162 Pkts.)
-------------------------------	---

**③Disable DHCP** 

Disable the DHCP server function of the SLK-R602. In this way, the SLK-R602 no longer assigns IP addresses to the connected devices, and all devices connected to the local area network are assigned IP addresses by the main wireless to realize communication on the same network segment.



Route Status	DHCP Server Settings			
Network Settings	Configurable DHCP Server.			
4G Modem				
WAN Setting				
LAN Setting	General Setup IPv6 Settings			
DHCP Setting	Ignore interface	o DHCP for this interface		
Wireless	UISADI	e <u>once</u> for this interface.		
Time Reboot				
Network Backup				
Network Backup Watchcat	Static Leases			
Network Backup Watchcat Diagnosis	Static Leases Static leases are used to assign fixed IP add	dresses and symbolic hostnames to DH	CP clients. They are also required for non-dyna	mic interface configurations where only hosts with a
Network Backup Watchcat Diagnosis Load Balancing	Static Leases Static leases are used to assign fixed IP add corresponding lease are served. Use the Add Button to add a new lease entry	dresses and symbolic hostnames to DH y. The MAC-Address indentifies the hos	CP clients. They are also required for non-dyna t, the IPv4-Address specifies to the fixed addre	mic interface configurations where only hosts with a ss to use and the Hostname is assigned as symbolic name to the
Network Backup Watchcat Diagnosis Load Balancing Route Settings	Static Leases Static leases are used to assign fixed IP add corresponding lease are served. Use the Add Button to add a new lease entry requesting host.	dresses and symbolic hostnames to DH y. The MAC-Address indentifies the hos	CP clients. They are also required for non-dyna t, the IPv4-Address specifies to the fixed addre	mic interface configurations where only hosts with a ss to use and the Hostname is assigned as symbolic name to the
Network Backup Watchcat Diagnosis Load Balancing Route Settings	Static Leases Static leases are used to assign fixed IP add corresponding lease are served. Use the Add Button to add a new lease entry requesting host. Hostname	dresses and symbolic hostnames to DH y. The MAC-Address indentifies the hos MAC-Address	CP clients. They are also required for non-dyna t, the IPv4-Address specifies to the fixed addre IPv4-Address	mic interface configurations where only hosts with a ss to use and the Hostname is assigned as symbolic name to the I <u>Pv6</u> -Suffix (hex)
Network Backup Watchcat Diagnosis Load Balancing Route Settings Service Manage	Static Leases Static leases are used to assign fixed IP add corresponding lease are served. Use the Add Button to add a new lease entry requesting host. Hostname	dresses and symbolic hostnames to DH y. The MAC-Address indentifies the hos <u>MAC</u> -Address	CP clients. They are also required for non-dyna t, the IPv4-Address specifies to the fixed addre IPv4-Address	mic interface configurations where only hosts with a ss to use and the Hostname is assigned as symbolic name to the IPv6-Suffix (hex)
Network Backup Watchcat Diagnosis Load Balancing Route Settlings Service Manage VPN Service	Static Leases Static leases are used to assign fixed IP add corresponding lease are served. Use the Add Button to add a new lease entr requesting host. Hostname	dresses and symbolic hostnames to DH y. The MAC-Address indentifies the hos <u>MAC</u> -Address Thi	CP clients. They are also required for non-dyna t, the IPv4-Address specifies to the fixed addre IPv4-Address s section contains no values yet	mic interface configurations where only hosts with a ss to use and the Hostname is assigned as symbolic name to the IPv6-Suffix (hex)
Network Backup Watchcat Diagnosis Load Balancing Route Settlings Service Manage VPN Service System	Static Leases Static leases are used to assign fixed IP add corresponding lease are served. Use the Add Button to add a new lease entr requesting host. Hostname	dresses and symbolic hostnames to DH y. The MAC-Address indentifies the hos <u>MAC</u> -Address Thi	CP clients. They are also required for non-dyna t, the IPv4-Address specifies to the fixed addre IPv4-Address s section contains no values yet	mic interface configurations where only hosts with a ss to use and the Hostname is assigned as symbolic name to the IPv6-Suffix (hex)
Network Backup Watchcat Diagnosis Load Balancing Route Settlings Service Manage VPN Service System	Static Leases Static leases are used to assign fixed IP add corresponding lease are served. Use the Add Button to add a new lease entr requesting host. Hostname	dresses and symbolic hostnames to DH y. The MAC-Address indentifies the hos <u>MAC</u> -Address Thi	CP clients. They are also required for non-dyna t, the IPv4-Address specifies to the fixed addre IPv4-Address s section contains no values yet	mic interface configurations where only hosts with a ss to use and the Hostname is assigned as symbolic name to the IPv6-Suffix (hex)

# 2.6 Time Reboot

Navigation bar "Network settings" - "Restart time", the user can check the enabling and set the daily restart time, pay attention to check whether the device time is correct, click the button to modify the correct time.

Route Status	Time Reboot	
Network Settings	Configure a timed reboot	
4G Modem		
WAN Setting		
LAN Setting	Local Time: 2023-06-06 09:01:40 SYNC WITH BROWSER	
DHCP Setting	Enable 🗋	
Wireless	Entable the device to restart during the configured time each day (the recommended time is between 2300 and 500 PM).	
Time Reboot	hour 06 v	
Network Backup	minute 00 🗸	
Watchcat		
Diagnosis		
Load Balancing		-
Route Settings		SAVE & APPI

# 2.7 Network backup

It is mainly used to connect the Internet, whether the wired (i.e. WAN port) or 4G network or WiFi client is preferred, the network with the main link is preferred, and the network with the backup route is used when the main link has no network.

Network backup is off by default. You need to check enable and then configure it according to the actual situation.



▲ Route Status	letwork Backup	
Network Settings		
4G Modem	General Settings	
WAN Setting	Enable 🛛	
LAN Setting	Dino ID address 114 114 114	
DHCP Setting	ring in sources in 114, 114, 114	
Wireless	Visite Osec to deel to deel to deel to tremon statue, il tier ring in statues is not addressing similar tier retrock time.	
Time Reboot	Main Lilli WAR	
- Network Backup	e in cool descup move, main Lain a pretenes.	
Diagnosis	Backwip Link None Belanus will not work if kings in advantation as Darking 1 ink	
Load Balancing	Renders Market and Statuty with not Youk is seed, and as backap Link.	
Route Settings	Use say more Use Backtor mode. Main Link will be salastad automatifields whather Main Link is back to normal.	
	Bernary Interval 1	
Service Manage     E VPN Service	Specify how many minutes to wait to switch back to Main Link to check whether Main Link is back to normal. 0 means no active switchback. Note: this function is	
★ System	Abnormal Restart OFF	
🕒 Logout	• Note: when enabled, the whole system will restart when no link is available.	
	SAVE & ADDIV	
	DAVED AFFL	

Configure accordir	ng to the table below.				
	General settings @ link management				
Project	oject Explain				
Main Chain	You can choose "WAN", "SIM1" or "WIFI".	WAN			
	WAN: using Wan as the main wired link				
	SIM1: use Sim1 as the main wireless link				
	WIFI: use the WiFi client as the main wireless link				
	Note: WiFi link is only available when WiFi client mode is				
	turned on. Please refer to "5.2" for details.				
Backup Link	You can choose "WAN", "SIM1", "WIFI" or "NONE".	NONE			
	WAN: a wired link using Wan as backup				
	SIM1: wireless link using Sim1 as backup				
	WIFI: wireless link using WIFI client as backup				
	Note: WIFI link is only available when WIFI client mode is				
	turned on. Please refer to "5.2" for details.				
	NONE: the backup link is not allowed				
Backup Mode	Select "Cold Backup" or "Hot Backup"	Cold Backup			
	Cold backup: the backup link is dialed online only when it is				
	switched				
	Hot backup: the backup link is always online				
	Note: hot backup is not applicable to dual sim card backup.				
Recovery Interval	When the backup link is used in cold backup mode, it	1			
	specifies how many minutes to wait to switch back to the				
	main link to detect whether the main link returns to normal. 0				
	means no active switchback.				
	Note: this function is displayed only when cold backup mode				
	is selected.				
Abnormal Restart	Click the button to turn on/off the abnormal restart function.	OFF			



When enabled, the device will restart when no link is available.

