

Edge Router

# User Manual

V1.0-2021.05

PDF



#### Declaration

Thank you for choosing our product. Before using this product, please read this manual carefully.

The contents of this manual cannot be copied or reproduced in any form without the written permission of InHand.

Due to continuous updating, InHand cannot promise that the contents are consistent with the actual product information, and does not assume any disputes caused by inconsistency of technical parameters. The information in this document is subject to change without notice. InHand reserves the right of final change and interpretation.

ER800 series include several model numbers, like ER805. This user manual is applied for all the ER800 series.

©2021 InHand Networks. All rights reserved.

#### Conventions

Symbol	Indication
11	Button name, for example, 'click Save button'.
cc>>	Indicates a window name or menu name, for example, the pop-up window "New User".
>>	A multi-level menu is separated by the double brackets ">>". For example, the multi-level menu File >> New >> Folder indicates the menu item [Folder] under the sub-menu [New], which is under the menu [File].
Cautions	Please be careful of the contens under Cautions, improper action may result in loss of data or device damage.
Note	Note contain detailed descriptions and helpful suggestions.

### **Technical Support**

Email: support@inhandnetworks.com

URL: www.inhandnetworks.com



# CONTENTS

1	Overview	1
2	Hardware	2
	2.1 Indicator Description	2
	2.2 Restoring to Default Settings via the Reset Button	3
3	Default Settings	4
4	Login and Network Access	5
	4.1 Network Access via Ethernet	5
	4.2 Network Access via SIM card	10
	4.3 Network Access via Wi-Fi	13
5	Network Management	17
	5.1 Network	17
	5.1.1 Bridge port	17
	5.1.2 VLAN Port	18
	5.1.3 ADSL Dialup (PPPoE)	20
	5.1.4 Wi-Fi	21
	5.1.5 Loopback Port	23
	5.1.6 Layer 2 Switch	24
	5.2 VPN	25
	5.2.1 IPsec	25
	5.2.2 GRE	29
	5.2.3 L2TP	
	5.2.4 OpenVPN	
	5.2.5 Certificate Management	



5.3 Service	
5.3.1 DHCP (Automatic IP Address Allocation)	
5.3.2 DNS	
5.3.3 DDNS	40
5.3.4 SMS	42
5.3.5 QoS	43
5.3.6 Traffic Control	44
5.4 Firewall	46
5.4.1 ACL	46
5.4.2 NAT	48
5.4.3 MAC-IP Binding	49
5.5 Routing	51
5.5.1 Static Routing	51
5.5.2 Dynamic Routing	51
5.6 Link Backup	59
5.6.1 SLA	59
5.6.2 Track	59
5.6.3 VRRP	61
5.6.4 Interface Backup	64
5.7 Wizards	67
5.7.1 New Cellular	67
5.7.2 New IPsec Tunnel	68
5.7.3 IPsec Experts Configuration	69
5.7.4 New L2TPv2 Tunnel	69



	5.7.5 New Port Mapping	.70
6 Sy	vstem Management	.72
	6.1 System	.72
	6.2 System Time	.74
	6.3 Management Services	.76
	6.4 User Management	.78
	6.5 AAA	. 79
	6.5.1 Radius	. 80
	6.5.2 Tacacs+	. 80
	6.5.3 LDAP	. 81
	6.5.4 AAA	. 82
	6.6 Configuration Management	. 84
	6.7 SNMP	. 85
	6.7.1 SNMP	. 85
	6.7.2 SNMP Trap (Alarm)	.86
	6.7.3 SnmpMibs	. 87
	6.8 Alarm	. 89
	6.9 System Logs	. 91
	6.10 System Upgrade	. 92
	6.11 System Reboot	. 93
7 Di	agnostic Tools	.94



# **1** Overview

InHand ER800 Edge Router is a new generation edge router launched by InHand Networks. With 4G wireless network and a variety of broadband services, this product can provide Internet access for all industries of IoT. The product adopts SD-WAN technology to provide uninterrupted data communication link experience for industry applications.

ER800, with its perfect security and agile wireless link services, realizes the networking of a variety of IoT devices, can help enter enterprises to realize informatization and digitization.



# 2 Hardware

# 2.1 Indicator Description

ER800 Indicator	LED Status and Definition				
System	Steady off Power off. Blinking in blue System starting. Steady in blue System operates properly. Blinking in red System faults. Blinking in green System upgrading.				
Network Status	<ul> <li>Blinking in red Network connection lost.</li> <li>Blinking in green Cellular network connecting.</li> <li>Steady in green Cellular network connected.</li> <li>Blinking in blue Ethernet network connecting.</li> <li>Steady in blue Ethernet network connected.</li> </ul>				
Wi-Fi 2.4G	Steady off Disabled. Steady in green Wi-Fi 2.4G connecting. Blinking in green Wi-Fi 2.4G working properly.				
Wi-Fi 5G	Steady off Disabled. Steady in blue Wi-Fi 2.4G connecting. Blinking in blue Wi-Fi 2.4G working properly.				

Note: If both cellular network and ethernet network are working properly, Network Status Indicator will be in blue. And it will show the color of the connecting network if another network is not connected. If either two network are not connected, this indicator will be in red.



# 2.2 Restoring to Default Settings via the Reset Button

To restore to default settings via the reset button, please perform the following steps:

- 1. Press the RESET button within 10 seconds after power on the device.
- 2. System indicator will be steady on after blinking for about 1 minute.
- 3. Release RESET button, System indicator will blink, and press the RESET button again.
- 4. When System indicator blinks slowly, release the RESET button. The device has been restored to default settings and will start up normally later.





# **3 Default Settings**

No.	Function	Default Settings
1	Cellular	- Dual SIM card enabled, use SIM1 by default.
		- Wi-Fi 2.4G AP mode enabled, SSID: ER800-
		Tollowed with 6 numbers.
		- WI-FI 5G AP mode enabled, SSID: ER800-5G-
2	Wi-Fi	followed with 4 numbers.
		<ul> <li>Auth Method is WPA2-PSK.</li> </ul>
		- Both WPA/WPA2 PSK keys in two mode are the last
		8 letters in serial number.
		- 4 LAN are enabled.
	Ethernet	- IP Address: 192.168.2.1
2		<ul> <li>Netmask: 255.255.255.0</li> </ul>
5		- DHCP server enabled, IP address is 192.168.2.2 to
		192.168.2.100, can provide IP address for
		downstream devices automatically.
		- HTTP(80) and HTTPS(443) are enabled.
	Management	<ul> <li>Telnet is disabled.</li> </ul>
4	Services	<ul> <li>SSH is disabled.</li> </ul>
		<ul> <li>Only allow HTTPS to access from cellular network.</li> </ul>
E	Username and	- adm/123456 (super administrator)
5	password	



### **4 Login and Network Access**

#### 4.1 Network Access via Ethernet

Step 1: Connect power and Ethernet cable to ER800, connect WAN port to public network, and one of LAN to PC.

Step 2: Configure PC to be in the same network segment as the IP address of the router.

(1) Enable PC to obtain an IP address from DHCP automatically (recommended).

(2) Configure a fixed IP address in the same network segment as the router for PC. The IP address should be one of the address in 192.168.2.2~192.168.2.254, Subnet mask should be 255.255.255.0, and Default gateway should be 192.168.2.1. DNS server should be 8.8.8.8 or the address of ISP' s DNS server.

ment		Garana				
The car get IP settings assigne supports this republicy, otherw administrator for the appropriat	t automatically if your metooris load, your need to ask your metoolick to 3° ontEmps	You can get 2' settings along supports this supplify. Other advantation for the appropri-	ned automatically if your network rivers, you need to ask your network new IP settings.			
Other an P address puter	naturity	Other of Faldree at	Ottam at IF address submittially			
Climits Mining Pailer		Che The following 2" pd	Gia fie felining P stitues			
T aites.	4754 78	7 aldress.	282 . 108 . 2 . 2			
have not	1 + 1-1 + - 17 + - 1	Tubort made:	255 . 258 . 255 . 8			
Industry gamments	1. 1. 1	Oxfoult galaxies;	192.198.2.1			
. Uttan DKS wever address	a adometically	Citrain mil innur add	en amongoly			
Citer He following 1851 and	and with some	(#) Link War following D4G a	erver addresses			
Performance and annual	1 1 1	Profested DKL servets	1.1.1.4			
Allertais (AP) second		Alemaits 245 server	- + ( + )			
Distance settings upon all	t Adams	ell	ad Aleman			

Obtain an IP address automatically/manually



Step 3: Access to the default IP address 192.168.2.1 in a browser, enter username and password(adm/123456 by default) in pop-up window and then access to router' s WEB management page. If the browser alarms the connection is not private, show advanced, and proceed to access to the



address.

Login to device' s WEB management page

Step 4: Create a WAN port in "Wizards >> New WAN" in the left menu. Configure an IP address for WAN port and let the router connect to Internet.

nhand					User Manual 🧲
inhand	Wiza	rds >> New WAt	4		
Administration	•				Your pas
Network	•				
Services	, Int	erface		bridge 1 🔻	
Link Backup	, Ту	pe		Static IP	•
Pouting	, Pri	mary IP			
Kouting	Ne	etmask		255.255.255.0	
Firewall	Ga	teway			
VPN	Pri	mary DNS			
Tools	* NI4	ΔT		~	1
Wizards	+	843		2011	
	10,111	Apply & Save	Cancel		

There are there types to obtain IP address: Dynamic DHCP (recommend). Static IP (Click Apply & Save after configure manually) and ADLS Dialup (Click Apply & Save after configure manually).

	New	WAN				
Administration	*			Your pa		
Network	•					
Services	, Int	erface		vlan 4000 🔻		
Link Backup	, Typ	be		Dynamic Address (DHCP) V		
Routing	► NA	Т		×		
Firewall	•	Apply & Save	Cancel			
/PN	•	Apply & Dave	Cancer			
Tools						
Wizards						

Obtain IP address by Dynamic Address (DHCP)



Obtain IP address by Static IP

-94,000	New WAN			
Administration	•			Your password has see
Network Services	, Interface		vian 4000 •	
Link Backup	. Type		ADSL Dialup (PPPoE	) •
Routing	• Username			Please ask ISP to
Firewall	, Password			get your username
VPN				and password
Tools	Apply & Save	Cancel		
Wizarda				

Step 5: Check the connectivity in "Tools >> Ping" .



#### User Manual 🧲

Administration	•	You	r password has security risk
Network	•		
Services	* Host	8888	Ping
Link Backup	Ping Count	4	
Routing	* Packet Size	32 Bytes	
Firewall	* Expert Options		
VPN		. 15-	
Tools			
Wizards	* 106 5.5.5.8 (8.6.8 40 bytes from 8.6.8 40 bytes from 8.6.8 40 bytes from 8.6.8 40 bytes from 8.8.8 40 bytes from 8.8.8 40 bytes from 8.8.8	10) 32 data bytes 18: seq=0 ttl=105 time=267.330 mp 18: seq=1 ttl=105 time=265.803 mp 18: seq=2 ttl=105 time=265.234 mp 18: seq=3 ttl=105 time=264.598 mp atistics ed. 4 packets received. 0% packet Los	a





# 4.2 Network Access via SIM card

Step 1: Insert the SIM card when device is power off. Connect 2 4G antennas to the router, and connect PC to router. Then power on.

