CP880-A LTE CPE

User Manual

Index

1 Ge	etting	g Started	4
	1.1	Welcome to the CPE	4
	1.2	Computer Configuration Requirements	4
	1.3	Logging In to the Web Management Page	4
2	Ove	rview	6
	2.1	Viewing Current Connection	6
	2.2	Viewing LTE Status	6
	2.3	Viewing WAN Status	6
3	Stat	istics	8
	3.1	Viewing CPU Usage	8
	3.2	Viewing Memory Usage	8
	3.3	Viewing APN List	9
	3.4	Viewing Throughput Statistics	9
	3.5	Viewing Device List	9
4	Upd	late	.11
	4.1	Version Manager	.11
		Viewing Version Info	.11
		Version Upgrade	.11
	4.2	Auto upgrade	.12
5	Sett	ings	.14
	5.1	Viewing the Device Information	.14
		Viewing the Version Information	.14
		Viewing LAN Status	.14
	5.2	Viewing Network	15
		LTE Settings	15
		Scan Mode	.18
		APN Management	.18
		PIN Management	.19
	SIM	Lock	21
		LAN Setting	.22
		DMZ Settings	.23
		Static Route	.24
	5.3	Firewall	25
		Setting Firewall	25
		MAC Filtering	26
		IP Filtering	.29
		URL Filtering	32
		Port Forwarding	.33
		UPnP	36
		DoS	.37

5.6 VPN	37
5.7 IPv6	38
Status	38
IPv6 WAN Settings	39
IPv6 LAN Settings	39
5.8 System	39
5.8.1 Maintenance	39
Reboot	39
Reset	40
Backup Configuration File	40
Upload Configuration File	41
5.8.2 TR069	41
5.8.3 Date & Time	42
5.8.4 DDNS	44
5.8.5 Diagnosis	45
Ping	45
Traceroute	46
5.8.6 Port Mirror	47
5.8.7 Syslog	48
Local	48
Network	48
5.8.8 WEB Setting	49
5.8.9 Account	50
5.8.10 Logout	51
6 FAQs	52

1 Getting Started

1.1Welcome to the CPE

In this document, the LTE (Long Term Evolution) CPE (customer premises equipment) will be replaced by the CPE. Carefully read the following safety symbols to help you use your CPE safely and correctly:

	Additional information
•••• •••	Optional methods or shortcuts for an action
	Potential problems or conventions that need to be specified

1.2Computer Configuration Requirements

For optimum performance, make sure your computer meets the following requirements.

Item	Requirement
CPU	Pentium 500 MHz or higher
Memory	128 MB RAM or higher
Hard disk	50 MB available space
Operating system	• Microsoft: Windows XP, Windows Vista, or Windows 7
	Mac: Mac OS X 10.5 or higher
Display resolution	1024 x 768 pixels or higher
Browser	• Internet Explorer 7.0 or later
	• Firefox 3.6 or later
	• Opera 10 or later
	• Safari 5 or later
	• Chrome 9 or later

1.3Logging In to the Web Management Page

Use a browser to log in to the web management page to configure and manage the CPE.

The following procedure describes how to use a computer running Windows XP and Internet Explorer 7.0 to log in to the web management page of the CPE.

1. Connect the CPE properly.

2. Launch Internet Explorer, enter <u>http://192.168.0.1</u> in the address bar, and press Enter. As shown in Figure 1-1.



Figure 0-1

- 3. Enter the user name and password, and click Log In.
- 4. You can log in to the web management page after the password is verified. As shown in Figure 1-2.





The default user name and password are both admin. If you want to view or configure the CPE more, you should use the super account to log in to the web management page.
 The default super user name is superadmin, and the password is admin.

To protect your CPE from unauthorized access, change the password after your first login.

The CPE supports diagnostic function. If you encounter problems, please contact customer service for the specific using method.

To ensure your data safety, it is recommended that you turn on the firewall, and conserve your login and FTP password carefully.

2 Overview

2.1Viewing Current Connection

To view the current connection, perform the following steps:

Choose Overview;

In the **Current Connection** area, view the connection status, such as DL/UL Data Rate and Online time. As shown in Figure 2-1.

C	C	
Current	Conn	ection

DL Data Rate	Current: 63 KB/s Max.: 63 KB/s Min.: 0 Bytes/s
UL Data Rate	Current: 51 KB/s Max.: 91 KB/s Min.: 0 Bytes/s
Online Time	00d 00h 33min

2.2Viewing LTE Status

To view the LTE network status, perform the following steps:

TE Ctature

- 1. Choose **Overview**;
- 2. In the **LTE Status** area, view the information about Connect status, Mode, Cell ID, Signal quality and so on. As shown in Figure 2-3.

LIE Status	
Status	Connected
Mode	TDD
Cell ID	203
RSRPO	-70 dBm
RSRP1	-81 dBm
RSRQ	-6 dB
SINR	30 dB

Figure 2-3

2.3Viewing WAN Status

To view the WAN status, perform the following steps:

- 1. Choose Overview;
- 2. In the WAN Status area, view the information about Connect Mode, IP, Subnet Mask,

DNS Server and so on. As shown in Figure 2-4.

WAN Status	
Connect Mode	NAT
IP Address	100.0.10.60
Subnet Mask	255.0.0.0
DNS Server	172.16.34.120
	114.114.114.114

Figure 2-4

3 Statistics

3.1Viewing CPU Usage

To view the CPU usage, perform the following steps:

- 1. Choose Statistics;
- 2. In the **CPU Usage** area, view the CPU usage information, such as Current CPU usage, Max CPU usage, Min CPU usage. As shown in Figure 3-1.



CPU Usage



3.2Viewing Memory Usage

To view the memory usage, perform the following steps:

- 1. Choose Statistics;
- 2. In the **Memory Usage** area, view the memory usage information, such as Total memory, Current memory usage, Max memory usage and Min memory usage. As shown in Figure 3-2.



Memory Usage

Figure 3-2

3.3Viewing APN List

To view the APN list, perform the following steps:

- 1. Choose Statistics;
- 2. In the **APN List**, view the information about APN information. As shown in Figure 3-3.

APN Name	81atus	IP Address	Subnet Wask
cont	L subk	120, 16, 14, 121	255.00.0
10 M	Croute.		-
- = 6X	Level de		
30Y	Citable		

Figure 3-3

3.4Viewing Throughput Statistics

To view the Throughput Statistics, perform the following steps:

- 1. Choose Statistics;
- 2. In the **Throughput Statistics** area, view the throughput statistics, such as APN throughput and LAN throughput.
- 3. In this area, also you can choose and click the button **Reset** to empty the throughput statistics. As shown in Figure 3-4.