### 2.8 Watchcat

In the navigation bar "Network Setting" - "Watchcat", the network self-check function is disabled by default, and the network self-check allows setting periodic restarts or restarts when the network is abnormal.

If you need to activate this function, click Add, enter the configuration and click "SAVE & APPLY".

▲ Route Status	Watchcat
• Network Settings	Watchcat allows to configure a periodic reboot and/or when internet connection has been lost for a certain period of time.
4G Modem	
WAN Setting	This section contains no values yet
LAN Setting	
DHCP Setting	ADD
Wireless	
Time Reboot	
Network Backup	SAVE & APPLY
Watchcat	

- A.Forced reboot delay: When rebooting the system the watchcat will trigger a soft reboot, Entering a non zero value here, will trigger a delayed hard reboot if the soft reboot fails. Enter a number of seconds to enable, use 0 to disable
- B.Period: In periodic mode, it defines the reboot period. In internet mode, it defines the longest period of time without internet access before a reboot is engaged.Default unit is seconds, you can use the suffix 'm' for minutes, 'h' for hours or 'd' for days
- C.Ping host: Host address to ping

D.Ping period:How often to check internet connection. Default unit is seconds, you can you use the suffix 'm' for minutes, 'h' for hours or 'd' for days

1.Reboot on internet connection lost

	DELETE
Operating mode	Reboot on internet connection lost
Forced reboot delay	0
	When rebooting the system the watchcat will trigger a soft reboot, Entering a non zero value here, will trigger a delayed hard reboot if the soft reboot fails. Enter a number of seconds to enable, use 0 to disable.
Period	
	In periodic mode, it defines the reboot period. In internet mode, it defines the longest period of time without internet access before a reboot is engaged.Default unit is seconds, you can use the suffix 'm' for minutes, 'h' for hours or 'd' for days
Ping host	8.8.8.8
	Host address to ping
Ping period	
	How often to check internet connection. Default unit is seconds, you can you use the suffix 'm' for minutes, 'h' for hours or 'd' for days
ADD	

#### 2.Periodic reboot



		DELETE	
Operating mode	Periodic reboot		
Forced reboot delay	0		
	$\ensuremath{\Theta}$ When rebooting the system the watchcat will trigger a number of seconds to enable, use 0 to disable	soft reboot, Entering a non zero value here, will trigger a delayed hard reboot if the soft reboot fails. Enter a	
Period			
	O In periodic mode, it defines the reboot period. In interm is seconds, you can use the suffix 'm' for minutes, 'h' for l	et mode, it defines the longest period of time without internet access before a reboot is engaged.Default un hours or 'd' for days	it 📃
ADD			

After adding and configuring, click "SAVE & APPLY" to take effect. To delete the configuration, just click the "DELETE" button in the upper right corner, and then "SAVE & APPLY".

# 2.9 Diagnosis

Through network diagnosis, you can determine whether the router and the connected device can communicate with each other, whether the device can access the Internet, and whether the device is successfully connected to the VPN. It can also be used to test other aspects, and you can test it according to your own needs.

Navigation bar "Network Setting" - "Diagnosis".

Baidu, seriallink, 8.8.8.8: It is generally used to test whether the device can access the Internet. If it can ping, it means the device can access the Internet. If it cannot ping, it means that the device cannot access the Internet.

<ul> <li>Route Status</li> </ul>	Diagnostics
Network Settings	
4G Modem	Network Unifies
WAN Setting	
LAN Setting	8888
DHCP Setting	8.8.8 V IPV4 V PINGcustom V IPV4 V TRACEROUTEcustom V NSLOOKUP
Wireless	
Time Reboot	
Network Backup	Collection data
Watchcat	**************************************
- Diagnosis	Find U.S. doub (U.S. doub), so tanks by res B4 bytes from 8.8.8. sequel this 5 time=18.468 ms
Load Balancing	64 bytes from 8.8.8; sequel til=55 time17.195 ms 64 bytes from 8.8 ; sequel til=55 time17.080 ms
1 Route Settings	64 bytes from 8.8.8.1: seq=3 til=5 time=24.557 ms 64 bytes from 8.8.8.1: seq=4 til=5 time=15.615 ms
7 Service Manage	
■ VPN Service	5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avy.max = 15.615/18.646/24.837 ms
🛠 System	

Custom input box: generally used to test whether the connected device can be pinged.



Route Status	Diagnostics	
Network Settings		
4G Modem	Network Utilities	
WAN Setting		
LAN Setting	192.168.8.1	
DHCP Setting	8.8.8. V IPv4 V PINGcustom V IPv4 V TRACEROUTEcustom V NSLOOKUP	
Wireless		
Time Reboot		
Network Backup	Collecting data	
Watchcat	TTTP 10 10 10 10 10 10 10 10 10 10 10 10 10	
Diagnosis	File 32-6 too.a.f (192.100.a.f). 30 bais syles 64 bytes from 192.108.1: see0 tuile4 time:1.427 ms	
Load Balancing	64 bytes from 192.168.8.1: seq=1 til=64 time=1.332 mm 64 bytes from 192.168.8.1: seq=2 til=64 time=0.955 mm	
🛱 Route Settings	64 bytes from 192.188.8.1: seq=3 ttl=64 time=1.216 mm	
Ch Service Manage	64 bytes from 192.168.8.1: seq=4 ttl=64 time=1.312 ms	
Service Manage	192.168.8.1 ping statistics	
VPN Service	5 packets transmitted, 5 packets received, 0% packet los round-trip min/avy/mar 0.055/1.128/1.427 ms	
🛠 System		



# **3 Firewall**

# 3.1 Firewall on and off

The firewall is enabled by default. When doing DMZ and port mapping, you need to disable the firewall. Steps to disable the firewall are in the navigation bar "Routing Setting"-"Firewall", select the firewall to disable, and click "SAVE & APPLY".

•	Routing Status	Firewall	
3	Network Setting		
<b>(11</b> )	Routing Setting	Firewall Disable Y	
	Routing Table		
	- Firewall	SAVE & APP	LY
	Port Mapping		
	DMZ		
(h	Application Manage	Copyright ©2017-2020 Seriallink inc. All rights reserved.	
	VPN Service		
45	Equipment Manage		
e	Logout		

# 3.2 DMZ setting

The DMZ function can map the WAN port address to a host on the LAN side; all packets to the WAN address will be forwarded to the destination. Set the LAN side host to achieve two-way communication. In fact, a host in the intranet is completely exposed to the Internet and all ports are opened. It is equivalent to all port mapping. It is equivalent to using the public IP directly.

First, you need to disable the firewall.