Note:

When insert or plug out SIM card, please unplug the power cable to prevent data loss or damage the router.

ER800 supports 4 antennas (2 WLAN antenna and 2 WWAN antennas), please

connect all antennas to obtain high communication guality.

Step 2: Open a browser and access to router' s WEB management page. (refer

to 4.1)

Step 3: Click "Network >> Cellular", set profile. The device enables the cellular by default, it will connect to Internet within a few minntes. If the device cannot connect to Internet, please disable and restart dialup. (If you use a private network SIM card, you also need to configure APN parameter)





miniatration	•					Yo	ut passw	ord has securi	ty risk, please clic
twork.									
vices	+ Enal	bie		*					
Beckup				SIM1	SIM2				
ting	+ Prof	the		84/10	• suto	•			
and a second	. Roa	ming		*					
100	PIN	Code							
	+ Net	work Type		Auto			•		
	Con	nection Mode		Aluay	a Online				
8793	Red	lai Intervai		10					
	1CM	P Detection Serv	er .			1.1			
				1					
	3CM	P Detection Inte	rvat	30	1				
	ICM	P Detection Time	tuon	5					
	ICM	ICMP Detection Max Retries ICMP Detection Strict		5					
	ICM								
	Sho	w Advanced Op	tions	ш.					
	Profi	le.							
	Ind	es Nativork Type	APN		Access No	mber	Auth Method	Usemame	Password
	1	QEM	Spret		199100	18	auto	-gpra	
		G5M +					Auto *		
									Add(1/10)

Step 4: Check the dialup status in "Status", if it shows Connected and there is IP address and other dialup parameters, the router has connected to Internet by SIM card.



User Manual 🧲

#### Network >> Cellular

Status Cellular

Modem

Active SIM	SIM 1				
IMEI Code	353593090129021				
IMSI Code	460110923582245				
ICCID Code	89860318040283846651				
Signal Level	(29 asu -55 dBm)				
RSRP	-85 d8m -15 d8				
RSRQ					
Register Status	registered				
Operator	CHN-CT				
Network Type	4G				
LAC	9811				
Cell ID	9D54212				
Network					
Status	Connected				
IP Address	10.65.120.18				
Netmask	255.255.255.252				
Gateway	10.65.120.17				
DNS	61.139.2.69 218.6.200.139				
MTH	1500				



# 4.3 Network Access via Wi-Fi

Step 1: Connect Wi-Fi antenna, and connect PC to the device. Access to router' s WEB management page. (refer to 4.1)

Step 2: Choose the frequent band of Wi-Fi. ER800 supports 2.4G and 5G Wi-Fi. These two Wi-Fi can work at the same time. You can check Wi-Fi status in "Network >> Wi-Fi".

uphand	Status Constant	MI-FI 50
Administration	·	Your passwore
Network		
Services	Wi-Fi 2.4G Status	
Link Backup	Station Role	AP
Routing	<ul> <li>Status</li> </ul>	Disabled
Eirensall	, SSID	ER800-332211
(05)	, MAC Address	00:00:00:00:00:00
(PN	Channel	Auto
fools	Auth Method	WPA2-PSK
Wizards	Encrypt Mode	CCMP
	IP Address	192.168.2.1
	Netmask	255.255.255.0
	Wi-Fi 5G Status	
	Station Role	AP
	Status	Disabled
	SSID	ER800-5G-3311
	MAC Address	00:00:00:00:00:00
	Channel	36
	Auth Method	WPA2-PSK
	Encrypt Mode	CCMP
	IP Address	192.168.2.1
	Netmask	255.255.255.0
Save Configurati	on	



Step 3: Set Station Role in "Wi-Fi 2.4G" or "Wi-Fi 5G" : AP or Client. AP mode (default mode): ER800 acts as an accsess point to radiate wireless signals, and other terminal devices can connect this device to access the Internet. It is necessary to ensure that ER800 itself has been connected to the Internet through wired or dialup mode. AP mode supports setting SSID name and encryption authentication mode, and terminal devices will need to input password when connecting.

dministration	•		Your pa			
etwork						
nvices		Enable				
the sector		Station Role	AP 🔻			
ік васкир		SSID Broadcast				
outing	,	AP Isolate				
rewall		Bridge				
PN .	*	Radio Type	802.11ng 🔻			
ools	- 10	Channel	Auto V			
izards		SSID	ER800-332211			
		Auth Method	WPA2-PSK T			
		Encrypt Mode	CCMP •			
		WPA/WPA2 PSK Key	••••••			
		Bandwidth	20MHz V			
		Stations Limit				





Client mode: ER800 connects to other AP Wi-Fi device to access the Internet.

1. Select Station Role to Client and save.



- 2. Click Scan to scan available AP, and click Connect to choose one of AP.
- 3. Configure Wi-Fi parameters and save. Then check the connection status in

"Status" .



User Manual 🧲

	Your	Dass
•		
, Enable	*	
, Station Role	Client •	
Default Route	*	
SNAT	×.	
SSID	linhand	
	Scan	
* Auth Method	WIDA2 DSK +	
Encryont Mode	CCMP .	
cherypeniode	Comir 1	
	Enable Station Role Default Route SNAT SSID Auth Method Encrypt Mode	Enable     Image: Client •       Station Role     Client •       Default Route     Image: Client •       SNAT     Image: Client •       SSID     Imhand       Auth Method     WPA2-PSK •       Encrypt Mode     CCMP •



# **5 Network Management**

In parameter settings, a green text box indicates a mandatory parameter, and a pure white text box indicates an optional parameter.

# 5.1 Network

### 5.1.1 Bridge port

A bridge port is intended to connect two different physical LANs over a bridge, enable storage and forwarding across LANs at the link layer.

#### Method for modifying the IP address of a bridge port and bridge members:

1. Click "Network >> Bridge" and select "Bridge". Choose a bridge and

#### click Modify.

Bridge	
	Your password has security risk, please click here to
Bridge 10	D*/Netmaak
- X	102148321/2852553850

2. Modify the IP address of the bridge port or bridge members. Among the bridge members, dot11radio and dot11radio2 are Wi-Fi 2.4G and Wi-Fi 5G port respectively.





ridge ID	¥	
dge		
imary IP		
IP Address	192.168.2.1	
Matematic	0.396.356.366	
econdary IP	233.233.233.0	
econdary IP IP Address	23.23.23.0	Netmask
condary IP IP Address	23.23.23.0	Netmask Add(0/10]
ige Member vlan 1	det11radie 1	Netmask Add(0/10) dot11radio :

#### 5.1.2 VLAN Port

A virtual LAN (VLAN) comprises a group of logical devices and users. These devices and users are not limited by physical locations, but can be organized base on functions, departments, applications, and other factors. They communicate with each other as if they are in the same network segment, which contributes to the name of VLAN.

Method for adding a port of VLAN2:

1. Click "Network >> VLAN >> Configure VLAN parameters >> Add" . Set the virtual IP address of the port of VLAN 2 and select the member port of VLAN 2 as required. Click Apply & Save.



along along a long a	2		
N Virtual Interface			
Imary IP		-	
P Address	192.168.3.1	1	
Netmask	255.255.255.0		
IP Addres		Netmask	
		1	101
		Add	
		IbbA	
AN Member Ports	69.13	Add	

2. Return to the VLAN list. The port of VLAN 2 has been added successfully.

Cant	gure VLAN Par	amaters			
VLAN ID	GE1/1	GEL/2	681/1	581/4	Primary IP/Netmask
£	w.	4			The second
- 2 -				1	182,168.33/255,255,255.0

Currently, VLAN ports of the device support two link types: access and trunk. An access port belongs to only one VLAN and is generally connected to a computer. A trunk port can be used for multiple VLANs and can receive messages from or send messages to multiple VLANs. It can be connected to a switch or a user's computer. You can select the link type as required on the "VLAN Trunk" page.



Port	Mode		Native VLAN
GE1/1	Access	۷	1
GE1/2	Access	۷	1
GE1/3	Trunk	۷	1
GE1/4	Trunk	~	2

### 5.1.3 ADSL Dialup (PPPoE)

#### Method for connecting ER800 to a PPPoE server:

1. Click "Network > > ADSL Dialup (PPPoE)", select the interface for connecting to the PPPoE server in the "Dial Pool" bar, and click Add.

2. Enter the user name, password, and pool ID of the PPPoE server in the "PPPoE

List" bar. The pool ID must be the same as that in the "Dial Pool" bar. Click Add, and then click Apply & Save.



hal Por	ol										
	Pad	di li			3	Interface					
1	_		bridge	1					3		
							109	(01\0)bbl			
PPoEl	List										
PPoE I Enable	List ID	Poel ID	Authentical Type	tion	Username	Password	Local IP Address	Remote IP Address	Keepalive Interval	Keepalive Retry	Debu
PPoE I	List ID 1	Pool ID 1	Authentical Type Auto	tion	Username	Password	Local IP Address	Remote IP Address	Keepalive Interval	Keepalive Retry 3	Debuj

#### 5.1.4 Wi-Fi

ER800 can be used as an AP or a client. When it is used as an AP, other users can access the Internet through the router via Wi-Fi. When it is used as a client, the router connects to an AP for Internet access. The Status bar shows router' s current Wi-Fi connection status.



#### Network >> Wi-Fi

Status Wi-Fi 2.4G Wi-Fi	5G
Wi-Fi 2.4G Status	
Station Role	AP
Status	Enabled
SSID	ER800-332211
MAC Address	66:55:44:33:22:11
Channel	Auto
Auth Method	WPA2-PSK
Encrypt Mode	CCMP
IP Address	192.168.2.1
Netmask	255.255.255.0
Wi-Fi 5G Status	
Station Role	AP
Status	Disabled
SSID	ER800-5G-3311
MAC Address	00:00:00:00:00:00
Channel	36
Auth Method	WPA2-PSK
Encrypt Mode	CCMP
IP Address	192.168.2.1
Netmask	255.255.255.0

Method for providing network access service for wireless terminals when the router is used as an AP:

Click "Wi-Fi >> Wi-Fi 2.4 or Wi-Fi 5G" and select "AP" for "Station Role". Enter the SSID, authentication method, and key consistent with those of the wireless AP. Click Apply & Save.





Network >> Wi-Fi	
Status Wi-Fi 2.4G Wi-Fi 5G	
Fnable	9
Station Role	AP V
SSID Broadcast	
AP Isolate	
Bridge	
Radio Type	802.11ng 🔻
Channel	Auto 🔻
SSID	ER800-332211
Auth Method	WPA2-PSK •
Encrypt Mode	CCMP •
WPA/WPA2 PSK Key	••••••
Bandwidth	20MHz 🔻
Stations Limit	
Apply & Save Cancel	

#### Method for connecting to an AP for Internet access when ER800 is used as a

#### client:

Select "Client", enter Wi-Fi SSID and key, and click Apply & Save. Or select

"Client", click Apply & Save, then click Scan to choose the AP you want.

