



Application Guide

H8922S-Link Backup- WAN/Modem- IPsec



Contents

Contents	2
Revision History	2
1 Overview	3
2 Description	3
2.1 Main-backup mode	3
2.2 Mutually backup mode.....	9
2.3 IPsec connection insurance when link switch.....	10

Revision History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Doc Version	Product	Release Data	Details
V1.0	Hongdian Router	2017.08.22	First Release

1 Overview

In some field applications, it needs to enable link backup for IPsec VPN, to make sure the stable VPN connection. After the IPsec connection having been established in Hongdian Router via WAN, how can it make the modem as backup link, so that if WAN is unavailable, the IPsec is still works via modem link?

Here we would guide you for this case.

There are two ways to achieve the link backup for dual moedm, and we firstly introduce the two link backup individually, next show you how to apply the link backup to existed IPsec connection.

2 Description

2.1 Main-backup mode

Regarding the scene about wan and modem linkbackup, when wan link as main, modem link as backup, it can be supported. Settings are on page>>Network>>Link Backup.

Steps are as below.

1. We finish the settings about wan and modem, wan port is dhcp (for example the wan port method of getting the IP), modem port is according to your custom.

wan:

The screenshot shows the router's configuration interface. At the top, there is a navigation bar with tabs for Network, Applications, VPN, Forward, Security, System, and Status. Below this, there is a sub-navigation bar with tabs for LAN, WAN, WLAN, Modem, Parameter Select, Network Type, Link Backup, and DHCP Server. The 'Link Backup' tab is selected. The main content area shows a 'Connection Type' dropdown menu set to 'dhcp'. At the bottom of the form, there are 'Save' and 'Refresh' buttons.

modem:

Network	Applications	VPN	Forward	Security	System	Status	
LAN	WAN	WLAN	Modem	Parameter Select	Network Type	Link Backup	DHCP Server

modem

Interface Name	APN	Service Code	Username	Simcard	Operation			
1	---	---	card	SIM1	Mod	Del	En	Dis

2. If your Network Type settings has changed, please recover to the following.

Network	Applications	VPN	Forward	Security	System	Status	
LAN	WAN	WLAN	Modem	Parameter Select	Network Type	Link Backup	DHCP Server

Default Route

DNS Type

Interface Name

3. We use Link Backup feature, as following:

Network	Applications	VPN	Forward	Security	System	Status	
LAN	WAN	WLAN	Modem	Parameter Select	Network Type	Link Backup	DHCP Server

Rule Name	Running Mode	Backup Mode	Operation			
0	main	hot	Mod	Del	En	Dis
1	backup	hot	Mod	Del	En	Dis

Rule0 is for checking eth0, if wan link fail, the link will switch to backup link.

Note: If don't want backup link switch to main link immediately when main link is back ready for working, can setup the Running Timeout setting on Main link. The setup means: unless the main link is back and stable for that specific time, link doesn't switch. It will ensure the stability of the internet access.

For example: in image below, the timeout setting is set in main link, that means when main link resume, it should stable available for 1 hour. Then the link will switch from backup link to main link. If main link resumes but not stable available long enough for 1 hour, the counter will restart every time the link interrupted.

Network	Applications	VPII	Forward	Security	System	Status	
LAN	WAN	WLAN	Modem	Parameter Select	Network Type	Link Backup	DHCP Server

Status	<input type="button" value="Enable"/> <input type="button" value="Disable"/>
--------	--

Rule Name	<input type="text" value="0"/> * 0-9
Running Mode	<input type="text" value="main"/>
Backup Mode	<input type="text" value="hot"/>
Running Timeout	<input type="text" value="3600"/> 1-65535 s
Interface Name	<input type="text" value="modem 0"/>
Check IP or Domain	<input type="text" value="8.8.8.8"/> Max length is 64
Normal Interval	<input type="text" value="5"/> 1-65535 s
Retry Times	<input type="text" value="3"/> 1-65535

<input type="button" value="Save"/> <input type="button" value="Return"/>

Rule1 is for checking modem, When Main link is resume available, the link will switch to main link.

Network	Applications	VPN	Forward	Security	System	Status
LAN	WAN	Modem	Parameter Select	Network Type	Link Backup	DHCP Server

Status

Rule Name	<input type="text" value="1"/> * 0-9
Running Mode	<input type="text" value="backup"/>
Backup Mode	<input type="text" value="hot"/>
Running Timeout	<input type="text"/> 1-65535 s
Interface Name	<input type="text" value="modem 0"/>
Check IP or Domain	<input type="text"/> Max length is 64
Normal Interval	<input type="text"/> 1-65535 s
Retry Times	<input type="text"/> 1-65535

4. We add MASQ about eth0 and modem.

MASQ

Interface	Operation
eth0	Delete
modem	Delete

SNAT

Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation
----------	------------------	---------------	-----------------	--------------	-----------

DNAT

Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation
----------	------------------	---------------	-----------------	--------------	-----------

5. Please delete the default setting in page>>Forward>>Routing. When using link backup feature, this setting should be empty.

