# 3G/4G无线路由器配置介绍

##

## H3C MSR810

### 电信脚本

<H3C\_example>dis current-configuration
#
 version 7.1.064, Release 0605P18
#
 sysname H3C\_example
#
时钟协议使用NTP
 clock protocol ntp
#
 telnet server enable
#
 ip load-sharing mode per-flow src-ip global
#
 dhcp enable
 dhcp server always-broadcast
#
 dns proxy enable
#
 password-recovery enable
#
vlan 1
#
vlan 10
#
dhcp server ip-pool lan1
 gateway-list 192.168.0.1
 network 192.168.0.0 mask 255.255.254.0
 address range 192.168.1.2 192.168.1.254
 dns-list 192.168.0.1
#
APN拨号账号定义
apn-profile dx
 apn static private.vpdn.zj
 authentication-mode chap user 809\_18969037291@caxyls.vpdn.zj password cipher $c$3$6
#

controller Cellular1/0
 eth-channel 0

 mode LTE
#
设备默认管理地址
interface Vlan-interface1
 ip address 192.168.0.1 255.255.254.0
 tcp mss 1280
#
本地网络网关地址
interface Vlan-interface10
 ip address 166.15.112.109 255.255.255.252
 undo dhcp select server
#
interface GigabitEthernet0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet0/2
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet0/3
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet0/4
 port link-mode bridge
#
interface Encrypt2/0
#
拨号接口参数配置（电信）
interface Eth-channel1/0:0
 dialer circular enable
 dialer-group 1
 dialer timer idle 0
 dialer timer autodial 60
 dialer number #777 autodial
 ip address cellular-alloc
 tcp mss 1280
 apn-profile apply dx
 ipsec apply policy map1
#
 scheduler logfile size 16
#
line class vty
 user-role network-operator
#
line con 0
 user-role network-admin
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
默认路由
 ip route-static 0.0.0.0 0 Eth-channel1/0:0
#
NTP配置
 ntp-service enable
 ntp-service source Eth-channel1/0:0
 ntp-service unicast-server 172.99.99.2
#
抓取vpn隧道第二阶段数据流（本地网段及允许访问网段）
acl advanced 3334
 rule 1 permit ip source 166.15.112.108 0.0.0.3 destination 145.0.0.0 0.255.255.255
#
domain system
#
 domain default enable system
#
user-group system
#
local-user admin class manage
 password hash $h$6$6wG
 service-type telnet http
 authorization-attribute user-role network-admin
#
建立证书域
pki domain test
 ca identifier 3G-root
 public-key rsa general name H3C\_example
 undo crl check enable
#
证书域策略调用group
pki certificate access-control-policy policy1
 rule 1 permit group1
#
证书域group（对端属性）
pki certificate attribute-group group1
 attribute 1 subject-name dn ctn topsec
#
ipsec第二阶段加密及认证参数
ipsec transform-set tran1
 esp encryption-algorithm sm1-cbc-128
 esp authentication-algorithm md5
#
ipsec第二阶段配置参数
ipsec policy map1 1 isakmp
 transform-set tran1
 security acl 3334
 remote-address 172.99.99.2
 ike-profile topsec
#
ike第一阶段配置参数
ike profile topsec
 certificate domain test
 local-identity dn
 match remote identity address 172.99.99.2 255.255.255.255
 match remote certificate policy1
 proposal 10
#
ike第一阶段加密及认证参数
ike proposal 10
 authentication-method rsa-signature
 encryption-algorithm sm1-cbc-128
 authentication-algorithm md5
#
 ip http enable
return

### 联通脚本

interface Eth-channel1/0:0
 dialer number \*99# autodial
 apn-profile apply lt

拨号接口注意修改dialer number 。其余配置和电信模板相同。

### 证书导入配置

证书申请（windows CA服务器）

申请证书-高级证书申请-创建并向此 CA 提交一个申请。



填写主要参数



安装此证书
INTERNET选项--内容--证书--找到证书名字,点击导出---是,导出私钥--密码12345678

H3C设备配置导入，先将中心证书及设备证书放到U盘根目录，然后在路由器中进入U盘路径。

#
cd usba0:/
sys
clock protocol none
quit
时间必须配置比证书申请时间晚，不然证书无法导入
clock datetime 12:12:12 2018/01/31
sys
#
pki domain test
 ca identifier 3G-root
 public-key rsa general name h3c
 undo crl check enable
quit
#
Pki import domain test pem ca filename root.cer
y
#
Pki import domain test p12 local filename h3c.pfx
12345678（证书从CA服务器上导出时配置的密码）
#

