SANGFOR

IAM

Network delay and packet loss Troubleshooting guide

Version 12.0.18

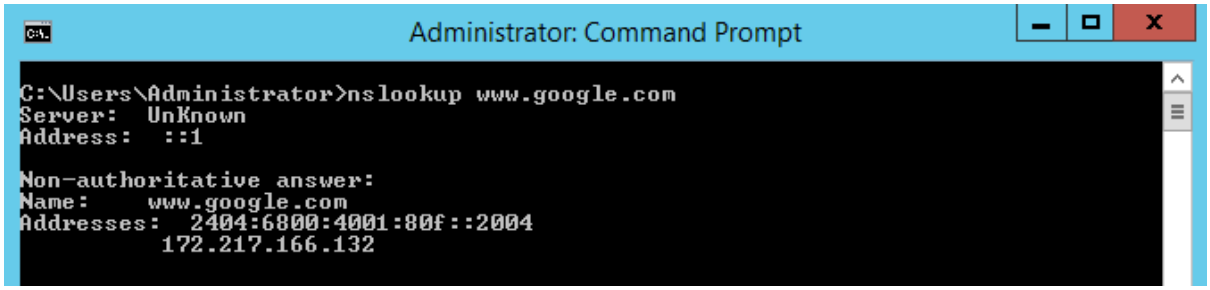
Change Log

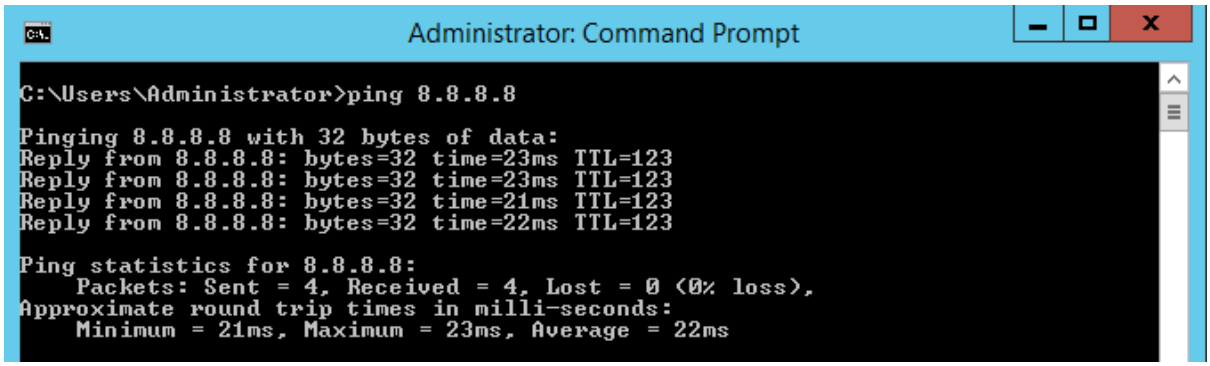
Date	Change Description
May 2, 2019	Version 12.0.18 document release.