After that, the link backup setting is done, you will see the default route is eth0, refer to pic1, if wan link fail, the link will switch to modem link, you will see the default route is modem, refer to pic2

pic1

Static Route

Network	Subnet Mask	Gateway	Interface	Metric
192.168.251.137	255.255.255.255	0.0.0.0	modem	0
192.168.1.0	255.255.255.0	0.0.0.0	eth0	0
192.168.8.0	255.255.255.0	0.0.0.0	br0	0
0.0.0.0	0.0.0.0	0.0.0.0	eth0	0

pic2

Network	Subnet Mask	Gateway	Interface	Metric
192.168.251.137	255.255.255.255	0.0.0.0	modem	0
192.168.1.0	255.255.255.0	0.0.0.0	eth0	0
192.168.8.0	255.255.255.0	0.0.0.0	br0	0
0.0.0.0	0.0.0.0	0.0.0.0	modem	0

PS: about the linkbackup totalswitch time instruction:

14-Jul 11:...	<30>Jul 14 11:38:12 linkbackup[6632]: ##### rule[0], main link[eth0], icmp check begin #####(linkbackup.c->1233)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:12 linkbackup[6632]: **** ICMP send icmp packet successful ****(icmp.c->219)	192.168.8.1
14-Jul 11:...	<31>Jul 14 11:38:15 time[250]: ntpclient -h ntp.sjtu.edu.cn -s return 14(time.c->111)	192.168.8.1
14-Jul 11:...	<27>Jul 14 11:38:15 time[250]: NTP failed!(time.c->302)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:15 linkbackup[6632]: recv_icmp_pack:select time out(icmp.c->79)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:15 linkbackup[6632]: **** ICMP Recv icmp packet timeout ****(icmp.c->299)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:17 linkbackup[6632]: **** ICMP send icmp packet successful ****(icmp.c->219)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:20 time[250]: last ntp failed, do ntp(time.c->188)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:20 linkbackup[6632]: recv_icmp_pack:select time out(icmp.c->98)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:20 linkbackup[6632]: **** ICMP Recv icmp packet timeout ****(icmp.c->299)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:22 linkbackup[6632]: **** ICMP send icmp packet successful ****(icmp.c->219)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:22 cloud_agent[6409]: cloud_agent version:140711-3.0.3[11-3.0.3](wmmp_main.c->216)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:22 cloud_agent[6409]: initialization failed, reset cloud_agent, initialize cloud_agent again(wmmp_main.c->...	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:24 cloud_agent[6691]: cloud_agent version:140711-3.0.3[11-3.0.3](wmmp_main.c->216)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:25 linkbackup[6632]: recv_icmp_pack:select time out(icmp.c->98)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:25 linkbackup[6632]: **** ICMP Recv icmp packet timeout ****(icmp.c->299)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:27 linkbackup[6632]: ##### rule[0], main link[eth0], icmp check end #####(linkbackup.c->1235)	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:27 linkbackup[6632]: now checking rule[0], check main link[eth0] ret[-2](0:success, <0failed)(linkbackup....	192.168.8.1
14-Jul 11:...	<30>Jul 14 11:38:28 linkbackup[6632]: switch from [rule:0] main [link:eth0] to [rule:1] backup [link:modem](linkbackup.c->...	192.168.8.1

From the log, the linkbackup switch from start to end, total cost 15s(retry time is 3), so every linkbakcup every check time cost 5s, we can draw the linkbakcup totalswitch time range is

Min: 5s*retry time<= linkbackup total switch time <= Max: normal interval+5s*retry time

2.2 Mutually backup mode

1. All settings are the same to Main/backup mode. The only difference in setting is to change main link rule name from 0 to 1-9 number. Then the main link rule will become a backup link which is equal to another rule. And the two rule are equal.

2. The working mode works this way:

When device start, device uses the rule with lower number rule at first.

When the link with lower rule number no longer available, device uses another rule.

When the link with higher rule number no longer available, device uses the other rule.

And this work mode continues. And no other case will trigger link switch.