## 主要流程分析

### 拨号流程

<H3C\_example>debugging dialer all
<H3C\_example>debugging ppp all
\*Jan  1 00:02:40:950 2011 H3C\_example DDR/7/EVENT: Auto dial timer timed out, and trying to dial on interface Eth-channel1/0:0.
\*Jan  1 00:02:40:950 2011 H3C\_example DDR/7/EVENT: Found free channel on interface Eth-channel1/0:0, and trying to dial with it.
\*Jan  1 00:02:40:950 2011 H3C\_example DDR/7/EVENT: Dialing #777 on interface Eth-channel1/0:0, with user ID 0.
%Jan  1 00:02:41:037 2011 H3C\_example IFNET/3/PHY\_UPDOWN: Physical state on the interface Eth-channel1/0:0 changed to up.
%Jan  1 00:02:41:038 2011 H3C\_example IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Eth-channel1/0:0 changed to up.
\*Jan  1 00:02:41:079 2011 H3C\_example DDR/7/EVENT: Received a connect indication on interface Eth-channel1/0:0, with user ID 0 and call ID 0.
\*Jan  1 00:02:41:080 2011 H3C\_example DDR/7/EVENT: Link negotiation up on interface Eth-channel1/0:0.
\*Jan  1 00:02:41:080 2011 H3C\_example DDR/7/EVENT: Link network up on interface Eth-channel1/0:0.
\*Jan  1 00:02:41:081 2011 H3C\_example DDR/7/EVENT: Refresh wadj: interface = Eth-channel1/0:0, nexthop = 0.0.0.0, result = 0x0
  Peer Address: 199.99.99.162
  Phy interface: Eth-channel1/0:0
  VA interface: N/A
  MTU: 1500
  Node: 0
\*Jan  1 00:02:41:081 2011 H3C\_example DDR/7/PACKET: Link up on interface Eth-channel1/0:0. Dequeue and send packets.  Map info:
    Interface: Eth-channel1/0:0
    Map type: dialer number
    NextHop: 0.0.0.0
    Mask: 0.0.0.0
    VPN instance: 0
    Broadcast: 1

### ipsec隧道建立流程

<H3C\_example>debugging ike all
<H3C\_example>debugging ipsec all

***第一阶段IKE***
\*Jan 31 01:10:37:764 2018 H3C\_example IKE/7/EVENT: Received packet successfully.
\*Jan 31 01:10:37:765 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received packet from 172.99.99.2 source port 500 destination port 500.
\*Jan 31 01:10:37:765 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500

  I-Cookie: 18bafc8383ab10b1
  R-Cookie: 0000000000000000
  next payload: SA
  version: ISAKMP Version 1.0
  exchange mode: Main
  flags:
  message ID: 0
  length: 200
\*Jan 31 01:10:37:765 2018 H3C\_example IKE/7/EVENT: IKE thread 1097143584 processes a job.
\*Jan 31 01:10:37:765 2018 H3C\_example IKE/7/EVENT: Phase1 process started.
\*Jan 31 01:10:37:765 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Begin a new phase 1 negotiation as responder.
\*Jan 31 01:10:37:767 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Responder created an SA for peer 172.99.99.2, local port 500, remote port 500.
\*Jan 31 01:10:37:767 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Set IKE SA state to IKE\_P1\_STATE\_INIT.
\*Jan 31 01:10:37:767 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Security Association Payload.
\*Jan 31 01:10:37:767 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Vendor ID Payload.
\*Jan 31 01:10:37:768 2018 H3C\_example IKE/7/EVENT: Vendor ID DPD is matched.
\*Jan 31 01:10:37:768 2018 H3C\_example IKE/7/EVENT: Vendor ID NAT-T rfc3947 is matched.
\*Jan 31 01:10:37:769 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Process SA payload.
\*Jan 31 01:10:37:769 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Check ISAKMP transform 0.
\*Jan 31 01:10:37:769 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Lifetime type is 1.
\*Jan 31 01:10:37:769 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Life duration is 86400.
\*Jan 31 01:10:37:769 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Encryption algorithm is SM1-CBC.
\*Jan 31 01:10:37:769 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  HASH algorithm is HMAC-MD5.
\*Jan 31 01:10:37:769 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Authentication method is RSA signature.
\*Jan 31 01:10:37:769 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  DH group is 1.
\*Jan 31 01:10:37:770 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Attributes is acceptable.
\*Jan 31 01:10:37:770 2018 H3C\_example IKE/7/EVENT: Oakley transform 0 is acceptable.
\*Jan 31 01:10:37:770 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Constructed SA payload
\*Jan 31 01:10:37:770 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct NAT-T rfc3947 vendor ID payload.
\*Jan 31 01:10:37:770 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct XAUTH Cisco Unity 1.0 vendor ID payload.
\*Jan 31 01:10:37:770 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct XAUTH draft6 vendor ID payload.
\*Jan 31 01:10:37:770 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
IKE SA state changed from IKE\_P1\_STATE\_INIT to IKE\_P1\_STATE\_SEND2.
\*Jan 31 01:10:37:771 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sending packet to 172.99.99.2 remote port 500, local port 500.
\*Jan 31 01:10:37:771 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500