Wi Fi 246	
Enable	2
Station Role	Client - Hote: please click "apply & save" button to enable scan funct
Default Route.	3
SNAT	2
SSID	Inhand
Auth Method	WPA2-PSK +
Encrypt Mode	CCMP +
WPA/WPA2 PSK Key	

5.1.5 Loopback Port



#### Method for adding Multi-IP Settings:

Click "Network >> Loopback >> Multi-IP Settings", configure any IP address

IP Address	127.0.0.1		
Netmask	255.0.0.0		
Multi-IP Settings			
IP Address	9	Netmask	

for the router, click Add, and then click Apply & Save.

### 5.1.6 Layer 2 Switch

Check the network connection status of GE1 to GE4. LINK UP indicates that the network is connected. LINK DOWN indicates that the network is disconnected.

twork >	> Layer2 Switch			
tatus				
Port	Link Status	Speed	Duplex	PVID
GE1/1	LINK UP	1000M	FULL	1
GE1/2	LINK DOWN	112	THE CONTRACTOR	1
GE1/3	LINK DOWN	****	<u>9339</u>	1
GE1/4	LINK DOWN	+++=	++++	1





## 5.2 VPN

VPN is intended to establish a private network on the public network for encrypted communication. A VPN router enables remote access by encrypting data packets and converting the destination address of data packets. VPN can be realized by a server, hardware, or software. Compared with the traditional DDN private line or frame relay, VPN provides a more secure and convenient remote access solution.

A common VPN application scenario: An employee on a business trip wants to access to the enterprise's intranet. The employee connects to enterprise's VPN server and then accesses to enterprise's intranet through the VPN server. Communication data between the VPN server and the client is encrypted and can be regarded as being transmitted on a dedicated data network. This ensures data security.

#### 5.2.1 IPsec

IPsec is a group of open network security protocols developed by IETF. At the IP layer, data source authentication, data encryption, data integrity, and anti-replay functions are used to ensure the security of data transmission between communication parties on the Internet. This reduces the risk of leakage and eavesdropping, ensures the integrity and confidentiality of data, and the security of service transmission for users.

**Scenario:** Data is transmitted between the subnet (192.168.1.0/24) of headquarters A and the subnet (172.16.1.0/24) of customer branch B through router A and router B. The transmission channels between router A and router B

25



are encrypted over IPsec, which protects the security of data transmission between headquarters A and customer branch B.



Method for encrypting the transmission channels between router A and

#### router B over IPcec:

Parameter	settings:
-----------	-----------

R	outer A		Router B
Set IKEv1	/v2 Parameters	Set IKE	/1/v2 Parameters
ID	Custom	ID	Custom
Encryption algorithm	AES128	Encryption algorithm	
Hash algorithm	SHA1	Hash algorithm	Same as that of Router
Diffie-Hellma n key exchange	Group2	Diffie-Hellm an key exchange	A
Lifecycle	86400	Lifecycle	
IPs	sec Policy	II	Psec Policy





Name	Custom	Name	Custom
Encapsulatio n	ESP	Encapsulatio n	
Encryption algorithm	AES128	Encryption algorithm	Same as that of Router
Authenticatio n method	SHA1	Authenticati on method	A
IPsec mode	Tunnel mode	IPsec mode	
IPsec tunr	nel configuration	IPsec tur	nnel configuration
Peer address	Address where router B establiches the IPsec service	Peer address	Address where router A establishes the IPsec service
Interface	Interface for establishing the IPsec service	Interface	Interface for establishing the IPsec service
IKE version	IKE version used	IKE version	Come as that of router
Authenticatio n method	Shared key	Authenticati on method	A A
Local subnet	IP address of the subnet of router A	Local subnet	IP address of the subnet of router B
Peer subnet	IP address of the subnet of router B	Peer subnet	IP address of the subnet of router A

#### Detailed configuration steps:

- 1. Configure router A and router B.
- (1) Add IKE and IPsec policies, and click Apply & Save.



(2) Add IPsec tunnels and click Apply & Save.

e1imput.		~				
IKEV1 Policy						
ID	Encryption	Hash	Diffie Hellman Gr	eup.	Lifetime	
1	AE\$128	SHA1	Group2		86400	
	AE5128 ~	SHA1 ~	Group2	~ B6400		
1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.					Addit	ANK .
IKEv2 Policy						
iD	Encryption	integrity	Diffie Hellman Gr	oup	Lifetime	
	AES128 -	SHA1 =	Group2	♥ 36400		
					Add(0)	101
IPsec Policy						
Name	Encapsulati	on Encrypt	ion Authentica	tion	IPsec Mode	
	ESP	AE513	E SHA1		Tunnel Mode	
0	ESP	<ul> <li>AES128</li> </ul>	✓ 5HA1	+ Tunne	i Mode	
					Add(1	/10]

2. Access the IPsec Status page. The IPsec VPN is established successfully if the

Add(1/8)

Modely

Delate

page is shown as below.

status (	Press & Joseph Letters of					
Tunnel Statue						
Name	Destination Address	Bestatus	Be Tim	de .	201	Pasc SAu
Pres 8, 518, 322 320, 22	338.127.138.22	ESTABLISHED	retablic	fred 120s; rea	urberretuation in \$5643s	192398883924===18238850/04
Paec SA Status						
IPiec SA	Tunnal North	Deatimati Address	Pri I	Rtetus	Prac Timer	Tunnel Row
112308-8-0/28+++1823	188.3-0/24 Prest_118.112	130.22 158.177.1	20.23	INITALLED	installed 126s releying in 2508	by Byten in Diparkets in 0 bytes m

Note:



The IPsec profile does not need to be configured when establish an IPsec VPN, but needs to be configured when establish a DM VPN.

#### 5.2.2 GRE

Generic Routing Encapsulation (GRE) protocol can be used to encapsulate datagrams of some network layer protocols, so that these encapsulated datagrams can be transmitted on the IPv4 network.

Scenario: GRE is enabled for ER800\_A and ER800\_B through the public network.



Method for enabling GRE for transmission channels of ER800\_A and ER800 B:

1. Click "VPN >> GRE" and then click Add.

PN >> GR	E								
GRE Entry									
Enable	Index	Local virtual IP	Local Address	Remote virtual IP	Peer Address	Key	NHRP Enable	iPasc Profile	Description
						1002/dthbA	34	14	Delete

2. Set "Index" as required. Select "Point to Point" or "Subnet" for "Network Type". Set "Local Virtual IP" and "Peer Virtual IP", ensuring that they are on the same network segment. Enter the source and peer IP addresses or interfaces and the key. Click Apply & Save.



nable	
ndex	1
Vetwork Type	Point to Point
ocal Virtual IP	1.1.1.1
Peer Virtual IP	1.1.1.2
Source Type	Interface v
Local Interface	cellular 1 🗸
Peer IP	118.122.120.2
(ey	
UTU	
NHRP Enable	
Psec Profile	Disable v
Description	

3. Set ER800\_B in the same way. The virtual and peer IP addresses of ER800\_B must correspond to those in ER800\_A, and the key must be the same as that of ER800\_A.

#### 5.2.3 L2TP

The Layer 2 Tunneling Protocol (L2TP) is an industrial-standard Internet tunneling protocol used to encrypt network data streams.

Method for setting a L2TP client in ER800:



1. Click "VPN >> L2TP >> L2TP Client >> L2TP Class", enter a name of an L2TP class, and click Add.

L2TP Clier	nt L2TP Server		
Class			
Name	Authentication	Hostname	Challenge Secre
class1	No		11182
			1

2. Configure the pseudowire class: Enter a name of any pseudowire class. "L2TP Class" is the same as that on the "L2TP Class" page. Set "Source Interface" to the interface connecting to the server. Select L2TPV2 for "Protocol" and click Add.

Name	L2TP Class	Source	Data Encapsulation Method	Tunnel Management Porotocol
Pse1	class1	cellular 1	L2TPV2	L2TPV2
	class1 v		L2TPV2 Y	LZTPV2 V

3. Set L2TPV2 tunnel parameters: Enter the server's domain name or IP address for "L2TP Server". "Pseudowire Class" is the same as that on the "Pseudowire Class" page. Enter the user name and password created on the server. Set other parameters as required. Click Apply & Save.




21942.10	innel										
Cruble 1	D	LIT# Server	Pseudowire Class	Authe	entication Type	Usemame	Pai	mored	Loca Add	i se	Remote IP Address
4. 1	1 1	18.122.120.22	Fyel	- 14	Auto	heat		*****			
10. 2			Pset v	Auto							
									-	1.44	(1/10)
TPv3 Tu	innel	Read ID	Pseudo	ivire	Berland	fame 8		Destina	tion	Re	annect
2TPv3 Tu Enable	innel ID	Pear ID	Paeudo Clar	udre a	Protocol	Source P	ort	Destina Port	tion t	Res Ind	annect erface
Enable	innel ID	Peer ID	Pseudo Ciar	a v	Protocol	Source P	ort	Destina Port	tion t	Res Ind	annact artaca ~
Enable Right a	innel 10	Peer 10	Petude	a a ~	Protocol	Source P	ort	Destina Port	tion	Her Ind	onnect erface (12/13)
27Pv3 Tu Enable 191 3	innel 10	Pear ID	Parvile	wtre a v	Protoco	Source P	ort	Destina For	tion t	Nor Ind	ormoet orface arface
27Pv3 Tu Enable R 1 27Pv3 Se	innel 10 ssion	Pear ID	Pseudo	wtre a ~	Protocol	Source P	tre	Destina Port	tion t	No Ind	annect arfaca strug
27Pv3 Tu Enable R 1 27Pv3 Se Local Seas	10 ssion	Pear ID Remote Secsion 10	Pseudo Clas	wtre a ~ Furmel	Protocol	Local Se	stim	Destina Port	tion t	No. Ind	annoct artace (0/10)
2TPv3 Tu Enable R 1 2TPv3 Se Local Semi	ID SSIGN	Pear ID Remote Sessie 10	Pseudo Clas M Local	wire a ~	Pratocol (P	Local Se	seitan	Destina Port	tion t	Res Ind	onnoct erface torial

4. After gateway A and gateway B are configured, access the L2TP status page

to view the L2TP connection status.

IN >> LETP						Digita
failes and and a	ATT Devel					
LTF Client						
Turnel Name	LITP Server	Balue	Local IP Address	Remote IP Address	Local Beaston 3D	Ramota Season 20
sintal sec 1	108.133.136.33	Convented (1418)	64.63	44.6.1	and the submed	store starts in the

### 5.2.4 OpenVPN

Based on the application-layer VPN of the OpenSSL library, OpenVPN supports multiple authentication methods such as the certificate, key, and user name/password. Compared with traditional VPN, it is simpler and easier to use.

Authentication methods	Operation on the web page
None	No authentication is required.
User	Enter the user name and password created on the

#### Authentication methods:



name/password	OpenVPN server, import the CA certificate, public key, and
	private key for authentication in "VPN >> Certificate
	Management".
Pre-shared key	Enter the pre-shared key created on the OpenVPN server.
Digital	Import the CA certificate, public key, and private key for
certificate	authentication in "VPN >> Certificate Management".
Disting	Enter the user name and password created on the
	OpenVPN server, import the CA certificate, public key, and
certificate/user	private key for authentication in "VPN >> Certificate
name/password	Management".
Digital	Enter the pre-shared key created on the OpenVPN server,
certificate/TLS	import the CA certificate, public key, and private key for
authentication	authentication in "VPN >> Certificate Management".
Digital	Future the new characteristic second second second second
certificate/TLS	Enter the pre-shared key, user name and password created
authentication/u	on the OpenVPN server, import the CA certificate, public
ser	key, and private key for authentication in "VPN >>
name/password	Certificate Management".