Port		Rece	eved			Se	nt	
	Total Traffic	Packets	Errors	Dropped	Total Traffic	Packets	Errors	Dropper
LAN	2.97 MB	18065	0	0	17.44 MB	24725	0	0
aprit	12.96 MB	16003	0		1.65 MB	12305	0	0
apn2	0 Dytes	0	0		0 Dyten	0		0
apn3	0 Bytes	0	0		0 Dytes	0		0
apro4	0 Bytes	0	0		0 Eytes	0	0	0



3.5Viewing Device List

To view the device list, perform the following steps:

Choose Statistics;

In the **Device List** area, view the device information which connect to the CPE, such as Device name, Mac address, IP address and Lease time. As shown in Figure 3-5.

Device List					
Index	Device Name	MAC Address	IP Address	Lease Time	Туре
1	jingjin-PC	c0.18.da.ab.38.64	192.168.1.173	0days 11:59:51	WIFI

Figure 3-5

4 Update

4.1 Version Manager

This function enables you to upgrade the software version of the CPE to the latest version. It is recommended that you upgrade the software because the new version, certain bugs have been fixed and the system stability is usually improved.

Viewing Version Info

To view the version info, perform the following steps:

- 1. Choose Update>Version Manager.
- 2. In the **Version Info** area, you can view the product name and software version. As shown in Figure 4-1.



Figure 4-1

Version Upgrade

To perform an upgrade successfully, connect the CPE to your computer through a network cable, save the upgrade file on the computer, and make sure the CPE is not connected to anything other than a power adapter and the computer.

To perform an upgrade, perform the following steps:

- 1. Choose Update>Version Manager.
- 2. In the **Version Upgrade** area, click **Browse**. In the displayed dialog box, select the target software version file.

- 3. Click **Open**. The dialog box choses. The save path and name of the target software version file are displayed in the Update file field.
- 4. Click Submit.
- 5. The software upgrade starts. After the upgrade, the CPE automatically restarts and runs the new software version. As shown in Figure 4-2.



During an upgrade, do not power off the CPE or disconnect it from the computer.

account and	TRACKING ACTOR	AND	
Version File	透掉又件	未透睡任何又件	
Submit			

Figure 4-2

4.2Auto upgrade

To perform a ftp auto upgrade successfully, make sure the CPE is connected to the Internet.

To perform a ftp auto upgrade, perform the following steps:

Choose Update>Auto upgrade.

Enable auto upgrade.

If you want to check new firmware after connect to Internet, you need to enable the item of **Check new firmware after connect to Internet**.

Set a ftp address to the Upgrade folder box.

Set Version file.

Set User name and Password.

Set the Interval of checking new firmware.

Set Start time.

Set Random time.

Click **Submit**. As shown in Figure 4-3.



The CPE will automatically upgrade according to the setting. During an upgrade, do not disconnect the power supply or operate the CPE.

Overview Statistics	Update	Settings			
🛞 Version Manager					
근 Auto Upgrade	Au	to Upgrade			
		Settings			
		Auto Upgrade	2 Enable		
		Check New FW after connected	Enable		
		Upgrade Folder	ftp • ://		
		Version File	version.bd		
		Usemame	admin	-	
		Password	~		
		Check New FW Every	24		
		Start Time(24hrs)	0 *		
		Random Time	3 *		

Figure 4-3

5 Settings

5.1 Viewing the Device Information

To view the System Information, perform the following steps:

Choose Settings;

In the **System Information** area, view the system status, such as Running time. As shown in Figure 5-1.

System Information

Running Time

00d 02h 23min

Figure 5-1

Viewing the Version Information

To view the Version Information, perform the following steps:

- 1. Choose Settings;
- 2. In the **Device Information** area, view the device information, such as Product name, Product Model, Hardware Version, Software version, UBoot version and CPE SN . As shown in Figure 5-2.

Version Information

Product Model	ZR612
Hardware Version	V1.0
Software Version	MG12_0.3.2.9_V1.0-Standard
UBOOT Version	V1.0.0
Serial Number	N/A
IMEI	860524031765272
IMSI	460680004600024
	Figure 5-2

Viewing LAN Status

To view the LAN status, perform the following steps: Choose **Settings**; In the **LAN Status** area, view the LAN status, such as Mac address, IP address and Subnet mask. As shown in Figure 5-4.

LAN Status

MAC Address	A8:93:52:0A:12:90
IP Address	192.168.0.1
Subnet Mask	255.255.255.0

Figure 5-4

5.2Viewing Network

Network Mode

To set the network mode, perform the following steps:

Choose Network >WAN Settings; In the Network Mode area, select a mode between NAT and ROUTER; Click Submit. As shown in Figure 5-5.

Settings		
etwork Morie	Aut *	Subret Caren



LTE Settings

Settings

To set the LTE network, perform the following steps:

- 1. Choose Network >LTE Settings;
- 2. In the Settings area, you can set the configuration of LTE network;
- 3. In the **Status** area, you can view the LTE network connect status, such as Frequency, RSSI, RSRP, RSRQ, CINR, SINR, Cell ID and so on. As shown in Figure 5-7.

Overview Statistics	Update Settings	
Device Information		
🚠 Network	LTE Settings	
WAN Settings		
LTE Settings	Settings	
Scan Mode	Status	Connected
APN Management	Status	Connecteu
PIN Management	Connect Method	Auto 🔻
SIM Lock		
LAN Settings		
DMZ Settings		
Static Route	Status	
Firewall	DL MCS	0
VPN	UL MCS	0
- Bilbis	DL Frequency	3660.0 MHz
	UL Frequency	3660.0 MHz
System	Bandwidth	20 MHz
	RSSI	-66 dBm
	RSRPO	-92 dBm
	RSRP1	-96 dBm

Figure 5-7

Connect Method Setting

To set the connect method, perform the following steps:

- 1. Choose Network > LTE Settings;
- In the Setting area, Select a connect method between Auto and Manual. As shown in Figure 5-8.

Settings

Connect Method Manual	
Mamuaal	
Audo	



Auto Connect LTE Network

To set the CPE automatically connect to the internet, perform the following steps:

- 1. Choose Network > LTE Settings;
- 2. In the **Setting** area, set the connect method as **Auto**, when the LTE network is ready, the CPE will be connected automaticity. As shown in Figure 5-9.

Settings			
Status	Connected		
Connect Method	Auto	٣	
Status			
DL MCS	28		
UL MCS	22		
DL Frequency	36600 KHz		
UL Frequency	36600 KHz		
Bandwidth	20 MHz		
RSSI	-52 dBm		
RSRP0	-78 dBm		
RSRP1	-85 dBm		
RSRQ	-6 dB		
SINR	30 dB		



Manual Connect Mobile Network

To set the mobile network manual connect to the internet, perform the following steps:

- 1. Choose Network > LTE Settings;
- 2. In the **Setting** area, set the connect method as **Manual**, when the LTE network is ready, you can set the CPE connect to the LTE network or disconnect from the LTE network. As shown in Figure 5-10.

