

5.1 Explain how different tools are used in network maintenance and performance monitoring.

Network Maintenance Tools

Help the network to run smoothly, identify potential issues, and perform regular maintenance.

Ping: Ping tool is used to check network connectivity and trace the path packets take to reach a destination, identifying latency issues or routing problems.

```
root@ip-10-10-172-234:~# ping -c 5 5.134.9.101
PING 5.134.9.101 (5.134.9.101) 56(84) bytes of data.
64 bytes from 5.134.9.101: icmp_seq=1 ttl=52 time=12.6 ms
64 bytes from 5.134.9.101: icmp_seq=2 ttl=52 time=12.6 ms
64 bytes from 5.134.9.101: icmp_seq=3 ttl=52 time=12.6 ms
64 bytes from 5.134.9.101: icmp_seq=4 ttl=52 time=12.5 ms
64 bytes from 5.134.9.101: icmp_seq=5 ttl=52 time=12.6 ms

--- 5.134.9.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 12.599/12.648/12.698/0.129 ms
```

Fig (5.1/1) shows the ping output of WAES IP address is online and reachable. It has transmitted five packets, and we received five replies. Also we can see it took 12.648 ms for the reply to reach to my system, with the maximum being 12.698 ms.

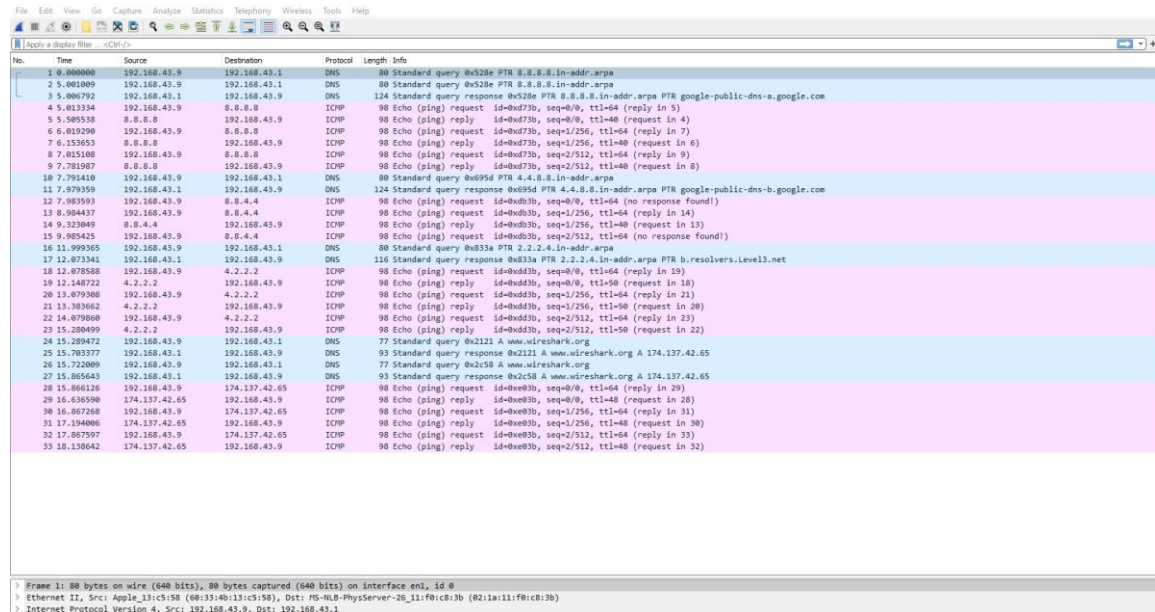
Traceroute: Traceroute tool is used to find the IP addresses of the routers or hops that a packet traverses between a system and host. This commands also reveals the number of routers between the two systems.

```
root@ip-10-10-172-234:~# traceroute waes.ac.uk
traceroute to waes.ac.uk (5.134.9.101), 30 hops max, 60 byte packets
 1  100.91.211.47 (100.91.211.47)  10.113 ms 100.91.211.1 (100.91.211.1)  9.431 ms 100.91.211.51 (100.91.211.51)  9.334 ms
 2  100.100.6.9 (100.100.6.9)  36.037 ms 100.100.6.41 (100.100.6.41)  36.132 ms 100.100.6.65 (100.100.6.65)  56.263 ms
 3  100.100.92.6 (100.100.92.6)  9.940 ms * 100.100.64.6 (100.100.64.6)  9.899 ms
 4  * 100.100.84.143 (100.100.84.143)  25.558 ms 100.100.89.143 (100.100.89.143)  9.811 ms
 5  100.100.14.82 (100.100.14.82)  9.401 ms 100.100.14.84 (100.100.14.84)  9.401 ms 100.100.14.86 (100.100.14.86)  9.395 ms
 6  ld5-linx.as29550.net (195.66.236.223)  9.774 ms 9.604 ms 9.552 ms
 7  ae0-cr0.the.as29550.net (91.186.5.254)  11.450 ms 11.398 ms 11.406 ms
 8  ae1-cr0.rdg.as29550.net (91.186.5.250)  11.563 ms 11.575 ms 11.560 ms
 9  213-229-127-74.static.as29550.net (213.229.127.74)  14.234 ms 14.249 ms 18.981 ms
10  85.92.93.66 (85.92.93.66)  15.442 ms 13.309 ms 13.345 ms
11  . (81.19.189.1)  19.430 ms 21.514 ms 20.076 ms
12  gsp13.guru.net.uk (5.134.9.101)  11.622 ms !X 11.617 ms !X 11.544 ms !X
```

Fig (5.1/2) Using traceroute to find the Ip addresses of the routers. In this traceroute output shows replies from 12 different routers/hops.

