**Control plane protocols:**

1. Service-Based Architecture (SBA) Protocols: These use modern web standards (HTTP/2 and RESTful APIs) to let different network functions share information and work together smoothly.

2. Non-Access Stratum (NAS) Protocols: NAS protocols manage how devices connect to the network and handle things like logging in, keeping connections secure, and managing ongoing sessions.

3. Access and Mobility Management Function (AMF) Protocols: AMF helps control how devices connect to the network and move around. It coordinates between the user’s device and the network’s base stations, and manages handovers when devices move from one base station to another.

4. Session Management Function (SMF) Protocols: SMF is in charge of managing data sessions, including setting up and adjusting the paths that data travels through the network.

5. User Plane Function (UPF) Protocols: UPF deals with routing and forwarding user data. It works with SMF to manage how data flows through the network.

6. Unified Data Management (UDM) Protocols: UDM handles user profiles and subscription information. It works with AMF for authentication and with other functions to provide data for applications.

7. Network Exposure Function (NEF) Protocols: NEF lets third-party applications access network data and services in a controlled way, making sure everything stays secure.

8. Network Slicing Protocols: Network slicing allows the creation of separate virtual networks on top of the same physical network. This means different types of services can operate independently and efficiently.

9. Location Management Protocols: These manage where devices are located in the network, helping with tasks like moving from one area to another and maintaining connectivity.

**User plane protocols:**

1. User Plane Function (UPF):

What It Does: UPF is the main controller for handling and forwarding user data. It makes sure data like videos and messages are sent from your device to where it needs to go, and vice versa.

Why It’s Important: It ensures that your data is delivered quickly and efficiently, and can also manage things like data speed and quality.

2. GPRS Tunneling Protocol (GTP):

What It Does: GTP creates "tunnels" in the network to carry user data. Think of it as a secure, private route that keeps your data protected and on the right path.

Why It’s Important: It makes sure your data travels securely and efficiently through the network from your device to its destination.

3. Internet Protocol (IP):

What It Does: IP assigns addresses to data packets so they know where to go. It's like the address on a letter, directing data to the right location.

Why It’s Important: It ensures that data packets can find their way through the internet and the network, so everything you do online works smoothly.

4. User Datagram Protocol (UDP) / Transmission Control Protocol (TCP):

What They Do: UDP and TCP are methods for sending data. UDP is faster but less reliable, while TCP ensures that data arrives correctly and in the right order.

Why They’re Important: They help manage how data is sent over the network. TCP is used when accuracy is crucial, while UDP is used for applications where speed matters more.