



SANGFOR



IAM

Network delay and packet loss Troubleshooting guide

Version 12.0.18



Change Log

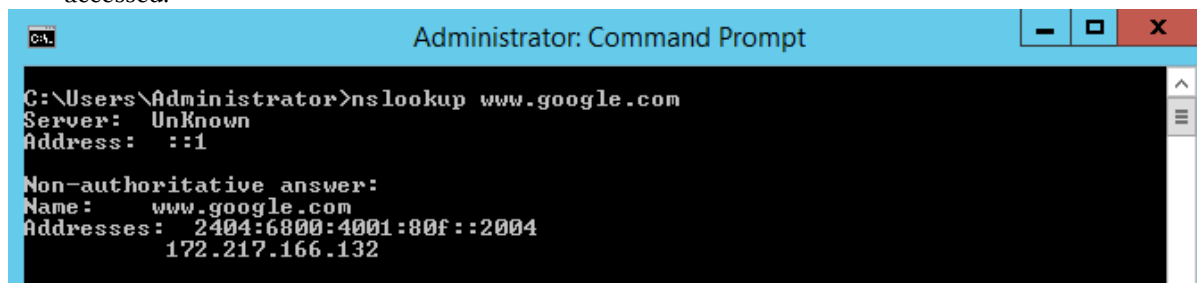
Date	Change Description
May 2, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Troubleshooting when the network is interrupted.....	1
Chapter 2 Troubleshooting when network latency is high.....	5

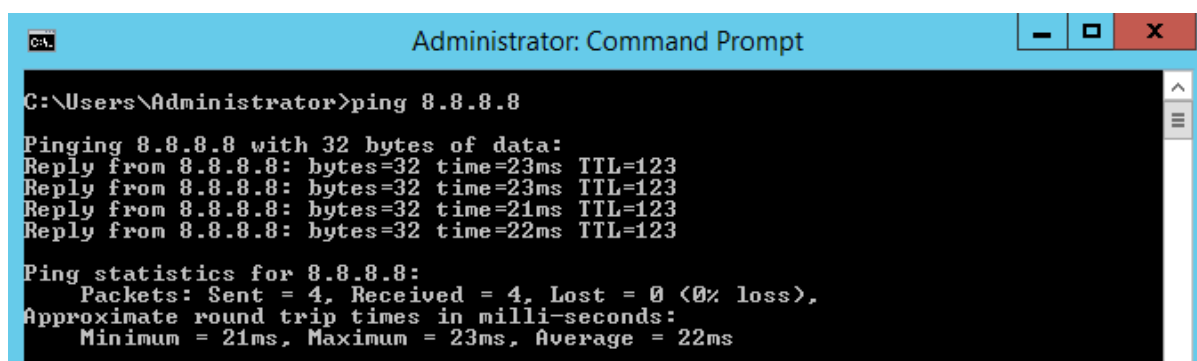
Chapter 1 Troubleshooting when the network is interrupted