# Method for setting OpenVPN client on ER800 when connecting to an OpenVPN server:

OpenVPN can be configured manually, or by importing config file. In the following example, the authentication type is a digital certificate.

1. Set the OpenVPN parameters for the gateway as shown in the figure below,

ensuring that the network parameters at both ends of the tunnel are consistent.

Click Apply & Save.



1.0004.1		100	1. 1. 1. 1. 1.
VPN		1 10 40	
****	10	VVEII	

Enable		1			
Index	)				
OpenVPN Server	Port	,	rotocol Type		
118.122.120.22	1194		udp		
	1194	i i det			
		Lindb	Addito		
	11.54	ling	Add[1/	4	
Authentication Type	1	509-cert	Add[1/	4	1
Authentication Type Description	1	509-cert	Add[1/	<b>1</b>	3
Authentication Type Description Local IP Address	[] []	509-cert	Add[1/	4	 ]
Authentication Type Description Local IP Address Remote IP Address	2 [ [	509-cert	Add(1/	4	]
Authentication Type Description Local IP Address Remote IP Address Show Advanced Optio	2 [ [ [ ]	509-cert	Add[1/	4	]
Authentication Type Description Local IP Address Remote IP Address Show Advanced Optio	2 [ [ ns [	509-cert	Add(1/	4	3
Authentication Type Description Local IP Address Remote IP Address Show Advanced Optio mport Configuration	 	509-cert	Add[1/	4	]

2. Select digital certificate in "Authentication Type", import the CA certificate,

public key, and private key in "VPN >> Certificate Management".

3. Click Apply & Save. Return to the "Status" page and view the tunnel status.

97.0 PC 77						
PN >> OpenVP	N .					
Cinetary .	Comments of the local division of the local	Concession of the local division of the loca				
Contractory of the local division of the loc	and the second s	and the second se				
	and the second second					
Turnel Name	Open//PN Server	Interface Type	Status	Local IP Address	Remote IP Address	Description

### 5.2.5 Certificate Management

Certificates used for IPsec and OpenVPN services can be imported or exported

in this page.

Method for importing certificates:



Click "VPN >> Certificate Management >> Browse", select the certificate obtained from the certificate server, click Import XX Certificate, and then click

#### Apply & Save.

6			
-			
	Bravelat	Input Public Key Certificate	Export Public key Certificate
	Browse	Import Private Key Certificate	Expert Private Key Certificate
	Brownel	Import CA Certificate	Export CA Certificate
	Browse	Bruselt CRL	Expert OIL
	Browne	Import PACS12 Combone	Export PKCS12 Centificatie
anagement ROOT CA			
		Territory N	ame
	anagement ROOT CA	I Rover	

If there is no local certificate available, check "Enable SCEP (Simple Certificate Enrollment Protocol)" to apply for a certificate online.

#### Method for applying a certificate for the router online:

1. Click "VPN >> Certificate Management". Check "Enable SCEP (Simple Certificate Enrollment Protocol)" and "Force to re-enroll". Enter the certificate protection key and confirm it. Enter the URL of the certificate server, certificate name, and FQDN. Click Apply & Save.



2. After the server issues the certificate, check the application status. If the application status is "Completion", certificate application succeeds.

Certificate Management	TCA		
Certificate Management			
Enable SCEP (Simple Certificate Enrollment Protocol)	3		
Force to re-enroll			
Status	Initiation		
Protect Key			
Protect Key Confirm			
Strict CA			
Server URL	http://192.1	68.2.111/cersrv/mscep/mscep.dll	
Common Name	VG7100116		
FQDN	VG71001160	Þinhand.com.cn	
Unit 1	[		
Unit 2	[		
Domain	L		
Serial Number			
Challenge			
Challenge Confirm			
Unstructured address			
RSA Key Length	1024	bits	
Poll Interval	60	5	



## 5.3 Service

### 5.3.1 DHCP (Automatic IP Address Allocation)

DHCP uses client/server communication mode. The client submits a configuration application to the server, and the server returns the IP address assigned to the client, in this way, DHCP realizes the dynamic configuration of the IP address.

DHCP server and DHCP forwarding function are mutually exclusive.

#### Method for setting DHCP server in ER800:

Click "Services >> DHCP". In the "DHCP Server" bar, check "Enable", select an interface, set the start and end IP addresses, click Add, and then click Apply & Save.

DHCP	Server	Second Change Co.		
HCP Server				
Enable	Interface	Starting Address	Ending Address	Lease(Minutes
4	bridge 1	102.168.2.2	192.168.2.100	1440
1 m 1	-			111440

#### Method for enabling DHCP forwarding in ER800:

Click "Services >> DHCP >> DHCP Relay", check "Enable", enter the server address, select the gateway interface, and click Apply & Save.





atus DHCP Server DHC	CP Relay DHCP Client
nable	
OHCP Server 1	10.5.16.98
DHCP Server 2	
OHCP Server 3	
HCP Server 4	
Relay Interface	bridge 1 🗸
Source IP	

### 5.3.2 DNS

Domain name service (DNS) is a distributed network directory service mainly used for mutual conversion between a domain name and an IP address.

### Method for enabling the DNS server in ER800:

Click "Services >> DNS >> DNS Server", enter the address of the DNS server, and click Apply & Save.





DNS Server DNS Rela	у
Primary DNS	8.8.8.8
Secondary DNS	114.114.114.114

#### Method for enabling DNS forwarding in ER800:

As a DNS agent, the router forwards DNS requests and response messages between DNS client and DNS server, and provides domain name resolution for client.

IF the router enables DHCP service, DNS forwarding will be enabled by default and cannot be disabled.

Click "Services >> DNS >> DNS Relay", check "Enable DNS Relay", set the mapping between the domain name and the IP address, click Add, and then click Apply & Save. After the settings are completed, when a DNS client on the LAN requests a host domain name in the list, the DNS agent server will return the corresponding IP address to the client.



e DNS Relay	96	
[Domain Name <=> II	Paddresses  Pairing	
Host	IF Address 1	IP Address 2
www.sohu.com	10.5.16.98	

### 5.3.3 DDNS

Dynamic domain name server (DDNS) maps the dynamic IP address of the router to a fixed DNS. Each time a user connects to the Internet, the client program will transmits the dynamic IP address of the host to the server program on the server host. The server program provides the DDNS service and realizes dynamic domain name resolution. In this way, you can access the Internet by entering the domain name, even if the IP address is changed.

#### Method for enabling the DDNS in ER800:

1. If use Custom service, set "Method Name" as required, select "Custom" for "Service Type", and enter the DDNS expression

"http://user name:password@ddns.oray.com/ph/update?hostname=host name" of the server for "Url". This expression is only for reference. The real URL is provided by the service provider (usually available on the official website of the service provider). Click Add.

If use a common domain name server, set "Method Name" and "Service Type" as required, enter the user name, password, and host name obtained from the server, and click Add.



If select as "Disable", the DDNS service will not enable.

2. Select the rotuer interface, enter the name of the DDNS method, click Add,

and then click Apply & Save.

<b>ONS Method</b>	List.					
Mathad Name	Service Type	un	Stername	Pesseard	Hasthame	Period
tille a T	Culture	Return/management/2 also 1210 dates program //P/Japatiete Prostnamer (52) 602 8006 Japatiete	1			1
				11		
				-		Additive
2010-141-225-1	1			H	.д.	Additive
pecify A Met	hod To Interfa	ан		н	A	Addition
pecify A Meth	hod To Interfa	C#		H	.A.	ANDA
pecify A Meth Interface	hod To Interfa	te Nutfod		1	A	AMEN

3. Wait several minutes after the DDNS settings are applied and saved. Then ping the host name (domain name) of the domain name server to check the stauts of application to the DDNS service.



Services >> DDNS	
Bridge 1	
Method	didns1
Hostname	
IP Address	118.122.120.22
Last Update	2020-01-16 15:27:33, 118.122.120.22
Last Response	2020-01-16 15:27:33, successful update for 118.122.120.22 (h2340c9004.iaik.in)



### 5.3.4 SMS

The router can restart or manual dialup via SMS messages, and some of routers can send alarm information to the SMS whitelist.

#### Method for controlling ER800 to restart and manual dialup via SMS:

When the cellular selects in SMS activation mode, click "Services >> SMS" and check "Enable". In the "SMS Access Control" bar, set "ID" as required, select "permit" for "Action", enter the phone number, and click Apply & Save. When you activate the dialup port via SMS, after the configuration is completed, you can restart the router by sending **reboot** to router' s SIM card number from the mobile phone in whitelist, or send **cellular 1 ppp up/down** to make the router redial or stop dialup.



nable				
ode		TEXT	~	
oll Interv	al	30	s(0: disable)	
ID	Actio	0	Phone Nu	mber
		the set of	the second se	

### 5.3.5 QoS

Quality of Service (QoS) is a network security mechanism that allows a network to provide better services for designated network communication by using various basic technologies. It is a technology for solving network delays and blocking problem.

### Method for setting the maximum egress bandwidth in ER800 via QoS:

Click "QoS >> Traffic Control >> Apply QoS", select the gateway interface, enter the egress maximum bandwidth, click Add, and then click Apply & Save.

briterface	Ingress Max Earthvidth (Khps)	Egress Mas Bandwidth (Kbpe)	Ingress Palicy	Egress Policy
cellular 1	1000	1000		
ridge 1 =				
				4.444.44

### Method for applying the ingress and egress policies in ER800 via QoS:

1. Add a network link classifier. Click "QoS >> Traffic Control >> Classifier", check "Any Packets", set the source and destination addresses of the link, select



transmit protocols for QoS control, and click Add.

2. Set transmission policies. Click "QoS >> Traffic Control >> Policy", enter a custom policy name for "Name", enter the classifier name for "Classifier", set the guaranteed bandwidth, maximum bandwidth, and policy priority, and click Add.

3. Click "QoS >> Traffic Control >> Apply QoS", select the gateway interface, enter the policy name for "Ingress Policy" and "Egress Policy", click Add, and then click Apply & Save.



### 5.3.6 Traffic Control

### Method for enabling traffic control in ER800:

Click "Services >> Traffic Control", enable traffic control, set traffic control parameters, and click Apply & Save. After the settings are completed, the system generates an alarm, stops forwarding, or disables the interface when the traffic exceeds the limit according to the settings on this page.



	24
Monitoring	
Daily Limit	КВ 🗸
Start Hour	0 VHour
When Over Daily Limit	Only Reporting
Monthly Limit	MB ~
Start Day	1 v Days
When Over Monthly Limit	Only Reporting 🖌



## 5.4 Firewall

### 5.4.1 ACL

Access control list (ACL) is an access control technology based on packet filtering. It can pass or discard the packets on the interface based on preset conditions.

**Scenario:** All devices in the LAN (bridge 1) can access the Internet, except the device with IP address 192.168.2.100.

### Method for setting in ER800:

1. Click "Firewall >> ACL >> Add". Enter the ID and sequence number. A smaller sequence number indicates a higher priority. Select "deny" for "Action". Set "Source IP" to "192.168.2.100" and "Source Wildcard" to "0.0.0.0". Leave "Destination IP" empty, which indicates 0.0.0.0/0, that is, all IP addresses. Click Apply & Save.



