

Network Troubleshooting and Tools Glossary

Created By: Ravi Raj, Teaching Assistant

1. **Fiddler:** Web debugging proxy tool to log all HTTP(S) traffic between your computer and the Internet. Inspect traffic, set breakpoints, and fiddle with request/response. **Source(s):** <https://www.telerik.com/fiddler>
2. **ICMP:** An internet layer protocol used mainly in networking for troubleshooting. Commands like Ping and traceroute use ICMP protocol. **Source(s):** https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol, <https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/>
3. **Ipconfig:** Command used in Windows OS to get the information related to the network related components like IP, MAC address, etc.
4. **Name Resolution:** The process of resolving an IP address from the name passed using DNS.
5. **nbtstat:** Displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. This command also allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS). Used without parameters, this command displays Help information. **Source(s):** <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/nbtstat>
6. **netsh:** Netsh is a command-line scripting utility that allows you to display or modify the network configuration of a computer that is currently running. Netsh commands can be run by typing commands at the netsh prompt and they can be used in batch files or scripts. **Source(s):** <https://docs.microsoft.com/en-us/windows-server/networking/technologies/netsh/netsh-contexts>
7. **netstat:** Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6)

protocols). Used without parameters, this command displays active TCP connections.

Source(s):

<https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat>

8. **Network card:** A network card or NIC is responsible for handling the networking operations() related to an OS.
9. **nslookup:** NsLookup queries the specified DNS server and retrieves the requested records that are associated with the domain name you provided. These records contain information like the domain name's IP addresses.
Source(s): <https://network-tools.com/nslookup/>
10. **ping:** Command used to check if a domain is live or not using ICMP protocol. It sends packets of data at timed intervals and checks the number of packets successfully transmitted.
11. **Ports:** In computer network ports refer to a designated channel used by an application to transfer data. Generally well known applications are associated with some predefined port. e.g HTTP is associated with port 80, DNS is associated with port 53.
12. **Protocols:** A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design.

Source(s): <https://www.comptia.org/content/guides/what-is-a-network-protocol>

13. **Round Trip Time:** Round trip associated with a signal is defined as total time it takes for a signal to be sent and the acknowledgement associated with it to be received.
14. **Route Tables:** It is a data table stored in a router or a network host that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table contains information about the topology of the network immediately around it.

Source(s): https://en.wikipedia.org/wiki/Routing_table

15. **TCP/IP:** The Internet protocol suite is the conceptual model and set of communications protocols used in the Internet and similar computer networks. It is commonly known as TCP/IP because the foundational protocols in the suite are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). Its implementation is a protocol stack.

Source(s): https://en.wikipedia.org/wiki/Internet_protocol_suite

- 16. telnet:** Telnet is remote login protocol used in earlier days. It is a client server protocol and provides the user a remote session to the server.
- 17. tracert:** Command used to map the path taken by a packet to reach the destination.
- 18. TTL:** Time to Live is defined as maximum time a packet is considered alive in a network. If the packet doesn't reach its destination within TTL it is lost and shouldn't be received.
- 19. WINS:** Windows Internet Name Service (WINS) is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names. Effectively, WINS is to NetBIOS names what DNS is to domain names — a central mapping of host names to network addresses.
Source(s): https://en.wikipedia.org/wiki/Windows_Internet_Name_Service
- 20. Wireshark:** A packet capture tool used to analyze the packets being transmitted in a network.