- 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.



```
Administrator: Command Prompt
C:\Users\Administrator>nslookup www.google.com
Server: UnKnown
Address: ::1

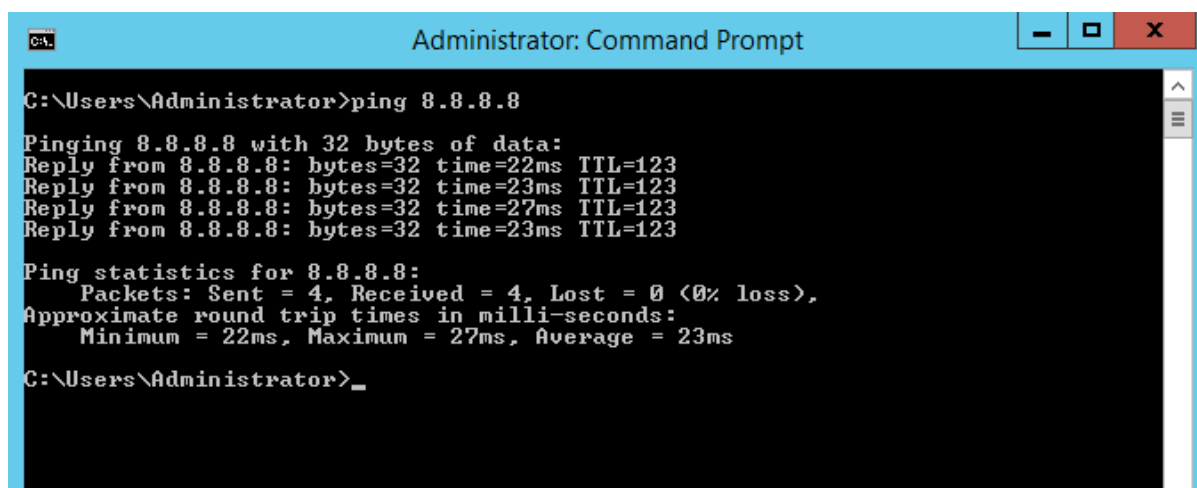
Non-authoritative answer:
Name: www.google.com
Addresses: 2404:6800:4001:80f::2004
          172.217.166.132
```



```
Administrator: Command Prompt
C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=23ms TTL=123
Reply from 8.8.8.8: bytes=32 time=23ms TTL=123
Reply from 8.8.8.8: bytes=32 time=21ms TTL=123
Reply from 8.8.8.8: bytes=32 time=22ms TTL=123

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 23ms, Average = 22ms
```



```
Administrator: Command Prompt
C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=22ms TTL=123
Reply from 8.8.8.8: bytes=32 time=23ms TTL=123
Reply from 8.8.8.8: bytes=32 time=27ms TTL=123
Reply from 8.8.8.8: bytes=32 time=23ms TTL=123

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 27ms, Average = 23ms

C:\Users\Administrator>_
```

- 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.

```

Web Console
Commands Supported by Console:
    cls[clear][ctrl+l]      Clear screen
    term[ctrl+c]           End the current program
    mii-tool                List connection status of network interface
    traceroute              Track packet forwarding path
    arp                    View ARP table
    ping                   Test connectivity of host
    ifconfig               View information of network interface
    route                  Display routing table
    ethtool                View information of network adapter
    telnet                 Test connectivity of port
    proxydbg               proxy [debug ip address]
> telnet www.google.com 443
Resolving ...
172.217.31.36:443 connect OK
    
```

- 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.