Туре		extended v
ID		101
Sequence Number		100
Action		deny 🗸
Match Conditions		
Protocol		ip v
Source IP		192.168.2.100
Source Wildcard		0.0.0
Destination IP		
Destination Wildca	rd	
Fragments		
Log		
Description		

2. Return to the ACL page, add the rule with the ID you set before to the management rule of bridge 1, and click Add. Then click Apply & Save.





AUR 519	er Pedey	Accept						
an Com	Sequence Number	Actes	Professal	Searce	Destructor	Mare Cerefilians	Description	
101	10	antrol .		And Add & Alan				
192	10	parreithing	- 14	any	arts:			
1(¢)]	38	dany	- 14	-	ange port-80			
102	- 24	dens	200	any	and periods			
180	-	deep	14	479	piete III			
nia -	30	dety	14	419	arty: particità			
100	- 44	deep -		414	any portable			
				1.11	d' Ma	âây .	lines.	
ben U								

### 5.4.2 NAT

Network address translation (NAT) can be used when some hosts on a private network have been assigned with local IP addresses (that is, private IP addresses used only on the private network), but expect to communicate with hosts on the Internet (without encryption).

**Scenario:** A user expects to access a camera on the LAN of the device through the public network. The camera' s address is 192.168.2.100, and the opens port 18000 to provide video service.

1. Click "Firewall >> NAT", and select "DNAT" for "Action", and "Outside" for "Source Network". Select "IP PORT to IP PORT" or "INTERFACE PORT to IP PORT" for "Translation Type". The public IP address obtained through cellular is not fixed, so "INTERFACE PORT to IP PORT" is more convenient. Select "TCP" for "Transmit Protocol" because video service is transmitted over TCP. Select "cellular 1" (dialup interface for the cellular network) for "Interface" and set



"Port" to "20000". Set "IP Address" and "Port" under "Translated Address" to "192.168.200" and "18000" respectively. Click Apply & Save.

The router will redirect the TCP service destined for port 20000 of the cellular 1 interface to the internal IP address 192.168.2.100 and port 18000.

Action	DNAT 🛩
Source Network	Outside 🛩
Translation Type	INTERFACE PORT to IP PORT ~
Transmit Protocol	TCP +
Match Conditions	
Interface	cellular 1 🛩
Port	20000 -
Translated Address	
IP Address	192.168.2.100
Port	18000 -
Description	
Loa	

### 5.4.3 MAC-IP Binding

After MAC-IP binding, downstream devices can access the public network through the router only by using the IP address bound to the MAC address of the device.

### Method for binding the device's MAC address and IP address:

1. Click "Firewall >> ACL" and select "Block" for "Default Filter Policy".





Default Fi	tter Policy	floc	k ~				
curss Cor	ntrol List						
10	Bequence Number	Action	Protocol	Source	Destination	More Conditions	Description
3100	10	permit	ίφ.	any :	any .		
292	20	permithing	top	any	port=443		
382	20	dury	THE	-	any: port+30		
112	3D	dary	top		any: port=25		
382	-40	dery	10	ety.	any: port=22		
312	50	dery.	Auge .	Cara C	any port=11		
192	60	dery	- de	-	any: port=53		
					dd Mo	ally .	Dalata

2. Click "Firewall >> MAC-IP Binding", check "Enable", enter the MAC address

and IP address of the connected device, click Add, and click Apply & Save.

NDW	30			
C-IP Binding List				
MAC Address	IP Autom	a Description	1.12	
010100300000	192.166.2	1		
00:00:00:00				



## 5.5 Routing

### 5.5.1 Static Routing

Set the destination network, subnet mask, and interface or gateway as required.

		and an a start of the start of	Gateway	Distance	Track I
0.0.0.0	0.0.0.0	cellular 1		255	
192.168.10.0	255.255.255.0	bridge 1			
			¥.		

### 5.5.2 Dynamic Routing

Scenario: Enable dynamic routing between two LANs for mutual

communication between them. The topology is shown below.



### 5.5.2.1 RIP

Routing Information Protocol (RIP) is a simple internal dynamic routing protocol mainly used on small-scale networks.

Method for enabling dynamic routing between ER800\_A and ER800\_B over RIP in the scenarie:



1. Configure ER800\_A. Click "Routing >> Dynamic Routing >> RIP", check "Enable", and configure ER800\_A in the "Network" bar to announce the routing entry of ER800\_A.

nable		
Jpdate Timer	30	S
imeout Timer	180	s
arbage Collection Timer	120	s
/ersion	Default v	
how Advanced Options		
how Advanced Options etwork IP Address		etmask
etwork IP Address 192.168.1.0	□ • • • •	etmask 255.255.0
etwork IP Address 192.168.1.0 192.168.2.0	□ 255. 255.	etmask 255.255.0 255.255.0
etwork IP Address 192.168.1.0 192.168.2.0	255. 255.	etmask 255.255.0 255.255.0

2. Configure ER800\_B.



Indate Timer 30	
spuare miler	S
Timeout Timer 180	s
Garbage Collection Timer 120	S
/ersion Defa	iult 🗸
how Advanced Options	

IP Address	_	Netmask
192.168.1.0		255.255.255.0
192.168.3.0		255.255.255.0
		Add[0/64]

3. After the configuration is completed, check whether PC 1 can communicate

to PC 2. If yes, the dynamic route has been added successfully.

outing >>	Dynamic I	Routin	ng .				
oute Table	100		27. Thinks the	S6			
Type:	All	- (¥					
Туре	Destina	tion	Netmask	Goteway	Interface	Distance/Metric	Time
5	0.0.0	Ó	0.0.0.0	10.25.327.169	cellular I	255/0	
С	10.25.22	7.168	255,255,255,252		cellular 1	0/0	
C	127.0/	0.0	255.0.0.0		loopback 1	0/0	
6	197.168	5.1.0	255.255.255.0		bridge 1	0/0	
*	192.160	1.2.0	255.255.255.0	192.168.1.1	bridge 1	120/2	00:00:15
0	192.168	1.3.0	255.255.255.0		vian 2	0/0	



### 5.5.2.2 OSPF

Open Shortest Path First (OSPF) protocol is a link-status-based internal gateway protocol mainly used in large-scale networks.

### Method for enabling dynamic routing between ER800\_A and ER800\_B over

#### **OSPF** in the scenarie:

1. Configure ER800\_A. Click "Routing >> Dynamic Routing >> OSPF", check

"Enable", enter a valid IP address for "Router ID", and configure ER800\_A in the

"Network" bar to announce the routing entry of ER800\_A.

19acre	2					
louter ID	192.10	11				
loute Advanced Op	ations 🛛					
terface						
Interface	Network	Helis Interval	Dead Interval	Retransmit Interval	. 1	ranamit Deylay
	isehad + 35		40	5	3	
•)()	isekat + 31		*1			A880/100
• 1	isehet + 31		*?	3	3	A802/100
• 1	Options		47	1	1	A88925005
• 1	Options		49	8		A805/1000
• 1 Interface Advanced etwork	Options		**	8	3	A885/100
• 1 interface Advanced where it is a second structure it is a second st	Options	Area	e9	8	1	A880/100

2. Configure ER800\_B.



	3					
iouter ID	192.1	198.1.2				
louts Advanced O	Pptions 🔲					
terfore						
Intraster.	(Manageria)	1	2019201008		- 10	
Interface	Featurors	PtoRio Detarival	Dead Interval	Retransmit Driterval	- 10	unamit Deylay
-	supercase - 10		0	19	1.0.1	
	20000000				-	
						Add(0/10
	000001					Add(0/10
						Add(0/10
ntarface Advance	d Options					Ask(0/10
Interface Advance	d Optiona 🛛					Addp/10
Interface Advance	d Options 📋					Add()/10
Interface Advance etwork IP Address	d Options 📋 Retmail	Ares ID				Addp/10
Interface Advance letwork IP Address 192196130	d Options 📋 Netmail 295.755.25	Ares 10				Add(0/10

3. After the configuration is completed, check whether PC 1 can communicate

to PC 2. If yes, the dynamic route is added successfully.

oute Table	Static Routing					
Type:	All ~					
Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
5	0.0.0.0	0.0.0.0	10.25.227.169	cellular 1	255/0	
C	10.25,227.168	255.255.255.252		cellular 1	0/0	
c	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192,158,1.0	255,255,255.0		bridge 1	0/0	
0	192.168.2.0	255,255,255,0	192.168.1.1	bridge I	110/20	00:00:12
c	192.168.3.0	255,255,255.0		vien 2	0/0	

### 5.5.2.3 BGP

### Method for enabling dynamic routing between ER800\_A and ER800\_B over

#### **BGP** in the scenarie:

1. Configure ER800\_A. Click "Routing >> Dynamic Routing >> BGP", check "Enable", and set "AS number" as required.





toute Table RIP OSPF	BGP Filtering R	oute
Enable		
AS number	50	(1-4294967295)
Router ID		
Keepalive Time	60	s(0-65535)
Hold Time	180	s(0-65535)

2. In the "Neighbor" bar, click Add, enter ER800\_B' s IP address 192.168.1.2, set

"AS number" as required, and click Apply & Save.

Neighbor													
-	AS	EAGP Multihep	Passand	Update Tires Interval	Respetive Yore	mold Time	Update Source Briefface	Default Originate	Disable Pear	Next Hop Attribute	Distribute List Filter	Profix List Filter	Descrip
107,168,8,2	100				80	100		IALSE .	NALDE	FALSE			
2.										1.4	UC/DB	Marthy .	(print)

3. Enter a valid IP address for "Router ID", configure ER800\_A in the "Network" bar, and click Add to announce the routing entry of ER800\_A. Then click Apply & Save.





Enable	~	
AS number	50	(1-4294967295)
Router ID	192.168.1.1	
Keepalive Time	60	s(0-65535)
Hold Time	180	s(0-65535)
Show Advanced Options		
letwork		
IP Address	Net	mask
192.168.2.0	255.25	5.255.0

4. Configure ER800\_B. The parameters are the same as or corresponding to those of in ER800\_A.

Enable A5 osanibet Rauter ID	98. 180 180,148.1.1	0.429496229								
Regulae Time Hold Time	84 3.80	100-655258 100-6553558								
lhow Advanced Optiona										
P Address 1811063.0	94 215	0448 1752152								
		ANELINE								
eighter										
P Address AS ESSP member Multiber	Passand 3	teral Time	noid Time	lipdate linaros Interfaca	Default Drightete	Diseble Pase	Next Hep Annihube	Distribute List Filter	Prefix List Filter	Deart
College and the second		-	1.011		100.18	GALM	64108			

5. After the configuration is completed, check whether PC 1 can communicate to PC 2. If yes, the dynamic route is added successfully.