•	Routing Status	Firewall
G	Network Setting	
Ľ	Routing Setting	Firewall Disable v
	Routing Table	
	Firewall	SAVE & APPLY
	Port Mapping	
	DMZ	
a	Application Manage	Copyright @2017-2020 Senallink inc. All rights reserved.
	E VPN Service	
*	Equipment Manage	
G	+ Logout	

In the navigation bar, "Route Setting"-"DMZ", click Enable, set the ip address assigned by the lan port to the connected device, and forward all the ports of the connected device, which can be directly accessed through the ip address of the wan port.



### Check Enable.

Internal IP address: Fill in the ip assigned by the lan port to the downstream device or the ip of the machine.

<ul> <li>Routing Status</li> <li>Network Setting</li> </ul>	DMZ The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service.	
Routing Setting	Configuration	
Routing Table	Enable 🗹	
— Firewall	Internal IP address 172.31.1.104	
- Port Mapping		
Application Manage	SAVE & APP	PLY

#### View wan port IP Address:

A F	Routing Status	Network Configuration		
1 📀	Network Setting	WAN Configuration		
- 4	4G Modem	Ctatua	Uptime: 0h 0m 23s	
V	WAN Setting	Status	MAC-Address: 5C:B1:5F:81:07:EB BX: 48:51 KB (113 Pkts)	
<b>L</b>	LAN Setting		eth0 TX: 1.89 KB (11 Pkts.)	
- C	DHCP Setting		IP24: 192.106.2.195/24	
۷	Wireless	Protocol	DHCP address 🗸	
Ë F	Routing Setting			
m l	Application Manage			SAVE & APPLY
٤ ١	VPN Service			

Through the device wan port ip, you can access all the ports of the device just filled in.

	Authorization Required	anguage : English	~	
	Password			
		Login		
	100			



# 3.3 Port Forwarding

Compared with DMZ, port forwarding is more refined control. Data packets sent to a certain port can be forwarded to a certain host on the LAN side, and different ports can be transferred to different hosts.

First, you need to disable the firewall.

<ul> <li>Routing Status</li> </ul>	Firewall	
Network Setting		
Routing Setting	Firewall Disable v	
Routing Table		
· Firewall	SAVE & APPLY	
Port Mapping		
DMZ		
Application Manage	Copyright @2017-2020 Seriallink inc. All rights reserved.	

Navigate to the "Routing Settings"-"Port Mapping" setting menu in the navigation bar, and enter the "Port Forwarding" interface to configure.

Name: Specify the name of this rule, you can give a meaningful name.

Protocol: Specify the protocol to be forwarded, which can be TCP, UDP, or TCP/UDP.

Internal IP address: select the IP address that needs to be forwarded to the external network.

Internal port: the port to be forwarded by the downstream device.

External port: add this external port through the wan port ip to access the downstream device

After configuration, click the "Add" button to add a forwarding rule. Click the "SAVE & APPLY" button to make the rule effective.

Routing Table	Name	Match	Forward to	Enable	Sort
- Firewall					
Port Mapping		This section	on contains no values yet		
مسر ۸ Application Manage			New port forward		
E VPN Service		Name	нттр		
Equipment Manage					
Logout		Protocol	TCP	~	
		Internal IP address	172.31.1.104 (SLK.lan)	~	
		Internal port	80		
		External port	500		
					ADD
					Listing for

After the addition is successful, there will be an additional port forwarding rule, click "Save & Apply" to



#### make the rule effective.

<ul> <li>Routing Status</li> </ul>	Port Forwards					
Network Setting	Port forwarding allows remote computers on the Int	ernet to connect to a specific computer	r or service withi	n the private LAN.		
Routing Setting	Port Forwards					
Routing Table	Name Match	Forward to	Enable	Sort		
Firewall	IPv4-tcp	IP 172 31 1 104 port 80 in Jap			DELETE	
— DMZ	Via <i>any router IP</i> at port 500	ii 172.01.1.104, port do in fan			DELETE	
n Application Manage		New port forward				÷
VPN Service		New porcioiwald				
🄹 Equipment Manage	N	ame New port forward				
🕒 Logout	Prot	ocol TCP+UDP	~			
	Internal IP add	ress	~			
	Internal	port				
	External	port				
					ADD	
				I		
					SAVE & APPLY	
View wan port IP Ac	ddress:					
<ul> <li>Routing Status</li> </ul>	Network Configuration					
Network Setting	WAN Configuration					
WAN Setting	Status Uptime	: 0h 0m 23s ddress: 5C:B1:5F:81:07:EB				
LAN Setting	eth0 TX: 1.8	51 KB (113 Pkts.) 9 KB (11 Pkts.)				
DHCP Setting	IPv4: 1	92.168.2.195/24				
Wireless	Protocol DHCP address	s <b>v</b>				
Routing Setting						
Application Manage					SAVE & APPLY	
E VPN Service						

Through the wan port ip: remote port number, you can access the port number opened by the port forwarding device just configured.(access 192.168.2.195:500 through 172.31.1.104:80)



← → C ▲ 不安全 | 192.168.2.195:500/cgi-bin/luci

☞ ☆ \varTheta :

Language : English v	
Authorization Required	
Password	
Login	

### 3.4 Intranet penetration (frp)

Frp uses machines behind the internal network or firewall to provide http or https services in multiple external network environments. For http and https services, it supports domain-based virtual hosts and supports custom domain name binding, so that multiple domain names share a port 80; Use machines behind the internal network or firewall to provide tcp and udp services in the external network environment, such as accessing the host in the company's internal network environment through ssh at home.

Frp mainly realizes the functions: the external network accesses the internal network machine through ssh; the external network accesses the internal network machine through the public network address plus the port number and the port forwarded by frp; the custom binding domain name accesses the internal network web service.

The prerequisite for configintranet penetration is to ensure that the router can access the Internet. If the router cannot access the Internet, the intranet penetration cannot be done. Navigation bar "Equipment Manage"-"diagnosis"; and disable the firewall, navigation bar "routing settings"-"firewall".

Ping Google on the diagnostic page. If it can ping, it means that the device can go online.

♠ Routing Status	Diagnostics
Network Setting	Network Utilities
🛱 Routing Setting	
Application Manage	Google vwww.google.com PING
E VPN Service	
🏡 Equipment Manage	Copyright @2017-2020 Seriallink inc. All rights reserved
Diagnosis	
— Date Time	
Language Setting	
Modify Password	
Update Firmware	



### Disable firewall:

ń	Routing Status	Firewall	
0	Network Setting		
۲	Routing Setting	Firewall Disable	
	Routing Table		
	Firewall	SAVE & APPI	
	Port Mapping		
	DMZ		
a	Application Manage	Copyright @2017-2020 Seriallink inc. All rights reserved.	

Preparation before configuration:

- (1) One public network server.
- (2) One router (a router that supports frp, that is, 1 intranet server).
- (3) One domain name is bound to the public network server.
- Frp client configuration is as follows:

(1) The client needs to add the server configuration first to connect to the server, the navigation bar "Application Manage"-"Frpc", select the Servers, there is an empty server by default, you can click to modify it directly, or You can directly delete and add one yourself.

Routing Status	Settings Rule	es Servers				
<ul> <li>Routing Setting</li> </ul>	Frpc - Frps Se	ervers				
Application Manage	Alias	Server Addr	Server Port	TCP Mux	Sort	
- Dynamic DNS	None	0.0.0.0	7000	True	× ×	EDIT
E VPN Service	ADD					
🔹 Equipment Manage	_					
🕒 Logout						SAVE & APPL
			Copyright ©201	7-2020 Seriallink inc. Al	l rights reserved	



Routing Status      Network Setting      Routing Setting	Settings Rules Ser	vers				
Application Manage Dynamic DNS	Alias	Server Addr	Server Port	TCP Mux	Sort	
Frpc     VPN Service     Equipment Manage	ADD	Th	is section contains no values yet			
🕒 Logout					SAVE &	APPLY
		Copyrig	nt ©2017-2020 Seriallink inc. All rig	ghts reserved.		