Rule Name	Running Mode	Backup Mode	Operation			
2	backup	hot	Mod	Del	En	Dis
1	backup	hot	Mod	Del	En	Dis

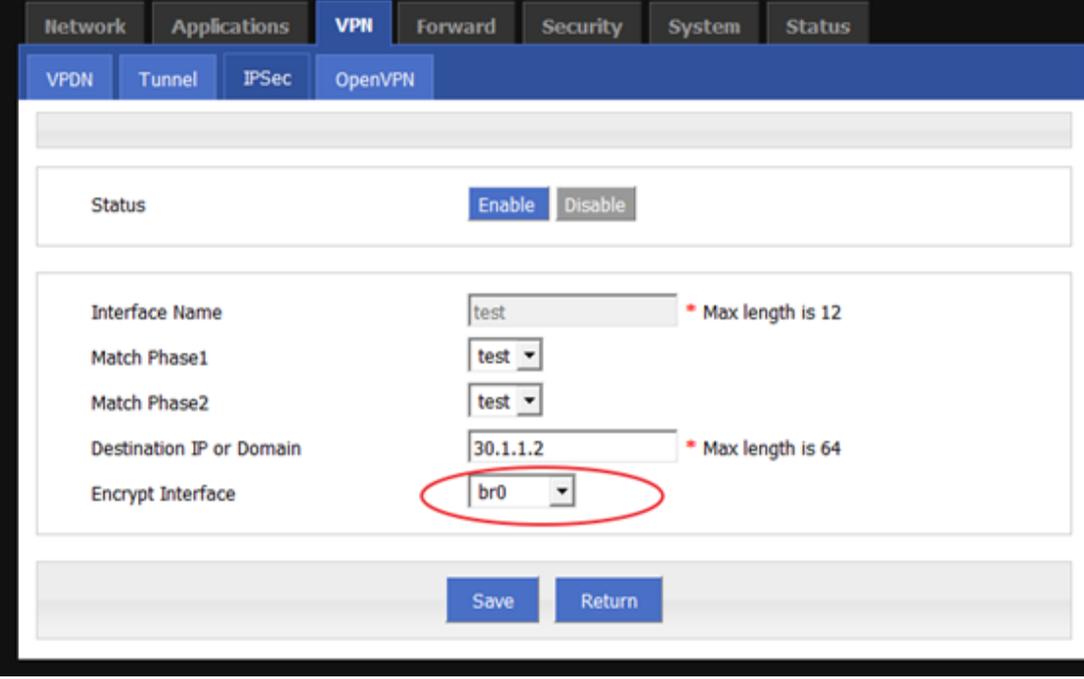
In the mutual backup mode, the “timeout “ is invalid.

2.3 IPsec connection insurance when link switch

When link switches between WAN and LTE, the IPsec connection need to rebuild.

To let WAN connection rebuild success through different link, the interface selection is important, Normally, when link not switch, the interface can be set to eth0 when link work on WAN. The interface can be set to modem, when use LTE.

However, in the link switch case, in order to let IPsec package be sent from correct interface, we should set the “Encrypt Interface” to “br0” as show in image below:



The screenshot displays the configuration page for an IPsec tunnel. The interface includes a navigation bar with tabs for Network, Applications, VPN, Forward, Security, System, and Status. Under the VPN tab, there are sub-tabs for VPDN, Tunnel, IPsec, and OpenVPN. The IPsec configuration section includes a Status toggle (Enable/Disable), an Interface Name field (test), Match Phase1 and Match Phase2 dropdowns (both set to test), a Destination IP or Domain field (30.1.1.2), and an Encrypt Interface dropdown menu (br0). The br0 option in the Encrypt Interface dropdown is circled in red. At the bottom of the configuration area, there are Save and Return buttons.

And to detect IPsec connection, and trigger it to restart when link switches, need to setup ICMP detection:
Make the source interface “br0” and make the command: `killall ipsec_init`

When IPsec cannot work, ICMP detection will trigger IPsec to reset, and IPsec will try to rebuild until connection is buildup successfully.

Network Applications VPN Forward Security System Status

ICMP Check DDNS SNMP Timing

ICMP Check Service

Basic Settings

Rule Name	<input type="text" value="IPSecdetect"/>	* Max length is 12
Destination Address	<input type="text" value="30.1.1.2"/>	* Max length is 64
Destination Backup	<input type="text" value="10.1.1.1"/>	Max length is 64
Normal Interval	<input type="text" value="10"/>	* 1-65535 s
Retry Times	<input type="text" value="3"/>	* 1-65535
Source Interface	<input type="text" value="br0"/>	
Timeout Action	<input type="text" value="custom"/>	
Run Commands	<input type="text" value="killall ipsec_init"/>	* Max length is 64



Create smart things



Contact us

 F14 - F16, Tower A, Building 14, No.12, Ganli 6th Road, Longgang District, Shenzhen 518112, China.

 +86-755-88864288-5

 +86-755-83404677

 hongdianchina

 www.hongdian.com

 sales@hongdian.com

 Hongdian_China