#### Routing >> Dynamic Routing

100 (CON ) 1	Pitting for	14			
Al v					
Destination	Netmask	Gateway	Interface	Distance/Metric	Time
0.0.0.0	0.0.0.0	10.25.227.169	cellular 1	253/0	
10.25.227.168	255,255,255,252		cellular 1	0/0	
127.0.0,0	255.0.0.0		loophack 1	0/0	
192.168.1.0	255,255,255,0		bridge 1	0/0	
192.168.2.0	255,255,255.0	192.568.1.1	bridge 1	20/0	00:04:52
192.168.3.0	255,255,255,0		vian 2	0/0	
	Al v Destination 0.0.0 10.75.227.168 1.27.0.0 192.168.1.0 192.168.2.0 192.168.3.0	Al ▼   Destination Netmask   0.0.0.0 0.0.0.0   10.25.227.168 255.255.255.252   127.0.0.0 255.0.00   192.168.1.0 255.255.255.0   192.168.2.0 255.255.255.0   192.168.3.0 255.255.255.0	All V   Destination Netmask Gateway   0.0.0 0.0.0 10.25.227.169   10.25.227.168 255.255.255.255 127.0.00   192.168.1.0 255.255.255.0 192.168.1.1   192.166.3.0 255.255.255.0 192.368.1.1	All V   Destination Netmask Gateway Interface   0.0.0 0.0.0 10.25.227.169 sellular 1   10.25.227.368 255.255.255.255 sellular 1   127.0.0.0 255.0.00 loopback 1   192.368.1.0 255.255.255.0 kridge 1   192.168.2.0 255.255.255.0 142.368.1.1   192.168.3.0 255.255.255.0 142.368.1.1	All V   Destination Netmask Gateway Interface Distance/Metric   0.0.0 0.0.0 10.25.227.169 sellular 1 255.0   10.25.227.168 255.255.255.255 sellular 1 0/0   127.0.0.0 255.0.0 loopback 1 0/0   192.168.1.0 255.255.255.0 intege 1 0/0   192.168.2.0 255.255.255.0 192.168.1.1 bridge 1 20/0   192.168.3.0 255.255.255.0 192.168.1.1 bridge 1 20/0



## 5.6 Link Backup

### 5.6.1 SLA

Service level agreement (SLA) is used to detect whether the router is disconnected with ISP.

### Method for adding an SLA entry in ER800:

Click "Link Backup >> SLA >> Add", enter the detected IP address for "Destination Address", set other parameters as required, click Add, and then click Apply & Save.

**Timeout (ms)** indicates the duration for determining a detection failure.

**Consecutive** indicates the number of detection failures resulting in a link failure.

laites (	SLA						_	
LA Ent	ry							
Index	Туре	Destination Address	Data size	Interval(s)	Timeout(ms)	Consecutive	Life	Start-tim
1	icmp-echo	118.122.120.22	56	30	5000	5	forever	riow
2	iong-echo v		56	30	5000	5	forever v	now y

### 5.6.2 Track

At present, track module can be used with following application modules: VRRP, static routing, and interface backup. If detection succeeds, the corresponding track entry will be in Positive state. If detection fails, the corresponding track entry will be in Negative state.

### Method for adding a track entry in ER800:



Click "Link Backup >> Track >> Track", set "Index" as required, select "SLA", "Interface", or "VRRP" for "Type", set "SLA/VRRP ID" based on the ID in the SLA list, set "Negative Delay (s)" and "Positive Delay (s)" as required, click Add, and then click Apply & Save.

**Negative Delay (s)**: Before switching in case of an abnormal state, system will delay for some time based on the Negative Delay setting (0 indicates switching immediatly).

Positive Delay (s): When a failure is recovered, system will delay for some time based on the Positive Delay setting before switch back to formar link(0 indicates immediate switching).

Index	Type	SLA ID/VRRP ID	Interface	Negative Delay(s)	Positive Delay(s)
1	slø	1		0	0
2 sla	1 B	1	• ]	0	0
					A00[0/10]
rack Actio	n				
Index	n Co	ntrol Service		Action	
Index	n Co ipsec	ntrol Service	positive-start;	Action /negative-stop	

#### Method for adding an IPsec track entry in ER800:

Click "Link Backup >> Track >> Track" and set "Index" as required. "positive-start/negative-stop" means starting the IPsec service when the track detection state is Positive and stopping the IPsec service when the track detection state is Negative.



#### Link Backup >> Track

ack O	bject				
ndex	Туре	SLA ID/VRRP ID	Interface	Negative Delay(s)	Positive Delay(s
1	sla	1		0	0
	sla y	1		0	0
	210	11.		0	
a <mark>ck A</mark>	ction				Add[0/10]
ack A	ction ex Co	ntrol Service		Action	Add[0/10]
ack A	ction ex Co	ntrol Service ipsec		Action positive-start/negative	Add[0/10]
ack A	ction ex Co	ntrol Service ipsec	positive-star	Action positive-start/negati t/negative-stop	Add[0/10] ve-stop

### 5.6.3 VRRP

**Scenario:** Multiple routers connect to one network at the same time. Router A acts as the host, and router B acts as a backup for router A. When router A fails, router B temporarily replaces router A as the host.

#### 1. Information of the VRRP backup group:

- Backup group ID is 1.
- The IP address of the virtual router in backup group is 10.5.16.88.
- Router A acts as the master router.
- Router B acts as a backup router.

#### 2. Network Diagram





Router	Ethernet port connected to host A	IP address of the port connected to host A	Priority	Work mode
ER800_A	bridge1	10.5.16.80	110	Preempti on
ER800_B	bridge1	10.5.16.81	100	Preempti on

## Method for configuring ER800\_A as the master router and ER800\_B as a

### backup router:

1. Configure ER800\_A.

Click "Link Backup >> VRRP", set "Virtual Route ID" as required, select the interface of ER800\_A, enter the virtual IP address, set the interface priority to 110, and click Add.



nable	Virtual Route ID	Interface		Virtual IP	Priority	Advertisement Interval(s)	Preemption Mode	Track ID
<b>H</b> (1		bridge I	۷	10.5.16.88	310	1	×.	

Click "Link Backup >> VRRP >> Status" to check the status of VRRP.

k Backup >> VRR	P			
tatus VRRP				
Virtual Route ID	Interface	VRRP Status	Priority	Track Status
1	bridge I	Master	110	*

2. Configure ER800\_B.

Click "Link Backup >> VRRP", set the interface priority to 100, and click Add.

Enable	Virtual Route ID	Interface	Virtual IP	Priority	Advertisement Interval(s)	Preemption Mode	Track ID
4	1	bridge 1	10.5.16.88	190	1	4	
2		bridge 1 👻		1	a - 1		

Click "Link Backup >> VRRP >> Status" to check the status of VRRP.

Backup >> VRR	•			
itus VRRP				
Virtual Route ID	Interface	VRRP Status	Priority	Track Status
1	bridge 1	Backup	100	

ER800\_A performs router functions under normal circumstances. When ER800\_A shuts down or fails, ER800\_B performs router functions. Preemption mode is intended to enable ER800\_A to continue to act as the master router



after it recovers.

### 5.6.4 Interface Backup

**Scenario:** VG710 accesses to the Internet via Wi-Fi, and an interface backup allows ER800 to access to the Internet through cellular when Wi-Fi is down. The topology is shown as below.



### Method for creating an interface backup in ER800:

1. Configure ER800 to access to the Internet via Wi-Fi.

Enable	
Station Role	Client 🛩
Default Route	
SNAT	
SSID	Inhand
	Scan
Auth Method	WPA2-PSK ¥
Encrypt Mode	CCMP v
WPA/WPA2 PSK Key	

2. Click "Link Backup >> SLA >> SLA", add an ICMP detection entry. Set the IP address to the host address that can be detected over ICMP on the public or



private network, for example, the public IP address 118.122.120.22. Click Apply

& Save.

LA Ent	try							
Index	Туре	Destination Address	Data size	Interval(s)	Timeout(ms)	Consecutive	Life	Start-tim
1	icmp-echo	118 122 170 22	56	30	5000	5	forever	now
2	icmp-echo v		56	30	5000	5	forever v	now -
2	icmp-echo v		56	30	5000	3	forever v	n

3. Click "Link Backup >> Track >> Track", add a track entry. Select "SLA" for "Type" and "dot11radio1" for "Interface", click Add, and then click Apply & Save.

Index	Туре	SLA ID/VRRP ID	Interface	Negative Delay(s)	Positive Delay(s
1	sla	1		0	0
2 sl	a v	/ 1	Y	0	0
					Add[0/10]
rack Acti	on				Add[0/10]
rack Acti Index	on Co	ntrol Service		Action	Add[0/10]
rack Acti Index	on Co ipsec	ntrol Service	positive-start	Action t/negative-stop	Add[0/10]

4. Click "Link Backup >> Interface Backup", select "dot11radio1" for "Main Interface" and "cellular 1" for "Backup Interface", and click Apply & Save.





Main Interface		Sackup Interface		Startup Delay	Up Delay	Down Delay	Track is
dot11radio 1	-	cellular 1	-	60	Ö	0	1
otiiradio 1	۷	cellular 1		60	0	0	1
otiiradio 1	XII	cellular 1	. 4	60	0	0	1

5. Click "Routing >> Static Routing", and add two routes for network access through the "dot11radio1" and "cellular 1" interfaces. A smaller value of "Distance" indicates a higher priority.

Destination	Netmask	Interface	Gateway	Distance	Track in
0.0.00	0.0.00	cellular 1		255	
0.0.00	0.0.0.0	dot11radio 1		244	
118.122.120.22	255.255.255.0	dot11radio 1		243	1
		*			.1.
				A	dd[2/128]

6. Trigger a Wi-Fi failure. According to the preset link detection policy, ER800 accesses tp the Internet through dial-up via the cellular port, and when Wi-Fi recovers, it will switch back to Wi-Fi immediately.



## 5.7 Wizards

Wizards module incorporates some common communication parameters, simplifies the operations.

### 5.7.1 New Cellular

After insert a common network interface card, click "Wizards >> New Cellular >> Apply & Save", then access to the status page to check the network connection status of the device.

ew Cellular			
Dial-up parameters		Auto	~
NAT		•	
Apply & Save	Cancel	1	


Network >> Cellular

Status Cellular	
Modem	
Active SIM	SIM 1
IMEI Code	353593090129021
IMSI Code	460110923582245
ICCID Code	89860318040283846651
Signal Level	(27 asu -59 dBm)
RSRP	-85 dBm
RSRQ	-14 dB
Register Status	registered
Operator	CHN-CT
Network Type	4G
LAC	9B11
Cell ID	9D54211

### 5.7.2 New IPsec Tunnel

Click "Wizards >> New IPsec Tunnel", set "Map Interface" to an interface ("bridge": bridge interface; "cellular": dialup interface; "dot11radio": Wi-Fi interface) for which you want to establish a tunnel, enter the peer IP address for "Destination Address", and enter the subnet IP addresses and masks at both ends of the tunnel. In Phase 1, enter the IDs at both ends of the tunnel and the connection key, and click Apply & Save.





lew IPsec Tunnel	
Basic Parameters	
Tunnel ID	1 ~
Map Interface	cellular 1 🗸 🗸
Destination Address	118.122.120.22
Negotiation Mode	Main Mode 🗸 🗸
Local Subnet	192.168.2.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.3.0
Remote Netmask	255.255.255.0
Phase 1 Parameters	
IKE Policy	3DES-MD5-DH2
IKE Lifetime	86400
Local ID Type	IP Address 🗸
Local ID	
Remote ID Type	IP Address ∨
Remote ID	
Authentication Type	Shared Key 🐱
Key	•••••
Phase 2 Parameters	
IPSec Policy	3DES-MD5-96
IDCoc Lifetime	2600

### 5.7.3 IPsec Experts Configuration

This function is only for specific users. Please contact our technical support.