Settings		
Inne	Connected	
Career, Method	thmat	
	Claconnect	
		Subst Canal
Status		
0.403	28	
VALNON .	31	
di. Perganny	30000 494	
UL Prigeres	30000 shu:	
(and other	3014FW	
1000	-02 (001)	
-marging	-TT ddiwi	
0000M*1	- HO dates	
intrio.	4.00	
(senio)	32.49	
LE Prem	4 airy	
PO	10	
CONTRACTOR	25.2.40	
Cablerin.	212.00	

Figure 5-10

Scan Mode

To set the lte network scan mode, perform the following steps:

choose Network>Scan mode;

You can choose **full mode**, a band the CPE supported Click **Submit**.

Setting Frequency (Earfcn)

To set the frequency, perform the following steps:

- 1 Choose Network>Scan Mode.
- 2 In the **Scan Mode** area, choose **Frequency Lock**.
- 3 In the **Frequency Lock** area, you can choose a band, then click **Add list** to choose a **Earfcn Number**.
- 4 Click Submit. As shown in Figure 5-11.

	Update Settings			
Cever Information				
.T. Network	To put the new configuration into et	fect, must click thabrid batton after Add List		
WAN Settings				
LTE Settings				
Scan Mode	Settings			
APN Management	Scan Mode	Pressent Lock •		
PIN Management	0.00	- manual boost		
SIM LOCK	Frequency Lock			
LAN Settings	PADECH	autoria Add		
DM2 Settings	CHAPCH	1000		
Static Route	Frequency Lock List (Max Limit :5)		
Q Presid				_
VPN	Index	Frequency	Operation	
O m		44500	Delete	
Ödystem				
			Submit Cancel	



APN Management

To set and manage APN, perform the following steps:

Choose Network>APN Management.

In the APN Management area, you can set the APN.

Choose a **APN number** which you want to set.

In the **APN Setting** area you can set the APN parameters, such as enable or disable the apn, apn name, username, password and so on.

If you want set a APN as **default gateway**, you should check that is enabled.

Click Submit. As shown in Figure 5-12.

Overview Statistics	Update Settings	
Device Information		
T. Network	APN Management	
WAN Settings		
LTE Settings	APN Selection	
Scan Mode	ADM Number	
APN Management	APIN Number	
PIN Management	APN Settings	
SIM Lock		C. Frankla
LAN Settings	Enable	✓ Enable
DMZ Settings	Profile Name	apn1 *
Static Route	APN Name	APN1
💭 Firewall	AV 14 Hours	
🗳 VPN	Authentication Type	NONE *
@IPv6	PDN Type	IPv4 v
🔅 System	Default Gateway	☑ Enable
	Apply To	TR069
	Figure 5-12	

PIN Management

To manage the PIN, you can perform the following operations on the PIN Management page:

- > Enable or disable the PIN verification.
- ➢ Verify the PIN.
- Change the PIN.
- Set automatic verification of the PIN. As shown in Figure 5-13

Overview Statistics	Undate Settions	
Supply a	obeau ocounda	
Device Information		
.Z. Network	PIN Management	
WAN Settings		
LTE Settings		
Scan Mode	The PIN lock of the USIM-card	protects the router against unauthorized accesses to the Internet. You can activate, modify, or deactivate the PTN
APN Management	Note: The router cannot provide	Internet services when the USM card is not inserted or the PIN verification failed.
PIN Management		
SIM Lock		
LAN Settings	PIN Management	
DMZ Settings	12284 Cast States	1000 Mound
Static Route	COM Card Status	USIM NOTTINE
U Firewall	PIN Verification	Enable () Disable
C VPN	PIN	- ·
8m	Demokrika Allemetri	
Ö System	Hernaning Azempis	2



Viewing the Status of the USIM Card

To view the status of the USIM card, perform the following steps:

1 Choose Network >PIN Management.

2 View the status of the USIM card in the USIM card status field.

Enabling PIN Verification

To enable PIN verification, perform the following steps:

- 1 Choose **Network >PIN Management**.
- 2 Set **PIN verification** to **Enable**.
- 3 Enter the PIN (4 to 8 digits) in the Enter PIN box.
- 4 Click Submit.

Disabling PIN Verification

To disable PIN verification, perform the following steps:

- 1 Choose Network >PIN Management.
- 2 Set PIN verification to Disable.
- 3 Enter the PIN (4 to 8 digits) in the Enter PIN box.
- 4 Click Submit.

Verifying the PIN

If PIN verification is enabled but the PIN is not verified, the verification is required. To verify the PIN, perform the following steps:

- 1 Choose **Network >PIN Management**.
- 2 Enter the PIN (4 to 8 digits) in the **PIN** box.
- 3 Click Submit.

Changing the PIN

The PIN can be changed only when PIN verification is enabled and the PIN is verified. To change the PIN, perform the following steps:

- 1 Choose Network>PIN Management.
- 2 Set PIN verification to **Enable**.
- 3 Set Change PIN to Enable.
- 4 Enter the current PIN (4 to 8 digits) in the **PIN** box.
- 5 Enter a new PIN (4 to 8 digits) in the **New PIN** box.
- 6 Repeat the new PIN in the **Confirm PIN** box.
- 7 Click Submit.

Setting Automatic Verification of the PIN

You can enable or disable automatic verification of the PIN. If automatic verification is enabled, the CPE automatically verifies the PIN after restarting. This function can be enabled only when PIN verification is enabled and the PIN is verified.

To enable automatic verification of the PIN, perform the following steps:

1.	Choose Network > PIN Management
2.	Set Pin verification to Enable.
3.	Set Remember my PIN to Enable.

4. Click Submit.

Verifying the PUK

If PIN verification is enabled and the PIN fails to be verified for three consecutive times, the PIN will be locked. In this case, you need to verify the PUK and change the PIN to unlock it.

To verify the PUK, perform the following steps:

Choose Network> PIN Management.

Enter the PUK in the **PUK** box.

Enter a new PIN in the **New PIN** box.

Repeat the new PIN in the **Confirm PIN** box.

Click Submit.

SIM Lock

If you want to connect a specify network, and the CPE can't connect other network, you can set a SIM lock.

To set the SIM lock, perform the following steps:

- 1. Choose Network>SIM Lock.
- 2. Enter the PLMN in the **PLMN** box.
- 3. Click **Submit**. As shown in Figure 3-9.



LAN Setting

Setting LAN Host Parameters

By default, the IP address is 192.168.0.1 with a subnet mask of 255.255.255.0. You can change the host IP address to another individual IP address that is easy to remember. Make sure that IP address is unique on your network. If you change the IP address of the CPE, you need to access the web management page with the new IP address.