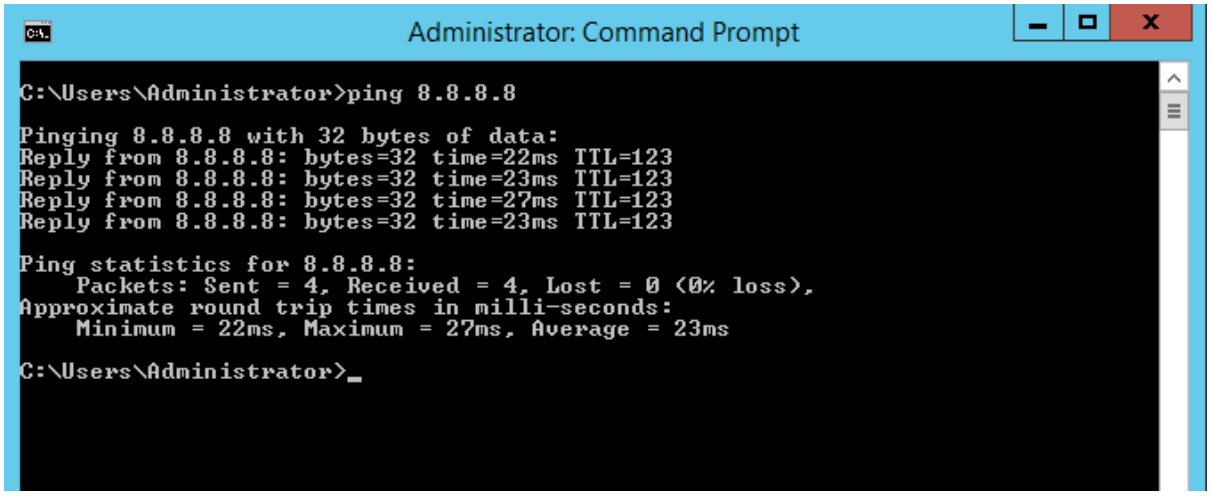
CONTENT

Chapter 1 Troubleshooting when the network is interrupted

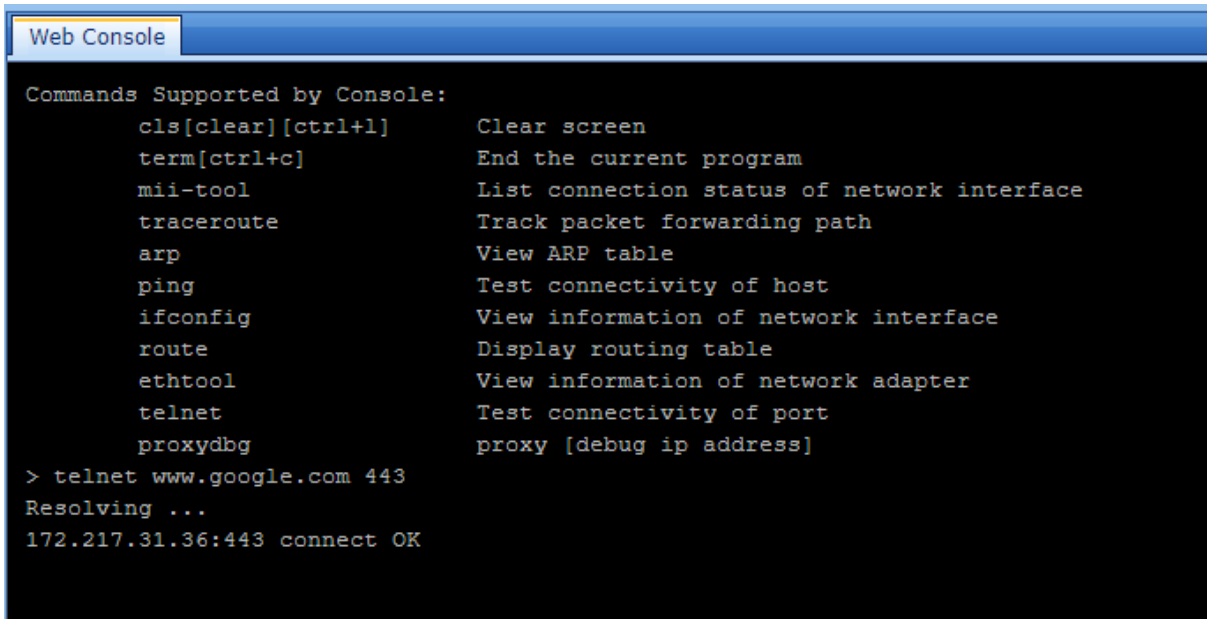
- Confirm the customer's network topology, check the interface status of each network device, whether the cable is damaged, and whether the ISP has interrupted the network. If you use the PPPoE dial-up mode to access the Internet, you must check whether the account is in arrears.
- Check whether the public IP address can be accessed and the domain name of the public network cannot be accessed. Use the **nslookup** and **tracert** commands on the PC to check whether the DNS works. You can use the **ping** command to check whether the public IP address can be directly accessed.