### 5.7.4 New L2TPv2 Tunnel

Set the parameters of the L2TP server and the local/remote address. Click Apply

& Save.



#### Wizards >> New L2TPv2 Tunnel

New L2TPv2 Tunnel

ID	1
L2TP Server	118.122.120.22
Source Interface	cellular 1 v
Username	test
Password	•••••
Authentication Type	Auto 🗸
Hostname	
Enable Challenge Secret	
Local IP Address	
Remote IP Address	
Remote Subnet	
Remote Netmask	255.255.255.0
Link Detection Interval	60 S
Max Retries for Link Detection	5
NAT	
MTU	1500
MRU	1500

### 5.7.5 New Port Mapping

Port mapping is to map a host' s port on the intranet to a port on the extranet. When a user accesses the port on the extranet, the server will automatically map the request to the internal machine on the corresponding port.

**Scenario:** Users on the extranet cannot directly access to a web server in the intranet. In this case, a port mapping in the router can automatically transfers



the data to port 80 of the web server in the intranet when a user on the extranet

accesses port 1000 via the cellular interface of the router.



#### Method for creating a port mapping in ER800:

Click "Wizards >> New Port Mapping". Enter the interface for "Outside Interface", port for "Service Port", IP address of the internal host for "Internal Address", and port ID of the internal host for "Internal Port". Click Apply & Save.

lew Port Mapping		
Transmit Protocol	TCP V	
Outside Interface	cellular 1 V	
Service Port	1000	
Internal Address	192.168.2.55	
Internal Port	80	
Description		



# 6 System Management

## 6.1 System

Click "Administration >> System >> Status" to check the current system and network status of the device.

System Status	
System Status	
Name	ER800
Model	ER805
Serial Number	IR8052113F65E43
MAC Address	0012.3344.5566
Firmware Version	V1.0.2
Bootloader Version	2012.07.r500
Device Time	2021-05-11 14:32:13
PC Time	2021-05-11 14:32:14 Sync Time
Jp <mark>time</mark>	1 day, 05:28:12
CPU Load (1 / 5 / 15 mins)	0.00 / 0.01 / 0.00
lemory consumption otal/Free	482.96MB / 314.69MB (65.16%)
Network Status	
Cellular 1 [Settings]	
Status	Disconnected
Signal Level	. (0 asu -113 dBm)
Register Status	registering
IP Address	0.0.0.0

Click "Basic Setup" to modify the system language and device name.



### Administration >> System

Status Basic Setup		
Language		English <b>v</b>
Device Name		ER800
Apply & Save	Cancel	



## 6.2 System Time

To ensure the coordination between the router and other devices, please set

the system time accurately.

#### Synchronize system time manually:

Click "Administration >> System Time >> System Time >> Sync Time" to

ensure consistency between the router time and PC time.

2020-01-16 17:02:50
Sync Time
2020 - / 01 - / 16 -
17 v]: 02 v : 38 v

#### Synchronize system time automatically:

Click "Administration >> System Time >> SNTP Client or NTP Server" and check "Enable" to synchronize the time between the router and SNTP or NTP server. After NTP is enabled, the router can synchronize time for all devices in the LAN.





Administration >> Syst	tem Time	
System Time SNTP Clie	ent NTP Server	
Enable	•	
Master	5	
Source Interface		¥
Source IP		
NTP Servers List		
Server Address	Prefer NTP Server	
	-	



## 6.3 Management Services

When need to access to router the via HTTP, HTTPS, TELNET, or SSH, click

"Administration >> Management Services", enable the services, and click Apply

& Save.



lanagement Services			
Enable		<b>v</b>	
Listen IP address		anv	T
Port		80	
Remote Access			
		_	
ITTPS			
Enable		×	
Listen IP address		any	•
Port		443	]
Remote Access			
Source Range	IP Wildcard		
		_	
	Add[0/5]		
ELNET			
Enable			
Listen IP address		any	Ŧ
Port		23	
Remote Access			
SH			
Enable			
Liston ID address			-



## 6.4 User Management

Click "Administration >> User Management" and create users, modify passwords, or delete users on the user management page.

#### Superuser and common user:

• Superuser: System will only create one superuser by default, with user name of **adm** and default password of **123456**. It has full access rights for function.

Note: You cannot delete the superuser, but can modify its password.

• Common user: Created by superuser, can check and modify router configurations.



## 6.5 AAA

AAA is a security management mechanism for access control in network security, which provides three security services: authentication, authorization, and accounting.

- Authentication: Verify whether a user has the right to access.
- Authorization: Authorize a user to use specific services.
- Accounting: Record a user' s network resource usage.

You can use only one or two of the security services provided by AAA. For example, if a company only expects to authenticate employees when they access to specific resources, the network administrator only needs to configure the authentication server. However, if a company expects to record the network usage of employees, the accounting server must be configured.

AAA usually works in client/server structure, which is highly scalable and convenient for centralized management of user information. as shown in the figure below.



## Note: Radius, Tacacs+ and LDAP indicate authentication and authorization

servers. Local indicates the local user name and password of the router.



### 6.5.1 Radius

Remote Authentication Dial in User Service (Radius) is a distributed information exchange protocol based on client/server structure. It protects the network from unauthorized access, and is usually used in various network environments that requires high security and allows remote user access.

#### Method for enabling Radius server in ER800:

Click "Administration >> AAA >> Radius". In "Server List", enter server address (domain name/IP address), port, and authentication key, click Add, and then click Apply & Save.

ver List			
Server	Port	Key	Source
	1812		
			Add[0/10

### 6.5.2 Tacacs+

Terminal Access Controller Access Control System + (Tacacs+) protocol is similar to Radius. It uses client/server mode for communication between the network access server (NAS) and the Tacacs+ server. However, Tacacs+ bases on TCP, and Radius bases on UDP. Tacacs+ protocol is mainly used for AAA' s end users, Point-to-Point Protocol (PPP) and virtual private dial-up network



(VPDN) access users. Its typical application is to authenticate, authorize, and perform accounting for end users who need to login the device. As a Tacacs+ client, the device sends user name and password to the Tacacs+ server for verification. After authentication and authorization, the user can login the device for operations.

#### Method for enabling Tacacs+ server in ER800:

Click "Administration >> AAA >> Tacacs+". In "Server List", enter server address (domain name/IP address), port, and authentication key, click Add, and then click Apply & Save.

List		
Server	Port	Key
	49	
		Addio

### 6.5.3 LDAP

The main advantage of Lightweight Directory Access Protocol (LDAP) lies in its quick response to users' search operations. For example, there will be massive user authentication operations perform concurrently. It will be inefficient if use database, because database is divided into various tables and will synthesise and filter in every searching. LDAP is equivalent to one table, and requires only user name, password, and some other parameters, which is quite simple. It can meet the authentication requirement regarding the efficiency and structure.



#### Method for enabling LDAP server in ER800:

Click "Administration >> AAA >> LDAP". In "Server List", enter any name for "Name", enter server address (domain name/IP address) and port, and enter the base DN obtained from the server. Set user name and password for accessing the server. Select "None", "SSL", or "StartTLS" for "Security". Click Add, and then click Apply & Save.

erver List							
Name	Server	Port	Base DN	Username	Paceword	Security	Verify Peer
		1				None +	10

### 6.5.4 AAA

#### Authentication methods:

- No authentication (**none**): No validity check is performed.
- Local authentication (local): User information is configured on the NAS.
  Local authentication is fast, which can reduce the operational costs, but the information storage amount is limited by hardware.
- Remote authentication: User information is configured on the authentication server. Remote authentication is supported over Radius, Tacacs+, and LDAP.

#### Authorization method:

• No authorization (**none**): No authorization is performed for users.



- Local authorization (**local**): Authorization is performed based on the properties configured by the NAS for the local account.
- Tacacs+ authorization: Users are authorized by the Tacacs+ server.
- Authorization after successful Radius authentication: Authorization is bound to authentication, and cannot be performed independently over Radius. Radius
- LDAP authorization

#### Method for enabling authentication and authorization in ER800:

Click "Administration >> AAA >> AAA Settings". 1, 2, and 3 are corresponding to Radius, Tacacs, ad LDAP respectively. Authentication entries 1, 2, and 3 must be corresponding to authorization entries 1, 2, and 3 respectively. If all of radius, tacacs+, and local are set, the priority sequence will be as follows: 1 > 2 > 3.

		1	Authenti	cation				3	Authoria	zation	0	
Service	1		2		3		1		2		3	
teinet	none	×.	none	6	none	100	none		none	÷	0006	
sah	none	¥	biorie	H	ridme	÷.	none	×	cons	÷	0008	
web	none	v	none	14	none	1	none		oone		opne	



## 6.6 Configuration Management

#### Method for importing configurations:

Click "Administration >> Config Management >> Config Management >>

Browse", select a configuration file, and click Import to import the configuration

file to the router.

# Method for backing up current running configurations to the PC (common):

Click Backup running-config.

#### Method for restoring default configurations:

Click Restore default configuration and then click OK.

Administration >> Config Management				
Config Management				
Configuration				
No file selected.	Browse	Import	Backup running-config	Backup startup-config
Auto Save after modify the configuration				
Encrypt plain-text password				
Backup running-config with private key				
Restore default configuration				



## 6.7 SNMP

### 6.7.1 SNMP

At present, the SNMP Agent in ER800 supports SNMPv1, SNMPv2c, and SNMPv3.

- SNMPv1 and SNMPv2c use community names for authentication.
- SNMPv3 uses user names and passwords for authentication.

#### Method for enabling SNMP in ER800:

Click "Administration >> SNMP >> SNMP", check "Enable", select "v1c" or

"v2c" for "SNMP Version", and click Apply & Save.

Enable	~			
Listen IP address	any	~		
SNMP Version	v2c ∨			
Contact Information	Beijing_Inha	nd_Network:		
Location Information	Beijing_Chin	a		
Community Name		Access Limit	MIB	/iew
public		Read-Only	Default	tView
		Read-Write	Default	tView
private			v DefaultView	
private		Read-Only	+ Derdalerren	

If use v3c, you need also to configure corresponding user and user group. Enter any name for "Groupname", select a security level, and click Add. Enter any name for "Username", select the new group name for "Groupname", set "Authentication" and "Authentication password", click Add, and then click Apply & Save.



labic									
sten IP address	any		¥						
NMP Version	v3 v	]							
ontact Information	Beijing	_Inhand_I	Networks						
ocation Information	Beijing	China							
	NoAuth/No	Priv v	DefaultVi	ew 🗸	Defau	ltView	~	Defa	aultView
	NoAuth/No	Priv v	DefaultVi	ew v	Defau	ltView	*	Defa	aultView Add[0/4
er Management(v3)	NoAuth/No	Priv v	DefaultVi	ew v	Defau	ltView	*	Defa	Add[0/4
er Management(v3) Username	Groupname	Priv v	DefaultVi	ew v	Defau	Encr	yption	Defa	Add[0/4 Encrypti passwo
er Management(v3) Username	Groupname	Priv v Authe None	DefaultVi intication	Authentic	Defau ation rd	Encr None	yption	Defa	Add[0/4 Add[0/4 Encrypti passwo

### 6.7.2 SNMP Trap (Alarm)

SNMP trap is a type of entrance. When this entrance is reached, the SNMP managed devices will actively notify the NMS, instead of waiting for the polling of NMS. In a SNMP-enabled network, the agents on managed devices can report errors to the NMS anytime, without waiting for the polling from NMS. The errors are reported to the NMS through traps.