To change the IP address of the CPE, perform the following steps:

- 1. Choose Network>LAN Settings.
- 2. In the LAN Host Settings area, set IP address and subnet mask.
- 3. In the **DHCP Setting** area, set the DHCP server to **Enable**.
- 4. Click **Submit**. As shown in Figure 5-14.

evice Information		
twork	LAN Settings	
ttings		
igs	LAN Host Settings	
ie	ID Addrass	102 169 0 1
gement	IP Poureas	192.100.0.1
nent	Subnet Mask	255.255.255.0
1	DUIDE CONTRACT	
S	DHCP Settings	
ute	DHCP Server	Enable

Figure 5-14

Configuration the DHCP Server

DHCP enables individual clients to automatically obtain TCP/IP configuration when the server powers on. You can configure the CPE as a DHCP server or disable it. When configured as a DHCP server, the CPE automatically provides the TCP/IP configuration for the LAN clients that support DHCP client capabilities. If DHCP server services are disabled, you must have another DHCP server on your LAN, or each client must be manually configured.

To configure DHCP settings, perform the following steps:

- 1. Choose Network Setting > LAN Settings.
- 2. Set the DHCP server to **Enable**.
- 3. Set Start IP address.

This IP address must be different from the IP address set on the LAN Host Settings area, but they must be on the same network segment.

4. Set End IP address.

This IP address must be different from the IP address set on the LAN Host Settings area, but they must be on the same network segment.

- 5. Set Lease time.
 - Lease time can be set to 1 to 10,080 minutes. It is recommended to retain the default

value.

6. Click **Submit**. As shown in Figure 5-15.

Overview Statistics	; Update ; Settings			
Director information				
2.Network	LAN Settings			
WWW Settings				
LTE Settings	LAN Host Settings			
Scan Mode	IP Address	100 H00 H	1.	
APN Management	P AUGESS	196.100.0.1		
PtN Management	Subnet Mask	255 255 255 0]•	
SIM Lock	Disco Californi			
LAN Settings	DHCP settings			
Dis2 Settings	DHCP Server	# Enable		
Static Route	Trail IT Assesses	100 100 0 10	1.	
⊽ recent	Contro People	192.105.2.10		
C VPN	End IP Address	192.168.0.100]•	
8ms	Long Try	720	1.	
O System				
			Submit	Cancel

Figure 5-15

DMZ Settings

If the demilitarized zone (DMZ) is enabled, the packets sent from the WAN are directly sent to a specified IP address on the LAN before being discarded by the firewall.

To set DMZ, perform the following steps:

- 1. Choose Network > DMZ Settings.
- 2. Set DMZ to Enable.
- 3. (Optional) Set ICMP Redirect to Enable.
- 4. Set Host address.

This IP address must be different from the IP address set on the LAN Host Settings page, but they must be on the same network segment.

5. Click **Submit**. As shown in Figure 5-18.

Overview Statistics	Update Settings	
Device Information		
T. Network	DMZ Settings	
WAN Settings		
LTE Settings	DMZ	
Scan Mode	DMZ	E Enable
APN Management	DML	Chable
PIN Management	ICMP Redirect	Enable
SIM Lock	Host Address	192 168 0 28
LAN Settings	T TANKS 7 THEM I SHOP	100.000.00
DMZ Settings		
Static Route		
💭 Firewall		
🗳 VPN		
⊛ı₽v6		
🔆 System		

Figure 5-18

Static Route

Add Static Route

To add a static route, perform the following steps:

Choose Network Setting>Static Route.

Click Add list.

Set the **Dest IP address** and **Subnet mask**.

Select an Interface from the drop-down list.

If you select **LAN** as the interface, you need set a Gateway.

Click Submit. As shown in Figure 5-19.

Overview Statistics	: Updata Settings						
Denke Information							
J. Network	Static Route						
WAN Settings							
LTE Settings	Static Route L	let (Max Limit:10)					
Scan Mode							Addiet
APN Management							
PIN Management	index.	Destination IP 5	Subnet Mask	Interface	Gateway	Status	Operation
SIM Lock							
LAN Settings	Static Route S	attions					
DMZ Settings	Stats House S	and a					
Static Route	Destination IP	200.1.2.0					
Q Firewall	Subset Mask	268.268.268.0					
4 VFN							
@ #%	interface	aper 1	•				
() System							
							Submit Cancel



Modify Static Route

To modify an access restriction rule, perform the following steps:

- 1. Choose Firewall>Static Route.
- 2. Choose the item to be modified, and click **Edit**.
- 3. Repeat steps 3 through 5 in the previous procedure.
- 4. Click **Submit**. As shown in Figure 5-20.

	Update Settings						
Device information							
J. Network	Static Route						
WAN Settings							
LTE Settings	Static Route	List (Max Limit :10	1)				
Scan Mode							Add Lint
APN Management							Plate Link
PIN Management	Bruche m	Destination IP	Subnet Mask	Interface	Gateway	Status	Operation
SIM Lock	1	200.1.2.0	295.255.255.0	APNI	-	Effective	Detete 1 Dati
LAN Settings							
CB42 Settings	Cipic Boute	Californ					
Static Route	addite Provide	orongs					
U Fermal	Destination IP	125.2.6.1	• 00				
4 VPN	Subnet Marik	266,266,2					
₿P4							
Ö farsten	Interface	apr2					
							Submit Cancel

Figure 5-20

Delete Static Route

To delete a static route, perform the following steps:

Choose Firewall>Static Route.

Choose the item to be deleted, and click **Delete**.

5.3 Firewall

Setting Firewall

This page describes how to set the firewall. If you enable or disable the firewall, you can modify the configuration.

To set the firewall, perform the following steps:

Choose Firewall>Firewall Setting.

Choose Enable or Disable to modify the configuration.

Click **Submit**. As shown in Figure 5-30.

()) Device Information ∴ Network State	Firewall Setting		
U Firewall	Settings		
Firewall Setting	Firewall	Enable	
MAC Fillering			
IP Filtering			Submit Cancel
URL Filtering			COLOR COLOR
Port Forwarding			
Access Restriction			
UPap			
Do8			

Figure 5-30

If you choose enable the firewall, you can modify the configuration about firewall, such as Mac filter, IP filter, URL filter and so on. If you choose disable, you can't modify any configurations about the firewall.

MAC Filtering

This page enables you to configure the MAC address filtering rules.

Enabling MAC Filter

To enable MAC address filter, perform the following steps:

- 1. Choose Firewall>MAC Filtering
- 2. Set MAC filtering to **Enable**.
- 3. Click **Submit**. As shown in Figure 5-31.

MAC Filtering

MAC Filtering Manager				
MAC Filtering	🗹 Enable			
Within The Rule To Allow/Deny	 Allow 			
	O Deny			



Disabling MAC Filter

To disable MAC address filter, perform the following steps:

1. Choose Firewall>MAC Filtering

- 2. Set MAC filtering to **Disable**.
- 3. Click **Submit**. As shown in Figure 5-32.

MAC Filtering Manager

MAC Filtering	Enable
Within The Rule To Allow/Deny	Allow
	Deny



Setting Allow access network within the rules

To set allow access network within the rules, perform the following steps:

1. Choose Firewall>MAC Filtering.

- 2. Set Allow access network within the rules.
- 3. Click **Submit**. As shown in Figure 5-33.

MAC Filtering

MAC Filtering Manager				
MAC Filtering	🗹 Enable			
Within The Rule To Allow/Deny	 Allow 			
	O Deny			

Figure 5-43

Setting Deny access network within the rules

To set deny access network within the rules, perform the following steps:

- 1. Choose Firewall>MAC Filtering.
- 2. Set **Deny access network** within the rules.
- 3. Click **Submit**. As shown in Figure 5-34.

MAC Filtering Manager

MAC Filtering	Enable
Within The Rule To Allow/Deny	O _{Allow}
	• Deny

Figure 5-35

Adding MAC Filtering rule

To add a MAC filtering rule, perform the following steps:

Choose Firewall>MAC Filtering.

Click Add list.

Set MAC address.

Click **Submit**. As shown in Figure 5-35.

MAC Filtering	List (Max Li	mit 32)
---------------	--------	--------	---------

		Add List
Unders	MAC Address	Operation
Settings		
MAC Address	00 12 61 AE: C0 89	
		Submit Cancel

Figure 5-36

Modifying MAC Filtering rule

To modify a MAC address rule, perform the following steps:

- 1. Choose Firewall>MAC Filtering.
- 2. Choose the rule to be modified, and click **Edit**.
- 3. Set MAC address.
- 4. Click **Submit**. As shown in Figure 5-36.

MAC Filtering List (Max Limit :32)

		Add List
Indes	MAC Address	Operation
1	00.12/01 AE C0.09	Control 1 Gall
Settings		
dAC Address	00.12.61 AE C0.89	
		Submit Cancel
	Figure 5-37	

Deleting MAC Filtering rule

To delete a MAC address filter rule, perform the following steps:

Choose Firewall>MAC Filtering.

Choose the rule to be deleted, and click **Delete**. As shown in Figure 5-37.

MAC Filtering	List	(Max	Limit	:32)
---------------	------	------	-------	------

		Add List
Index	MAC Address	Operation
1	00:12:61.AE.C0:89	Delete Edit

Figure 5-38

IP Filtering

Data is filtered by IP address. This page enables you to configure the IP address filtering rules.

Enabling IP Filtering

To enable IP Filtering, perform the following steps:

- 1. Choose Firewall>IP Filtering.
- 2. Set IP Filtering Enable.
- 3. Click **Submit**. As shown in Figure 5-38.

IP Filtering Manager IP Filtering ☑ Enable Except The Rules To ◎ Allow Allow/Deny ○ Deny



Disabling IP Filtering

To disable IP Filtering, perform the following steps:

- 1. Choose Firewall>IP Filtering.
- 2. Set IP Filtering **Disable**.
- 3. Click **Submit**. As shown in Figure 5-39.

IP Filtering Manager

IP Filtering	Enable
Except The Rules To Allow/Denv	Allow
- and a cong	Deny



Setting Allow access network outside the rules

To set allow access network, perform the following steps:

- 1. Choose Firewall>IP Filtering.
- 2. Set Allow access network outside the rules.
- 3. Click **Submit**. As shown in Figure 5-40.

IP Filtering Manager

IP Filtering	Enable
Except The Rules To Allow/Denv	Allow
	⊖ _{Deny}



Setting Deny access network outside the rules

To set allow access network, perform the following steps:

- 1. Choose Firewall>IP Filtering.
- 2. Set **Deny access network** outside the rules.
- 3. Click **Submit**. As shown in Figure 5-41.

IP Filtering Manager

IP Filtering	Enable
Except The Rules To Allow/Denv	O _{Allow}
,	 Deny



Adding IP Filtering rule

Add an IP address filtering rule, perform the following steps:

- 1. Choose Firewall>IP Filtering.
- 2. Click Add list.
- 3. Set Service.
- 4. Set Protocol.
- In the Source IP Address Range box, enter the source IP address or IP address segment to be filtered.
- 6. In the **Source port range** box, enter the source port or port segment to be filtered.
- 7. In the **Destination IP Address Range** box, enter the destination IP address or IP address segment to be filtered.
- 8. In the **Destination port Range** box, enter the destination port or port segment to be filtered.
- 9. In the Status box, choose a status the rule will be executed.
- 10. Click **Submit**. As shown in Figure 5-42.

											-Add L
Index	Protocol		Source IF Address Rep	pe R	ourse Port 2004	Address Range	Deathrathin Range	(Port	Shine	14	Operation.
Settings											
Service .		Cetter		3							
Percol		41	-	8							
Same P. Addre	ou Range	102 805 1	99	1							
Insen Post Riv	er i										
Technalise (P. II	ation linge	100.13.64	128	3							
Centrality Put	Barge										
Data:		About	-								

Figure 5-13

Subret Cancel

Submit Gaocei

Modifying IP Filtering rule

To modify an IP filtering rule, perform the following steps:

- 1. Choose Firewall > IP Filtering.
- 2. Choose the rule to be modified, and click **Edit**.
- 3. Repeat steps 3 through 9 in the previous procedure.
- 4. Click **Submit**. As shown in Figure 5-43.

Index	Protocol	(;	Address Range	Range	Destination IP Address Range	Dealination Port Range	Shefter	Operation
91).	AL		182.168.1.320	NA	108.36.64.323	NA:	Alex	Denis 12.0
lettinge								
inves		Culton						
toimui		341						
iana 17 Adda	ni filesat	182 168.1	120					
iante Pati Rat	98							
holiptice ICA	dites. Birge	10.11.54	123					
estiption Port	Reat							
haf-m-		/9)e						



Deleting IP Filtering rule

To delete an IP address filtering rule, perform the following steps:

- 1. Choose Firewall > IP Filtering.
- 2. Choose the rule to be deleted, and click **Delete**. As shown in Figure 5-44.

IP Filtering Lis	st (Max Limit :	12)					
							Add List
Index	Protocol	Source IP Address Range	Source Port Range	Destination IP Address Range	Destination Port Range	Status	Operation
1	ALL	192.168.1.120	NDA	100.10.64.123	NA.	Allow	Delete I Edit
Figure 5-15							

URL Filtering

Data is filtered by uniform resource locator (URL). This page enables you to configure URL filtering rules.

Enabling URL Filtering

To enable URL Filtering, perform the following steps:

- 3. Choose Firewall>URL Filtering.
- 4. Set URL Filtering to Enable.
- 5. Click **Submit**. As shown in Figure 5-45.

URL Filtering Manager

URL Filtering

Enable

Figure 5-16

Disabling URL Filtering

To disable URL Filtering, perform the following steps:

- 1. Choose Firewall>URL Filtering.
- 2. Set URL Filtering to Disable.
- 3. Click **Submit**. As shown in Figure 5-46.