(2) After clicking "Add" or "Modify", a page for Edit-Frps Server will pop up. Configure it according to the settings of the server. After the configuration is complete, click "SAVE & APPLY".

Alias: Customize a frp server alias, which will be used when using the server.

Server addr, Server port, Token, Tcp mux Must be consistent with the server.

<ul> <li>Routing Status</li> </ul>	Settings Bules Servers			
Network Setting	octangs hales octaves			
Routing Setting	Frpc - Edit Frps Server			
Application Manage	Alias	frps		
Dynamic DNS				
Frpc	Server addr			
VPN Service	Server port	1000		
🔹 Equipment Manage	Token		2 2	
🕒 Logout	TCP mux	<b>v</b>		
	BACK TO OVERVIEW	Copyright ©2017-2020	) Seriallink inc. All rights reserved.	SAVE & APPLY

(3) After successful configuration, there will be a server, click "SAVE & APPLY" to let the server run.



Routing Status     Network Setting	Settings Rul	es Servers					
Routing Setting	Frpc - Frps S	ervers					
Application Manage	Alias	Server Addr	Server Port	TCP Mux	Sort		
Dynamic DNS	frps			True	^ ×	EDIT DELETE	
VPN Service	ADD						
🔹 Equipment Manage							
🕒 Logout			Copyright @2017	2020 Seriallink inc. All	rights reserved.	SAVE & APPLY	

(4) Next, enter the "Settings" page of "Intranet Penetration", start the frpc client, and configure according to the following figure. After the configuration is completed, click "Save & Apply", and the "Settings" page will appear after the configuration is completed The service is running", which proves that the frp client has been started.

Enabled: Enable frpc service.

Server: Fill in the server alias you just customized.

Run daemon as user: One group is the default choice, you can choose according to your needs.

Enable logging: Check according to your needs.

Click "SAVE & APPLY" after configuration.

<ul> <li>Routing Status</li> </ul>	Frp is a fast reverse proxy to help you expose a local server behind a NAT or firewall to the internet.	
Network Setting	Not Running	
🛱 Routing Setting	General Options Advanced Options	
Application Manage     Dynamic DNS	Enabled 🗹	
Frpc	Client file /tmp/etc/frpc/frpc	
VPN Service	Version: 0.25.1	
🏡 Equipment Manage	Server frps 🗸	
🗗 Logout	Run daemon as user default 👻	
	Enable logging	
	SAVE & A	PPLY

The "Setting" page shows that it is running, indicating that frpc is started.



puting Status     Settings     Rules     Servers       etwork Setting     Frpc - Common Settings       puting Setting     Frpc - Common Settings       plication Manage     Running       namic DNS     Running
etwork Setting     Frpc - Common Settings       plication Manage     Frp is a fast reverse proxy to help you expose a local server behind a NAT or firewall to the internet.       namic DNS     Running
Frpc - Common Settings       plication Manage       namic DNS
plication Manage namic DNS
General Uptions Advanced Uptions
vice Enabled V
nt Manage
Client lie /tmp/etc/rtpc
Server frps ~
Run daemon as user default 🗸
Enable logging

(5) Next, enter the "Rules" page of "Intranet Penetration". The page itself has a rule. You can modify this rule or delete this rule and add a new rule. The final effect of the two methods is the same. Choose to modify the original rules or add new rules.

<ul> <li>Routing Status</li> </ul>	Satting Rule							
Network Setting	Settings Nule	s pervers	e)					
📋 Routing Setting	Frpc - Proxy R	ules						
Application Manage	Disabled	Name	Туре	Local IP	Local Port	Remote Port	Sort	
— Dynamic DNS		eeh	TCP	127.0.0.1	22	6000		
		3311	1 GF	121.0.0.1	22	0000		
VPN Service	ADD							
C L								
🗗 Logout								SAVE & APPLY
				Copyright	©2017-2020 Seria	llink inc. All rights rese	rved.	

(6) After adding, a "Edit Proxy Rules" page will pop up, and there will be different protocol types, and different protocol types implement different functions.



<ul> <li>Routing Status</li> </ul>	Settings Rules Servers	
Network Setting		
Routing Setting	Frpc - Edit Proxy Rule	
Application Manage     Dynamic DNS	Disabled	
Frpc	Proxy Name	
VPN Service	Туре тср ч	
🔹 Equipment Manage	Local IP UDP HTTP	
🕒 Logout	Local port STCP	
	Remote port	
	Use encryption	
	Use compression	
	BACK TO OVERVIEW SAVE & APPLY	

### 3.4.1 Add TCP proxy protocol

The TCP protocol supports ssh connection, and also supports forwarding the page port (usually port 80), and the page of the local device can be accessed through the public network: remote port.

On the "Edit Proxy Rules" page, configure as shown below according to your needs. After the configuration is complete, click "Save & Apply" and you will return to the "Proxy Rules" page. There will be an extra rule on the page. Click "Save &" again. Apply" to make the rule effective, and finally through the public network ip: port number (format: 111.111.111:6001 where 111.111.111 is the public network address) to access the local port opened by the local device. You can add multiple tcp rules, just ensure that the remote port is not the same. If the remote port is the same as the previous setting, the latest one will overwrite the previous one, and the previous rule will not take effect.

Disable: Check it to disable this rule.

Proxy Name: Customize a Proxy Name.

Type: Choose TCP protocol.

Local IP: Fill in the IP of the device to be accessed remotely. The ip is mainly the ip address of the local device or the ip address assigned by the lan port for the device connected to it.

Local port: Fill in which port to remotely access the device.

Remote port: Fill in a port number that is not used by the server, and you can access the Local port opened by the internal device through the public network ip and this remote port number.

Use encryption, Use compression: These two are checked according to your needs.

Click "SAVE & APPLY" after configuration.



Notwork Sotting				
Network Setting				
Routing Setting	pc - Edit Proxy Rule			
Application Manage	Disabled	0		
Dynamic DNS	Proxy Name	tcp1		
VPN Service	Туре	тср	~	
Equipment Manage	Local IP	172.31.1.104		
Logout	Local port	80		
	Remote port	6001		
	Use encryption	0		
	Use compression	0		

After successfully adding a new rule, click "SAVE & APPLY" to make the rule effective.

<ul> <li>Routing Status</li> </ul>	Sattings Pul	oc Sorvor							
Network Setting	Settings Ind		2						
Routing Setting	Frpc - Proxy I	Rules							
Application Manage	Disabled	Name	Туре	Local IP	Local Port	Remote Port	Sort		
Dynamic DNS									-
Frpc		tcp1	TCP	172.31.1.104	80	6001	<b>^ *</b>	EDIT DELETE	
E VPN Service	ADD								_
🔉 Equipment Manage									
🕒 Logout								SAVE & A	APP

Through the public network ip: remote port, you can access the corresponding device's open port on the public network (that is, 111.111.111.111:6001 to access 172.31.1.104:80)

Language : English V	
Autorization negation	
Password	
Login	
	Language : English v Authorization Required Password

You can add multiple tcp rules, and you need to ensure that the remote port number is not repeated with the previous setting. If it is repeated, the previous rules will be overwritten and the previous rules will



not take effect. You can connect to the device through ssh, the same is the public network ip: remote port number (111.111.111.6000).