#### Method for enabling SnmpTrap in ER800:

Click "Administration >> NMP >> SnmpTrap". Enter IP address of the NMS. Enter the corresponding group name when v1c or v2c is selected, or the corresponding user name when v3c is selected, ensuring that the name consists of 1–32 characters. By default, the UDP port ID ranges from 1 to 65535.



#### Administration >> SNMP

gure SnmpTrap		
Host address	Security Name	UDP Port
		162
		Add[0/4]

### 6.7.3 SnmpMibs

In SNMP messages, management variables are used to describe the managed objects in the device. SNMP uses a hierarchical naming scheme to identify the managed objects uniquely. The entire hierarchical structure is like a tree. Nodes of the tree represent the managed objects. As shown in the figure below, each node can be uniquely identified by a path starting from the root.



Management information base (MIB) is used to describe the hierarchical structure of the tree. It is a set of standard variable definitions for the monitored network device. In the above figure, managed object B can be



uniquely determined by a string of numbers {1.2.1.1}, which named object identifier (OID) of this managed object.

#### Method for downloading a SnmpMibs file to the PC:

Click "Administration >> SNMP >> SnmpMibs", select a folder, and click download to download it to the PC. Find the folder on the PC and import it to NMS.

Administration >> SNI SNMP SnmpTrap Sn	MP mpMibs	
Please select mib file:	IANAifType-MIB IANAifType-MIB IF-MIB INHAND-IPSECMONITOR-MIB INHAND-OVERVIEW-MIB INHAND-OVERVIEW-MIB INHAND-WAN3G-MIB RFC-1212 RFC1155-SMI RFC1213-MIB SNMPv2-MIB SNMPv2-SMI SNMPv2-TC	download





## 6.8 Alarm

The alarm function allows users to identify router's abnormalities in time. When an abnormality occurs, the router will report an alarm. You can select system-defined abnormalities and choose an appropriate notification way to obtain the abnormality information. All alarms are recorded in alarm logs so that users can identify abnormalities and perform troubleshooting in time.

#### Alarm states:

- Raise: indicates that the alarm has been generated but not been confirmed.
- Confirm: indicates that the alarm cannot be solved currently.
- All: indicates all generated alarms.

#### Alarm levels:

- EMERG: The device undergoes a serious error that causes a system reboot.
- CRIT: The device undergoes an unrecoverable error.
- WARN: The device undergoes an error that affects system functions.
- NOTICE: The device undergoes an error that affects system performance.
- INFO: A normal event occurs.

**1. Status:** Click "Administration >> Alarm >> Status" and view all alarms generated in the system since power-on.

dministration >> Alarm		Hard I				
Alarm State	48 14					
to stands beyon some	Rator	system runs	carbin			
Oear All Alarma	Cartere	unfirm All Alarm	a	Refead .		



**2. Alarm Inputs:** Select an alarm type as required. When this item is abnormal, an alarm is generated.

**3. Alarm Output:** When an alarm is generated, the system will send the alarm content to the destination email address automatically. Set the sender mail address in "Email Alarm" and the receiver mail address in "Mail Address". "Mail Server IP/Name" can be searched in the Internet.

nail Alarm			
inable Email Alarm:			
Mail Server IP/Name:			
Mail Server Port:	25		
Account Name:			
Account Password:			
Crypto:	NO	v	

**4. Alarm Map:** Alarms can be received in two ways: command line interface (CLI) (console interface) and Email. Some devices support SMS alarms. Please enable and set the email address on the "Alarm Output" page.



## 6.9 System Logs

#### Method for checking system logs:

Click "Administration >> System Log" to view system logs.

This page also provides the following operations: "Clear Log", "Download Log File", "Download Diagnose Data", "Clear History Log", and "Download History Log". History logs are those stored for extended time as specified on the "System Log" page. The diagnose data file is encrypted, you need to decrypt the file with the decryption tool provided by InHand.

dministration > + Log		autho.
Warmen Jan 16 17(2/15	Two many lags, skil dags are not displayed. Please disordinal lags like to their more lagst shaft(2000-00) as MDD as informatic encounted response (2): Solar response (2): Solar	
Warning Aut 10 17:12:15	obd/1450; PD at MID at WD to infoTypeiD miamatchinequeet ID Sulls, response ID: Sulla).	
Warning Int 16 1712-21	shult1850 misnatch between response length(); and aspected length();	
Warning Jan 16 LP/L2/65	(Driftenii Indonese regenza lang fick and aspected langfich)	
Warning Ast 18 LT-LLIS	obd() (50) PD in MD in MD in Mr. (and him and him and him and the QPA (201) (201) (201)	
Warning Jan 18 17(12)(5)	shattance mo a web or intelligent) minimately manual to doi:1, response to held.	
Warning law 18 17(12)31	obd(1498) PED to MEE to only Type(E) econstitutions and ED (balls, response ED (ball)	
Warning Ian 18 17(1)(1)	olog(1450) missiatuh between response bergth(2) and expected long(felt)	
Warning last 16 EP 12:03	und(1450) PED or MED or infoTypeED minimatchpreguest ED 5x21, response ED 5x28.	
Warning last 18 171310	obd(1410) PD or MD or info[god) econochimgoet (0-0623, regence (0-0623)	
Warning Am 18 17(1115)	shattand interaction have a supposed langthing and expected langthing	
Warning Ian 38 17(13-15	abd(145%) mianatch larturer response length(2) and expected langth(4)	
Warning Am 18 17(12)15	obd(1498) microbio between response length(3) and aspected length(3)	
Warning Net 18 17(12)15	ulu()4550 microstati between response length(3) and expected length(4)	
Warning Ser 18 1742-41	uto(\$1430) mianatch between miganise length(4) and paparited (sigh(3)	
Warning Aut 18 17(12)(1)	obd(1498) micrutch between response length(2) and expected length(4)	
Warning Ian 18 5712151	und(1456) PED or MED to Info/TypeED ensemble/groupeet ED Date, improved ED Date!	
Warning Am 10 1712151	ubd(1450) mianatch between response length(R and aspected lange(R)	
Warning Jan 10 LT112/35	obd(1458) PDD in MOD in reformation minimation equater ID: 0x5c, response ID: 0x5c)	
Warring Ian 16 17(13.0)	used[3456] mismatch between respince length(2) and espected length(4)	
	Cear Log Downland Log File Described Degrees 1943	
	Clear Wildowy Lag Barevilload Heldary Lag	

The storage space of the router is limited (512 KB by default). To save all the logs, you need to use a remote log server (for example, Kiwi Syslog Daemon). Set the address and port of the log server on the web page. The router will upload all the system logs to the remote log server.





og to Remote System	•	
Syslogd server address	P	ort Number
92.168.2.100	514	
		Add[0/4]
og to Console		
listory log size	512	KBytes(64-2048)
		land shaws

## 6.10 System Upgrade

Click "Administration >> Upgrade >> Browse", select an upgrade file, and click

Upgrade. Then restart the system after the upgrade is completed.

```
Administration >> Upgrade
```

Select the file to use:		
No file selected.	Browse	Upgrade
Firmware Version : V1.0.2	Diowse	opgrade

Note:

During the software upgrade, do not perform any operation on the web page;

otherwise, the software upgrade may be interrupted.





## 6.11 System Reboot

Click "Administration >> Reboot >> OK" to reboot the system.



# 7 Diagnostic Tools

Diagnostic tools are used to detect the network connection of the router: Ping,

Traceroute, Tcpdump, and Link Speed Test.

**Ping:** It is used to detect the external network connection of the device. Enter any common website for "Host" and click Ping. If data transmission occurs, the network is connected properly.

Host	8.8.8.8		Ping
Ping Count	4		
Packet Size	32	Bytes	
Expert Options			



#### Traceroute: Enter the IP address of the peer host and click "Trace" to detect the

lost	10.5 31 131	Trace
Aaximum Hops	20	
Timeout	3 s	
ransmit Protocol	UDP .	
xpert Options		

Tcpdump: Select an interface ("any" or "bridge1"), set "Capture Number", and

click Start Capture, Stop Capture and finally Download Capture File.

COT FILES	any *
apture Number	10 (10-1000)
pert Options	



#### Link Speed Test: Upload and download files to test the link speed.

Tools >> Link Speed Test						
Link Speed Test						
upload speed: 34100.17 kbps Back						

Note:

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

User Manual 🤇



### FCC Warning

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

♦ —Reorient or relocate the receiving antenna.

↔ —Increase the separation between the equipment and receiver.

 —Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

↔ —Consult the dealer or an experienced radio/TV technician for help.

#### ♦ FCC Caution

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The user manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

#### ♦ RF Exposure Statement

This equipment must be installed and operated in accordance with provide instructions and the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operation in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

♦ EUT configuration:

(FCC ID: 2AANYER805 contains FCC ID: XMR201807EP06A, IC: 11594A-ER805 contains IC: 10224A-201807EP06A)





## $\geq$

#### ISED statement

This device complies with Innovation, Science and Economic Development Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) This device may not cause interference, and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d' Innovation, science et développement économique au Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

#### **ISED RF Exposure Statement**

This equipment must be installed and operated in accordance with provide instructions and the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operation in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance. *ce matériel doit être installé et exploité conformément à des instructions et l'antenne utilisée pour cet émetteur doit être installé pour fournir une distance d'au moins 30 cm de toutes les personnes et ne doit pas être installé ou opération conjointement avec toute autre antenne ou transmitter.les utilisateurs finals et les installateurs doivent fournir des instructions d'installation et d'antennes - conditions relatives à l'exposition aux champs rf de conformité.* 

This radio transmitter [IC: 11594A-ER805] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Cet émetteur radio [IC: 11594A-ER805] a été approuvé par le Ministère canadien de l'innovation, de la science et du développement économique et peut fonctionner avec le type d'antenne indiqué ci - dessous et indiquer un gain maximal autorisé.Le gain d'un type d'antenne qui ne figure pas dans cette liste est supérieur au gain maximal de tout type énuméré et est strictement interdit d'utilisation avec le dispositif.

#### Antenna Information:

Antonna	Manufacturer	Model Number	Madal Number Antenna Gain	Impedance	Antenna	Antenna
Antenna		(Max)	(ohm)	Connector	Туре	
			2.72 dBi			
WiEi Ant 1	SHENZHEN		2412-2462MHz			
VVI-FI AIIL I	GUYOU		0.21 dBi	50		Mananala
Wi-Fi Ant. 2	TECHNOLOGY	GY-XPF-BCL2.5-GJG22	5150-5250MHz	50	RP-SMA(male)	Monopole
	CO.LTD		0.02 dBi			
			5725-5850MHz			
LTE Main Ant	SHENZHEN	GY-XPL-BDL2-AJG30				
	GUYOU			50		Managala
	TECHNOLOGY		U dBI	50	SMA-J(male)	Monopole
LIE Diversity Ant.	CO.LTD					