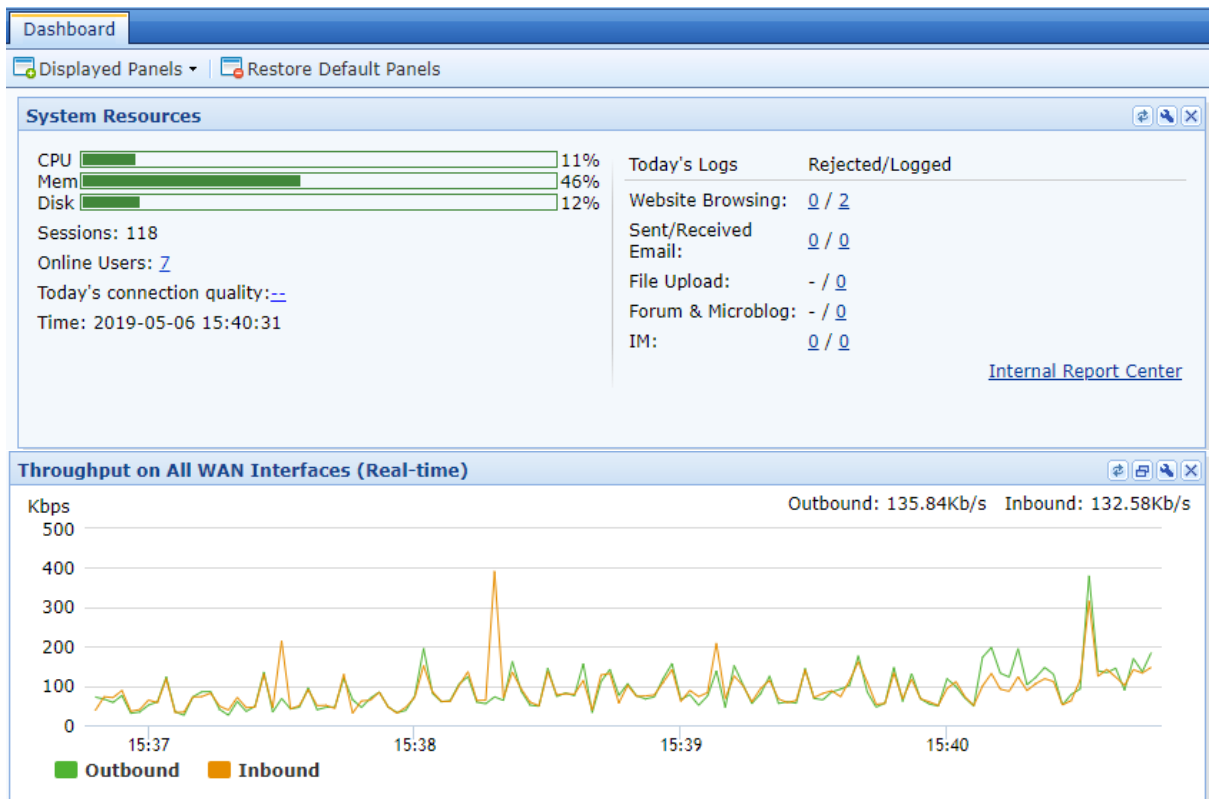
```

Administrator: Command Prompt
C:\Users\Administrator>ping 192.168.19.1

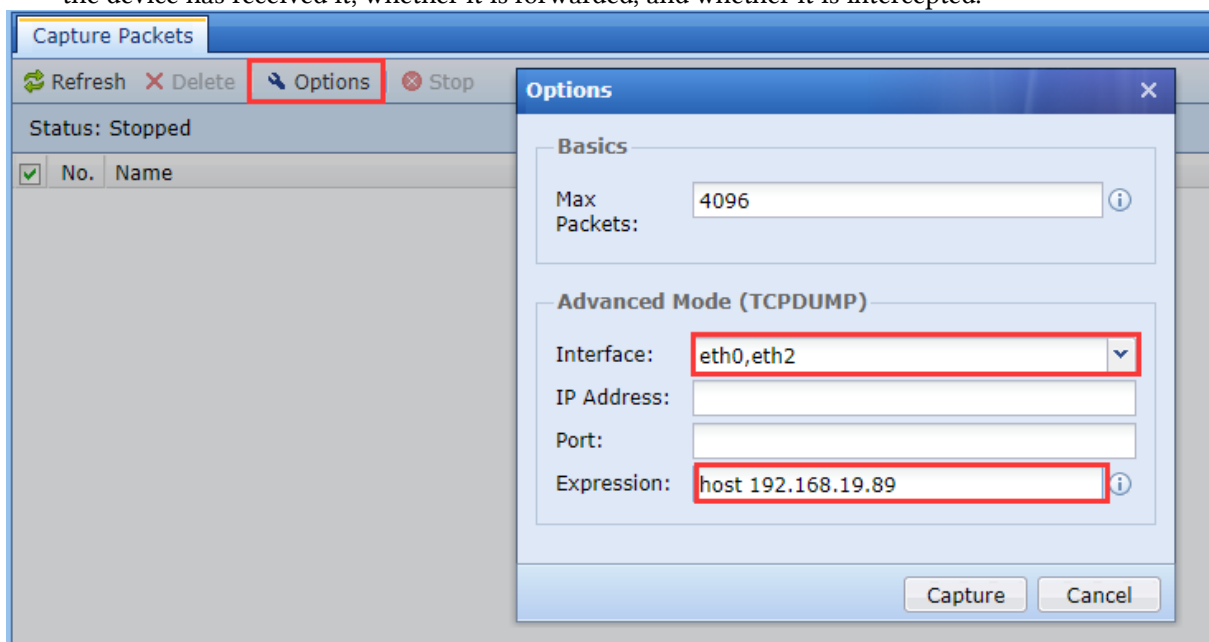
Pinging 192.168.19.1 with 32 bytes of data:
Reply from 192.168.19.1: bytes=32 time=1ms TTL=64
Reply from 192.168.19.1: bytes=32 time=1ms TTL=64
Reply from 192.168.19.1: bytes=32 time<1ms TTL=64
Reply from 192.168.19.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.19.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
    
```