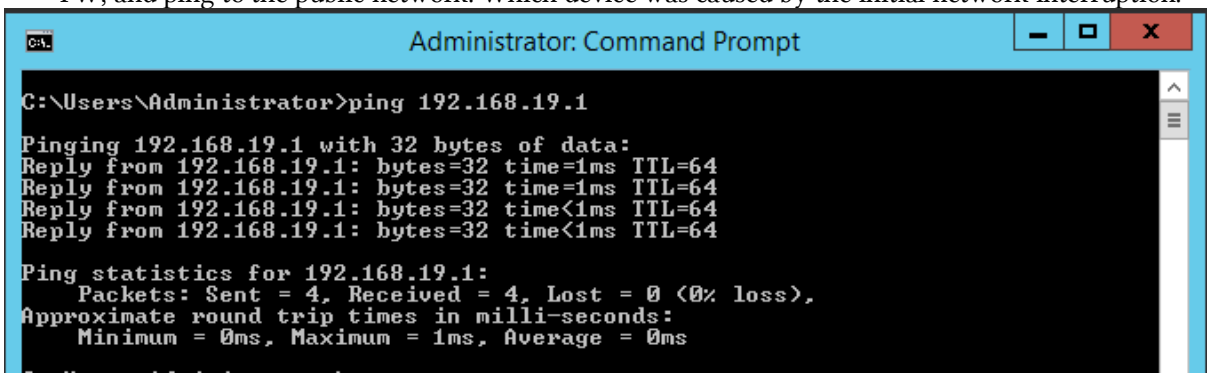




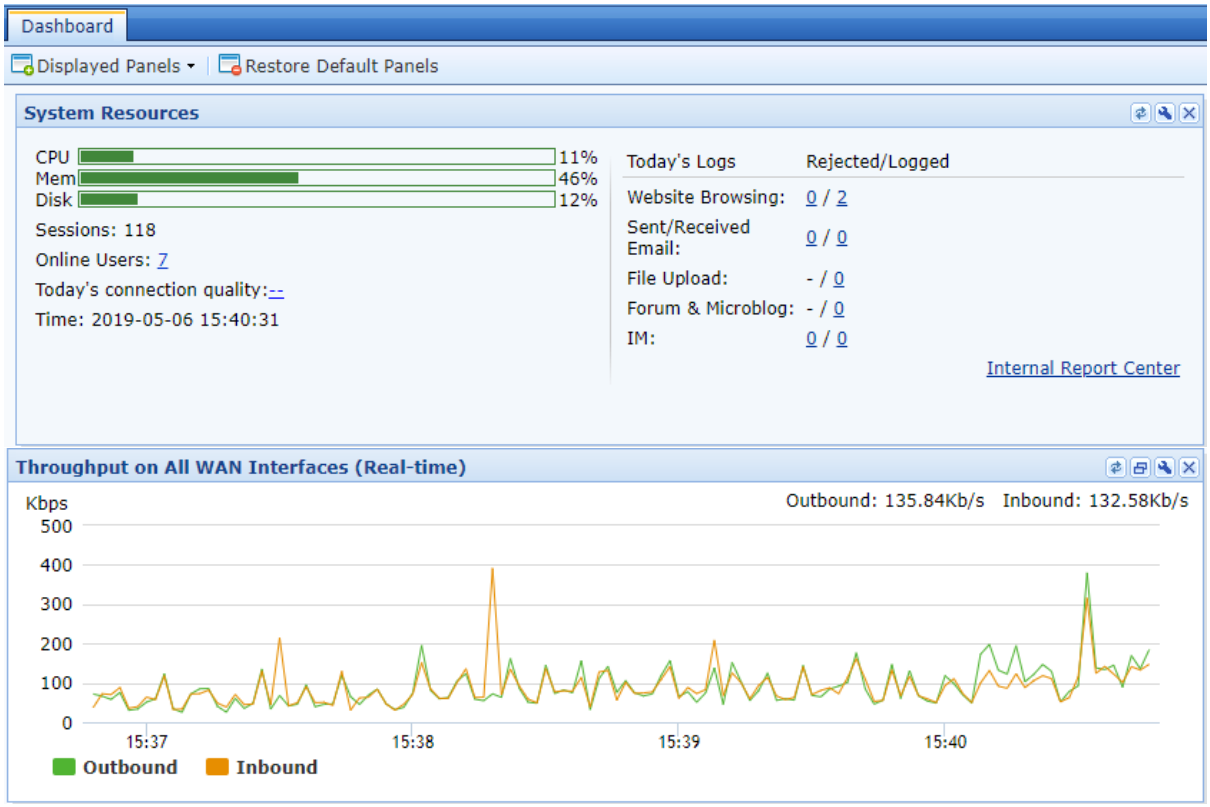
- If it is a proxy environment, confirm whether it is an IAM or other device acting as a proxy server. Check whether the proxy server itself can access the Internet. You can use the **telnet** command on the IAM to check whether the website can be accessed.