Network Performance monitoring tools

Wireshark – is a packet analysis tool used to capture and analyzes network traffic at the packet level. It creates and analyzes PCAPs (network packet capture files) and helps diagnose network issues and identify security threats.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.9	192.168.43.1	DNS	98	Standard query 0x528e PTR 8.8.8.8.in-addr.arpa
2	0.001009	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e PTR 8.8.8.8.in-addr.arpa
3	0.006792	192.168.43.1	192.168.43.9	DNS	124	Standard query response 0x528e PTR 8.8.8.8.in-addr.arpa PTR google-public-dns-a.google.com
4	5.013334	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request id=0xd73b, seq=0/0, ttl=64 (reply in 5)
5	5.505538	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd73b, seq=0/0, ttl=64 (request in 4)
6	6.012920	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request id=0xd73b, seq=1/256, ttl=64 (reply in 7)
7	6.153653	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd73b, seq=1/256, ttl=64 (request in 6)
8	7.015108	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request id=0xd73b, seq=2/512, ttl=64 (reply in 9)
9	7.701907	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd73b, seq=2/512, ttl=64 (request in 8)
10	7.791410	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x695d PTR 4.4.8.8.in-addr.arpa
11	7.979359	192.168.43.1	192.168.43.9	DNS	124	Standard query response 0x695d PTR 4.4.8.8.in-addr.arpa PTR google-public-dns-b.google.com
12	7.983993	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request id=0xd03b, seq=0/0, ttl=64 (no response found)
13	8.904437	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request id=0xd03b, seq=1/256, ttl=64 (reply in 14)
14	9.320409	8.8.4.4	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd03b, seq=1/256, ttl=64 (request in 13)
15	9.905425	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request id=0xd03b, seq=2/512, ttl=64 (no response found)
16	11.099365	192.168.43.9	192.168.43.1	DNS	98	Standard query 0x833a PTR 2.2.2.4.in-addr.arpa
17	12.073341	192.168.43.1	192.168.43.9	DNS	116	Standard query response 0x833a PTR 2.2.2.4.in-addr.arpa PTR b.resolvers.level3.net
18	12.078588	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request id=0xdd3b, seq=0/0, ttl=64 (reply in 19)
19	12.148722	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply id=0xdd3b, seq=0/0, ttl=64 (request in 18)
20	13.079300	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request id=0xdd3b, seq=1/256, ttl=64 (reply in 21)
21	13.383662	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply id=0xdd3b, seq=1/256, ttl=64 (request in 20)
22	14.079800	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request id=0xdd3b, seq=2/512, ttl=64 (reply in 23)
23	15.200499	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply id=0xdd3b, seq=2/512, ttl=64 (request in 22)
24	15.208472	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2121 A www.wireshark.org
25	15.703377	192.168.43.1	192.168.43.9	DNS	93	Standard query response 0x2121 A www.wireshark.org A 174.137.42.65
26	15.722009	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2c58 A www.wireshark.org
27	15.965643	192.168.43.1	192.168.43.9	DNS	93	Standard query response 0x2c58 A www.wireshark.org A 174.137.42.65
28	15.866126	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request id=0xe03b, seq=0/0, ttl=64 (reply in 29)
29	16.636590	174.137.42.65	192.168.43.9	ICMP	98	Echo (ping) reply id=0xe03b, seq=0/0, ttl=64 (request in 28)
30	16.867268	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request id=0xe03b, seq=1/256, ttl=64 (reply in 31)
31	17.134006	174.137.42.65	192.168.43.9	ICMP	98	Echo (ping) reply id=0xe03b, seq=1/256, ttl=64 (request in 30)
32	17.867597	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request id=0xe03b, seq=2/512, ttl=64 (reply in 33)
33	18.138642	174.137.42.65	192.168.43.9	ICMP	98	Echo (ping) reply id=0xe03b, seq=2/512, ttl=64 (request in 32)

> Frame 1: 88 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface eni, id 0
 > Ethernet II, Src: Apple13:c5:58 (08:33:4b:13:c5:58), Dst: HG-NLB-PhysServer-26_11:f0:c8:3b (02:1a:11:f0:c8:3b)
 > Internet Protocol Version 4, Src: 192.168.43.9, Dst: 192.168.43.1

Fig (5.1/3) In this screen, Wireshark gives important information about each packet including packet number, time, source, destination, protocol, length, and packet info.

Nagios – Monitor network devices, services, and applications for performance and availability. It sends alerts on breaches. Also provides detailed reports and includes a wide range of extended functionality.

SolarWinds Network Performance Monitor (NPM) - a tool to monitor network performance including real-time visibility into bandwidth usage, device status, and network health. Its features include intuitive dashboards, automated network discovery, and advanced alerting.

ManageEngine OpManager – monitor network performance, servers, and virtual environments by providing real-time status and alerts. It can perform network mapping, root cause analysis, and performance reports.