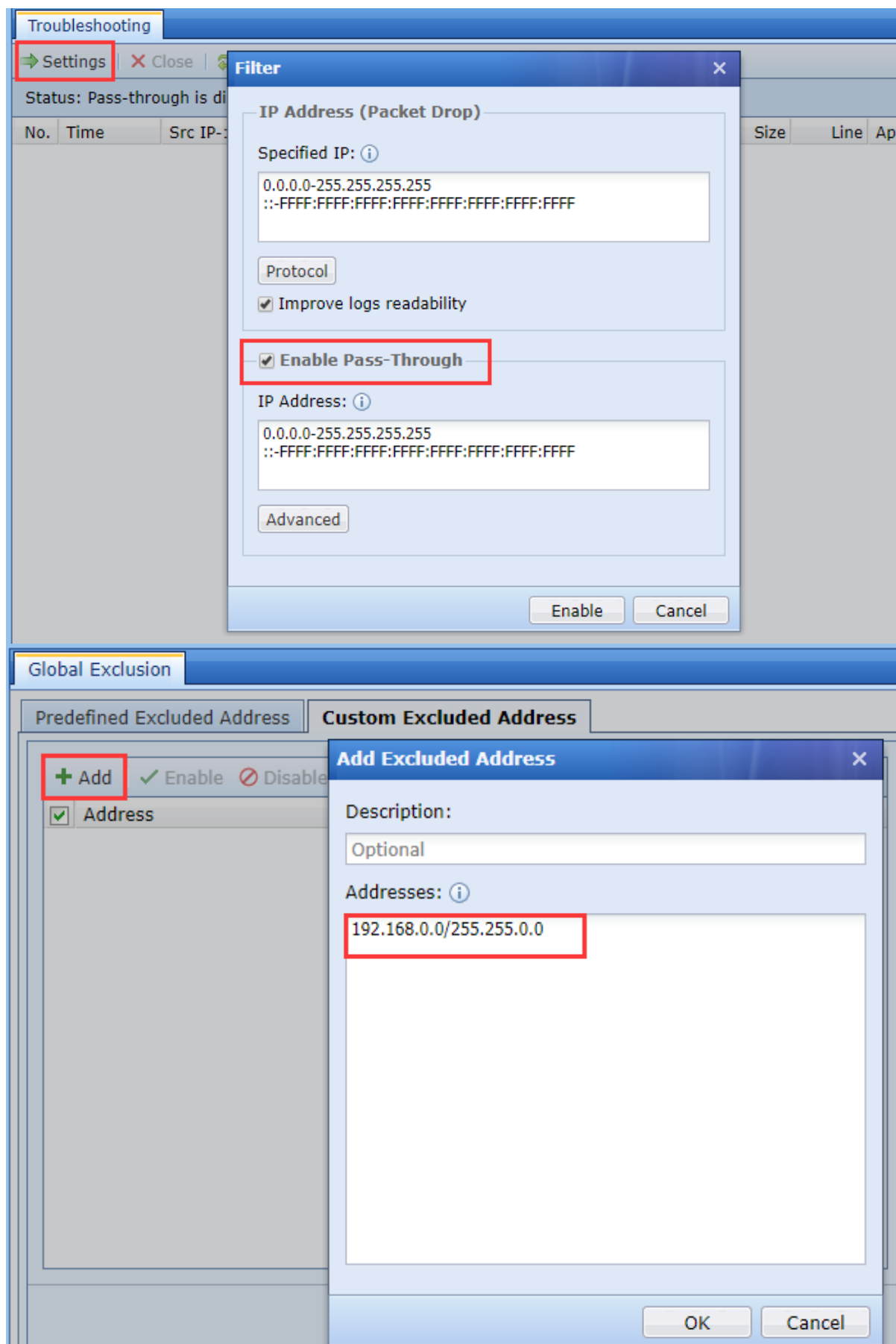
- If the computer does not pass to its gateway, check the internal network problem first to confirm whether the route is incorrect, whether there is ARP spoofing, whether the wiring is incorrect, and whether a loop is formed.
- If the IAM is the gateway of the PC, in addition to confirming the internal 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.