URL Filtering Manager

URL Filtering

Enable

Figure 5-17

Adding URL Filtering list

To add a URL filtering list, perform the following steps:

Choose Firewall>URL Filtering.

Click Add list.

Set URL.

Click **Submit**. As shown in Figure 5-47.

			Addition
Index	URL	Operation	
Settings			
046.	www.google.com		



Modify URL Filtering list

To modify a URL filtering rule, perform the following steps:

- 1. Choose Firewall>URL Filtering.
- 2. Choose the rule to be modified, and click **Edit**.
- 3. Set URL address.

URL Filtering List (Mas Limit :32)

4. Click **Submit**. As shown in Figure 5-48.

tister.		LHL	Constation	Add List
0		anne gangte state	- Delive I Tall	
Settings				
UNL	jours projector	•		

Figure 5-19

Deleting URL Filtering list

To delete a URL list, perform the following steps:

- 1. Choose Firewall>URL Filtering.
- 2. Choose the item to be deleted, and click **Delete**. As shown in Figure 5-49.

URL Filtering List (Max Limit 32)

		Add List
indea	URL	Concetton
1)	and the first state of	Tomos ritat



Port Forwarding

When network address translation (NAT) is enabled on the CPE, only the IP address on the WAN side is open to the Internet. If a computer on the LAN is enabled to provide services for the Internet (for example, work as an FTP server), port forwarding is required so that all accesses to the external server port from the Internet are redirected to the server on the LAN.

Adding Port Forwarding rule

To add a port forwarding rule, perform the following steps:

	Choose Firewall > Port Forwarding.
	Click Add list.
	Set Service .
	Set Protocol .
	Set Remote port range.
ę	The port number ranges from 1 to 65535.
	Set Local host.
	This IP address must be different from the IP address that is set on the LAN Host Settings page, but they must be on the same network segment.
	Set Local port.
—	The port number ranges from 1 to 65535.
	Click Submit . As shown in Figure 5-50.
Port Forwarding List ()	Mass Larvett (32.)

					And List
Indes	Printacell	Bernole Purt Range	Local Heat	Cascal Plant	Openation
Settings					
Samer	Castet				
Photocoli	TOP .	· ·			
Service Part Dange	2008	-			
and Heat	102 100 1 100				
Local Pert	3000				

Figure 5-21

Modifying Port Forwarding rule

To modify a port forwarding rule, perform the following steps:

- 1. Choose Firewall > Port Forwarding.
- 2. Choose the item to be modified, and click **Edit**.
- 3. Repeat steps 3 through7 in the previous procedure.
- 4. Click **Submit**. As shown in Figure 5-51.

ndes:	Prattool	Remote Port Range	Local Hoat	Local Part	Operation
	117	388	10.1081-00	300	Colors (12.8)
ettings					
118.0	Cuttor	-			
shout.	10P				
more Port Range	2068	•			
risk Heart	192 168 1.128	•			
11.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1	Since				



Deleting Port Forwarding rule

To delete a port forwarding rule, perform the following steps:

Choose Firewall > Port Forwarding.

Choose the item to be deleted, and click **Delete**. As shown in Figure 5-52.

Port Forwarding List	(Max Limit :32)				
					Add List
Index	Protocol	Remote Port Range	Local Host	Local Port	Operation
1	TCP	2000	192.168.1.120	3000	Delete I Edit

Figure 5-23

Access Restriction

Access Rest	riction List (Max),	mt :22.)				
						Anti
litelane.	Ender	Nume	Mevice	Washdays	Tinie	Operation
Settings						
Codine -	g but	84				
fame:	ADC	+				
Desira	00.12.63	with the second				
Weektops	(and a	Tue West The	Tel Bat Sun			
Title	14	1.10 - 21	50 - No 100			

Subret Cancel



Add Access Restriction

To add a access restriction rule, perform the following steps:

- 1. Choose Security>Access Restriction.
- 2. Click Add list.
- 3. Set Access Restriction to Enable.
- 4. Set Access Restriction Name.
- 5. Set Device MAC address or IP address.
- 6. Set Weekdays and time.
- 7. Click Submit.

Modify Access Restriction

To modify a access restriction rule, perform the following steps:

- 1. Choose Security>Access Restriction.
- 2. Choose the item to be modified, and click **Edit**.
- 3. Repeat steps 4 through 6 in the previous procedure.
- 4. Click Submit.

Delete Access Restriction

To delete a access restriction rule, perform the following steps:

- 1. Choose Security>Access Restriction.
- 2. Choose the item to be deleted, and click **Delete**.

UPnP

On this page, you can enable or disable the Universal Plug and Play (UPnP) function.

To enable UPnP, perform the following steps:

- 1. Choose Firewall > UPnP.
- 2. Set UPnP to Enable.
- 3. Click **Submit**. As shown in Figure 5-54.

UPnP					
Settings					
UPnP	🖸 Enable				
					Submit
Current UPnP Sta	itus				
Index	Description	Protocol	IP Address	External Port	Internal Port

Figure 5-24

DoS

On this page, you can enable or disable the Denial of service (DoS) function.

- 1 Choose Firewall > DoS.
- 2 Set UPnP to Enable.
- 3 Click **Submit**. As shown in Figure 5-55.

Device Information			
22. Network	DoS		
\$¢m-R			
💭 Firewali	DoS Setting		
Firewall Setting	De8	Enable Disable	
MAC Filtering			
IP Filtering	Bync Rood	Enable	
URL Filtering	Ping flood	Enable	
Port Forwarding	TCD and some	C. Freedow	
Access Restriction	TCP por scan	E trace	
UPnP	UDP port scan	Enable	
DeS			
C VPN			Submit Cancel
A			



5.6 VPN

This function enables you to connect the virtual private network (VPN).

To connect the VPN, perform the following steps:

Choose VPN.

In the VPN Settings area, enable VPN.

Select a protocol from **Protocol** drop-down list.

Enter Username and Password.

Click Submit.

You can view the status in **VPN Status** area. As shown in Figure 5-55.

🗶 Enable		
L21P		
172.16.14.120	1.0	
Yest	-	
F==	- ·	
Local Address	Remote Address	Online Time
	✓ Enable L21# 172.16.34.120 Feat Feat Local Address	Enable L21 T72:16:34:120 Feat Feat Feat



5.7 IPv6

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP). Every device on the Internet is assigned a unique IP address for identification and location definition.

Status

The status page shows IPv6 information. As shown in Figure 5-56.

IPv6 Information	
IPv6 Status	Active
WAN Connection Type	AutoConfiguration
IPv6 MGMT Global Addre	SS
IPv6 MGMT Global Addre	SS Configuration
IPv6 MGMT Global Addre LAN Address Auto IPv6 DATA Global Addres IPv6 Link-Local Address	ss Configuration is fe80::da55:a3ff:fe61:c4e0

IPv6 WAN Settings

In this page, user can enable or disable IPv6 function. Meanwhile, user can set WAN Connection Type and the type of DNS.As shown in Figure 5-27

WAN		
IPv6 Enable	🛛 Enable	
WAN Settings		
WAN Settings	AutoConfiguration	
WAN Settings MAN Connection Type Pv6 MGMT Global Addre	AutoConfiguration	·

Figure 5-57

IPv6 LAN Settings

In this page, user can chose the AutoConfiguration Type. As shown in Figure 5-58.





5.8 System

5.8.1 Maintenance

Reboot

This function enables you to restart the CPE. Settings take effect only after the CPE restarts. To restart the CPE, perform the following steps:

- 1. Choose System>Maintenance.
- 2. Click **Reboot**. As shown in Figure 5-59.

The CPE then restarts.



Reset

This function enables you to restore the CPE to its default settings.

- To restore the CPE, perform the following steps:
- 1. Choose **System>Maintenance**.
- Click Factory Reset. As shown in Figure 5-60. The CPE is then restored to its default settings.

Fa	actory Reset		
	Click Factory Reset	to restore device to its factory settings	
ĺ	Factory Reset		

Figure 5-60

Backup Configuration File

You can download the existing configuration file to back it up. To do so:

- 1. Choose System>Maintenance.
- 2. Click **Download** on the **Maintenance** page.
- 3. In the displayed dialog box, select the save path and name of the configuration file to be backed up.
- Click Save. As shown in Figure 5-61.
 The procedure for file downloading may vary with the browser you are using.

Backup Configuration File

To backup the current configuration file, click Download.

Download

Figure 5-61

Upload Configuration File

You can upload a backed up configuration file to restore the CPE. To do so:

- 1. Choose System>Maintenance.
- 2. Click **Browse** on the **Maintenance** page.
- 3. In the displayed dialog box, select the backed up configuration file.
- 4. Click **Open**.
- 5. The dialog box choses. In the box to be right of Configuration file, the save path and name of the backed up configuration file are displayed.
- 6. Click **Upload**. As shown in Figure 5-62.

The CPE uploads the backed up configuration file. The CPE then automatically restarts.

Restore Configuration File

To restore the configuration file, specify the path of the local configuration file, import the file, and click Upload to restore the configuration file

Configuration File 选择文件 未选择任何文件

Upload

Figure 5-62

5.8.2 TR069

TR-069 is a standard for communication between CPEs and the auto-configuration server (ACS). If your service provider uses the TR069 automatic service provision function, the ACS automatically provides the CPE parameters. If you set the ACS parameters on both the CPE and ACS, the network parameters on the CPE are automatically set using the TR-069 function, and you do not need to set other parameters on the CPE.

To configure the CPE to implement the TR-069 function, perform the following steps:

- 1. Choose System>TR069.
- 2. Set acs URL source. There are two methods, such as URL and DHCP.
- 3. In the ACS URL box, enter the ACS URL address.
- 4. Enter ACS user name and password for the CPE authentication.
 - To use the CPE to access the ACS, you must provide a user name and password for authentication. The user name and the password must be the same as those defined on the ACS.
- 5. If you set **Periodic inform** to **Enable**, set **Periodic inform interval**.
- 6. Set connection request user name and password.
- 7. Click **Submit**. As shown in Figure 7-5.

TR069

Settings		
Enable TR069	😤 Eriable	
ACS URL Source	URL Y	
ACS URL	http://192.168.0.10/acs	*
ACS Usemane	1069	*
ACS Plassword		
Enable Periodic Inform	🗷 Enable	
Periodic Inform Interval	3600	
Connection Request Usemaine	9069	
Connection Request Pastsword		

Figure 5-63

5.8.3 Date & Time

You can set the system time manually or synchronize it with the network. If you select **Sync from network**, the CPE regularly synchronizes the time with the specified Network Time Protocol (NTP) server. If you enable daylight saving time (DST), the CPE also adjusts the system time for DST.

To set the date and time, perform the following steps:

- 1. Choose System > Date & Time.
- 2. Select Set manually.
- 3. Set Local time or click Sync to automatically fill in the current local system time.
- 4. Click **Submit**. As shown in Figure 5-64.



Figure 5-64

To synchronize the time with the network, perform the following steps:

- 1. Choose **System > Date & Time**.
- 2. Select Sync from network.
- 3. From the **Primary NTP server** drop-down list, select a server as the primary server for time synchronization.
- 4. From the **Secondary NTP server** drop-down list, select a server as the IP address of the secondary server for time synchronization.
- 5. If you don't want to use other NTP server, you need to enable **Optional ntp server**, and set a server IP address.
- 6. Set Time zone.
- 7. Click **Submit**. As shown in Figure 5-65.

Settings	
Current Time	2017-10-26 15:23:33
) Set Manually	
Sync from Network	
rimary NTP Server	pool.ntp.org 🔻
condary NTP Server	asia.pool.ntp.org 💌
tional NTP Server	192.168.0.10
ne Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Figure 5-65

To set DST, perform the following steps:

- 1. Choose System>Date&Time.
- 2. Set **DST** enable.
- 3. Set Start Time and End Time.
- 4. Click **Submit**. As shown in Figure 5-66.

DST

DST	Enable
Start Time	Mar V Second V Mon V (2017-03-13) at 2 o'clock
End Time	Nov V First V Sun V (2017-11-05) at 2 o'clock
Status	Not Running

Figure 5-66

The CPE will automatically provide the DST time based on the time zone.

5.8.4 DDNS

Dynamic Domain Name Server (DDNS) service is used to map the user's dynamic IP address to a fixed DNS service.

To configure DDNS settings, perform the following steps:

- 1. Choose System > DDNS.
- 2. Set DDNS to Enable.
- 3. In Service provider, choose DynDNS.org or oray.com.
- 4. Enter **Domain name** and **Host name**. For example, if the domain name provided by your service provider is test.customtest.dyndns.org, enter customtest.dyndns.org as Domain name, and test as Host name.
- 5. Enter User name and Password.
- 6. Click **Submit**. As shown in Figure 5-67.

DDNS Settings

DDNS	😵 Enable	
Service Provider	WWW.DYNDNS	ORG 🔻
Dumain		•
Usemame		•
Password	-	
Refrests	0	
Enable Wildcard	E: Enable	
WAN IP and domain verif	lication 📄 Enable	



Submt

Cancel

5.8.5 Diagnosis

If the CPE is not functioning correctly, you can use the diagnosis tools on the **Diagnosis** page to preliminarily identify the problem so that actions can be taken to solve it.

Ping

If the CPE fails to access the Internet, run the ping command to preliminarily identify the problem. To do so:

Choose System>Diagnosis.

In the Method area, select Ping.

Enter the domain name in the **Target IP or domain** field, for example, <u>www.google.com</u>.

Set Packet size and Timeout.

Set Count.

Click Ping. As shown in Figure 5-68.