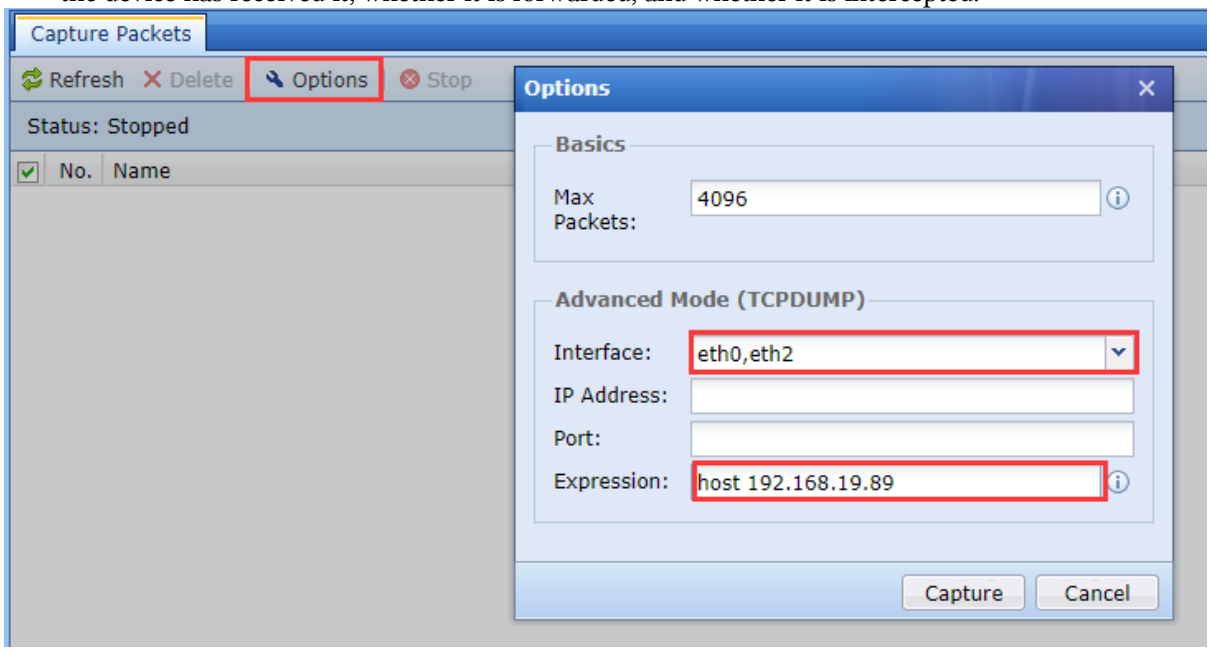
- To find a network interrupt computer, first use the **ping** command to test the connectivity of the network. It is recommended to ping the gateway to the gateway, ping to the IAM device, ping to the FW, and ping to the public network. Which device was caused by the initial network interruption.



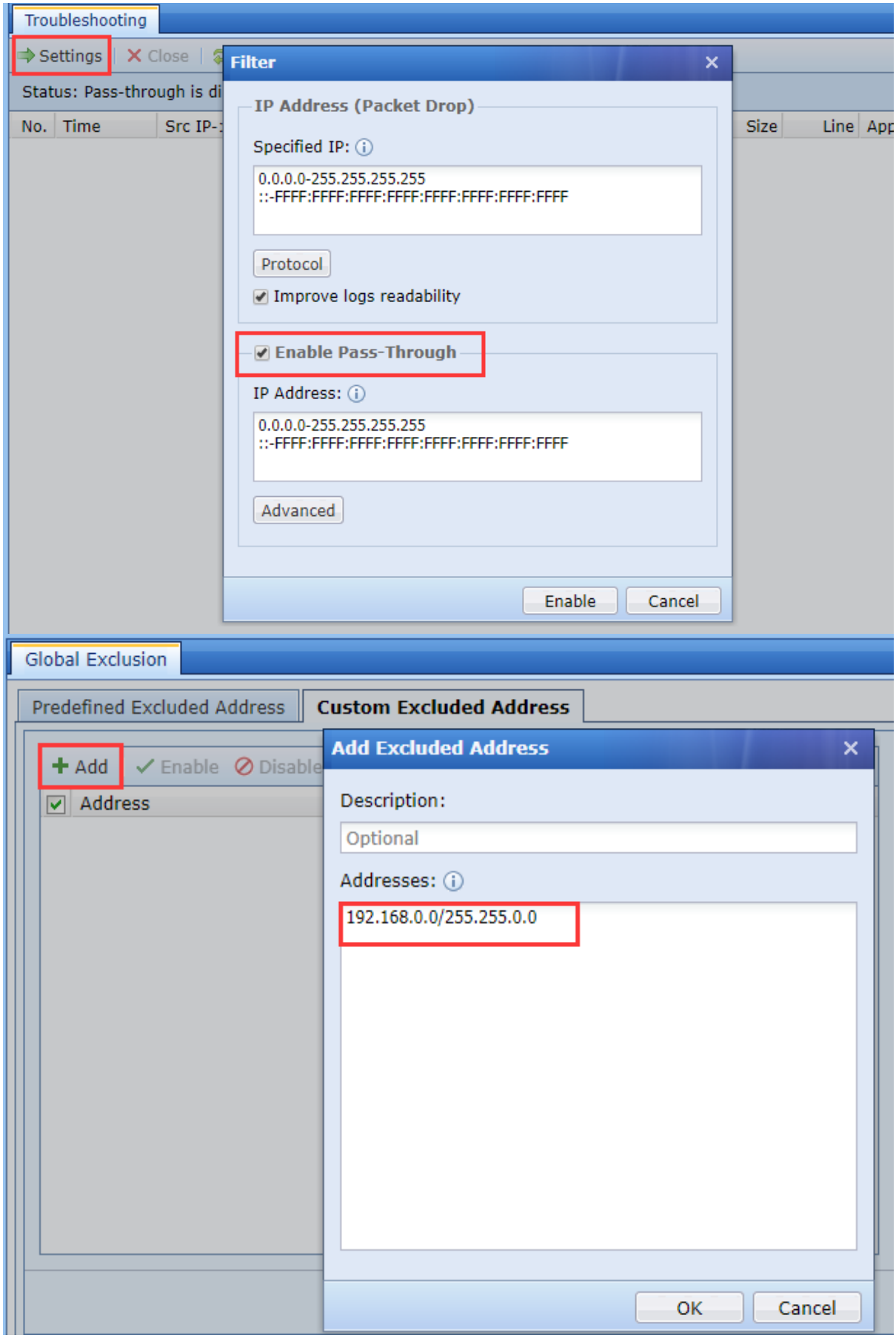
- If the computer does not pass to its gateway, check the internal network problem first to confirm whether the route is incorrect, whether there is ARP spoofing, whether the wiring is incorrect, and whether a loop is formed.
- If the IAM is the gateway of the PC, in addition to confirming the internal network problem, you need to check whether the IAM device is running normally, for example, whether the CPU and memory utilization are high, and whether there is a large amount of traffic.