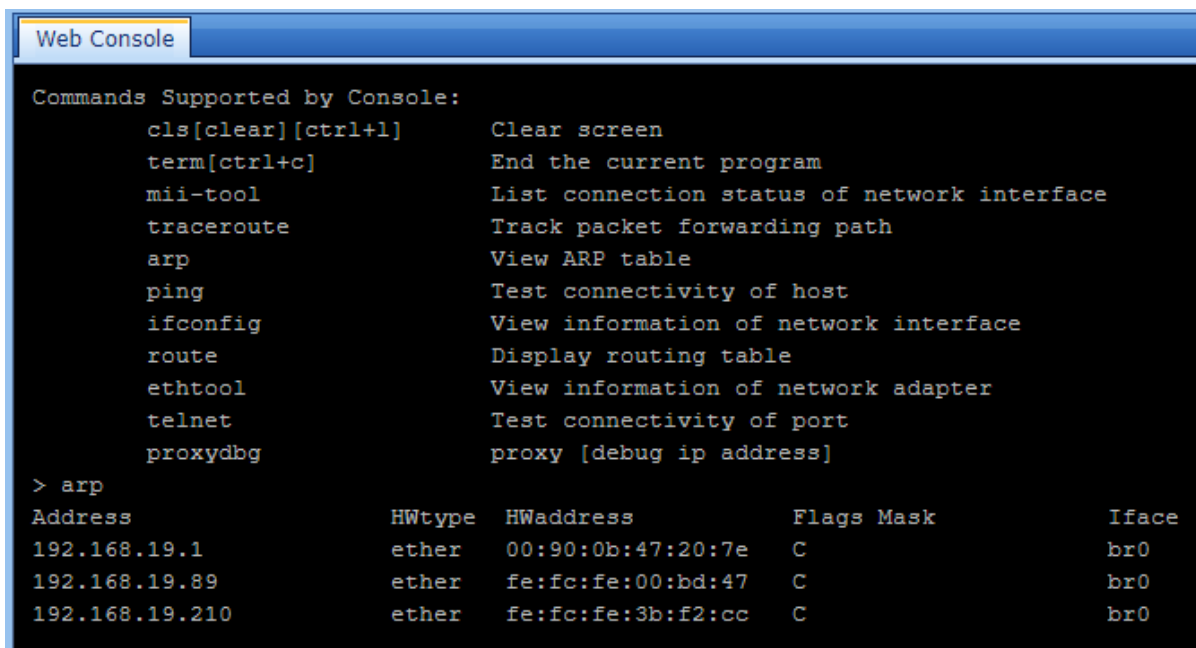


- If the packet is confirmed to be normal through the IAM, select the test PC to access the public network, and then capture the packet at the internal and external network ports of the IAM to see if the device has received it, whether it is forwarded, and whether it is intercepted.



