DHCP Trouble Shooting

Models: N5860 Series; N8560 Series; NC8200 Series; NC8400 Series

Contents

1. Fault Phenomenon

The client cannot obtain the IP address or the obtained information is incomplete

Click on the lower left corner of the computer: Start-Run, enter cmd in the dialog box, enter ipconfig /all in the cmd command line to determine the fault phenomenon.

2. Possible Cause of Failure

①PC terminal or operating system problem

②Environmental problem (loop, or attack) physical link is unblocked

③The device configuration is incorrect or unreasonable, mainly concentrated on:

The HCP snooping uplink trust port setting is incorrect.

The VLAN assignment on the switch is incorrect. The Layer 3 interface address is not configured in the DHCP server.

The relay function is not enabled on the Layer 3 interface.

The DHCP server is not configured with an address pool or the address pool is set to exclude addresses, resulting in no address in the address pool that can be assigned.

The lease time of the DHCP server is set too long, and the address cannot be released.

The network segment of the DHCP server address pool is incorrectly configured.

The DHCP function of the network device is not enabled.

④DHCP server performance is insufficient.

⑤Defective software version.

⑥DHCP architecture error: When the DHCP relay and DHCP SNOOPING are deployed on the customer's existing network, the improper opening position causes the client to obtain an abnormal DHCP acquisition. Reason explanation: dhcp relay will modify the source MAC address of the dhcp message sent by the pc (relay device). If the dhcp relay is deployed before snooping, the DHCP message will be discarded by the snooping device.

Deploy the architecture correctly:

dhcp snp and dhcp relay can be deployed on the same device, ie pc - dhcp snooping+dhcp relay - dhcp server.

dhcp snp can be deployed on devices connected to dhcp relay, ie pc - dhcp snooping - dhcp relay - dhcp server.

3. Processing Steps

3.1 Troubleshoot Client and Operating System Problems

① Determine the symptom and check whether the client is correctly set to dynamically obtain the address.

② Confirm whether the problem is that there is a problem with a single client or that a large area of clients cannot obtain addresses. If a large area of users cannot obtain an IP address, continue to the next step.

③ If the problem exists with a single client, install the packet capture software on the PC, or mirror the packet capture on the access switch to confirm whether the PC sends the DHCP discover message normally.

④ If not, try to disable/reactivate the network card again. If it is a service disk system, it may be recommended to re-do the diskless server system.

⑤If the DHCP discover message can be sent normally and the packet capture process message is retained, then continue to the next step.

3.2 Troubleshoot Network Issues

① Make sure the physical connection between the client and server is normal.

Try to set the PC to a static IP address and gateway. On the premise of confirming that the switch is specified as a restricted dynamic IP address for the configuration, ping the server IP address to determine connectivity. If it can be pinged and the delay is less than 100ms,

there is no packet loss or jitter. The connection is smooth and you can eliminate physical line failures. Go to the next step to troubleshoot. If the connection cannot be pinged or the delay is large, and there is a packet loss, there is a problem with the line, or the server is unstable due to the tight loop, you need to determine the point-by-point packet capture from the client to the DHCP server to determine the packet loss or delay Local cause.

② Check whether the line is interrupted, make sure the line interface connection is normal, check whether the device has the correct route, and adjust the route correctly.

3.3 Check Whether the Network Device Configuration Is Correct

Log in to the access device through the console port and execute the "show run" command to view the configuration information of the current device.

Compare the following typical configurations and check whether the DHCP configuration of the device is correct.

The recommended configuration of the FS switch as a DHCP server:

① Enable DHCP function

```
FS(config)#service dhcp
```

② Configure DHCP address pool

```
FS(config)#ip dhcp pool vlan2
FS(dhcp-config)#lease 1 2 3
FS(dhcp-config)#network 192.168.2.0 255.255.255.0
FS(dhcp-config)#dns-server 8.8.8.8    6.6.6.6
FS(dhcp-config)#default-router 192.168.2.254
FS(dhcp-config)#exit
FS(config)#ip dhcp pool vlan3
FS(dhcp-config)#network 192.168.3.0 255.255.255.0
FS(dhcp-config)#dns-server 8.8.8.8
FS(dhcp-config)#default-router 192.168.3.254
FS(dhcp-config)#exit
```

③ Reserve some addresses

```
FS(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
```

④ Configure DHCP statically assigned address

```
FS(config)#ip dhcp pool test
FS(dhcp-config)# client-identifier 01bc.aec5.4bca.8d
FS(dhcp-config)# host 192.168.2.2 255.255.255.0
FS(dhcp-config)# dns-server 8.8.8.8 6.6.6.6
FS(dhcp-config)#default-router 192.168.2.254
```

⑤ The recommended configuration of FS switch as DHCP relay

```
FS(config)#service dhcp
FS(config)#ip helper-address 172.16.1.2
```

⑥ Recommended configuration of FS switch DHCP snooping

```
FS(config)#ip dhcp snooping
FS(config)#int FastEthernet0/24
FS(config-FastEthernet 0/24)#ip dhcp snooping trust
```

⑦ Configure dhcp snooping verify mac-address globally. It is recommended to enable protection against address exhaustion attacks. If the source MAC and the MAC address in the Client field do not match, the DHCP request message will be discarded.

```
FS(config)#ip dhcp snooping verify mac-address
```

Note: In the event of a fault, the simplest configuration can be used to ensure that the user can obtain the address.

According to the above typical configuration, check whether the DHCP-related configuration of the device is correct, and determine whether the user can obtain the IP address dynamically in the above simplified configuration mode.

3.4 Troubleshoot DHCP Server Performance

① Check if the capacity and performance of the DHCP server is exceeded

②Is there an available IP in the address pool

Check whether there are available IP addresses in the address pool.

```
show ip dhcp server statistics
```

Check whether there is an expired IP address, and the IP address and the interface address are on the same network segment.

```
clear ip dhcp conflict
```

Check to see if there is an IP address check conflict, resulting in no available addresses. If you find a lot of entries, you can try clear ip dhcp conflict to clear it and try to obtain an IP address to see if there is a conflict.

```
show ip dhcp conflict
```

After performing the above steps, if the available IP addresses, expired IP addresses, and conflicting IP addresses in the address pool do not exist, it means that the IP addresses in the address pool have been exhausted.

③ Increase the available address range of the address pool

3.5 Troubleshoot Network Device Software Versions

Log in to the FS official website, check the release notes of the latest version of the product, determine whether there are software defects known by DHCP, and verify the device after upgrading.

4. Seek FS Technical Support

If the fault cannot be solved after the above steps are checked, please collect the following fault information and contact FS technical support for assistance.

```
show run
show log
show dhcp lease
show ip dhcp binding
show ip dhcp conflict
show ip dhcp server statistics
```

You can troubleshoot the process logs and collate the packet capture messages from the client's DHCP address acquisition process.