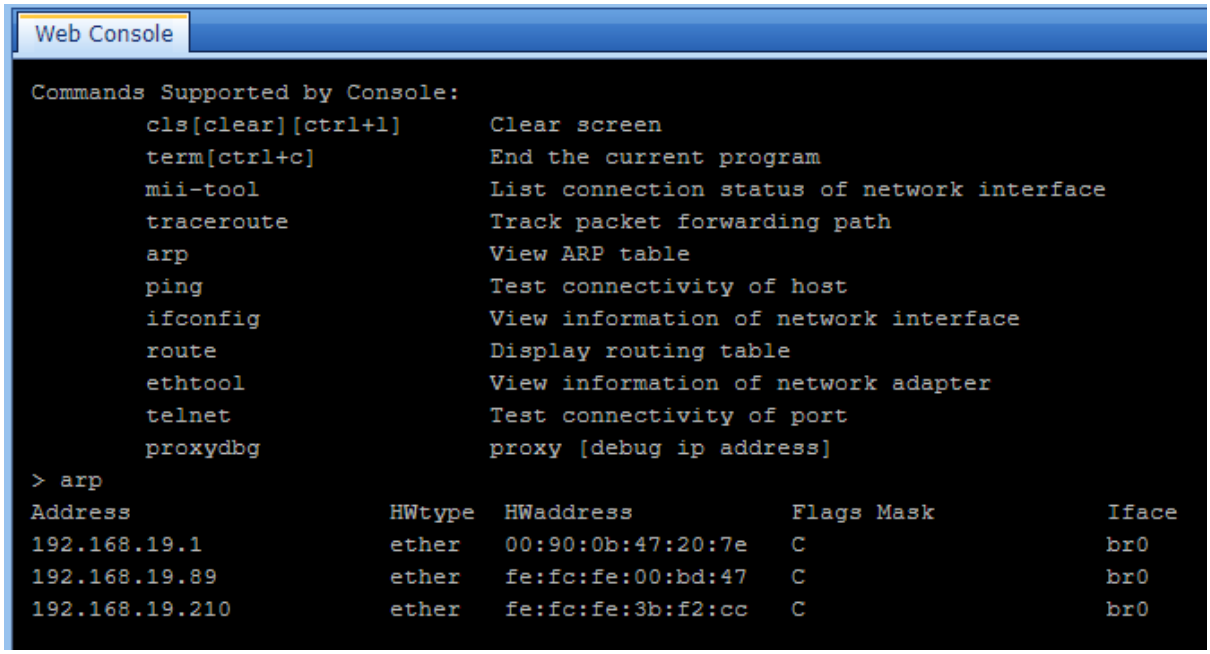


- If the packet is confirmed to be normal through the IAM, select the test PC to access the public network, and then capture the packet at the internal and external network ports of the IAM to see if the device has received it, whether it is forwarded, and whether it is intercepted.



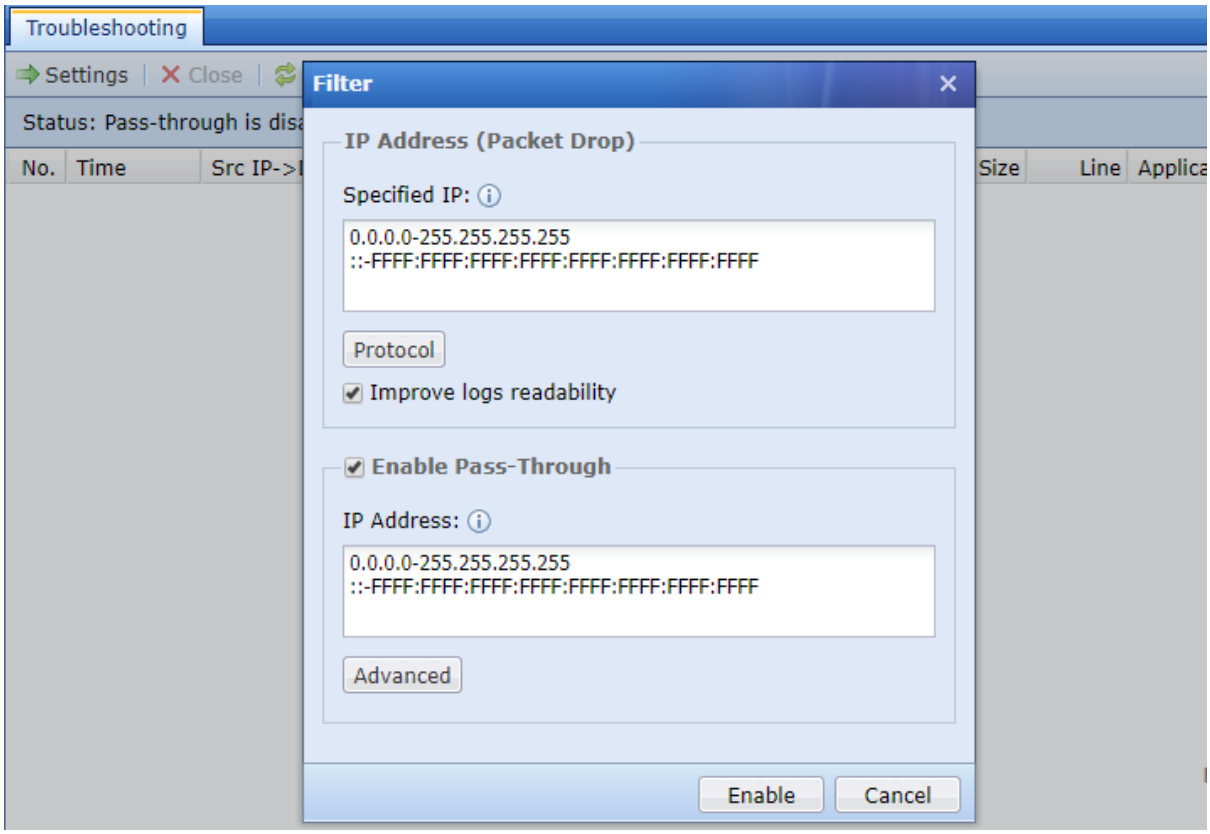
- Check whether the IAM device console can log in normally. If you can, you can enable the global pass-through test to check whether it is restored. Use the arp command to check the ARP table of the device in the IAM console to check whether the ARP information of the device is correct. Check the routing information of the IAM. If the route is incorrectly filled.


Troubleshooting
Settings
Close
Status: Pass-through is di
No.
Time
Src IP-
Size
Line
App
Filter
IP Address (Packet Drop)
Specified IP:
0.0.0.0-255.255.255.255
::-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Protocol
Improve logs readability
Enable Pass-Through
IP Address:
0.0.0.0-255.255.255.255
::-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Advanced
Enable
Cancel
Global Exclusion
Predefined Excluded Address
Custom Excluded Address
Add
Enable
Disable
Address
Add Excluded Address
Description:
Optional
Addresses:
192.168.0.0/255.255.0.0
OK
Cancel

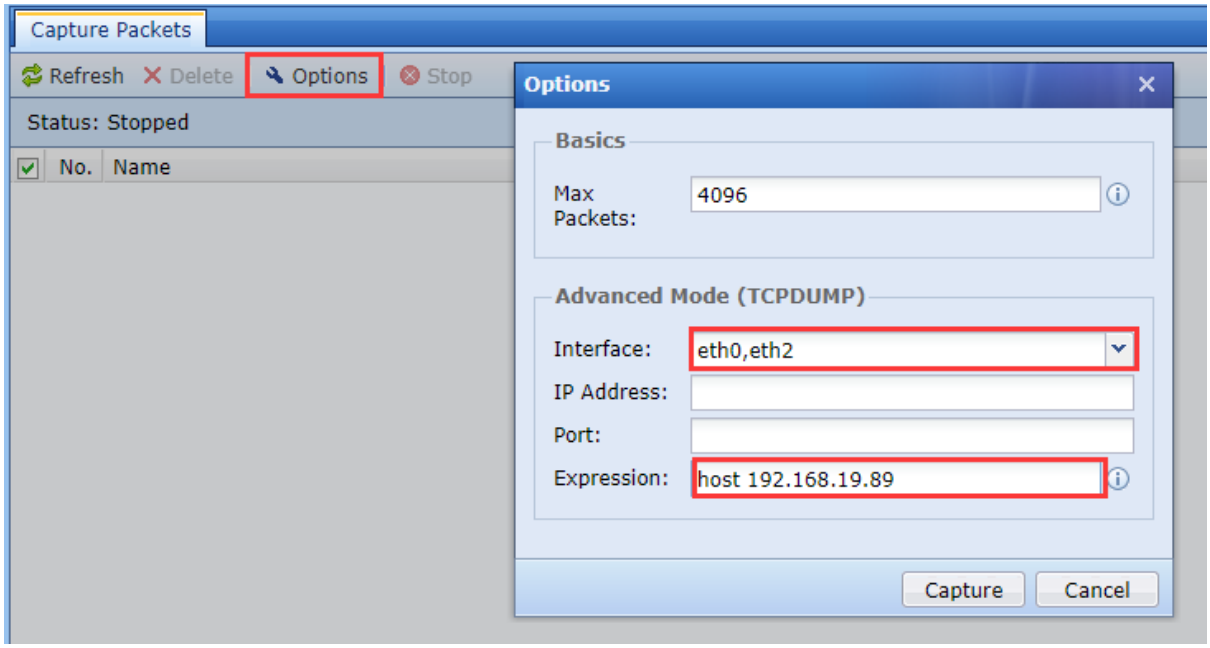


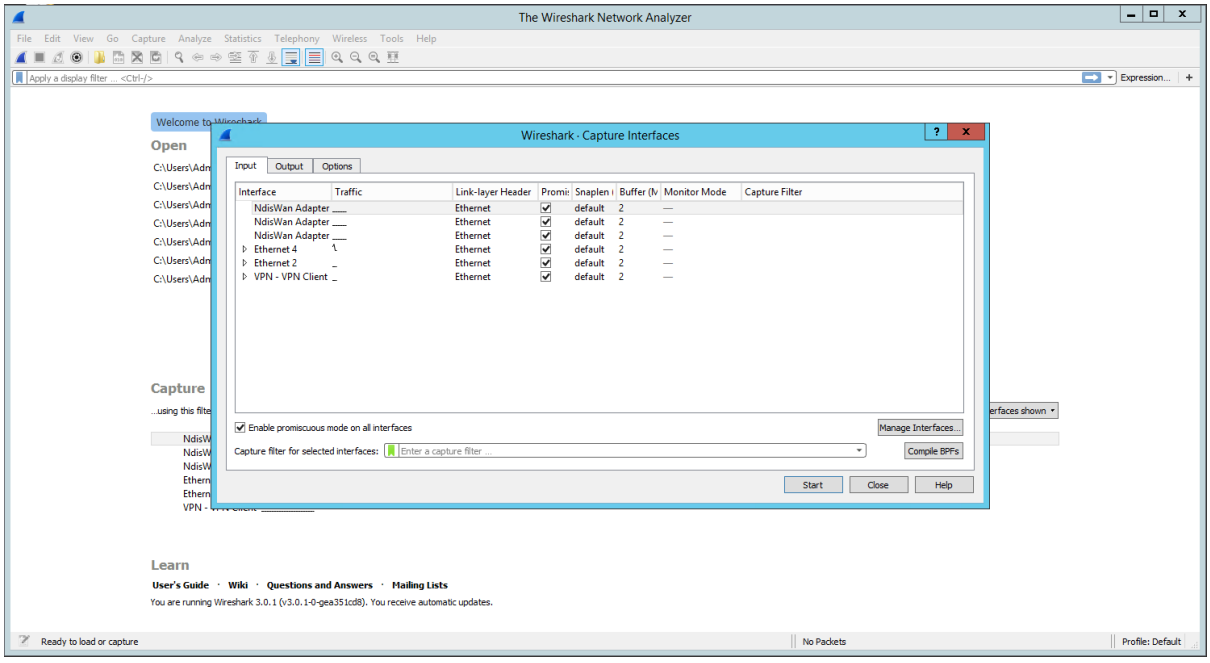
Chapter 2 Troubleshooting when network latency is high

- Turn on full pass-through, check that the flow control policy limits the network speed.