### 3.4.2 Add STCP proxy protocol

(1) STCP needs to configure the client and access terminal. Among them, 192.168.2.99 (the device connected to the lan port) is used as the client, and the PC is the access terminal. The access terminal can access the client by binding the local IP and port.

Disable: Check it to disable this rule.

Proxy Name: Customize a Proxy Name.

Type: Choose STCP protocol.

Local IP: Fill in the IP of the device to be accessed remotely. The ip is mainly the ip address of the local device or the ip address assigned by the lan port for the device connected to it.

Local port: Fill in which port to remotely access the device.

SK: Set a password, which is needed when the client accesses it.

Use encryption, Use compression: These two are checked according to your needs.

Role, Server name, Bind addr, Bind port: These four parameters do not need to be filled in as the client. Click "SAVE & APPLY" after configuration.

Routing Setting	Frpc - Edit Proxy Rule		
Application Manage	Disabled		
Dynamic DNS Frpc	Proxy Name	stcp1	
VPN Service	Туре	STCP 🗸	
Equipment Manage	Local IP	172.31.1.104	
Logout	Local port	4001	
	Use encryption	0	
	Use compression		
	Role		
	Server name		
	SK	slk100200	đ
	Bind addr		]
	Bind port		

A new rule is successfully generated, click "Save & Apply" to make the rule effective.



Frpc       Disabled       Name       Type       Local IP       Local Port       Remote Port       Sort         Dynamic DNS       Image: Construct of the pink of the	Disabled       Name       Type       Local IP       Local Port       Remote Port       Sort         namic DNS	buting Setting	Frpc - Proxy Rules	S					
Application Manage       Disabled       Name       Type       Local IP       Local Port       Remote Port       Sort         Dynamic DNS       Image: Constraint of the point in the point i	Disabled     Name     Type     Local IP     Local Port     Remote Port     Sort       namic DNS     tcp1     TCP     172.31.1.104     80     6001     ^     ¥     EDIT     DELETE       N Service     stcp1     STCP     172.31.1.104     4001     Not set     EDIT     DELETE       uipment Manage     ADD     ADD     Image: Stop 1     Stop 1     Stop 1     Stop 1     Stop 1								
Dynamic DNS         Frpc       tcp1       TCP       172.31.1.104       80       6001       A       Y       EDIT       DELETE         VPN Service       Image: Stcp1       STCP       172.31.1.104       4001       Not set       EDIT       DELETE	namic DNS c tcp1 TCP 172.31.1.104 80 6001 ^ V EDIT DELETE N Service uipment Manage ADD	plication Manage	Disabled Na	ame Type	Local IP	Local Port	Remote Port	Sort	
VPN Service Equipment Manage	N Service Stcp1 STCP 172.31.1.104 4001 Not set EDIT DELETE	namic DNS	🗆 tej	cp1 TCP	172.31.1.104	80	6001	~ <b>~</b>	EDIT DELETE
Equipment Manage	uipment Manage	PN Service			170 01 1 104	4001	Neterat		
	aout ADD	uipment Manage	stc	tepi STCP	172.31.1.104	4001	NOT SET		EDIT
Logout		ogout	ADD						
	SAVE & /								SAVE & APF

If the PC wants to be the access terminal to access the router's downstream equipment, it needs to be a frp client, and it is also the stcp protocol, but it must set the visitor role and bind the local address and port. Windows frp files can be downloaded from the company's official website. After downloading, open the frpc\_602.ini configuration file for configuration.

名称 ^	修改日期	类型	大小
<b>III</b> frpc.exe	2020-09-03 9:56	应用程序	9,962 KB
📓 frpc.ini	2020-09-07 12:52	配置设置	2 KB
🚮 frpc_602.ini	2020-12-08 17:07	配置设置	1 KB
📓 frpc_full.ini	2019-03-15 17:10	配置设置	7 KB
Frps.exe	2019-03-15 17:08	应用程序	10,694 KB
🔄 frps.ini	2019-03-15 17:10	配置设置	1 KB
📓 frps_full.ini	2019-03-15 17:10	配置设置	3 KB
LICENSE	2019-03-15 17:10	文件	12 KB



🧊 frpc_602.ini - 记事本	<u> </u>	
文件(E)编辑(E)格式(Q)查看(V)帮助(H)		
#Connect to the server		29
[common]		
#Server public IP address		
server_addr=		
#Server port		
server_port=5443	Consistant with public notwork conver	
#The server provides a token for verification	Consistent with public network server	
token=slk100200		
#Connect to the server through the tcp protocol		
protocol=tcp		
#Consistent with server configuration		
tcp_mux=true		
#Prevent exit after a connection failure		
login_fail_exit=false		
#Connect client 1-192.168.2.99		
[stcp1 visitor]		
#Select STCP protocol		
type = stcp fill in stcp		
#As a visitor		
role=visitor the role of the visitor should	be configured as a visitor	
#Agent name of client 1		
server_name=stcp1 fill in the Proxy Nam	e just set	
#Same as the SK of client 1		
sk=slk100200 fill in the SK set in the c	lient section just now	
#Bind the local address and port to access client 1		
bind_addr=127.0.0.1	v binding local in and part	
bind_port=6006 access the client b	y binding local ip and port	





Use the shortcut key "win+R" and enter "cmd" to quickly open the cmd command line.

🖾 运行		×	
0	Windows 将根据你所输入的名称,为你打开相应的程序、 文件夹、文档或 Internet 资源。		
打开(0):	cmd ~		
	● 使用管理权限创建此任务。		
	确定 取消 浏览( <u>B</u> )		

Enter in the command line: "cd C:\Users\Administrator\Desktop\frp\_0.25.1\_windows\_amd64", then enter "frpc.exe -c frpc\_602.ini".

國 管理员: C:\Windows\system32\cmd.exe			×
Microsoft Windows [版本 10.0.19041.264] (c) 2020 Microsoft Corporation. 保留所有权利。			
C:\Users\Administrator> C:\Users\Administrator} C:\Users\Administrator}cd C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64			
C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64>_			
画 选择管理员: C:\Windows\system32\cmd.exe - frpc.exe -c frpc_602.ini	-		×
Microsoft Windows [版本 10.0.19041.264] (c) 2020 Microsoft Corporation. 保留所有权利。			
C:\Users\Administrator> C:\Users\Administrator> C:\Users\Administrator>cd C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64			
C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64 frpc.exe -c frpc_602.ini 2020/12/17 15:02:04 [I] [service.go:221] login to server success, get run ia [c7p44136f74c7fa0], server u 2020/12/17 15:02:04 [I] [visitor manager.go:69] [stcp] visitor] start visitor success	dp por	t [0]	

#### Access the client according to the local address and port bound by frpc\_602.ini



K SSCOM V5.13.1 Serial/Net data debugger,Author:Tintin,2618058@qq.com	<u>(200</u> ))		×
PORT COM_Settings Display Send_Data Multi_Strings Tools Help 联系作者 PCB打样			
[18:20:14.047]0UT→◇ ["Status": "Get", "Name": "4GIP"] [18:20:14.099]IN↔◆ ["Status": "Get", "Name": "4GIP"] [18:20:14.503]0UT→◇ ["Status": "Get", "Name": "4GIP"] [18:20:14.935]0UT→◇ ["Status": "Get", "Name": "4GIP"] [18:20:14.991]IN↔◆ ["Status": "Get", "Name": "4GIP"] [18:20:18.480]0UT→◇ ["Status": "Get", "Name": "4GIP"] [18:20:18.538]IN↔ ["Status": "Get", "Name": "4GIP"]			^
ClearData OpenFile Stop ClearSend OnTop	✓ English Save(	Config	EXT
ComNum TCPClient 🗾 🗖 HEXShow SaveData 🗖 ReceivedToFile 🗖 SendHEX 🗖 SendBvery	:500 ms/Tim	AddC:	rLf 🦼
Remot 127.0.0.1 6006 Connect 🔽 Show Time and Packe OverTime: 20 ms No 1 BytesTo 末尾 🗸 Ver	ifyNone	•	
Local 192.168.100.66 💌 777 Disconr [["Status":"Get", "Name":"4GIP"]			~
为了更好地发展SSCOM软件 请您注册嘉立创F结尾客户			~

(2) If there are two routers, one router wants to remotely access the other router or the downstream equipment of the other router, then one will be the stcp access terminal and the other will be the stcp client. The configuration is as follows

① Configure the client

Add new rule

Disable: Check it to disable this rule.

