Q1. Explain packet tracer.

Ans
- Packet tracer is a cross-platform visual simulation tool designed by cisco systems that allows users to create network topologies and imitate modern computer networks.
- The software allows users to simulate the configuration of cisco routers and switches using a simulated command line interface.
- Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.
- The software is mainly focused towards Cisco Networking Academy students as an educational tool for helping them learn fundamental CCNA concepts.
- Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.
- Packet tracer can be ~~use~~ run on Linux, microsoft windows, macOS.
- Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP.

Q2. Explain packet tracer tools.

Ans. Tools in packet tracer include:

1. Ping:
- The ping command is a very common method used to troubleshoot accessibility of devices.
- It uses a series of Internet control message

Protocol (ICMP).

2. Traceroute:
- The traceroute command allows you to determine the path a packet takes in order to get to a destination from a given source by returning the sequence of hops the packet has traversed
- It is used to discover the routes that packets usually take when they travel to their destination.

3. Debug:
- The debug command displays information about the cisco device operations, generated on received traffic, and any error messages
- The information is provided in real-time until the user disables debugging or the device is restarted.

4 Wireshark:
- Wireshark is a network protocol analyzer, or an application that captures packets from a network connection.

Q3. Explain header format of packet tracer.

Ans 1. Ver:
- It is the field that contains the IP protocol version
- The current version is 4.5 is an experimental version

2. HEL (Header length):

- Specifies the length of IP header in 32-bit words.

3. Service type:
- Indicates quality of service requested for this IP datagram.

4. Total length:
- Specifies total length of the datagram, header and data

VER	HEL	Service Type	Total length
4 bits	4 bits	8 bits	16 bits
Datagram Identification		Flags	Fragment offset
16 bits		3 bits	13 bits
Time to live	Protocol	Header checksum	
8 bits	8 bits	16 bits	
Source IP address			
32 bits			
Destination IP address			
32 bits			

5. Identification:
- Used for uniquely identifying fragments of an IP datagram when fragmentation occurs

6. Flags:
- contains control flags

7. Time to live:
- Specifies number of routers the packet can traverse

8. Protocol:
- Identifies protocol used in TCP, UDP, ICMP.

Q4. Explain wireshark.

Ans. • Wireshark is a free open-source network analyzer that captures and displays network traffic in real time.

• It's a popular tool for troubleshooting network issues, analyzing protocols, and ensuring network security.

→ Here are some of the things wireshark can do:

1. Capture packets:

• Wireshark can capture packets from a network connection, such as from a computer to the internet.

2. Analyze network protocols:

• Wireshark can understand the structure of different networking protocols and display the fields and their meaning.

3. Identify security threats:

• Wireshark can help identify potential security threats and cybercriminal activity.

4. Diagnose network performance:

• Wireshark can help diagnose network performance issues.

5. Filter output:

• Wireshark can filter the output of captured traffic using various settings, times and filters.