  I-Cookie: 18bafc8383ab10b1
  R-Cookie: 48c6c8b7cdc64805
  next payload: SA
  version: ISAKMP Version 1.0
  exchange mode: Main
  flags:
  message ID: 0
  length: 136
\*Jan 31 01:10:37:771 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sending an IPv4 packet.
\*Jan 31 01:10:37:771 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sent data to socket successfully.
\*Jan 31 01:10:37:804 2018 H3C\_example IKE/7/EVENT: Received packet successfully.
\*Jan 31 01:10:37:804 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received packet from 172.99.99.2 source port 500 destination port 500.
\*Jan 31 01:10:37:805 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500

  I-Cookie: 18bafc8383ab10b1
  R-Cookie: 48c6c8b7cdc64805
  next payload: KE
  version: ISAKMP Version 1.0
  exchange mode: Main
  flags:
  message ID: 0
  length: 188
\*Jan 31 01:10:37:805 2018 H3C\_example IKE/7/EVENT: IKE thread 1097143584 processes a job.
\*Jan 31 01:10:37:805 2018 H3C\_example IKE/7/EVENT: Phase1 process started.
\*Jan 31 01:10:37:805 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Key Exchange Payload.
\*Jan 31 01:10:37:805 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Nonce Payload.
\*Jan 31 01:10:37:805 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP NAT-D Payload.
\*Jan 31 01:10:37:806 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP NAT-D Payload.
\*Jan 31 01:10:37:806 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Process KE payload.
\*Jan 31 01:10:37:806 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Process NONCE payload.
\*Jan 31 01:10:37:806 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received 2 NAT-D payload.
\*Jan 31 01:10:37:842 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct KE payload.
\*Jan 31 01:10:37:845 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct NONCE payload.
\*Jan 31 01:10:37:845 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct certificate request payload.
\*Jan 31 01:10:37:845 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct NAT-D payload.
\*Jan 31 01:10:37:846 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct DPD vendor ID payload.
\*Jan 31 01:10:37:877 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
IKE SA state changed from IKE\_P1\_STATE\_SEND2 to IKE\_P1\_STATE\_SEND4.
\*Jan 31 01:10:37:877 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sending packet to 172.99.99.2 remote port 500, local port 500.
\*Jan 31 01:10:37:877 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500

  I-Cookie: 18bafc8383ab10b1
  R-Cookie: 48c6c8b7cdc64805
  next payload: KE
  version: ISAKMP Version 1.0
  exchange mode: Main
  flags:
  message ID: 0
  length: 236
\*Jan 31 01:10:37:878 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sending an IPv4 packet.
\*Jan 31 01:10:37:878 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sent data to socket successfully.
\*Jan 31 01:10:37:934 2018 H3C\_example IKE/7/EVENT: Received packet successfully.
\*Jan 31 01:10:37:934 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received packet from 172.99.99.2 source port 500 destination port 500.
\*Jan 31 01:10:37:934 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500

  I-Cookie: 18bafc8383ab10b1
  R-Cookie: 48c6c8b7cdc64805
  next payload: ID
  version: ISAKMP Version 1.0
  exchange mode: Main
  flags: ENCRYPT
  message ID: 0
  length: 1036
\*Jan 31 01:10:37:935 2018 H3C\_example IKE/7/EVENT: IKE thread 1097143584 processes a job.
\*Jan 31 01:10:37:935 2018 H3C\_example IKE/7/EVENT: Phase1 process started.
\*Jan 31 01:10:37:935 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Decrypt the packet.
\*Jan 31 01:10:37:935 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Identification Payload.
\*Jan 31 01:10:37:936 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Certificate Payload.
\*Jan 31 01:10:37:936 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Certificate RequestPayload.
\*Jan 31 01:10:37:936 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Signature Payload.
\*Jan 31 01:10:37:936 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Process ID payload.
\*Jan 31 01:10:37:936 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Peer ID type: DER\_ASN1\_DN (9).
\*Jan 31 01:10:37:937 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Peer ID value: DN C=CN, CN=topsec
\*Jan 31 01:10:37:939 2018 H3C\_example PKI/7/PKI\_DEBUG: PKI\_Certificate\_ACP: Matches the attribute 1 in attribute group 'group1'. Checking the next attribute.
\*Jan 31 01:10:37:939 2018 H3C\_example PKI/7/PKI\_DEBUG: PKI\_Certificate\_ACP: Matched rule number: 1, which has the action permit, in access control policy 'policy1'. The certificate is trusted.
\*Jan 31 01:10:37:939 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
The profile topsec is matched.
\*Jan 31 01:10:37:939 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Process certificate payload.
\*Jan 31 01:10:37:947 2018 H3C\_example PKI/7/PKI\_DEBUG: Verify certificate by domain test successfully.
\*Jan 31 01:10:37:947 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Verify signature payload.
\*Jan 31 01:10:37:948 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
HASH:
 cc0c99bb 7f58c196 2a3ebb2e 3ea3db64
\*Jan 31 01:10:37:949 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Signature verification succeeded.
\*Jan 31 01:10:37:949 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Process certificate request payload.
\*Jan 31 01:10:37:952 2018 H3C\_example PKI/7/PKI\_DEBUG: Get Local keypair successfully.
\*Jan 31 01:10:37:953 2018 H3C\_example PKI/7/PKI\_DEBUG: Get local certificate from cache successfully.
\*Jan 31 01:10:37:953 2018 H3C\_example PKI/7/PKI\_DEBUG: Get Local Certificates and keypair successfully.
\*Jan 31 01:10:37:953 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Local ID type: DER\_ASN1\_DN (9).
\*Jan 31 01:10:37:953 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Local ID value: DN.
\*Jan 31 01:10:37:953 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct ID payload.
\*Jan 31 01:10:37:954 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct certificate payload.
\*Jan 31 01:10:37:954 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
HASH:
 d0b64f9f b8ea4a07 e99ef2b1 de8baee5
\*Jan 31 01:10:37:994 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct authentication by private key.
\*Jan 31 01:10:37:995 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Encrypt the packet.
\*Jan 31 01:10:37:995 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
***IKE SA state changed from IKE\_P1\_STATE\_SEND4 to IKE\_P1\_STATE\_ESTABLISHED.第一阶段成功***
\*Jan 31 01:10:37:995 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sending packet to 172.99.99.2 remote port 500, local port 500.
\*Jan 31 01:10:37:995 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500

***ipsec第二阶段协商***
  I-Cookie: 18bafc8383ab10b1
  R-Cookie: 48c6c8b7cdc64805
  next payload: ID
  version: ISAKMP Version 1.0
  exchange mode: Main
  flags: ENCRYPT
  message ID: 0
  length: 1036
\*Jan 31 01:10:37:996 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sending an IPv4 packet.
\*Jan 31 01:10:37:996 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sent data to socket successfully.
\*Jan 31 01:10:37:996 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Add tunnel, alloc new tunnel with ID [1].
\*Jan 31 01:10:38:052 2018 H3C\_example IKE/7/EVENT: Received packet successfully.
\*Jan 31 01:10:38:052 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received packet from 172.99.99.2 source port 500 destination port 500.
\*Jan 31 01:10:38:052 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500

  I-Cookie: 18bafc8383ab10b1
  R-Cookie: 48c6c8b7cdc64805
  next payload: HASH
  version: ISAKMP Version 1.0
  exchange mode: Quick
  flags: ENCRYPT
  message ID: b1af4311
  length: 156
\*Jan 31 01:10:38:052 2018 H3C\_example IKE/7/EVENT: IKE thread 1097143584 processes a job.
\*Jan 31 01:10:38:052 2018 H3C\_example IKE/7/EVENT: Phase2 process started.
\*Jan 31 01:10:38:053 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Set IPsec SA state to IKE\_P2\_STATE\_INIT.
\*Jan 31 01:10:38:053 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Decrypt the packet.
\*Jan 31 01:10:38:054 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Hash Payload.
\*Jan 31 01:10:38:054 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Security Association Payload.
\*Jan 31 01:10:38:054 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Nonce Payload.
\*Jan 31 01:10:38:054 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Identification Payload (IPsec DOI).
\*Jan 31 01:10:38:054 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Identification Payload (IPsec DOI).
\*Jan 31 01:10:38:054 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Process HASH payload.
\*Jan 31 01:10:38:055 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Validated HASH(1) successfully.
\*Jan 31 01:10:38:055 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Process IPsec ID payload.
\*Jan 31 01:10:38:055 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Process IPsec ID payload.
\*Jan 31 01:10:38:055 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Set inside vrf to Nego flow info.
\*Jan 31 01:10:38:057 2018 H3C\_example IPSEC/7/EVENT:
 Could not find tunnel, ike profile name is topsec.
\*Jan 31 01:10:38:058 2018 H3C\_example IPSEC/7/EVENT:
Successfully get sp when getting SP for IKE, SP Index is 0, SP Seq is 1.
\*Jan 31 01:10:38:058 2018 H3C\_example IPSEC/7/EVENT:
 Succeed to get SP by flow.
\*Jan 31 01:10:38:058 2018 H3C\_example IKE/7/EVENT: Received message from ipsec, message type is 10.
\*Jan 31 01:10:38:058 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
IPsec SA state changed from IKE\_P2\_STATE\_INIT to IKE\_P2\_STATE\_GETSP.
\*Jan 31 01:10:38:059 2018 H3C\_example IKE/7/EVENT: IKE thread 1097143584 processes a job.
\*Jan 31 01:10:38:059 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Process IPsec SA payload.
\*Jan 31 01:10:38:059 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Check IPsec proposal 0.
\*Jan 31 01:10:38:059 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Parse transform 0.
\*Jan 31 01:10:38:059 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Encapsulation mode is Tunnel.
\*Jan 31 01:10:38:060 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Lifetime type is in seconds.
\*Jan 31 01:10:38:060 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Life duration is 28800.
\*Jan 31 01:10:38:060 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Authentication algorithm is HMAC-MD5.
\*Jan 31 01:10:38:060 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Key length is 128 bytes.
\*Jan 31 01:10:38:060 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Transform ID is SM1-CBC.
\*Jan 31 01:10:38:060 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
The proposal is acceptable.
\*Jan 31 01:10:38:061 2018 H3C\_example IKE/7/EVENT: Received message from ipsec, message type is 9.
\*Jan 31 01:10:38:061 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
IPsec SA state changed from IKE\_P2\_STATE\_GETSP to IKE\_P2\_STATE\_GETSPI.
\*Jan 31 01:10:38:061 2018 H3C\_example IKE/7/EVENT: IKE thread 1097143584 processes a job.
\*Jan 31 01:10:38:062 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Install IPsec SAs.
\*Jan 31 01:10:38:062 2018 H3C\_example IKE/7/EVENT:   Inbound flow: 145.0.0.0/8->166.15.112.108/30
\*Jan 31 01:10:38:062 2018 H3C\_example IKE/7/EVENT:   Outbound flow: 166.15.112.108/30->145.0.0.0/8
\*Jan 31 01:10:38:062 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Lifetime in seconds: 3600
\*Jan 31 01:10:38:062 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Lifetime in kilobytes: 1843200
\*Jan 31 01:10:38:062 2018 H3C\_example IKE/7/EVENT:
  Protocol: 50
  Inbound  SPI: 0x4ab0d9ca
  Outbound SPI: 0x4601ace3
\*Jan 31 01:10:38:063 2018 H3C\_example IPSEC/7/EVENT:
Invalid flow context, testing same flow.
\*Jan 31 01:10:38:063 2018 H3C\_example IPSEC/7/EVENT:
IPsec tunnel successfully added in kernel.
\*Jan 31 01:10:38:064 2018 H3C\_example IPSEC/7/EVENT:
SA successfully added in kernel.
\*Jan 31 01:10:38:064 2018 H3C\_example IPSEC/7/EVENT:
SA successfully added in kernel.
\*Jan 31 01:10:38:063 2018 H3C\_example IPSEC/7/EVENT:
Added tunnel to kernel successfully.
\*Jan 31 01:10:38:063 2018 H3C\_example IPSEC/7/EVENT:
Sent add tunnel message to Slot:0 Cpu:0, message type is 0x13.
\*Jan 31 01:10:38:063 2018 H3C\_example IPSEC/7/EVENT:
Save IPsec Tunnel to DBM, tunnelIndex 0, refreshCnt 0, createTime 574
\*Jan 31 01:10:38:064 2018 H3C\_example IPSEC/7/EVENT:
Added an IPsec tunnel when adding ISAKMP SA: tunnel index = 0, tunnel sequence number = 1.
\*Jan 31 01:10:38:064 2018 H3C\_example IPSEC/7/EVENT:
Added SA to kernel successfully.
\*Jan 31 01:10:38:064 2018 H3C\_example IPSEC/7/EVENT:
Added ISAKMP SAs. Number of SAs added is 2.
\*Jan 31 01:10:38:064 2018 H3C\_example IPSEC/7/EVENT:
No.1 SA index: 1, sequence number: 1.
\*Jan 31 01:10:38:064 2018 H3C\_example IPSEC/7/EVENT:
No.2 SA index: 0, sequence number: 1.
\*Jan 31 01:10:38:064 2018 H3C\_example IPSEC/7/EVENT:
Added SA context to IKE.
\*Jan 31 01:10:38:065 2018 H3C\_example IKE/7/EVENT: Received message from ipsec, message type is 11.
\*Jan 31 01:10:38:065 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
IPsec SA state changed from IKE\_P2\_STATE\_GETSPI to IKE\_P2\_STATE\_SA\_CREATED.
\*Jan 31 01:10:38:065 2018 H3C\_example IKE/7/EVENT: IKE thread 1097143584 processes a job.
\*Jan 31 01:10:38:065 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Set attributes according to phase 2 transform.
\*Jan 31 01:10:38:066 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Encapsulation mode is Tunnel.
\*Jan 31 01:10:38:066 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  in seconds
\*Jan 31 01:10:38:066 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Life duration is 28800.
\*Jan 31 01:10:38:066 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Authentication algorithm is HMAC-MD5.
\*Jan 31 01:10:38:066 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Key length is 128 bytes.
\*Jan 31 01:10:38:066 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
  Transform ID is SM1-CBC.
\*Jan 31 01:10:38:066 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct transform 1.
\*Jan 31 01:10:38:066 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct IPsec proposal 1.
\*Jan 31 01:10:38:067 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct IPsec ID payload.
\*Jan 31 01:10:38:067 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct IPsec ID payload.
\*Jan 31 01:10:38:067 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct IPsec RESPONDER\_LIFETIME payload.
\*Jan 31 01:10:38:067 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Construct HASH(2) payload.
\*Jan 31 01:10:38:067 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Encrypt the packet.
\*Jan 31 01:10:38:068 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
IPsec SA state changed from IKE\_P2\_STATE\_SA\_CREATED to IKE\_P2\_STATE\_SEND2.
\*Jan 31 01:10:38:068 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sending packet to 172.99.99.2 remote port 500, local port 500.
\*Jan 31 01:10:38:068 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500

  I-Cookie: 18bafc8383ab10b1
  R-Cookie: 48c6c8b7cdc64805
  next payload: HASH
  version: ISAKMP Version 1.0
  exchange mode: Quick
  flags: ENCRYPT
  message ID: b1af4311
  length: 188
\*Jan 31 01:10:38:068 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sending an IPv4 packet.
\*Jan 31 01:10:38:068 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sent data to socket successfully.
\*Jan 31 01:10:38:155 2018 H3C\_example IKE/7/EVENT: Received packet successfully.
\*Jan 31 01:10:38:156 2018 H3C\_example IPSEC/7/EVENT:
Updated outbound SA of IPsec tunnel(SA index = 1).
\*Jan 31 01:10:38:155 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received packet from 172.99.99.2 source port 500 destination port 500.
\*Jan 31 01:10:38:155 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500

  I-Cookie: 18bafc8383ab10b1
  R-Cookie: 48c6c8b7cdc64805
  next payload: HASH
  version: ISAKMP Version 1.0
  exchange mode: Quick
  flags: ENCRYPT
  message ID: b1af4311
  length: 60
\*Jan 31 01:10:38:155 2018 H3C\_example IKE/7/EVENT: IKE thread 1097143584 processes a job.
\*Jan 31 01:10:38:155 2018 H3C\_example IKE/7/EVENT: Phase2 process started.
\*Jan 31 01:10:38:155 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Decrypt the packet.
\*Jan 31 01:10:38:155 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received ISAKMP Hash Payload.
\*Jan 31 01:10:38:156 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Process HASH payload.
\*Jan 31 01:10:38:156 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Validated HASH(3) successfully.
\*Jan 31 01:10:38:156 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
***IPsec SA state changed from IKE\_P2\_STATE\_SEND2 to IKE\_P2\_STATE\_ESTABLISHED.第二阶段成功***
\*Jan 31 01:10:38:156 2018 H3C\_example IPSEC/7/EVENT:
Sent switch SA message to Slot:0 Cpu:0, message type is 0x1a.
\*Jan 31 01:10:38:156 2018 H3C\_example IPSEC/7/EVENT:
Switched SA successfully.
\*Jan 31 01:10:38:157 2018 H3C\_example IKE/7/EVENT: Received message from ipsec, message type is 15.
\*Jan 31 01:10:38:158 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Add P2 SA to triple successfully.
\*Jan 31 01:11:08:979 2018 H3C\_example IKE/7/EVENT: Received packet successfully.
\*Jan 31 01:11:08:979 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Received packet from 172.99.99.2 source port 500 destination port 500.
\*Jan 31 01:11:08:981 2018 H3C\_example IKE/7/PACKET: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sending an IPv4 packet.
\*Jan 31 01:11:08:981 2018 H3C\_example IKE/7/EVENT: vrf = 0, local = 199.99.99.161, remote = 172.99.99.2/500
Sent data to socket successfully.

### 隧道状态及参数查看

<H3C\_example>dis ike sa
    Connection-ID   Remote                Flag         DOI
------------------------------------------------------------------
    1               172.99.99.2           RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
<H3C\_example>dis ipsec sa
-------------------------------
Interface: Eth-channel1/0:0
-------------------------------

  -----------------------------
  IPsec policy: map1
  Sequence number: 1
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1428
    Tunnel:
        local  address: 199.99.99.161
        remote address: 172.99.99.2
    Flow:
        sour addr: 166.15.112.108/255.255.255.252  port: 0  protocol: ip
        dest addr: 145.0.0.0/255.0.0.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 3403264074 (0xcad9b04a)
      Connection ID: 4294967296
      Transform set: ESP-ENCRYPT-SM1-CBC-128 ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/3559
      Max received sequence-number: 0
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 3819700550 (0xe3ac0146)
      Connection ID: 4294967297
      Transform set: ESP-ENCRYPT-SM1-CBC-128 ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/3559
      Max sent sequence-number: 0
      UDP encapsulation used for NAT traversal: N
      Status: Active

## 主要问题及排错

### MSR路由器4G拨号不成功

**正常状态为拨号成功后，设备LTE灯绿色长亮。 ipsec vpn隧道建立成功后 vpn灯绿色长亮。**

1.确认4G卡状态是否良好；
2.确认4G卡是否设置了PIN码；
3.确认4G卡是否能够被识别；
4.信号强度是否足够；
5.确认4G卡是否注册成功；
6.APN配置是否正确；
7.最后再确认路由器4G相关配置是否正确。

[**MSR路由器4G拨号不成功排查步骤**](http://help.h3c.com/robot/p4data/a307c3211a124560810e562e4d4b6966/)

1. **组网需求**

MSR路由器部分款型支持4G拨号上网，如下介绍4G拨号配置上网不成功时的排查方法。

2. **排查步骤**

MSR路由器4G拨号不成功问题定位故障的思路是：先确认4G卡状态是否良好，信号强度是否正常，确认4G卡是否注册成功，最后再确认路由器4G相关配置



1) 确认4G卡状态是否良好

确认4G卡的状态是否为可用状态，是否因为4G卡有异常状态，导致4G拨号不成功。

MSR V5路由器使用如下命令：

display cellular-ethernet x/0 all

MSR V7路由器使用如下命令：

display cellular x/0

例如：通过命令查看到如下结果：



说明：当前请求PIN码状态为disable，说明不需要输入PIN码，当前SIM卡状态也是OK。

2) 确认4G卡是否设置了PIN码

MSR V5路由器使用如下命令：

display cellular-ethernet x/0 all

MSR V7路由器使用如下命令：

display cellular x/0

如果当前PIN Verification为Enable状态，则需要用户输入相应的PIN码或者PUK码解锁4G卡，例如：



可以看到当前4G卡使能了PIN码认证状态（PIN Verification = enable）

PIN码状态为PIN码请求状态（PIN Status = PIN Requirement），此时需要输入4G卡的PIN码；

如果PIN码状态为PUK码请求状态（PIN Status = PUK Requirement），此时需要输入4G卡的PUK码。

需要注意的是，如果PIN码连续输错3次，4G卡将被锁卡，需要使用PUK码来解锁，如果PUK码连续错10次，4G卡将被彻底锁死，需要联系当地4G卡的运营商解锁。

输入PIN码信息的命令如下：

[H3C-Cellular1/0]pin verify simple 1234

输入PUK码信息的命令如下：

[H3C-Cellular1/0]pin unlock 87654321 1234 //87654321为运营商提供的PUK码，1234为设置新的PIN码

3) 确认4G卡是否能够被识别

如果当前SIM状态为Not Inserted状态，则说明Modem没有识别出SIM，需要排查是否为SIM问题，可以将此SIM插到4G手机或者其他4G Modem中查看是否能够识别，如果其他设备同样无法识别，需要更换此SIM再做测试。

如果其他设备能够识别且配置无误，插入我们路由器无法识别，则需要拨打400-600-9999电话判断是否为路由器故障问题导致的。

4) 确认4G信号强度是否足够

信号是影响4G拨号的关键因素，如果信号不好的情况，会直接导致4G拨号无法成功，所以遇到问题时，查看4G信号也是关键的一步，使用的命令如下：

MSR V5路由器使用如下命令：

display cellular-ethernet x/0 all

MSR V7路由器使用如下命令：

display cellular x/0

例如显示如下：



查看信号强度之前，需要先查看当前网络连接类型是什么，由于4G是可以向下兼容3G的，所以当4G信号不好的时候，4G路由器默认情况下会向下选择3G网络接入。

当Technology Selected字段为LTE时，说明当前接入的是4G网络，需要关注Current RSRP字段，当选择4G网络时，RSRP值不得低于-95 dBm。例如，如果当前RSRP值为-100 dBm，则说明当前4G信号非常不好。

当Technology Selected字段为WCDMA（联通3G)、TD-SCDMA（移动3G）或者EVDO（电信3G）时，说明当前接入的是3G网络，需要关注Current RSSI字段，RSSI值不得低于-90 dBm。例如，如果当前RSSI值为-100 dBm则说明当前3G信号非常不好。

当Technology Selected字段为非上述的情况的时候，说明3G和4G信号都很差，或者没有3G、4G信号，需要移动路由器设备到信号较好的地方。

5) 确认4G卡是否注册成功

4G卡需要注册到运营商之后，才能接入到运营商网络，所以我们需要检查4G卡是否已经注册到了运营商当中，使用命令如下：

MSR V5路由器使用如下命令：

display cellular-ethernet x/0 all

MSR V7路由器使用如下命令：

display cellular x/0

例如如下显示：



当前服务状态（Current Service Status）必须是服务可用状态（Service Available）；

注册状态（Registration Status）必须是已注册状态（Registered）；

当前服务（Current Service）必须是Combined状态；

以上三个状态，只要有任意一个和上边情况不符合，则说明4G网络是注册失败的。

当注册失败的时候，需要确认3点：

A. SIM卡支持的模式与modem当前设置的模式是否一致，例如：

Technology Preference = 1xRTT //网络优选类型

表示4G Modem被限制只能连到电信的1xRTT网络，而电信的1xRTT网络带宽很小，是无法完成数据交换的，所以会出现网络注册失败的问题。

遇到这种问题，需要使用mode命令修改Modem的网络优选模式，命令如下：

**[H3C-Cellular1/0]mode lte或者mode auto**

mode lte命令表示强制Modem只能选择4G网络，如果当前没有4G信号，无法向下选择3G信号。mode auto命令表示Modem自动选择网络，选择规则为4G>3G>2G，当有4G信号时，优选4G网络，当没有4G网络，或者4G网络信号很差时，会自动切换到3G网络。

B. 需要排查APN配置是否正确，APN排查方法见下一章节。

C. 请确认4G卡是否欠费。

6) APN配置是否正确

在VPDN网络中，如果APN配置错误也会导致注册失败，APN查看方法命令如下：

MSR V5路由器使用如下命令：

display cellular-ethernet x/0 all

MSR V7路由器使用如下命令：

display cellular x/0

例如：



注释：Access Point Name（APN）即为当前4G网络的APN接入点，需要和当地运营商咨询APN具体名称，也要确认APN认证使用的认证方式是CHAP还是PAP方式，用户名和密码是什么。

APN修改命令如下：

MSR V7路由器R0304P04及其之后版本命令如下：

[H3C] apn-profile test

[H3C-apn-profile-test] apn static apn1

[H3C] interface Eth-channel0/0:0
[H3C-Eth-channel0/0:0]apn-profile apply test

7) 查看4G拨号相关配置是否正确

3. **注意事项**

1) **移动和联通网络的拨号串是“\*99#”，电信网络的拨号串是“#777”**。

2) 保证配有下一跳为eth-channel（V7路由器）或者Cellular-Ethernet（V5路由器）接口的路由。

3) 保证APN接入点配置正确。（APN由运营商提供，缺省情况下为自动获取的模式，如果在其他配置均正确的情况下4G拨号依然不成功，则需要联系当地运营商确认APN是否与设备当前配置的一致。

4**. 3G/4G Modem管理显示和维护**

操作

命令

显示3G/4G Modem的呼叫连接信息

**display cellular** [ *interface-number* ]

显示Cellular接口的相关信息

**display controller** [ **cellular** [ *interface-number* ] ]

显示派生出来的以太网通道接口的相关信息

**display interface** [ **eth-channel** [ *channel-id* ] ] [ **brief** [ **description** | **down** ] ]

显示派生出来的Serial接口的相关信息

**display** **interface** [**Serial** [ *channel-id* ] ] [ **brief** [ **description** | **down** ] ]

清除派生出来的Cellular接口的统计信息

**reset counters controller** [ **cellular** [ *interface-number* ] ]

清除以太网通道接口的统计信息

**reset counters interface**[ **eth-channel** [ *channel-id* ] ]

清除派生出来的Serial接口的统计信息

**reset** **counters** **interface** [**Serial** [ *channel-id* ] ]

### MSR路由器4G虚拟专网VPN建立失败

####  以下报错日志显示证书获取成功，但是证书处于不可用状态

原因一般都是因为设备clock 时间与证书有效时间不匹配。需要同步NTP时钟服务器到最新时间

\*Jan  1 00:17:14:835 2011 B8111111 PKI/7/PKI\_DEBUG: Failed to verify certificate by domain test.
\*Jan  1 00:17:14:836 2011 B811111 IKE/7/ERROR: vrf = 0, local = 166.99.100.128, remote = 192.16.15.2/500
Failed to verify the peer certificate. Reason: certificate is not yet valid.
\*Jan  1 00:17:14:836 2011 B811111 IKE/7/ERROR: vrf = 0, local = 166.99.100.128, remote = 192.16.15.2/500     Invalid certificate.
\*Jan  1 00:17:14:837 2011 B8111111IKE/7/PACKET: vrf = 0, local 166.99.100.128, remote = 192.16.15.2/500  Construct notification packet: INVALID\_CERTIFICATE.

#### 以下报错日志显示证书获取失败，需要重做证书，检查证书配置及导入参数。

\*Feb 22 09:43:16:575 2017 H3C IKE/7/ERROR: vrf = 0, src = 166.15.101.250, dst = 172.16.15.2/500
Failed to get the certificate and key by certificate request.
\*Feb 22 09:43:16:575 2017 H3C IKE/7/ERROR: vrf = 0, src = 166.15.101.250, dst = 172.16.15.2/500
Failed to get certificate.
\*Feb 22 09:43:16:575 2017 H3C IKE/7/PACKET: vrf = 0, src = 166.15.101.250, dst = 172.16.15.2/500
Construct notification packet: CERTIFICATE\_UNAVAILABLE.

#### 以下报错日志显示对端ipsec证书认证要求为DN C=CN, CN=topsec 。 但是在本地IKE profile 配置中并未找到匹配的配置信息。检查配置是否错误。

      举例配置

pki certificate attribute-group group1
 attribute 1 subject-name **dn ctn topsec**

\*Feb 22 12:30:33:868 2017 H3C IKE/7/PACKET: vrf = 0, src = 166.15.101.250, dst = 172.16.15.2/500  Peer ID value: **DN C=CN, CN=topsec**
\*Feb 22 12:30:33:868 2017 H3C IKE/7/PACKET: vrf = 0, src = 166.15.101.250, dst = 172.16.15.2/500  No profile is matched.