Proxy Name: Customize a Proxy Name.

Type: Choose STCP protocol.

Local IP: Fill in the IP of the device to be accessed remotely. The ip is mainly the ip address of the local device or the ip address assigned by the lan port for the device connected to it.

Local port: Fill in which port to remotely access the device.

SK: Set a password, which is needed when the client accesses it.

Use encryption, Use compression: These two are checked according to your needs.

Role, Server name, Bind addr, Bind port: These four parameters do not need to be filled in as the client. Click "SAVE & APPLY" after configuration.



<ul> <li>Routing Status</li> </ul>	Cattings Bulas Capitare				
Network Setting	Settings Rules Servers				
Routing Setting	Frpc - Edit Proxy Rule				
Application Manage     Dynamic DNS	Disabled				
Frpc	Proxy Name	stcp1			
VPN Service	Туре	STCP	~		
🚓 Equipment Manage	Local IP	172.31.1.104			
🗗 Logout	Local port	4001			
	Use encryption				
	Use compression				
	Role				
	Server name				
	SK	slk100200	2		
	Bind addr				
	Bind port				
	<u></u>				
	BACK TO OVERVIEW			SAVE & AF	PPLY

A new rule is successfully generated, click "Save & Apply" to make the rule effective.

Routing Status	Settings Dul	oc Sorvor	c						
Network Setting	Settings Ito	es derver	a.						
Routing Setting	Frpc - Proxy I	Rules							
Application Manage	Disabled	Name	Туре	Local IP	Local Port	Remote Port	Sort		
Dynamic DNS									
Frpc		tcp 1	TCP	172.31.1.104	80	6001	<b>^</b>	EDIT	DELETE
VPN Service		stcp1	STCP	172.31.1.104	4001	Not set		EDIT	DELETE
Equipment Manage									
Logout	ADD								

(2) Configure access point

The binding address can be the ip address of your own machine, or the ip assigned by the lan port to the connected device.

Disable: Check it to disable this rule.

Proxy Name: Customize a Proxy Name.

Type: Choose STCP protocol.

Local IP, Local port: These two do not need to be filled in as the access point.

Role: The role of the visitor should be filled in "visitor".



Server name: "Proxy Name" set by the client.

SK: Fill in the "SK" set by the client to be consistent

Bind addr, Bind port: Bind the ip and port of the machine, the client can be accessed through this ip and port.

Use encryption,Use compression: These two are checked according to your needs. Click "SAVE & APPLY" after configuration.

Routing Status	tinge Bules Convers			
Network Setting	ungs Rules Servers			
T Routing Setting	c - Edit Proxy Rule			
Application Manage	Disabled			
Dynamic DNS Frpc	Proxy Name	stcp1_visitor		
E VPN Service	Туре	STCP	~	
🏡 Equipment Manage	Local IP			
Cogout	Local port			
	Use encryption			
	Use compression			
	Role	visitor		
	Server name	stcp1		
	SK		1 Alexandre	
	Bind addr	192.168.2.20		
	Bind port	6007		

A new rule is successfully generated, click "Save & Apply" to make the rule effective.

<ul> <li>Routing Status</li> </ul>	Sottingo Bul	a Servere						
Network Setting	Settings	es dervers						
🛱 Routing Setting	Frpc - Proxy F	lules						
Application Manage	Disabled	Name	Туре	Local IP	Local Port	Remote Port	Sort	
Dynamic DNS		0. 1014 1010			-	ANNON - M		
Frpc		stcp1_visitor	STCP	?	?	Not set	^ ×	EDIT DELETE
VPN Service	ADD							
🔹 Equipment Manage								
🗗 Logout								SAVE & APP

Access the client through the bound ip address and bound port of the access terminal.



SSCOM V5.13.1 Serial/Net data d	ebugger,Author:Tintin,2618058@qq.com	- 1	o ×	
PORT COM_Settings Display Ser	id_Data Multi_Strings Tools Help 联系作者 PCB打样			
<pre>[18:19:16.607]0UT→◇{"Status": "Get", [18:19:16.708]IN←◆{"Status": "Get", [18:19:17.190]0UT→◇{"Status": "Get", [18:19:17.296]IN←◆{"Status": "Get", [18:19:17.639]0UT→◇{"Status": "Get", [18:19:17.720]IN←◆{"Status": "Get",</pre>	"Name":"4GIP"} Name":"4GIP"} Name":"4GIP"} Name":"4GIP"} Name":"4GIP"} Name":"4GIP"}			
3				4
ClearData OpenFile	SendFile Stop ClearSend OnTop	🔽 English SaveCor	fig EXT	_
ComNum TCPClient 💌	HEXShow ReceivedToFile SendHEX SendEvery	y: 500 ms/Tim	AddCrLf	2
Lemot 192.168.2.20 6007 Connect	▼ Show Time and Packe OverTime: 20 ms No 1 BytesTo 末尾 ▼ Ver	rifyNone	-	
Local 192.168.100.66 💌 777 Disconn	[ <sup>{</sup> "Status":"Get","Name":"4GIP"}			0
为了更好地发展SSCOM软件 请您注册嘉立创『结尾客户				0

### 3.4.3 Add UDP proxy protocol

The UDP protocol is used to transmit a large amount of data. The port of the connected device needs to support the udp protocol. Open the port that supports the udp protocol to the public network, and then data can be transmitted through the public network plus the remote port number. Multiple udp protocol rules can be configured.

Disable: Check it to disable this rule.

Proxy Name: Customize a Proxy Name.

Type: Choose UDP protocol.

Local IP: Fill in the IP of the device to be accessed remotely. The ip is mainly the ip address of the local device or the ip address assigned by the lan port for the device connected to it.

Local port: Fill in which port to remotely access the device.

Remote port: Fill in a port number that is not used by the server, and you can access the Local port opened by the internal device through the public network ip and this remote port number.

Use encryption, Use compression: These two are checked according to your needs.

Click "SAVE & APPLY" after configuration.



Network Setting	Settings Rules Servers			
Routing Setting	Frpc - Edit Proxy Rule			
Application Manage	Disabled	0		
Dynamic DNS Frpc	Proxy Name	udp1		
VPN Service	Туре	UDP	~	
Equipment Manage	Local IP	172.31.1.100		
Logout	Local port	4001		
	Remote port	606		
	Use encryption	0		
	Use compression	0		

A new rule is successfully generated, click "Save & Apply" to make the rule effective.

Routing Status	Settings Bul	es Server	c						
Network Setting	octangs nu		9						
] Routing Setting	Frpc - Proxy I	Rules							
Application Manage	Disabled	Name	Туре	Local IP	Local Port	Remote Port	Sort		
Dynamic DNS									
Frpc		udp1	UDP	172.31.1.100	4001	606	<b>^ *</b>	EDIT	DELETE
E VPN Service	ADD								
Equipment Manage									
- Logout									SAVE & AP
									GATEG

Select the udp protocol, use the public network ip and remote port to access the router's downstream equipment.