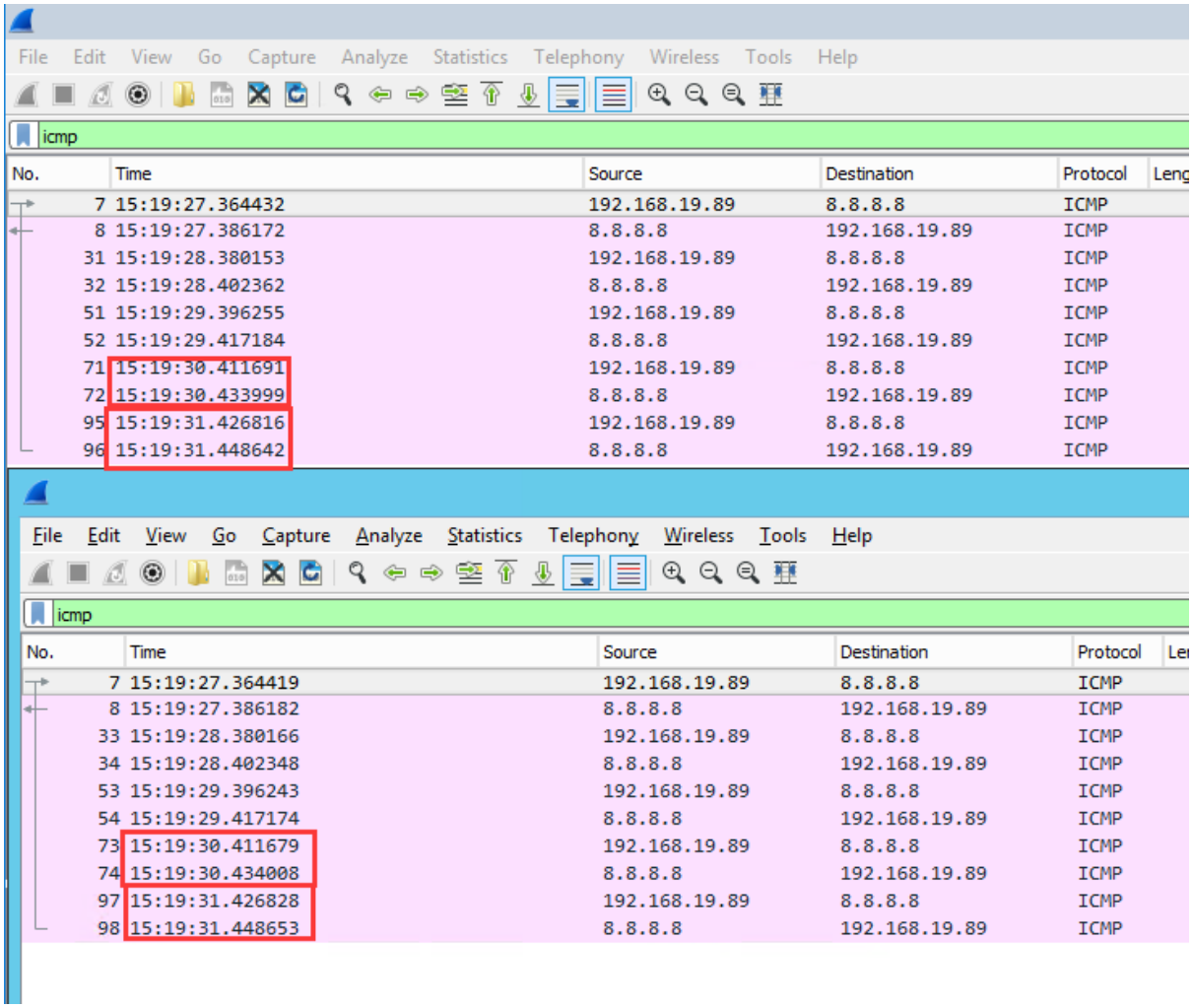


- Simultaneously capture data packets on the internal and external network ports of the PC and IAM, and analyze the timestamp of the data packets. If the data packets are not caused by IAM, please check other network devices first.





- Check the timestamp of the data packet passing through the internal and external network ports of the IAM, and judge whether the delay is generated during the process of the data packet passing through the IAM according to the time difference.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Leng
7 15:19:27.364432 192.168.19.89 8.8.8.8 ICMP
8 15:19:27.386172 8.8.8.8 192.168.19.89 ICMP
31 15:19:28.380153 192.168.19.89 8.8.8.8 ICMP
32 15:19:28.402362 8.8.8.8 192.168.19.89 ICMP
51 15:19:29.396255 192.168.19.89 8.8.8.8 ICMP
52 15:19:29.417184 8.8.8.8 192.168.19.89 ICMP
71 15:19:30.411691 192.168.19.89 8.8.8.8 ICMP
72 15:19:30.433999 8.8.8.8 192.168.19.89 ICMP
95 15:19:31.426816 192.168.19.89 8.8.8.8 ICMP
96 15:19:31.448642 8.8.8.8 192.168.19.89 ICMP
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Le
7 15:19:27.364419 192.168.19.89 8.8.8.8 ICMP
8 15:19:27.386182 8.8.8.8 192.168.19.89 ICMP
33 15:19:28.380166 192.168.19.89 8.8.8.8 ICMP
34 15:19:28.402348 8.8.8.8 192.168.19.89 ICMP
53 15:19:29.396243 192.168.19.89 8.8.8.8 ICMP
54 15:19:29.417174 8.8.8.8 192.168.19.89 ICMP
73 15:19:30.411679 192.168.19.89 8.8.8.8 ICMP
74 15:19:30.434008 8.8.8.8 192.168.19.89 ICMP
97 15:19:31.426828 192.168.19.89 8.8.8.8 ICMP
98 15:19:31.448653 8.8.8.8 192.168.19.89 ICMP