



How To Guide: *Diagnose Network with Packet Sniffer*

Diagnose Network with Packet Sniffer

Packet sniffer is commonly used to diagnose network-related problems. The following are the parameters commonly used for *Packet sniffer* on the appliance:

1. and = “&&” ; or = “||” ; not = “!”
2. tcp \ udp \ arp \ icmp
3.
 - i Listen on interface. (Listen on all interfaces by default)
 - l Put the interface in "monitor mode"
 - v Produce verbose output.
 - n Do not convert host addresses to names.

Signal of output: S (SYN) ; P (PUSH) ; R (RST) ; F (FIN)

Diagnose Network with Packet Sniffer

Examples:

1.Sniffer 192.168.1.0/24 's icmp packets and exclude 192.168.1.26

icmp and net 192.168.1.0/24 and ! 192.168.1.26

2.Sniffer all IPSEC service

proto 50 or proto 51 or port 500 or port4500

3.Sniffer 10.10.10.1's traffic on port 1 , exclude icmp and ssh

-i eth0 host 10.10.10.1 and not icmp and not port 22

4.Sniffer source Ip = 192.168.1.26 or source subnet = 192.168.1.0/24

src 192.168.1.26 ; src net 192.168.1.0/24

5.Sniffer source port = 21 or destination port = 80

src port 21 ; dst port 80

Diagnose Network with Packet Sniffer

For the NATed networks, running the command **tcpdump** using destination IP as a parameter is required if you need to examine the full path of packet flows. For example, to capture **ping** packets destined for 168.95.1.1 in a NATed network, the following are the commands for your reference:

*net dst. IP (e.g., net 168.95.1.1),
subnet (e.g., net 168.95.1.1/32),
host IP (e.g., host 168.95.1.1)*

```
192.168.1.26 > 168.95.1.1: ICMP echo request, id 1, seq 21144, length 40
13:47:16.529802 device eth0_6, direction OUT: IP (tos 0x0, ttl 127, id 3599, offset 0, flags [none], proto ICMP (1),
length 60)
203.67.222.40 > 168.95.1.1: ICMP echo request, id 1, seq 21144, length 40
13:47:16.529804 device eth0, direction OUT: IP (tos 0x0, ttl 127, id 3599, offset 0, flags [none], proto ICMP (1), length
60)
203.67.222.40 > 168.95.1.1: ICMP echo request, id 1, seq 21144, length 40
13:47:16.549288 device eth0, direction IN: IP (tos 0x0, ttl 245, id 37886, offset 0, flags [DF], proto ICMP (1), length 60)
168.95.1.1 > 203.67.222.40: ICMP echo reply, id 1, seq 21144, length 40
13:47:16.549288 device eth0_6, direction IN: IP (tos 0x0, ttl 245, id 37886, offset 0, flags [DF], proto ICMP (1), length
60)
168.95.1.1 > 203.67.222.40: ICMP echo reply, id 1, seq 21144, length 40
13:47:16.549343 device eth3_5, direction OUT: IP (tos 0x0, ttl 244, id 37886, offset 0, flags [DF], proto ICMP (1), length
60)
```

The screenshot shows a web-based interface for network diagnostics. It features a list of radio buttons for different scan types: Network Port Scan, Netbios Scan, Measure Tunnel Speed, and Speedtest over WAN link. Below this is a section titled "Options of Packet Sniffer" which contains a text input field with the value "net 168.95.1.1 -lvn" and a blue "OK" button. A red oval highlights the text in the input field.

Diagnose Network with Packet Sniffer

Base on the previous case, the following is the command to capture packets using source IP 192.168.1.26 as a parameter.

net 192.168.1.26 -lvn

```
13:55:36.688139 device eth3, direction IN: IP (tos 0x0, ttl 128, id 4123, offset 0, flags [none], proto ICMP (1), length 60)
192.168.1.26 > 168.95.1.1: ICMP echo request, id 1, seq 21636, length 40
13:55:36.688139 device eth3_5, direction IN: IP (tos 0x0, ttl 128, id 4123, offset 0, flags [none], proto ICMP (1), length 60)
192.168.1.26 > 168.95.1.1: ICMP echo request, id 1, seq 21636, length 40
13:55:36.707386 device eth3_5, direction OUT: IP (tos 0x0, ttl 244, id 27760, offset 0, flags [DF], proto ICMP (1), length 60)
168.95.1.1 > 192.168.1.26: ICMP echo reply, id 1, seq 21636, length 40
13:55:36.707390 device eth3, direction OUT: IP (tos 0x0, ttl 244, id 27760, offset 0, flags [DF], proto ICMP (1), length 60)
168.95.1.1 > 192.168.1.26: ICMP echo reply, id 1, seq 21636, length 40
13:55:36.850898 device eth3, direction IN: ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.10 tell 192.168.1.26, length 46
13:55:36.850898 device eth3_9, direction IN: ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.10 tell 192.168.1.26, length 46
13:55:36.850898 device eth3_3, direction IN: ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.10 tell 192.168.1.26, length 46
```

- Show ARP Cache
- Open Port Check
- Network Port Scan
- Netbios Scan
- Measure Tunnel Speed
- Speedtest over WAN link

Options of Packet Sniffer

Options **net 192.168.1.26 -lvn**

The following command is to capture ***ping*** packets from IP 192.168.1.26.

```
13:55:36.688139 device eth3, direction IN: IP (tos 0x0, ttl 128, id 4123, offset 0, flags [none], proto ICMP (1), length 60)
192.168.1.26 > 168.95.1.1: ICMP echo request, id 1, seq 21636, length 40
13:55:36.688139 device eth3_5, direction IN: IP (tos 0x0, ttl 128, id 4123, offset 0, flags [none], proto ICMP (1), length 60)
192.168.1.26 > 168.95.1.1: ICMP echo request, id 1, seq 21636, length 40
13:55:36.707386 device eth3_5, direction OUT: IP (tos 0x0, ttl 244, id 27760, offset 0, flags [DF], proto ICMP (1), length 60)
168.95.1.1 > 192.168.1.26: ICMP echo reply, id 1, seq 21636, length 40
13:55:36.707390 device eth3, direction OUT: IP (tos 0x0, ttl 244, id 27760, offset 0, flags [DF], proto ICMP (1), length 60)
168.95.1.1 > 192.168.1.26: ICMP echo reply, id 1, seq 21636, length 40
```

- Show ARP Cache
- Open Port Check
- Network Port Scan
- Netbios Scan
- Measure Tunnel Speed
- Speedtest over WAN link

Options of Packet Sniffer

Options **net 192.168.1.26 and icmp -lvn**