SSCO	M V5.13.1	串口/网	络数据	调试器,作者	:大虾丁丁	,26180	)58@qq.co	m. QQ群:	5250244	49(最新版本	(4			×
通讯端口	串口设置	显示	发送	多字符串	小工具	帮助	联系作者	PCB打样	5					
[10:00:26. [10:00:26. [10:00:26. [10:00:27. [10:00:27.	446]发→◇: 469]收←◆ 766]发→◇: 200]发→◇: 230]收←◆	fdospjg fdospjg fdospjg fdospjg fdospjg fdospjg	fsddgen fsddgen fsddgen fsddgen fsddgen fsddgen	rgD rg rgD rgD rg										
清除窗口	打开文件						发	送文件	止清发	送区 [ ]	员前 □ E	English <u>保</u> 存	参数	扩展 -
端口号 1003	P			🛨 🗆 нех	堀示 _ (	呆存数排	目 接收	数据到文件	<b>厂</b> HEX发	送厂定时	拔送: 1	ms/次	「加回	<u> 车换行</u>
远程		606		· 」 □ 加	时间戳和	分包显示	<b>心</b> 超时时间	]: 20 ms	第 1 字1	节 至 末尾	▼ 加校验	None	•	100
本地 [192.	168.100.66	<b>•</b> 111	_ 助7	# [tdosp]	)gfsddger	g								<u></u>
为了更好地 请您注册嘉	发展SSCOM的 立创F结尾客	沪	发;	ž										~

### 3.4.4 Add HTTP proxy protocol

For http and https services, it supports domain-based virtual hosts, and supports custom domain name binding, so that multiple domain names share a port 80, and access intranet web pages through custom domain names. Multiple http rules can be configured, and can be accessed directly through a custom domain name. After the configuration is complete, you can access the corresponding web page through the custom domain name plus the http penetration port provided by the server (vhost\_http\_port).

Disable: Check it to disable this rule.

Proxy Name: Customize a Proxy Name.

Type: Choose HTTP protocol.

Local IP: Fill in the IP of the device to be accessed remotely. The ip is mainly the ip address of the local device or the ip address assigned by the lan port for the device connected to it.

Local port: Fill in the web port number of the device

Use encryption,Use compression, HTTP user, HTTP password: These four are checked according to your needs.

Click "SAVE & APPLY" after configuration.



] Routing Setting	- Luit i loxy huic		
Application Manage	Disabled	0	
— Dynamic DNS	Proxy Name	http1	
E VPN Service	Туре	нттр 👻	
Equipment Manage	Local IP	172.31.1.100	
Logout	Local port	80	
	Use encryption		
	Use compression		
	HTTP user		
	HTTP password		
	Subdomain		
	Custom domains	open1.frp1.sifangtx.com	

A new rule is successfully generated, click "Save & Apply" to make the rule effective.

<ul> <li>Routing Status</li> </ul>	Settings Bul	oc Sorvor	c						
Network Setting			3						
Routing Setting	Frpc - Proxy I	Rules							
Application Manage	Disabled	Name	Туре	Local IP	Local Port	Remote Port	Sort		
Dynamic DNS									
Frpc		http1	HTTP	172.31.1.100	80	Not set	^ ×	EDIT	DELETE
VPN Service	ADD								
😘 Equipment Manage	_								
🕒 Logout									SAVE & /

Browser login openwrt1.frp1.sifangtx.com:8080 to enter the client routing management page, where 8080 port is the intranet penetration port provided by the server (ie vhost\_http\_port), and openwrt1.frp1.hytera.com is a custom domain name.Multiple http rules can be configured in this way, and the custom domain names need not be the same.

# **4 VPN (Virtual Private Network)**

When configuring VPN, you need to disable the firewall first. No matter which VPN you use, you need to disable the firewall first.



♠ Routing Status	Firewall		
Network Setting			
Routing Setting		Firewall Disable 🗸	
Routing Table			
Firewall			SAVE & APPLY
Port Mapping			
DMZ			
Application Manage		Copyright ©2017-2020 Senaillink Inc. All rights reserved.	

# 4.1 PPTP VPN

In the navigation bar "Virtual Private Network"-"PPTP VPN", select Enable, fill in the server address, fill in the user name and password according to the server settings, and click "Save & Apply".

<ul> <li>Routing Status</li> </ul>	PPTP Client								
Network Setting	Configurable PPTP access to VPN.								
Routing Setting	Status	Uptime: 0h 0m 18s							
Application Manage	pptp-pptp TX:116.08 (7 Pkts.) IPv4: 192.168.0.234/32								
E VPN Service	Enable	<b>v</b>							
PPTP VPN									
L2TP VPN	Server Address								
OpenVPN	Username	slk							
🆚 Equipment Manage	Password		<i>₽</i>						
🕒 Logout	Metric	8							
		Configure the priority of this network	¢						
				SAVE & APPLY					
		Copyright @2017-2020 Serialli	ink inc. All rights reserved.						

After the connection is successful, an address assigned by the server will appear in the status bar.

# 4.2 L2TP VPN

In the navigation bar "Virtual Private Network"-"L2TP VPN", select Enable, fill in the user name and password according to the server settings, and click "Save & Apply".



<ul> <li>Routing Status</li> </ul>	L2TP Client				
Network Setting	Configurable L2TP access to VPN.				
Routing Setting	Applying changes				
Application Manage	/etc/config/network				
VPN Service     PPTP VPN	Status	<b>RX</b> : 0.00 B (0 Pkts.) I2tp-I2tp <b>TX</b> : 0.00 B (0 Pkts.)		1	
DpenVPN	Enable	2			
🔹 Equipment Manage	Server Address				
🕒 Logout	Username	slk			
	Password		1		
	Metric	9			
		O Configure the priority of this network			

After the connection is successful, an address assigned by the server will appear in the status bar.

A	Routing Status	L2TP Client		
3	Network Setting	Configurable L2TP access to VPN.		
Ċ	Routing Setting	Status	Uptime: 0h 0m 7s	
a	Application Manage		I2tp-I2tp TX: 54.00 B (3 Pkts.)	
=	VPN Service	Enable	2	
	PPTP VPN			
-	- L2TP VPN	Server Address	106.55.45.169	
	OpenVPN	Username	slk1	
4	Equipment Manage	Password		8
B	Logout	Metric	9	
			Configure the priority of this network	
				SAVE & APPLY

# 4.3 OPENVPN

Navigation bar "Virtual Private Network"-"openvpn",

Choose tun or tap as you are using on the server.

Connecting to a TCP or UDP server depends on your server config.

If your server IP is 123.123.123.123, 1194 as remote port ,then fill port with 1194 and complete remote with 123.123.123.123.123 1194

Separately upload the corresponding files including ca.crt ,client.crt and client.key

Click "SAVE & APPLY" after all configurations are consistent with the server



Routing Status Ope	enVPN Settings			
Network Setting				
Routing Setting	eneral Settings Advanced Set	ttings		
Application Manage	Status	Uptime: 0h 0m 36s MAC-Address: 00:00:00:00:00:00		
VPN Service		tun0 TX: 464.00 B (6 Pkts.)		
PTP VPN	Enchia	• • • • • • • • • • • • • • • • • • • •		
L2TP VPN	Enable			
penVPN	dev	tun	~	
Equipment Manage		I tun/tap device		
oqout	proto	udp	~	
Logout		O Use protocol		
	port	1194		
		TCP/UDP port # for both local and remo	ote	
	remote	1194		
		• Remote host name or ip address		
	са	8		
		Oploaded File (1.16 KB)		
	cert	Ø		
	Gert	Uploaded File (4.37 KB)		
	·····	Local certificate		
	key	Uploaded File (1.66 KB)		
		O Local private key		

Check relink to indicate that you can disconnect and reconnect the server after restoring the networ. Other configurations are supposed to consistent with the server configuration.

verb is the log output verbosity, the higher the verbosity, the more detailed the log content.

We disable comp\_lzo by default, if you configure it as yes on your server, choose yes.

Selet server in option remote\_cert\_tls.

If you want to communicate between clients, click client\_to\_client. SAVE & APPLY.



▲ Routing Status	OpenVPN Settings		
Network Setting	<b>1</b>		
Routing Setting	General Settings Advanced Set	ettings	
Application Manage	relink		
E VPN Service		Auto connect server	
PPTP VPN	verb	3 V Q Set output verbosity	
L2TP VPN	auth	SH4512	
OpenVPN		HMAC authentication for packets	
<ul> <li>Equipment Manage</li> <li>Logout</li> </ul>	cipher	AES-256-CBC	
		Encryption cipher for packets	
	complzo	o Set Comp_Izo	
	remote_cert_tls	server  Require explicit key usage on certificate	
	nobind	<ul> <li>Do not bind to local address and port</li> </ul>	
	client	Configure client mode	
	client_to_client		
		WAHOW CHENT-TO-CHENT TRATTIC	
		SAVE & APPLY	

After the connection is successful, an address assigned by the server will appear in the status bar.



<ul> <li>Routing Status</li> </ul>	OpenVPN Settings	
Network Setting		
🗂 Routing Setting	General Settings Advanced Settings	
Application Manage	Status Uptime: 0h 1m 38s MAC-Address: 00:00:00:00:00:00	
VPN Service	tun0 TX: 1.09 KB (13 PKts.)	
- PPTP VPN - L2TP VPN	Enable 🗹	
OpenVPN	dev tun 🗸	
🚓 Equipment Manage	© tun/tap device	
🕒 Logout	proto udp ~	
	Use protocol	
	port 1194	
	TCP/UDP port # for both local and remote	
	remote 1194	
	Remote host name or ip address	
	ca Uploaded File (1.16 KB)	
	Certificate authority	
	Cert Uploaded File (4.37 KB)	
	Local certificate	
	key Uploaded File (1.66 КВ)	
	Local private key	
	SAVE	E& APPLY

# **5 Basic Management (Device Management)**

# 5.1 Date Time

The default time synchronization is enabled. If necessary, you can change the NTP server to synchronize the time of the server.

Navigation bar "Equipment Manage"-"Date Time"



♠ Route Status	NTP time server	
Network Settings	After the wireless gateway is powered off, the date and time settings are not saved. Enable the Sync from network function to keep the date and time current.	
🛱 Route Settings		
n Service Manage	Synchronize browser time	
E VPN Service	Local Time 2023-06-06 10:22:06 SYNC WITH BROWSER	
🛠 System	Timezone Asia/Shanghai 🗸	
Date Time		
Language Setting		
Modify Password	Time Synchronization	
Backup File	Enable NTP client 🗹	
Update Firmware		
Factory Reset	NTP server 0.lede.pool.ntp.org	
Reboot		
🗗 Logout		
	SAVE & APPLY	

# 5.2 Language Setting

Change the language displayed on the page according to your needs. You can choose English or Chinese and change it in the navigation bar "Device Management"-"Language Settings".

▲ Route Status	Language Setting
Network Settings	
🗂 Route Settings	Language Setting
n Service Manage	Language English V
VPN Service	
🛠 System	
Date Time	SAVE & APPLY
- Language Setting	

# 5.3 Backup File

The backup function can be used to generate device configuration files and download them locally.

▲ Route Status	Backup File
Network Settings	
📋 Route Settings	Backup
A Service Manage     A	Click "Generate archive" to download a tar archive of the current configuration files.
VPN Service	Download backup: GENERATE ARCHIVE
🛠 System	nescore
Date Time	
Language Setting	Restore backup: 选择文件 未选择任何文件 UPLOAD ARCHIVE
Modify Password	Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.
Backup File	



Backup File

The downloaded configuration file is as follows.

下载	D	Q	 $\Rightarrow$
interfacture backup-SLK-2023-03-21.tar.gz 封开文件			

The recovery function restores device configuration through local configuration files, and during the recovery process, the device will restart.

Backup		
Click "Gene	erate archive" to downloa	ad a tar archive of the current configuration files.
	Download backup:	GENERATE ARCHIVE
Restore		
To restore	configuration files, you c	an upload a previously generated backup archive here.
	Restore backup:	选择文件 backup-SLK23-06-06.tar.gz UPLOAD ARCHIVE
	(	Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

### 5.4 Upgrade firmware

Navigation bar "Equipment Manage"- "Upgrade Firmware", Uncheck "keep setting", select the file and click "UPDATE". After uploading, a page with MD5 verification code will appear. Click "Execute" to upgrade. The upgrade will take a certain amount of time, about 1~ 2 minutes, after the upgrade is complete, log in to the page again through "192.168.2.1".

▲ Route Status	Flash operations
Network Settings	
🛱 Route Settings	Flash new firmware image
n Service Manage	Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires a compatible firmware image).
E VPN Service	Keep settings:
System	Image: 选择文件 未选择任何文件 FLASH IMAGE
Language Setting Modify Password Backup File Update Firmware	Copyright ©2013-2022 Seriallink Inc, All Rights Reserved.
Route Status	Flash Firmware - Verify
Network Settings	The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
🛱 Route Settings	Click "Proceed" below to start the flash procedure.
α Service Manage	Checksum MD5: 634245738-7944:b980c9a0ba0b3df7 SHA256: a301978ec85a4f2ada39c1e741d09e491218a842bfc8ac5140e6a889038a064 Size: 7.50 MB (41.60 MB available)
E VPN Service	Configuration files will be kept.
Date Time	



# 5.5 Factory Reset

Factory reset is generally when the device fails to enter the device page, or there are many function settings, when you want to reset, you can restore the factory settings, the navigation bar "Equipment Manage"-"Factory Reset", Click "Execute Reset" to restore the device to factory defaults.

▲ Route Status	Factory Reset
Network Settings	
🛱 Route Settings	Reset to defaults PERFORM RESET
n Service Manage	
VPN Service	
🛠 System	
— Date Time	Copyright ©2013-2022 Seriallink Inc, All Rights Reserved.
Language Setting	
Modify Password	
— Backup File	
Update Firmware	
Factory Reset	

### 5.6 Device restart

The device can be restarted through the page, the navigation bar "device management"-"restart", click "execute restart" to restart the device.

You can also set the scheduled restart. To set the scheduled restart, you need to check "Enable", and click "SAVE & APPLY" after setting the time.

♠ Route Status	Device Reboot
Network Settings	Configure Device Reboot
🛱 Route Settings	
A Service Manage	Restart now. PERFORM REBOOT
E VPN Service	
🛠 System	
Date Time	SAVE & APPLY
Language Setting	
Modify Password	
Backup File	Copyright ©2013-2022 Seriallink tnc, All Rights Reserved.
Update Firmware	
Factory Reset	
Reboot	
2	



# 5.7 Page Exit

Click "Exit" to exit the page.

