Some important computer network-related terms along with brief explanations:

1. **Attenuation:**

   - **Explanation:** Attenuation refers to the reduction of signal strength as it travels over a medium, such as a cable or a wireless link. It is a common concern in communication systems, and the goal is to minimize attenuation to maintain signal integrity.

2. **Bandwidth:**

   - **Explanation:** Bandwidth is the maximum data transfer rate of a network or communication channel. It is usually expressed in bits per second (bps) and determines how much data can be transmitted over the network in a given time.

3. **Latency:**

   - **Explanation:** Latency is the time delay between the sending and receiving of data. It includes various factors such as propagation delay (time for signals to travel through a medium) and processing delay.

4. **Router:**

   - **Explanation:** A router is a networking device that forwards data packets between computer networks. It operates at the network layer of the OSI model and makes decisions based on IP addresses.

5. **Firewall:**

   - **Explanation:** A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks.

6. **DNS (Domain Name System):**

   - **Explanation:** DNS is a system that translates domain names (e.g., www.example.com) into IP addresses. It allows users to access websites using human-readable domain names instead of remembering numerical IP addresses.

7. **LAN (Local Area Network):**

   - **Explanation:** A LAN is a network that is limited to a small geographic area, such as a single building or a campus. It allows connected devices to communicate with each other.

8. **WAN (Wide Area Network):**

- **Explanation:** A WAN is a network that spans a larger geographic area, often connecting multiple LANs. It may use public or private communication links, such as leased lines or the Internet.

9. **TCP/IP (Transmission Control Protocol/Internet Protocol):**

- **Explanation:** TCP/IP is a suite of communication protocols used for transmitting data across networks. It is the foundation of the Internet and provides a reliable and standardized communication method.

10. **Packet:**

- **Explanation:** A packet is a unit of data that is transmitted over a network. It consists of a header containing control information and the actual data being transmitted.

11. **MAC Address (Media Access Control Address):**

- **Explanation:** A MAC address is a unique identifier assigned to each network interface for communication on a network. It is used at the data link layer of the OSI model.

12. **Subnet:**

- **Explanation:** A subnet is a portion of a network that shares a common address component. It allows for efficient use of IP addresses and helps in organizing and securing network traffic.

13. **Jitter:**

Jitter refers to the variation in the delay of received packets in a network. In the context of latency, jitter is the irregularity in the time it takes for a packet to travel from the source to the destination. Unlike latency, which measures the overall delay, jitter focuses on the inconsistency or variability in that delay.

Jitter can be caused by several factors, including:

Network Congestion: Increased traffic and congestion on a network can lead to variations in packet delivery times.

Routing Changes: If the network routes change dynamically, it can result in varying delays for packets as they take different paths to reach the destination.

Packet Queuing: In situations where packets are queued before being transmitted, variations in the queue length can introduce jitter.

Wireless Networks: In wireless networks, interference, signal strength fluctuations, and other wireless issues can contribute to jitter.

Network Switching Equipment: The processing time within routers and switches can introduce variability in packet delivery times.

Jitter is particularly important in real-time applications such as voice over IP (VoIP) and video conferencing, where a consistent and low-latency communication experience is crucial. Excessive jitter can result in poor audio or video quality, as the irregular arrival of packets may lead to disruptions or delays in the playback.

VoIP (Voice over IP):

Good Jitter Range: Typically, for VoIP applications, a jitter of 20 milliseconds or less is considered acceptable. Lower values contribute to a smoother and more natural voice communication experience.

Video Conferencing:

Good Jitter Range: Similar to VoIP, for video conferencing, a jitter of 20 milliseconds or lower is often targeted to ensure a seamless and high-quality video experience.

Gaming:

Good Jitter Range: Gamers may aim for even lower jitter, ideally below 10 milliseconds, to minimize delays and ensure a responsive gaming environment.

Checking the attenuation, bandwidth, and latency (RTT) of a network involves using various tools and methods.

1. **Attenuation:**

- **Method: Signal Strength Measurement**

- Use a network analyzer or a specialized tool to measure the signal strength at different points in the network.

- Compare the strength of the signal at the source with the strength at the destination to calculate attenuation.

- Alternatively, if you have access to network equipment, check logs or management interfaces for information on signal strength.

2. **Bandwidth:**

- **Method: Network Performance Testing**

- Utilize network performance testing tools, such as iPerf or Ookla Speedtest, to measure the actual data transfer rates between devices.

- Conduct tests at different times to account for variations in network usage.

- Check the specifications of network equipment, such as routers and switches, for information on their maximum supported bandwidth.

3. **Latency:**

- **Method: Ping and Traceroute**

- Use the ping command to measure the round-trip time between two devices. This provides a basic measure of latency.

```
ping [destination IP or domain]
```

- Use the traceroute command to trace the route taken by packets to reach a destination and identify delays at each hop.

```
traceroute [destination IP or domain]
```

- **Method: Network Monitoring Tools**

- Implement network monitoring tools like Wireshark or Nagios to capture and analyze packet-level information, including latency metrics.

- Set up alerts to be notified when latency exceeds predefined thresholds.