Wait until the ping command is executed. The execution results are displayed in the Results box.

• Prog	
O Toestian	
www.gough.com	
a*	
a .	
× -	
	Ping Caree
Pasa	
PRECenses groups constit 125: 199 1251 35 data tutos 64 hydro linux 61: 155 559 125; suppl titri 2 linux 701 209 mi 64 hydro linux 61: 155 169 226; suppl 109-12 linux 701 109 mi 64 hydro linux 61: 155 169 226; suppl 109-12 linux 702 199 mi 64 hydro linux 61: 155 169 226; suppl 109-24 https://22.109.109 mi	
	Prog Transflade Transflade

Figure 5-68

Traceroute

If the CPE fails to access the Internet, run the Traceroute command to preliminarily identify the problem. To do so:

- 1. Choose System>Diagnosis.
- 2. In the Method area, select **Traceroute**.
- 3. Enter the domain name in the Target IP or domain field. For example, <u>www.google.com</u>.
- 4. Set Maximum hops ad Timeout.
- 5. Click Traceroute. As shown in Figure 5-69

Wait until the traceroue command is executed. The execution results are displayed in the Results box.

Diagnostics			
Method			
Method of Diagnostics	O Proj		
	19 Transflande		
Traceroute			
Tiegel #*Donner	Sever people term		
Manmon Piers	18 · · ·		
Trund	(u		
		- spiniously in	
147012		Datatota	Cancal
Hasult			
Hendl	Pass		
Depaie	Tenedotoda Tanana geogla con XV1 126. 100.1221; 30 teges tran. 20 http speciale. 1 90: 1942. 1943. 21,42 (1902. 1963.22,42); 151.5573 ena 2 492. 1943.23 5 (1992. 1963.22,14); 1963.700 ena 1 972.14,34.1 (172.14,34.11); 1962.446; ena 1 972.14,144.1993 (122.14,144.194.1975); 186.446; ena 1 972.14,144.1993 (122.14,144.194.1975); 186.446; ena 1 978.226; 1967.1127 (126.226,144.194.1975); 186.230; ena 2 200.336; 15.809 (213.156,141.89); 191.671; ena	*	

Figure 5-69

5.8.6 Port Mirror

Port mirroring is used on a network switch to send a copy of network packets seen on one switch port. To do so:

- 1. Choose System>Port Mirror.
- 2. Enable Port Mirror.
- 3. Select the **WAN Interface** which you want a copy.
- 4. Type the **Monitor IP**, where the copy will send to.
- 5. Click **Sbumit**. As shown in Figure 5-70.

Port Mirror

A sale of a	SPRINGLAR - 1			
Lhube	Europe			
WAN Interface	apnt	~		
Forward IP Address	192.168.1.120	- i •	9	



5.8.7 Syslog

The syslog record user operations and key running events.

Local

To set the syslog to local, perform the following steps:

- 1. Choose System>Syslog.
- 2. In the **Setting** area, set the method to **Local**.
- 3. In the Level drop-down list, select a log level.
- 4. Click **Submit**. As shown in Figure 5-71.

-			
Method	 Network Local 		
Network			
Forward IP Address	192.168.1.120	•	

Figure 5-71

Viewing local syslog

To view the local syslog, perform the following steps:

In the **Keyword** box, set a keyword.

Click **Pull**, the result box will display.

Network

To set the syslog to network, perform the following steps:

- 1. Choose System>Syslog.
- 2. In the **Setting** area, set the method to **Network**.

- 3. In the Level drop-down list, select a log level.
- 4. In the Forward IP address box, set a IP address.
- 5. Click **Submit**. As shown in Figure 5-72.

The syslog will transmit to some client to display through network.

Syslog

Network
Local
168.1.120 *

Figure 5-72

5.8.8 WEB Setting

To configure the parameters of WEB, perform the following steps:

- 1. Choose System> WEB Setting.
- 2. Set **HTTP** enable. If you set HTTP disable, you will can't login the web management page with the HTTP protocol from WAN side.
- 3. Set **HTTP port**. If you want to change the login port, you can set a new port in the box, the default HTTP port is 80.
- 4. Set **HTTPS** enable. If you want to login the web management page with the HTTPS protocol from WAN side, you need to enable the HTTPS.
- 5. If you want to login the web management page form the **WAN**, you need to Enable **Allowing login from WAN**.
- 6. Set the **HTTPS port**.
- 7. Click **Submit**. As shown in Figure 5-73.

WEB Setting

HTTP Enable	😥 Enable	
HTTP Port	80	*
HTTPs Enable	😹 Enable	
Allow HTTPs Login tiom WAN	🗄 Enable	
Allow PING from VAN	E Enable	
HTTPy Port	44)	34 (A)
Refresh Time	10	*:
Session Timeout	10	
Landuader	English +	

Figure 5-73

5.8.9 Account

This function enables you to change the login password of the user. After the password changes, enter the new password the next time you login.

To change the password, perform the following steps:

- 1. Choose System>Account.
- 2. Select the **user name**, if you want to change the password of normal user, you need to set **Enable User** enable.
- 3. Enter the current password, set a new password ,and confirm the new password.
- 4. New password and Confirm password must contain 5 to 15 characters.
- 5. Click **Submit**. As shown in Figure 5-74.

Account

Usemame	admin	•	
Current Password		~ ·	
New Password		<u> </u>	
Confirm Password	1		

Figure 5-74

5.8.10 Logout

To logout the web management page, perform the following steps:

Choose System and click Logout

It will back to the login page.

6 FAQs

The POWER indicator does not turn on.

- Make sure that the power cable is connected properly and the CPE is powered on.
- Make sure that the power adapter is compatible with the CPE.

Fails to Log in to the web management page.

- Make sure that the CPE is started.
- Verify that the CPE is correctly connected to the computer through a network cable. If the problem persists, contact authorized local service suppliers.

The CPE fails to search for the wireless network.

- Check that the power adapter is connected properly.
- Check that the CPE is placed in an open area that is far away from obstructions, such as concrete or wooden walls.
- Check that the CPE is placed far away from household electrical appliances that generate strong electromagnetic field, such as microwave ovens, refrigerators, and satellite dishes.

If the problem persists, contact authorized local service suppliers.

The power adapter of the CPE is overheated.

The CPE will be overheated after being used for a long time. Therefore, power off the CPE when you are not using it.

Check that the CPE is properly ventilated and shielded from direct sunlight.

The parameters are restored to default values.

If the CPE powers off unexpectedly while being configured, the parameters may be restored to the default settings.

After configuring the parameters, download the configuration file to quickly restore the CPE to the desired settings.

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

 This device may not cause harmful interference, and 2) This device must accept any interference received, including interference that may cause undesired operation.

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 communication. 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.

Caution: Changes or modifications not expressly approved by BTI could void the user's authority to operate the equipment.

FCC Radiation Exposure statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.