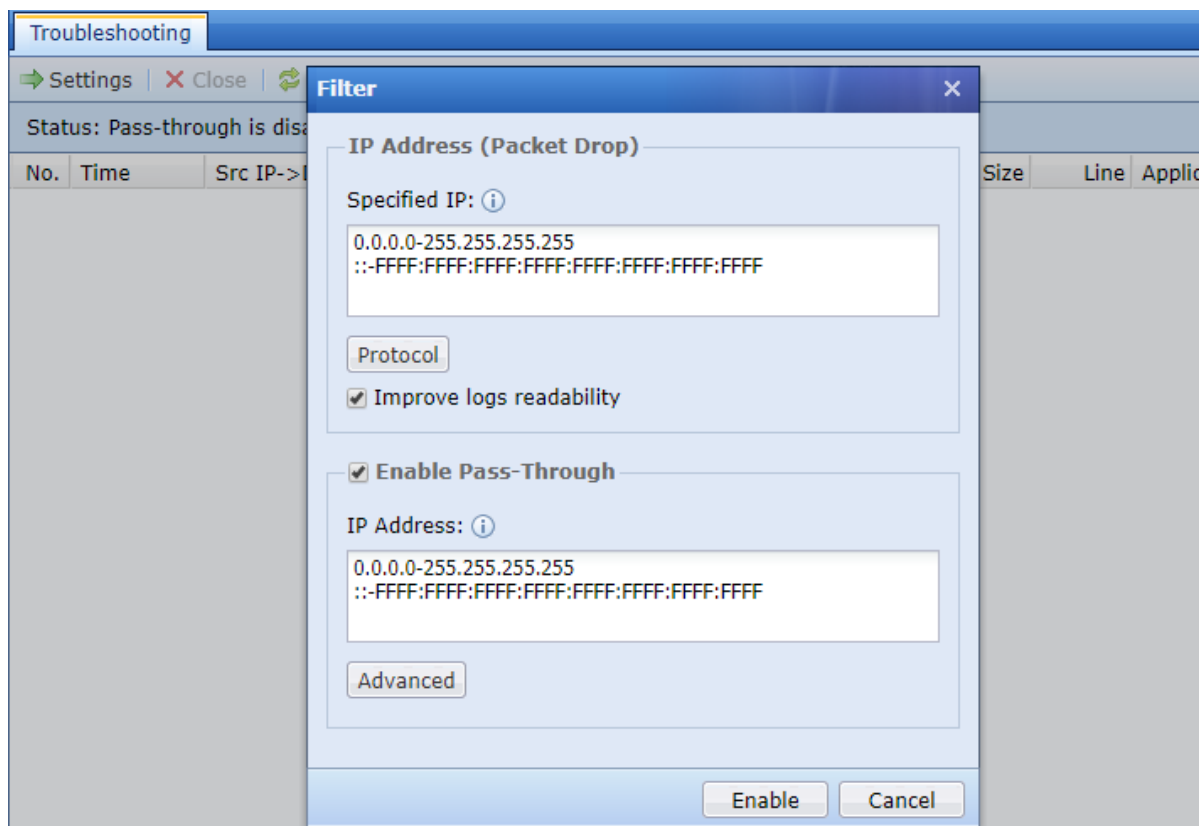
- Check whether the IAM device console can log in normally. If you can, you can enable the global pass-through test to check whether it is restored. Use the arp command to check the ARP table of the device in the IAM console to check whether the ARP information of the device is correct. Check the routing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



