Ruijie Networks – Innovation Beyond Networks

RG-Router FAQs V1.0

Ruijie Networks Co., Ltd.

Copyright Statement

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

1 Preface

This document describes usage limitations of Ruijie routers and problems that frequently arise during implementation, so as to provide guidance for post sales engineers to deploy and implement products and improve the deployment efficiency and quality

Audience

- Ruijie Partner Engineers
- Network Administrator

Obtain Technical Assistance

- Ruijie Networks Websites : http://www.ruijienetworks.com
- Ruijie Service Portal : http://case.ruijienetworks.com

Welcome to report error and give advice in any Ruijie manual to Ruijie Service Portal

Related Documents

- RGOS Configuration Guide for different Router series

Revision History

Date	Change contents	Reviser
2016.3	Initial publication V1.0	TAC Oversea

2 Contents

3 RSR Series Routers

Q1: How do I configure a combo port on RSR series routers?

By default, the combo port uses a coppor port. To configure a fiber port as the combo port, perform the following configuration:

```
Ruijie(config-GigabitEthernet 0/0)#media-type basex force
```

Note: baset indicates a coppor port, whereas basex indicates a fiber port.

Q2: Can I use the debug ip packet command to display the traffic that passes an RSR series router?

No. The **debug ip packet** command is only used to display the traffic initiated by or destined for the specified router.

To display the traffic that passes the router, run the **show ip fpm flow | include [IP address]** command with the corresponding IP address specified.

Q3: Are the RSR series router line cards hot-swappable?

The 1002E, 2004E, 14E, and 14F line cards of the RSR10/20 routers are not hot-swappable.

Q4: Can an RSR series router work as a DHCP relay and a DHCP server at the same time?

No. On an RSR series router, the DHCP relay and DHCP server features are mutually exclusive.

How do I use the MGMT interface on the RSR77 engine to upgrade the router?

1. Place the system file in the **TFTP** directory.
2. Log in to the RSR77 router by using the console cable.
3. Run the following command to display the current version:

```
Ruijie#sh version
```

4. Use a network cable to connect the TFTP server and the router's MGMT interface.
5. Configure the IP address and gateway of the MGMT interface to enable the interface to communicate with the TFTP server.

```
Ruijie(config)#interface mgmt 0
Ruijie(config-if-Mgmt 0)#ip address 172.18.10.23 255.255.255.0
Ruijie(config-if-Mgmt 0)#gateway 172.18.10.1
```

6. Test the connectivity to the TFTP server.

```
Ruijie#ping oob 192.168.33.51 //IP address of the PC
```

7. Check the free space of the flash memory.

```
Ruijie#dir
```

8. Transfer the firmware to the router's flash memory.

```
Ruijie#copy oob_tftp://192.168.51.23/RSR77_10.4(3b21)_R171722_install.bin flash:rgos.bin
```

9. After the automatic upgrade package is successfully downloaded to the device, run the **upgrade system rgos.bin** command to upgrade the line card.

```
Ruijie#upgrade system rgos.bin
```

10. Reload the system.

```
Ruijie#Reload
Proceed with reload?[no] y
```

11. Run the following command to check whether the router is upgraded successfully:

```
show version
```

Q5: Does the RSR77 router in running state support fan hot-swap?

Yes.

Q6: How do I log in to theRSR77 router line card?

Firstly, run the **show version slot** command to display the slot number for the line card, and then run the **vtty slot_id** command to log in to the line card. To log out of the line card, press the shortcut key **Ctrl+X**.

```
Ruijie#show version slot
DevSlot   MaxPorts   Configured-Module   Online-Module       Status
-------   --------   -----------------   -----------------   ------
1M1     1RSR7708-SRCMIRSR7708-SRCMI       master
1M2none
11/0    0none
12/0    0             none
13/0    0RSR77-SIP1RSR77-SIP1running
13/1    4FNM-4GE-1FNM-4GE-1running
13/2    0none
14/0    2RSR77-SIP2RSR77-SIP2running
14/1    0none
14/2    0none
Ruijie#vtty 3/1
```

```
[LC3/1]>
```

Q7: The message "access failed, now in use." Was displayed when I logged in to theRSR77 router line card.

For a version later than 10.4 (3b15), run the **Ruijie#clear vtty** *xx* command to clear the line (*xx* is the slot number for the line card, which can be obtained by running the **show version slot** command).

Q8: Why were no network address translation (NAT) entries displayed after I ran the show ip nat translation command on the RSR77 router?

The RSR77 router is a distributed router. You can view NAT entries by using any of the following methods:

1. Display NAT translation entries on specified line card on which NAT outside interface is configured such as **Ruijie#sh ip nat translations slot 2/1**.
2. Log in to the specified line card on which NAT outside interface is configured and display NAT translation entries using commands **show ip nat translation** or **show ip fpm flow** (which displays NAT traffic or non-NAT traffic). For example:

```
Ruijie#vtty 3/1
[LC3/1]>en
[LC3/1]#show ip nat translation
```

Note: The **show ip nat translation** command may return many results, which are displayed by screen. If the pipe operator (|) is added to the end of the command to filter results, the returned results will not be displayed by screen, which may lead to frequent screen refresh. The **show ip nat translation** command may affect services on a device with a large number of sessions; therefore, avoid using the command during peak hours.

Q9: Why is a conflict message displayed after the line card on the RSR77 router is replaced?

The conflict message indicates "Inserted line card in slot 3/1 is not matched with the line card configured".

The message is displayed because the old line card is not uninstalled before it is replaced by the new one. To solve the problem, do the following:

1. Run the **no install** command to uninstall the old line card.
2. Run the **wr** command to save the setting.
3. Run the **install** command to install the new line card.

Q10: RSR77 redundancy status information

Run the following command:

```
Ruijie#sho redundancy
 Redundancy stats:
 my state = 19 -Active
peer state = 37 -Standby Hot
```

The numbers must be converted to 8-bit hexadecimal format. The first four bits indicate the role, and the last four bits indicate the state.

Roles: 0 – unknown; 1 – master; 2 – slave

States: 0 – being initialized; 1 – already selected as the master; 2 –synchronization in progress; 3 – hot backup completed; 4 – the slave in cold standby; 5 – the slave in hot standby; 6 –switchover in progress

For example, the number 19 converted to hexadecimal format is 13, of which 1 indicates the master role and 3 indicates hot backup completed on the master.

4 3G

Q1: Why does the router fail to recognize the SIC-3G line card?

- Check whether the line card is inserted in the correct slot.
- Check whether the router is upgraded to the latest software version.
- Check whether the line card or the slot is faulty (by replacing the line card or inserting it to another slot).

Q2: Why does the show cellular info RSSI command return the value 0 after the SIC-3G line card is inserted?

Possible causes:

- The network condition of your operator is abnormal.
- No SIM card is inserted to the line card.
- The SIM card is in arrears.
- The antenna is improperly connected or is broken.

Q3: What 3G standards does the SIC-3G line card support?

Currently, the SIC-3G line card supports WCDMA and CDMA2000.

Q4: What is the received signal strength indicator (RSSI) threshold under 3G standards?

WCDMA	RSSI Signal Strength
good	>-80dBm
normal	-80dBm~-90dBm
bad	-90dBm~-100dBm
CDMA2000	RSSI Signal Strength
good	>-75dBm
normal	-75dBm~-85dBm
bad	-85dBm~-95dBm

Q5: Are 3Gdevices and related accessories support hot-swap?

The SIC-3G line card is not hot-swappable. You need to power off the device before you install and uninstall the SIM card or antenn

Q6: show cellular info command

The **show cellular info** command can be used to display the current state of the system. WCDMA is used as an example.

```
show cellular info
Tty No.:1     /* TTY number, which is consistent with the corresponding async interface*/
Slot:    2      /*Number of the slot where the SIC-3G line card is located*/
Interface: Async 1     /*Corresponding 3G interface*/
3G Type:   WCDMA /* Type of the 3G card, 3G network type that the SIC-3G line card support*/
RSSI:      -69 dBm        /* Current RSSI value; a larger value indicates higher signal strength */
Sys mode:  WCDMA(5)         /* Working mode of the SIC-3G line card */
Sim status:     Valid USIM card state(1)
Service status: Valid service(2)
Roaming status:  Non roaming state(0)
Service domain: PS+CS service(3)
Available PLMN's:
List 1: Status = Registered, SP name = China Unicom, Network = WCDMA
List 2: Status = Available, SP name = China Unicom, Network = GSM/GPRS
```

Explanation:

1. RSSI

RSSI generally ranges from –85 dBm to –51 dBm. A signal reception of –61 dBm is stronger than that of –85 dBm. Because 3G antennas have unstable signal reception, and the router refreshes RSSI values every 28s, you need to wait for at least 28s to obtain the latest results.

2. Values of service domain:

service domain indicates the service domain of the system.

no service: Indicates that services are unavailable.

only CS service: Indicates that only circuit-switched (CS) services (voice services, such as making and receiving calls) are available.

only PS service: Indicates that only packet-switched (PS) services (data services, such as data upload and download) are available.

PS+CS service: Indicates that voice and data services are available.

CS and PS not registered, searching: Indicates that the user is connecting to a 3G network and has not completed voice or data service registration.

3. Values of SIM status:

SIM status indicates the state of the SIM card.

invalid USIM card state or pin code locked: Indicates that the USIM card is invalid.

valid USIM card state: Indicates that the USIM card is valid.

USIM is invalid in case of CS: Indicates that the USIM card is invalid in the CS domain. That is, the user cannot make and receive calls or perform other voice services.

USIM is invalid in case of PS: Indicates that the USIM card is invalid in the PS domain. That is, the user cannot upload and download data or perform other data services.

USIM is invalid in case of either CS or PS: Indicates that the USIM card is invalid in the CS and PS domain. That is, the user cannot perform voice and data services.

USIM card is not existent: Indicates that the USIM card does not exist.

4. PS and CS:

The 3G core network is divided into the CS domain and PS domain. When a user accesses the network, the user will register in the PS or CS domain based on service requirements.

The CS domain provides voice services. After CS registration, the user can make and receive calls.

The PS domain provides data services. After PS registration, the user can perform data transfer (such as download) and other multimedia services.

Q7: Permanent-online and auto-dialing features of the SIC-3G line card

CLI command for using the auto-dialing feature:

```
Ruijie(config)#interface async 1
Ruijie(config-if-Async 1)#dialer  auto-dial
```

CLI command for using the permanent online feature:

```
Ruijie(config)#interface async 1
Ruijie(config-if-Async 1)#dialer idle-timeout 0
```

Q8: How do I adjust a 3G router to use an external antenna?

When you need to install an antenna on your router, install an external antenna preferentially. A command is provided to switch between the external antenna and the internal antenna. It is required to restart the router after you switch an antenna.

```
Ruijie(config)# interface async 1
Ruijie(config-if)#plmn antenna outer  (inner)// outer indicates enabling the external antenna, whereas inner indicates enabling the internal antenna.
```

5 4G

Q1: Can I install a 3G antenna on a 4G router?

No. A 3G antenna and a 4G antenna work in different frequency bands; therefore, they cannot be used alternately on the same router.

Q2: Can I install only one antenna on RSR820-T?

It is recommended that two antennas be installed. The device has two antenna interfaces: ANT0 and ANT1 for installing the main antenna and auxiliary antenna respectively. The main antenna receives and transmits signals, whereas the auxiliary antenna only receives signals. By default, the antenna on Interface ANT0 is the main antenna. If you need to install only one antenna, you are advised to install it on Interface ANT0.

Q3: What is the RSSI range indicated by the signal indicator on a 4G router?

Indicator Off: RSSI smaller than –105 dBm

One bar On: RSSI between –105 dBm and –95 dBm

Two bars On: RSSI between –95 dBm and –75 dBm

Three bars on: RSSI larger than –75 dBm

Q4: Is the 4G module hot-swappable?

No. You need to power off the device before you install or replace the SIM card; otherwise, the 4G module may be damaged.

6 NAT

Q1: The PC in LAN fails to access the internal server by server's domain name.

1. Test whether the public IP address mapped to the domain name is accessible and whether the domain name is successfully resolved to the public IP address.
2. The permit-inside feature should be configured on the Internet NAT router.
3. Test whether the PC on the intranet can access the internal server by using an internal IP address to confirm whether the problem is due to an exception of the intranet or the server.
4. Check whether policy-based routing (PBR) is applied to the internal network port on the Internet NAT router. If yes, configure the PBR ACL to reject the traffic generated by access to the internal server by the intranet PC.

Example:

```
R1(config)#ip access-list extended 110        //Configure ACL 110 mapped to PBR.
R1(config-ext-nacl)#10 deny ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255 //Configure the PBR ACL to reject the traffic generated by access to the internal server (172.16.2.0/24) from the intranet IP address 172.16.0.0/24.
R1(config-ext-nacl)#20 permit ip 172.16.1.0 0.0.0.255 any//Match the traffic generated by access to the Internet from the intranet IP address 172.16.1.0/24.
```

Q2: Do RSR series routers support NAT under Virtual routing forwarding (VRF)?

Yes.

Q3: Do the RSR series routers support NAT on locally originated traffic?

No.

Q4: What is the permit-inside feature?

A server on the intranet is mapped to a public IP address, which is registered in a domain. When a user on the intranet accesses the server by using the domain name, the domain name server (DNS) resolves the server address to the registered public IP address. When the user uses the public IP address to access the server, by default, the router determines that the traffic is normal passing traffic and converts the source IP address. Before the conversion, the router detects that the public IP address and the external network port are on the same network segment, and then sends an ARP request for resolving the MAC address from the public IP address. Because the network segment does not have any terminal configured with the public IP address, the router receives no response to the ARP request. As a result, source IP address conversion fails. The following

happens when a user on the intranet accesses the server by using its public IP address: The router without any related NAT entry sends an ARP request only on the external network port, and the user receives no response. To solve this problem, you need to configure the permit-inside feature.

Run the following command to configure the permit-inside feature on the router:

```
ip nat inside source static tcp 192.168.1.254 23 10.0.0.1 23 permit-inside
```

Telnet to 10.0.0.1 from 192.168.1.2 on the intranet, and then check whether the following NAT entry exists on the router:

```
RSR#sh ip nat tran
Pro Inside global    Inside local         Outside localOutside global
tcp 10.0.0.1:1046192.168.1.2:104610.0.0.1:23192.168.1.254:23
```

After the permit-inside feature is configured, the router converts the source and destination IP addresses of corresponding packets.

	Source IP address	**Destination IP address**
Before NAT	192.168.1.2:1046	10.0.0.1:23
After NAT	10.0.0.1:1046	192.168.1.254:23

Q5: What is the difference between ip nat inside source and ip nat outside source?

Commands	The Operation to Packets
ip nat outside source	1.When IP packets are transfering from outside to inside , NAT translates the source IP address of the packets 2.When IP packets are transfering from inside to outside , NAT translates the destination IP address of the packets
ip nat inside source	1.When IP packets are transfering from inside to outside , NAT translates the source IP address of the packets 2.When IP packets are transfering from outside to inside , NAT translates the destination IP address of the packets

7 Digital Certificate

Q1: What is a digital certificate?

A digital certificate is used to verify the identity of an entity that communicates with other entities on the Internet. It is digitally signed and issued by a Certification Authority (CA), and contains the owner information and files of a public key. A digital certificate typically contains a public key, name, and digital signature of the issuer.

Q2: What is the application scenario of a digital certificate?

Currently, the digital certificates of Ruijie RSR series routers are mainly used for peer verification at the first stage of Internet Protocol Security (IPsec) virtual private network (VPN) implementation.

8 L2TP VPN

Q1: When working as L2TP network servers (LNSs), do the RSR series routers support the configuration of multiple virtual private dialup network (VPDN) groups to receive L2TP dial-in requests from multiple L2TP access concentrators (LACs)?

Yes.

- If a VPDN group is configured with terminate-from hostname xx, the LAC named xx can dial in to the group.
- If a VPDN group is configured with source-ip x.x.x.x, the LAC with the destination IP address x.x.x.x can dial in to the group.
- If the name of a remote LAC is not specified, the LAC can dial in to the default VPDN group.

Q2: Do the RSR series routers support the feature of allowing the same L2TP account to be used by only one client at a time?

No. This feature needs to be implemented with the assistance of a Remote Authentication Dial In User Service (RADIUS) server.

Q3: When working as LNSs, do the RSR series routers support the remote dial-in by mobile terminals?

Yes from the theoretical perspective, but depending on the system that a specific mobile terminal uses.

9 IPSec VPN

Q1: Do the RSR series routers support IPsec Internet Key Exchange (IKE) negotiation in aggressive mode?

Yes.

.

Q2: Do RSR series routers support NAT traversal (NAT-T)?

Yes.

Q3: Do the RSR series routers support NAT-T in aggressive mode?

Yes.

Q4: show crypto ipsec sa command

```
ruijie#show crypto ipsec sa
Interface: Async 1//Local encrypted interface
Crypto map tag:3gtest, local addr 30.160.230.11  //Local IP address used for negotiation with the peer end
media mtu 1500
================================
item type:static, seqno:1, id=32
local  ident (addr/mask/prot/port): (192.168.1.0/0.0.0.255/0/0))   //Source network segment for IPsec interesting traffic
remote  ident (addr/mask/prot/port): (192.168.2.0/0.0.0.255/0/0))  //Destination network segment for IPsec interesting traffic
PERMIT
#pkts encaps: 336, #pkts encrypt: 336, #pkts digest 0 //Number of encapsulated packets, encrypted packets, and digest packets sent by the specified port
#pkts decaps: 58, #pkts decrypt: 58, #pkts verify 0  //Number of decapsulated packets, decrypted packets, and verification packets received by the specified port
#send errors 0, #recv errors 0 //Number of incorrect packets that are sent and received

Inbound esp sas:
spi:0x39aea73c (967747388) //Incoming SPI number of the security association (SA)
transform: esp-sm1        //Transform-set in use
in use settings={Tunnel,} //Tunnel mode
```

```
    crypto map 3gtest 1//Map name invoked
    sa timing: remaining key lifetime (k/sec): (4606685/3364)  //Lifetime of the SA: remaining traffic
and time
    IV size: 16 bytes
    Replay detection support:N
    Outbound esp sas:
    spi:0x437d9610 (1132303888) //Outgoing SPI number of the SA
    transform: esp-sm1        //Transform-set in use
    in use settings={Tunnel,} //Tunnel mode
    crypto map 3gtest 1
    sa timing: remaining key lifetime (k/sec): (4606685/3364)  //Lifetime of the SA: remaining traffic
and time
    IV size: 16 bytes
    Replay detection support:N
```

Q5: Do the RSR series routers support the IPsec tunnel auto-trigger and permanent-online features?

To configure the IPsec tunnel auto-trigger and permanent-online features on the RSR series routers, run the following command:

```
    crypto map mymap 10 ipsec-isakmp
    set autoup
```

Q6: What certificate import modes do the RSR series routers support?

1. Offline import: supports the import of PEM and P12 certificates.
2. Online application: A certificate is imported through application via the Simple Certificate Enrollment Protocol (SCEP).
3. Offline application

Q7: What is the function of the *self-identity* command used for IPsec negotiation using digital certificates?

The **Ruijie(config)# self-identity address | fqdn |user-fqdn identity | dn** command identifies the local end. The command has the following parameters:

address: specifies the main IP address of the local interface that initiates negotiation.

fqdn: specifies the local identity as a domain name.

user-fqdn: specifies the local identity in the form of *user@domain name*.

dn: specifies the DN value of the certificate.

Q8: Can the peer address used in IPsec negotiation be the local loopback address or the IP address of another interface?

Yes. You need to use the **Ruijie(config)#crypto map local-address** *x.x.x.x* command to modify the IP address used to perform IPsec negotiation on the local device.

By default, the IP address of the interface that sends IPsec data is used as the local IP address for IPsec negotiation.

IPsec VPN Common Failure – pre-share key at the peer end not configured

The **debug cry is** and **debug cry ipsec** commands show the following prompt messages:

```
*Oct 26 11:11:06: %7: (33) received packet from 1.1.1.1, (I) MM_SI2_WR2, MM_KEY_EXCH
*Oct 26 11:11:06: %7:Exchange type: 0x2<key><nonce>
*Oct 26 11:11:06: %7:extract_payload done!
*Oct 26 11:11:06: %7: main mode process R2:(33) processing NONCE payload.
*Oct 26 11:11:06: %7:(33) No no pre-shared keys with remote peer 1.1.1.1
*Oct 26 11:11:06: %7: main mode process R2:no fit share key was found!
*Oct 26 11:11:06: %7: IKE message packet process over.
```

Q9: IPsec VPN Common Failure – mismatch of pre-share keys at the local end and peer end

The **debug cry is** and **debug cry ipsec** commands show the following prompt messages:

```
*Oct 26 11:16:51: %7: (33) received packet from 1.1.1.1, (I) MM_SI3_WR3, MM_VERIFY
*Oct 26 11:16:51: %7:Exchange type: 0x5
*Oct 26 11:16:51: %7: Error: ISAKMP: payload malformed !
*Oct 26 11:16:51: %CRYPTO-4-ISAKMP_BAD_MESSAGE: IKE message from 1.1.1.1 failed its sanity check or is malformed.
```

Q10: IPsec VPN Common Failure – mismatch of transform-sets at the local end and peer end

The debug cry is and debug cry ipsec commands show the following prompt messages:

```
*Oct 26 11:36:11: %7: (33) received packet from 1.1.1.1, (I) QM_IDLE
*Oct 26 11:36:11: %7:Exchange type: 0x5<hash><notify>
*Oct 26 11:36:11: %7:extract_payload done!
*Oct 26 11:36:11: %7: Receive notify:no proposal chosen.
*Oct 26 11:36:11: %7: Find the next payload.
*Oct 26 11:36:11: %7:information exchange: processing NOTIFY payload. message ID = 859916303
*Oct 26 11:36:11: %7:unknown notify type 14.
*Oct 26 11:36:11: %7:get notify 1.1.1.1-->1.1.1.2: no proposal chosen.
*Oct 26 11:36:11: %7: Process isakmp notify payload end.
```

```
*Oct 26 11:36:11: %7: IKE message packet process over.
```

Q11: IPsec VPN Common Failure – inconsistent configuration of IPsec interesting traffic at the local end and peer end

```
*Oct 26 11:25:34: %7: (33) received packet from 1.1.1.1, (I) QM_IDLE
*Oct 26 11:25:34: %7:Exchange type: 0x5<hash><notify>
*Oct 26 11:25:34: %7:extract_payload done!
*Oct 26 11:25:34: %7:unknown notification type 0
*Oct 26 11:25:34: %7: Find the next payload.
*Oct 26 11:25:34: %7:information exchange: processing NOTIFY payload. message ID = 2138422166
*Oct 26 11:25:34: %7:unknown notify type 0.
*Oct 26 11:25:34: %7:unknown notification type 0
*Oct 26 11:25:34: %7: Process isakmp notify payload end.
*Oct 26 11:25:34: %7: IKE message packet process over.
```

Q12: IKE security association (SA) negotiation fails at the first stage of IPsec VPN implementation.

1. Check whether the correct peers are specified at the local end and peer end respectively. (If a dynamic diagram is used at the local end, no peer needs to be specified manually.)

```
crypto map mymap 10 ipsec-isakmp
set peer 1.1.1.1 //The IP address of the peer end must be the IP address of the crypto map interface configured at the peer end, and cannot be the loopback address.
```

2. Check whether the IP address of the crypto map interface configured at the peer end can be pinged from the local end, and vice versa.
3. Check whether both ends of the tunnel have consistent IKE security proposal configuration.
4. Check whether both ends of the tunnel have consistent pre-share key configuration.
5. If the problem persists, run the following commands at the local end and peer end respectively, and submit a case on Ruijie Service Portal to seek for help.

```
sh version
show run
Run the following commands to enable debugging, trigger IPsec negotiation, and collect debugging information:
debug crypto iskamp
debug crypto ipsec
```

After negotiation, run the following commands to display the SA information at the first and second stages of IPsec VPN implementation:

```
show crypto iskamp sa
```

```
show crypto ipsec sa
```

Q13: IPsec SA negotiation fails at the second stage of IPsec VPN implementation.

1. Check whether IKE SA is successfully established at the first stage of IPsec VPN implementation.
2. Check whether the local end and peer end have consistent transform-set configuration.
3. Check whether the local end and peer end have consistent configuration of IPsec encrypted traffic. (If a dynamic diagram is used at the local end, IPsec interesting traffic does not need to be configured manually.)
4. If the problem persists, run the following commands at the local end and peer end respectively, and submit a case on Ruijie Service Portal to seek for help.

```
sh version
show run
```

Run the following commands to enable debugging, trigger IPsec negotiation, and collect debugging information:

```
debug crypto iskamp
debug crypto ipsec
```

After negotiation, run the following commands to display the SA information at the first and second stages of IPsec VPN implementation:

```
show crypto iskamp sa
show crypto ipsec sa
```

Q14: SA negotiation is successful at the first and second stages of IPsec VPN implementation, but IPsec encrypted traffic is abnormal.

1. Check whether the SA is correctly established at the first and second stages of IPsec VPN implementation.
2. Check whether the local end and peer end have consistent configuration of IPsec encrypted traffic.
3. Check whether IPsec encrypted traffic is normal after the crypto map configuration is deleted from the interfaces at both ends. (If IPsec encrypted traffic is abnormal, check the route configuration.)
4. Check whether the next hop for the IPsec interesting traffic sent to the peer end is the crypto map interface recorded in the routing table at the local end.

   Assume that the IPsec interesting traffic is sent from 192.168.1.0 to 192.168.2.0, and crypto map is configured on the fastethernet 0/0 interface.

   The next-hop outbound interface destined for 192.168.2.0 should be the fastethernet 0/0 interface recorded in the local routing table.
5. If the problem persists, run the following commands at the local end and peer end respectively, and submit a case on Ruijie Service Portal to seek for help

```
sh version
show run
show ip route
```

Run the following commands to enable debugging, trigger IPsec negotiation, and collect debugging information:

```
debug crypto iskamp
debug crypto ipsec
```

After negotiation, run the following commands to display the SA information at the first and second stages of IPsec VPN implementation:

```
show crypto iskamp sa
show crypto ipsec sa
```

The local end and peer end send IPsec interesting traffic, which will trigger IPsec SA encryption. During this process, run the following command multiple times to collect the IPsec SA information at the local end and peer end respectively, and check whether the encrypted packets and decrypted packets at the local end and peer end increase:

```
show crypto ipsec sa
```

Q15: IPsec VPN-protected traffic is normal, but many packets are lost.

1. Check whether IPsec interesting traffic encounters packet loss after the crypto map configuration is deleted from the interfaces at both ends.
2. Check whether packet loss also occurs in the traffic that is sent by the encrypted interfaces at the local end and peed end respectively to other destinations.
3. Check whether the devices at the local end and peer end handle IPsec SAs and traffic that exceed the performance limit. (You can run the **show cpu** and **show memory** commands to display the devices' resource usage rates.)
4. If the problem persists, run the following commands at the local end and peer end respectively, and submit a case on Ruijie Service Portal to seek for help

```
sh version
show run
show slot
show cpu
show memory
```

After negotiation, run the following commands to display the SA information at the first and second stages of IPsec VPN implementation:

```
show crypto iskamp sa
show crypto ipsec sa
```

The local end and peer end send IPsec interesting traffic, which will trigger IPsec SA encryption. When packets are lost, run the following command multiple times to collect the IPsec SA information at the local end and peer end respectively, and check

whether the increased quantity of encapsulated packets and encrypted packets and at the local end is the same as the increased quantity of decapsulated packets and decrypted packets at peer end:

```
show crypto ipsec sa
```

Q16: The RSR10 router is used to perform digital certificate-based IPsec authentication, but negotiation fails after the router is restarted.

Because the RSR10 router does not have an embedded clock chip, the router will restore the default time setting after restart. If digital certificate-based IPsec authentication is performed at the same time, the validity of the certificate will fail to be verified. To solve the problem, use any of the following methods:

1. Configure a Network Time Protocol (NTP) server on the RSR10 router so that the system time of the router can be synchronized correctly after the router is restarted.
2. Configure **time-check none** under the trustpoint of the certificate to disable certificate time check.

```
crypto pki trustpoint ruijie
time-check none
```

Q17: The IPsec digital certificate is not displayed by the show run command on the RSR series routers.

Run **the show crypto pki cer** command to display certificate information.