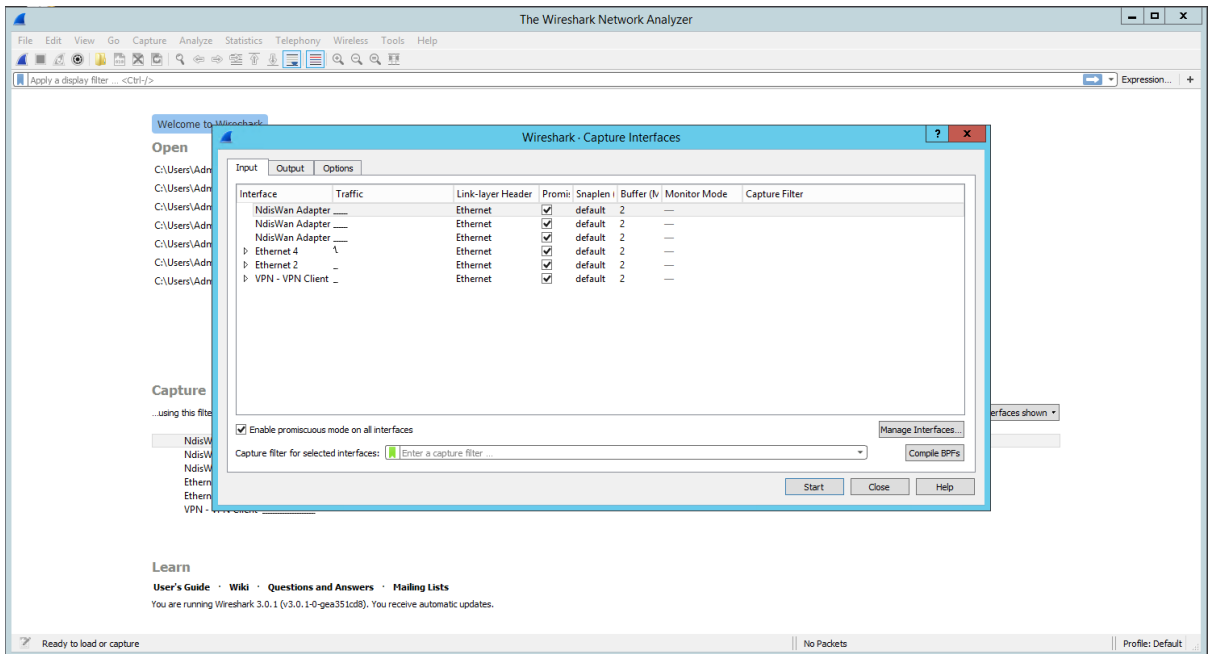
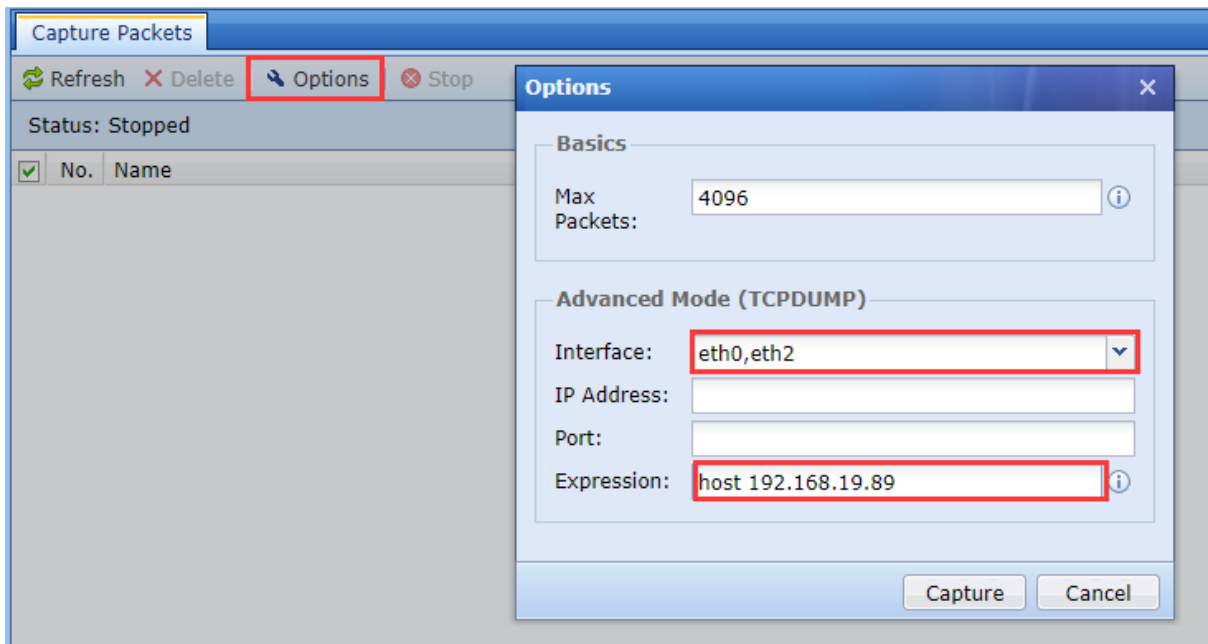


Chapter 2 Troubleshooting when network latency is high

- 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.

The image displays two screenshots of a network traffic analysis tool, likely Wireshark, showing ICMP traffic. Both screenshots show a list of packets with columns for No., Time, Source, Destination, Protocol, and Length. The top screenshot shows packets 7 through 96, and the bottom screenshot shows packets 7 through 98. In both screenshots, packets 71 and 72 in the top view, and 73 and 74 in the bottom view, are highlighted with red boxes. The source IP address for all packets is 192.168.19.89, and the destination IP address is 8.8.8.8. The protocol for all packets is ICMP.

No.	Time	Source	Destination	Protocol	Length
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	

No.	Time	Source	Destination	Protocol	Length
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	



SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc