

[Obkio Blog](#)[Subscribe](#)[HOW TO](#) [FEATURES](#) [NETWORK METRICS](#) [JITTER](#)

# How to Measure Jitter & Keep Your Network Jitterbug Free

Alyssa Lamberti

Last updated on Apr 9, 2023

## Table of Contents

- [What is Network Jitter?](#)
- [How Do You Measure Jitter?](#)
- [Step 1. Use a Jitter + Network Monitoring Tool](#)
- [Step 2. Measure Jitter in All Network Locations](#)
- [Step 3. Collect Jitter Measurements](#)
- [Step 4. Continuously Test Jitter](#)
- [Step 5. Measure the Impact of Jitter](#)
- [Step 6. Identify the Causes of Jitter](#)
- [Step 7. Set Up Jitter Alerts](#)
- [Step 8. Troubleshoot Network Jitter](#)
- [Step 9. Fix & Reduce Jitter](#)
- [Step 10: Continuous Network Jitter Monitoring](#)
- [More Tools to Measure Jitter](#)
- [Jitter Monitoring Tools vs. Network Monitoring Tools](#)



Has your network been bitten by the jitterbug? Are you tired of your network dancing the jitterbug? Do you find yourself constantly tapping your foot waiting for pages to load or downloads to finish?

Network jitter is your network's biggest enemy when using unified communications and real-time apps like IP telephony, video conferencing, and virtual desktop infrastructure. Troubleshooting and measuring jitter helps you avoid sounding like a robot on video calls.

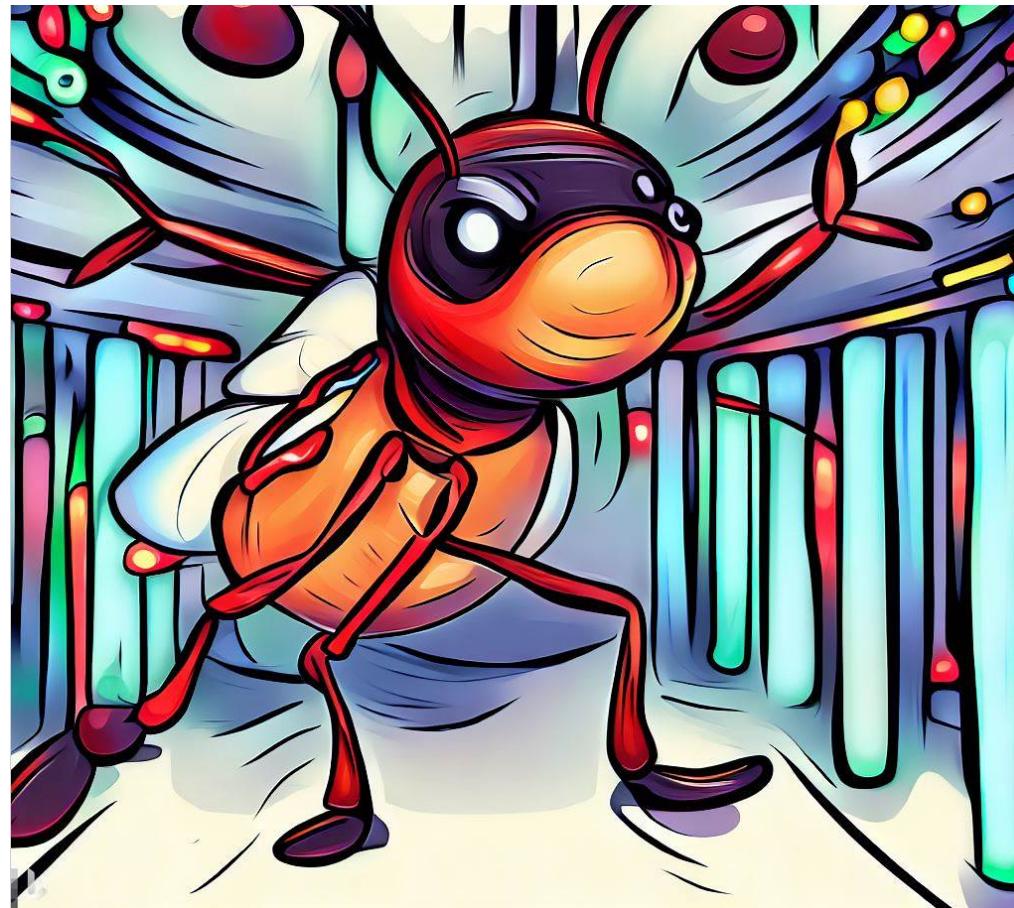
Well, fear not, because in this blog post we're going to teach you how to measure jitter, test jitter on a network using Obkio Network Monitoring, and keep your network jitterbug free! We'll guide you through the steps to diagnose and fix any jitter issues, so that your network can perform smooth moves without any annoying jitters.

## What is Network Jitter in Networking?

Network Jitter is one of the core network metrics that you should be measuring when monitoring your network performance.

What is jitter in networks? Network Jitter is a variation in delay of the arrival of data packets - also known as a disruption that occurs while data packets travel across the network. The jitter definition in networking refers to the variation in time between packets of data that are sent and received over a network.

Jitter can cause issues in real-time applications such as video conferencing, online gaming, and voice-over-IP (VoIP) calls, where timing is critical. If packets arrive too late or too early, it can result in glitches, delays, or lost data, leading to a poor user experience. Therefore, measuring and reducing jitter is an important aspect of network performance optimization.



Measure Network Jitter Now!

## How Do You Measure Jitter?

Jitter is often expressed as the standard deviation of the packet delay time. In simpler terms, jitter is the difference in the time it takes for packets to reach the destination. Network jitter is also usually measured in **milliseconds (ms)**



Network jitter is measured by calculating the average time difference between each packet sequence. So, to measure jitter, we need to calculate the variation in delay between packets that are sent and received over a network. This variation is measured in milliseconds (ms) and is typically represented as an average deviation from the mean delay.

## MEASURING JITTER

$$J = \sqrt{\frac{1}{N} \sum_{i=1}^N (D_i - \bar{D})^2}$$

↓                    ↓                    ↓                    ↓  
 Jitter      The total number of measured packets.      The delay of the i-th packet.      The average delay of all the measured packets.

**Here's an example:** Let's say we send 10 packets of data over a network and measure the time it takes for each packet to arrive at its destination. The time between each packet arrival is recorded, and the average delay is calculated. If the average delay is 100ms and the variation in delay between packets is between 5ms and 10ms, then the jitter would be calculated as the average deviation from the mean delay, which would be somewhere between 5ms and 10ms.

### #2. Use MD and MAD to Measure Jitter

Another way to measure jitter is to use the mean deviation (MD) or mean absolute deviation (MAD) from the mean delay. This is calculated by subtracting the mean delay from each packet delay, taking the absolute value of the result, and then calculating the average of those values. The MD or MAD represents the average



### #3. Use Average Delay to Measure Jitter

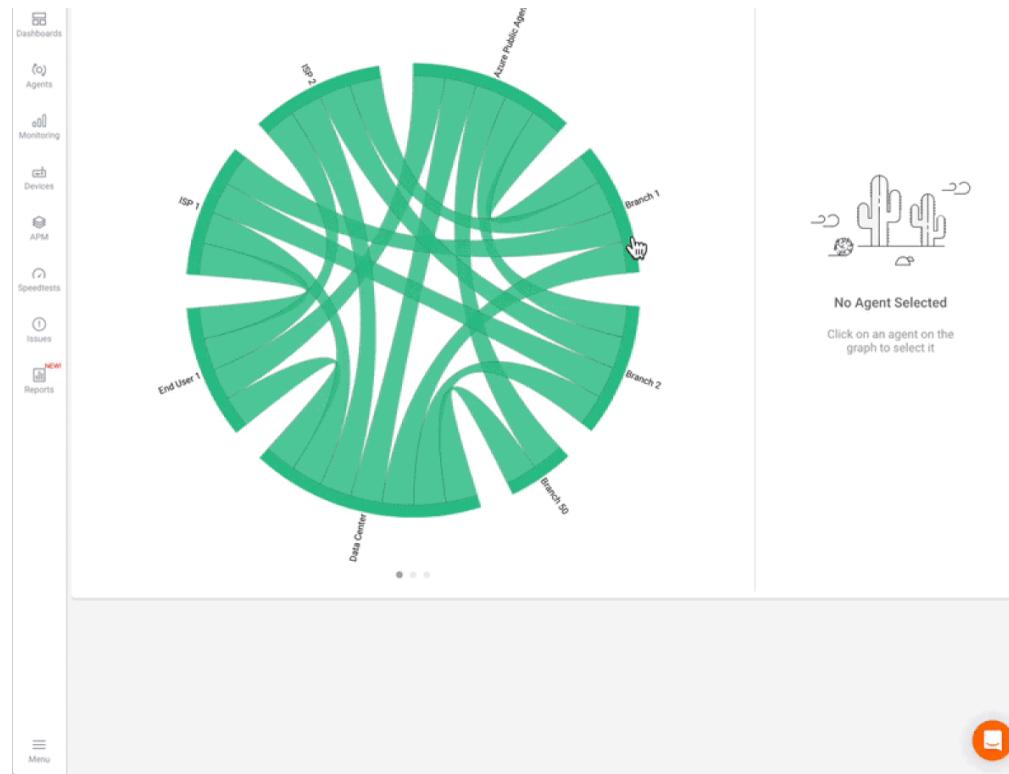
Jitter can also be represented as a percentage of the average delay. For example, if the average delay is 100ms and the jitter is 10ms, then the jitter percentage would be 10% of the average delay.

Overall, there are different ways to measure network jitter, but the basic principle is to calculate the variation in delay between packets and represent it as an average deviation from the mean delay, in milliseconds or as a percentage.

### Step 1. Measure Jitter With A Comprehensive Network Jitter Monitoring + Network Monitoring Tool

Jitter is a network problem that you can hear - mostly because it makes you sound like a robot or laggy. Regardless, it's still important to continuously measure jitter in your network to determine where it's coming from and what's causing it.

The most accurate way to test jitter is by using a tool like Obkio Network Performance Monitoring Software.



Obkio is a network performance monitoring tool that is designed to continuously measure network jitter and other metrics. One of the ways it does this is by sending packets at regular intervals of 500ms (or half a second). This is a common technique used to monitor network performance in real-time applications, such as voice-over-IP (VoIP) and unified communications (UC), where timing is critical.

By sending packets every 500ms, Obkio can capture any variations in delay or packet loss that may be affecting VoIP or UC applications. This information is then used to calculate the jitter and other metrics that are essential for maintaining optimal network performance.

Obkio's comprehensive approach encompasses not only jitter monitoring but also provides a holistic view of network performance, making it a powerful solution for addressing jitter-related issues. With Obkio users gain access to real-time

[Features](#)[Pricing](#)[Customers](#)[MSPs](#)[Documentation](#)[Screenshots](#)[Blog](#)[Contact](#)[Login](#)[Try for Free](#)

packet loss, latency, and overall [network health](#).

Get started with Obkio's free trial!

[Try Now!](#)

## Step 2. Deploy Network Jitter Monitoring: Measure Jitter in All Network Locations

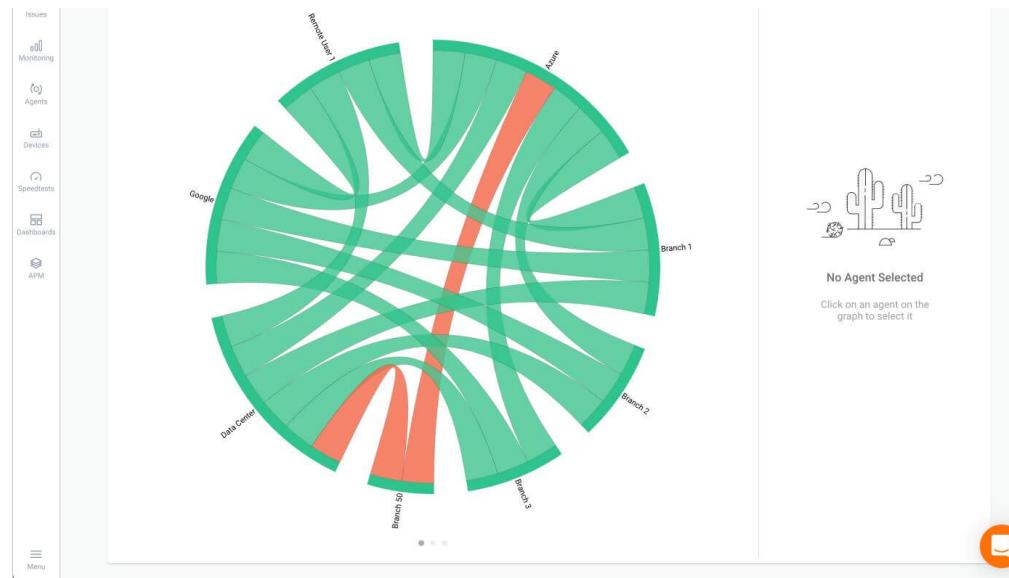
Obkio measures network jitter using continuous synthetic traffic from [Network Monitoring Agents](#) deployed in your most important network locations like offices, data centers and clouds. The Agents measures jitter in your network by sending and monitoring data packets through your network every 500ms using for the most precise jitter measurements.

This is extremely important for ensuring end-to-end network jitter monitoring, and catching high jitter in all network locations and applications.

**For example:** You can measure network jitter between your head office and the [AWS network](#), or even between AWS and your data center.

To deploy jitter monitoring in all your network locations, we recommend deploying:

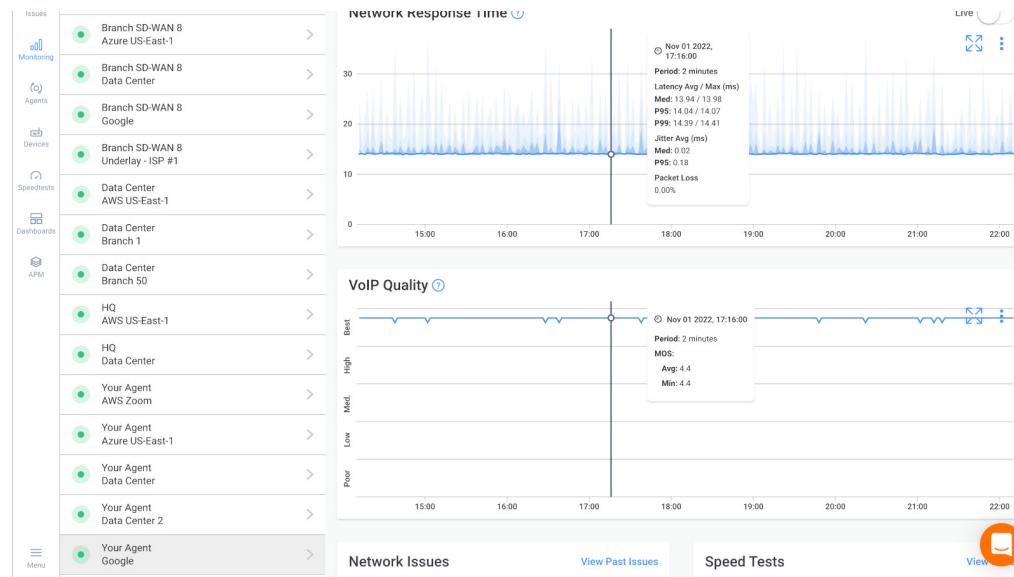
1. [Local Agents](#): Installed in the targeted office location experiencing high jitter issues. There are several Agent types available (all with the same features), and they can be installed on MacOS, Windows, Linux and more.
2. [Public Monitoring Agent](#): Which are deployed over the Internet and managed by Obkio. They compare performance up to the Internet and quickly identify if the jitter is global or specific to the destination. For example, measure packet loss between your branch office and [Google Cloud](#).



### Step 3. Collect Network Jitter Measurements: Measure High vs. Low Jitter Levels

Once you've set up your Monitoring Agents, they will start measuring metrics like jitter and collecting data, which you can easily analyze on Obkio's Network Response Time Graph.

Identify and measure jitter anywhere in your network with updates every minute. You can also further drill-down to identify where exactly the network jitter is happening, and start troubleshooting network issues.



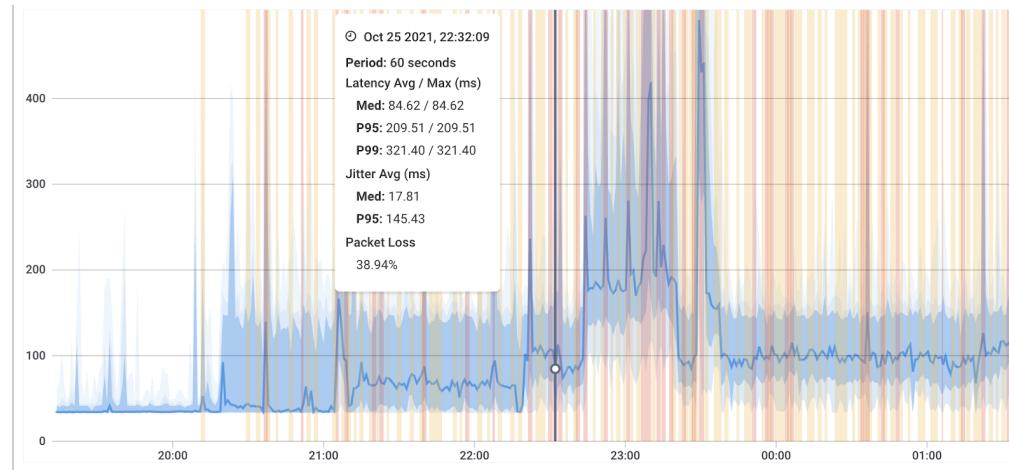
## I. Acceptable Levels of Jitter

The acceptable level of network jitter can vary depending on the type of application and the network environment. However, in general, **a jitter level of up to 30ms is considered acceptable for most applications.**

If the jitter level exceeds 30ms, it can start to impact real-time applications like VoIP, video conferencing, and gaming. In these cases, a **VoIP jitter level of up to 50ms may still be acceptable, but beyond that, the user experience is likely to be significantly impacted.**

For applications that are less time-critical, such as email or file transfers, jitter levels of up to 100ms may be acceptable, but any higher than that could result in noticeable delays and reduced performance.

It's important to note that these are general guidelines, and the acceptable level of jitter may vary depending on the specific requirements of the application or network. For example, in environments where real-time applications are critical, such as emergency services or healthcare, a much lower jitter level may be required to ensure optimal performance. Therefore, it's important to measure network jitter



## II. What Is A Good Jitter Speed?

A good jitter speed can depend on the specific requirements of the application and the network conditions. However, in most cases, a jitter value of 30 milliseconds (ms) or less is considered acceptable for real-time communication. Lower jitter values are even better, as they provide a smoother and more reliable experience for users.

It's important to note that while low jitter is desirable, achieving consistently low jitter can be challenging in networks, especially over the public internet. Network congestion, packet loss, and other factors can contribute to increased jitter. To manage jitter effectively, network administrators may implement Quality of Service (QoS) mechanisms, prioritize traffic, and use buffering techniques to minimize its impact.

## III. How Much Jitter is Bad in Networking?

While the threshold for "bad" jitter can vary depending on the specific use case and application requirements, generally speaking, **jitter values exceeding 50 milliseconds (ms)** are often considered problematic for real-time applications like VoIP calls, video conferencing, and online gaming.

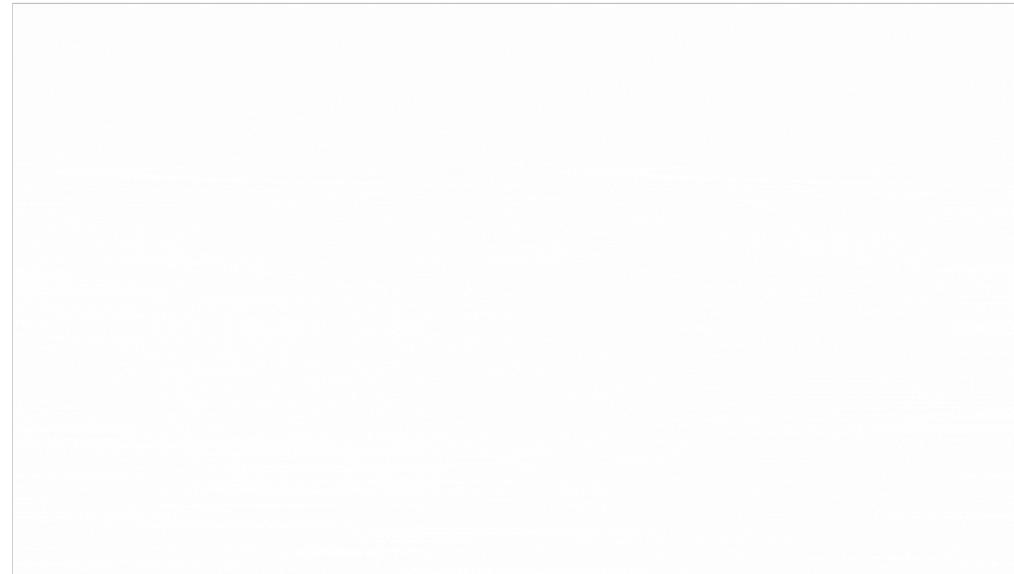
When jitter exceeds this threshold, it can lead to:



- **Delay and Latency:** Excessive jitter contributes to increased latency, making real-time interactions feel sluggish and less responsive.
- **Packet Loss:** Jitter can contribute to packet loss, where packets may arrive too late to be processed or are dropped due to buffer limitations.
- **Quality Degradation:** Overall call or communication quality can deteriorate significantly, affecting the user experience.

## Step 4. Continuously Test Jitter for More Accurate Jitter Measurements

Network monitoring tools, like Obkio, typically test jitter by analyzing the timing characteristics of packet delivery between two points on a network. Here's a general overview of how network monitoring tools test jitter:



### 1. Synthetic Traffic:



## 2. Packet Timestamping:

Network monitoring tools use packet timestamping to record the time of transmission and time of arrival for each packet. This information is crucial for calculating delay and jitter.

## 3. Calculation of One-Way Delay:

By subtracting the timestamp of packet transmission from the timestamp of packet reception, your network monitoring tool calculates the one-way delay for each packet.

## 4. Calculation of Jitter:

Jitter is the variation in delay between successive packets. Your monitoring tool will calculate jitter by measuring the differences in one-way delay between consecutive packets.

## 5. Statistical Analysis:

Network monitoring tools often use statistical methods to analyze the collected delay and jitter data. Common statistical measures include mean (average) delay, standard deviation (jitter), and other metrics that provide a comprehensive view of network performance.

## I. Aggregate Jitter Test Measurements

Unlike most monitoring solutions, Obkio automatically aggregates data over time to be able to display graphs over a large period of time.

With aggregation, Obkio shows you the worst jitter measurements in the aggregated graph. For example, the network jitter measurement displayed over an aggregated period of 1h is the worst median jitter of all the small 1-min periods within that hour.

This is important because only showing you the average amount of jitter on your network may hide network issues.



using real-time applications.

Compared to other monitoring solutions, Obkio shows you the worst jitter measurements in order to highlight network issues, where they're located and what's causing them.



**HOW TO MEASURE**  
**Laten~~cy~~cy**

**How to Measure Latency**  
Learn how to measure latency with Obkio's Network & Latency Monitoring tool. Check for latency in your network & analyze latency measurements.

[Learn more →](#)

## II. More Methods To Test Jitter in Your Network

Testing jitter in a network involves measuring the variation in packet delay times. Although we just showed you how a Network Monitoring tool does this easily, automatically, and continuously, there are other methods you can use to test netowrk jitter.

### i. Test Jitter with Ping (ICMP Echo):

The most basic method is to use the ping command, which sends Internet Control Message Protocol (ICMP) echo requests to a destination and measures the round-trip time. While ping primarily measures latency, variations in round-trip times can give an indication of jitter.

Example: `ping -n 100 [destination_ip]`

### ii. Test Jitter with IPSLA (IP Service Level Agreements):

Cisco's IP Service Level Agreements can be used to monitor network performance, including jitter. It sends synthetic traffic to a destination and measures various



For Voice over Internet Protocol (VoIP) networks, specialized [VoIP monitoring tools](#) often provide detailed information on packet delays and jitter specifically tailored for real-time communication.

#### **iv. Test Jitter Packet Capture and Analysis:**

Some tools test jitter by capturing and analyzing of network packets. By examining timestamps and sequence numbers, you can identify jitter in real-time communication.

When testing jitter, it's essential to consider the specific requirements of your network and the applications running on it. Choose the method that best fits your needs, and consider using a combination of tools for a comprehensive analysis of network jitter.

### **Step 5. Measure the Impact of Jitter on Different Applications**

Jitter can affect different applications in different ways, depending on the nature of the application and the level of sensitivity to timing. With an end-to-end monitoring solution like Obkio, you have visibility of all your network locations, devices, and applications to understand how jitter is affecting different parts of your network.

Here are some examples:

#### **I. Jitter on Voice-over-IP (VoIP):**

Jitter can cause delays in the transmission of voice packets, resulting in poor call quality, choppy audio, and even dropped calls. In VoIP, timing is critical, and any variations in delay can be very noticeable.

#### **Timing Sensitivity in VoIP:**

VoIP systems digitize analog voice signals into data packets that are transmitted over the internet. These packets need to arrive at their destination in a specific order and within a predictable time frame to reconstruct the original audio signal accurately. In traditional telephone systems, timing is tightly controlled, ensuring



## Variation in Packet Arrival Time:

Jitter refers to the variation in the arrival time of data packets. When packets arrive with inconsistent timing, it disrupts the reconstruction of the audio signal at the receiving end. In VoIP, each packet carries a small portion of the voice signal. If packets arrive out of order or with irregular spacing, the receiving device may struggle to piece together the voice signal correctly, resulting in disruptions.

## Impact on Call Quality:

The variations caused by jitter can lead to the following issues:

- **Choppy Audio:** If packets arrive too late or out of order, it can create gaps in the audio stream, causing interruptions or missing words in the conversation.
- **Delay and Latency:** Increased jitter contributes to higher latency, causing noticeable delays between the time someone speaks and when the other party hears the response. This delay can make conversations feel unnatural and disjointed.
- **Echo and Overlapping:** Jitter can lead to audio packets arriving at the receiver with inconsistent timing. This can result in overlapping or echoed audio, making it difficult to understand the conversation.

## Dropped Calls:

In extreme cases of jitter, packets might arrive so late that they are considered irrelevant and are discarded. This can lead to dropped calls or significant parts of the conversation being lost.

## Real-World Impact:

Imagine a scenario where a person is speaking, and their voice packets are delayed due to jitter. The receiving party might experience unnatural pauses, broken sentences, or overlapping audio, making the conversation difficult to follow. In professional settings like business calls or customer support, such quality issues can harm communication and lead to misunderstandings.



Service or QoS for VoIP, buffering, packet reordering, and jitter buffers. Jitter buffers store incoming packets briefly to reorder them and mitigate timing variations before playing them out. Additionally, Quality of Service (QoS) mechanisms can prioritize voice traffic and allocate network resources to ensure more predictable packet delivery.

## II. Jitter on Video Conferencing:

Like VoIP, video conferencing apps like Zoom and Microsoft Teams are highly sensitive to timing. Jitter can cause delays in the transmission of video packets, resulting in poor video quality, frozen frames, and delayed audio.

### Timing Sensitivity in Video Conferencing:

Video conferencing applications operate in a manner similar to VoIP, but they transmit both audio and video data in real-time. Just as in VoIP, the precise timing of packet delivery is crucial to maintaining seamless communication during video calls.

### Impact of Jitter on Video Conferencing:

Jitter can introduce timing variations in the arrival of video and audio packets, leading to several issues:

- **Poor Video Quality:** Jitter can cause video packets to arrive out of order or with irregular spacing. This disrupts the synchronization between audio and video, resulting in pixelation, blurriness, or distortion in the video feed.
- **Frozen Frames:** Excessive jitter can delay the arrival of video frames, causing certain frames to be held back or skipped altogether. This can lead to frozen video frames, where participants appear to be stuck in a single position.
- **Delayed Audio:** Just as in VoIP, jitter in video conferencing can also lead to delayed audio, creating an unnatural delay between a person's speech and the corresponding audio reaching the other participants.

### User Experience Impact:



making it difficult for participants to follow along. Participants' facial expressions and body language can also be affected, leading to misinterpretations and misunderstandings.

### Mitigation Strategies:

Video conferencing applications employ various strategies to mitigate the effects of jitter:

- **Buffering:** Jitter buffers store incoming packets briefly to reorder and synchronize audio and video streams before presentation.
- **Adaptive Bitrate:** These apps may adjust the quality of video streams based on network conditions to ensure smoother playback.
- **Network Optimization:** Some apps prioritize network traffic using QoS mechanisms to ensure smoother video and audio transmission.

### III. Jitter on Gaming

Online gaming requires fast and reliable network connections with low latency and minimal jitter. Jitter can cause delays in game response times, leading to lag, stuttering, and other performance issues that can significantly impact the player experience.

### IV. Jitter on File transfers

While file transfers are not as sensitive to timing as real-time applications like VoIP and gaming, they can still be affected by jitter. Jitter can cause delays in the transmission of data packets, resulting in slower transfer speeds and longer wait times.

In general, any application that relies on real-time data transmission, such as voice or video, is likely to be sensitive to jitter. Even applications that are less time-critical, such as email or web browsing, can be impacted by excessive jitter if it leads to significant delays in packet delivery.



## Step 6. Identify the Causes of Jitter - Measure Jitterbug Syndrome

There are several factors that can cause network jitter, and they're not obvious to catch. Part of measuring jitter is understanding what is causing high levels of jitter in networking, and taking steps to solve it. A tool like Obkio will help you drill-down to understand what's causing jitter in your network.

But let's go over some of the most common causes of jitter:

1. **Congestion:** When there is too much traffic on a network, it can cause delays in the transmission of packets, leading [network congestion](#) and jitter.
2. **Buffering:** If packets are held in a buffer for too long before being sent, it can cause jitter when they are finally transmitted.
3. **Network latency:** Latency is the time it takes for a packet to travel from one point to another on the network. When latency is high, it can cause jitter.
4. **Network equipment issues:** Faulty network devices such as routers, switches, or cabling can cause jitter by delaying or dropping packets.



It's important to identify the root cause of jitter in networking in order to effectively mitigate it and [improve network performance](#).

A screenshot of the Obkio Network Performance Monitoring software interface. On the left, there's a sidebar with the Obkio logo and the text "Obkio Network Performance Monitoring" followed by "Network monitoring &amp; troubleshooting made easy." Below this is an orange button labeled "Start Your Free Trial". The main area features a large circular chart divided into several segments, each representing a different network agent or location. The segments are color-coded, with green being the largest proportion. To the right of the chart, there's a small icon of a person and the text "No Agent Detected Click here to see the agents you have".

## Step 7. Set Up Network Jitter Alerts: Proactively Measure Jitter Levels

To more accurately measure jitter in networking, and be alerted of when it happens, Obkio sends jitter alerts based on historical data and not just static thresholds.

As soon as there's a deviation in the historical data, and your network is experiencing jitter, Obkio sends you an alert.

Why do we do this? For simplicity.

Network performance is always measured between two points, but depending on where you're monitoring performance, and even which technology (cable, DSL, fiber) you're using, the amount of jitter can vary. This would force you to set up different jitter thresholds for every monitoring session - which is a lot of work.

By measuring jitter based on your baseline network performance, Obkio makes the setup much quicker and easier.

## Step 8. Troubleshoot Network Jitter: Just Measuring Jitter Isn't Enough



- Obkio Vision Visual Traceroute tool
- Obkio Device Monitoring to identify exactly where, when, and why the network jitter is happening, and how to solve it.

Troubleshooting network jitter can be a complex process, but here are some steps you can take to identify and resolve jitter issues:

- 1. Identify the source of the jitter:** Start by monitoring network traffic to identify the source of the jitter. Jitter can be caused by a range of issues, including network congestion, packet loss, or hardware failures. Using a network monitoring tool like Obkio can help you quickly identify the source of the problem.
- 2. Check for network congestion:** Network congestion is a common cause of jitter, especially during peak [network usage hours](#). Check for network congestion or [network overload](#) by monitoring network traffic, looking for spikes in traffic volume or [network utilization rates](#). You may need to optimize network settings, such as Quality of Service (QoS) settings, to reduce congestion.
- 3. Monitor for packet loss:** Packet loss can cause significant jitter, especially for real-time applications like VoIP or video conferencing. Monitor for packet loss by examining network performance metrics, such as packet loss rates, and investigating any patterns or trends that may be contributing to the problem.
- 4. Check hardware components:** Faulty hardware components, such as routers or switches, can also cause jitter. Check the hardware components on your network and ensure they are functioning correctly. Replace any components that are faulty or outdated.
- 5. Adjust network settings:** Adjusting network settings, such as buffer sizes or packet sizes, can help reduce jitter. Experiment with different settings to find the optimal configuration for your network.
- 6. Test and monitor:** Once you have identified and resolved any issues contributing to network jitter, test and monitor network performance to ensure the problem has been resolved. Use a network monitoring tool to continuously monitor



Following these steps can help you identify and resolve network jitter issues. This will ensure that your network and applications perform optimally without any annoying glitches or delays. So, get ready to bust some moves and keep your network Jitterbug-free with these troubleshooting tips!



Measure Network Jitter Now!



are two things to do as this point: First you'll need to fix that high amounts of jitter happening in your network, and then you'll have to take steps to optimize your network to reduce jitter happening in the future.

## I. How to Fix Jitter in Networking

Fixing jitter in networking involves identifying and addressing the underlying causes that lead to variations in packet delay. Here are some steps you can take to mitigate jitter and improve network performance:

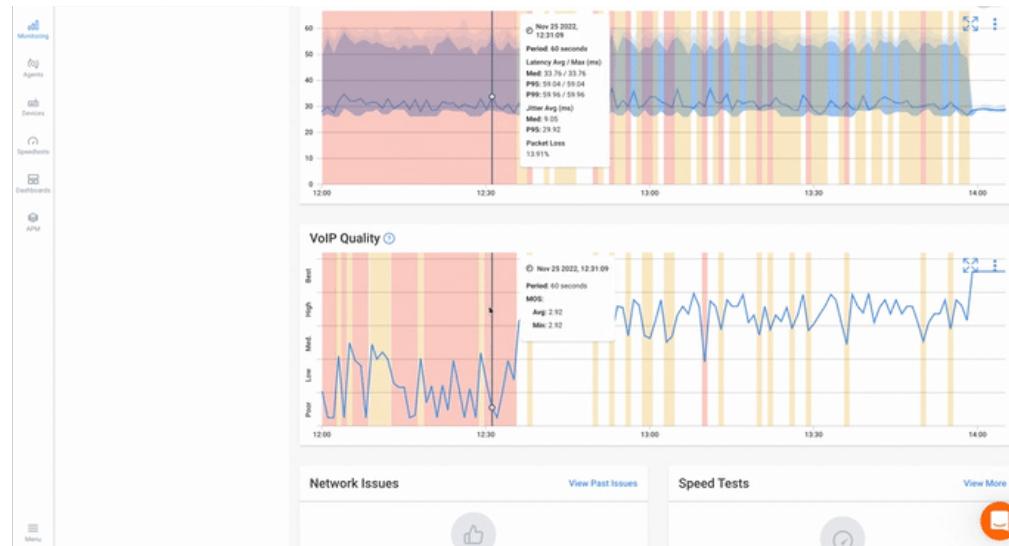
- 1. Check Network Congestion:** Jitter often arises from network congestion, where traffic overwhelms network resources. Identify and manage peak usage times, and consider implementing Quality of Service (QoS) settings to prioritize real-time traffic like VoIP or video conferencing.
- 2. Optimize Network Hardware:** Ensure that your networking equipment, including routers, switches, and modems, are up to date and properly configured. Outdated or misconfigured hardware can contribute to jitter.
- 3. Use Wired Connections:** Wired connections generally offer more consistent and reliable performance compared to wireless connections, which can be more susceptible to interference and latency.
- 4. Check for Packet Loss:** Packet loss often correlates with jitter. Measure and troubleshoot packet loss issues, which may involve investigating faulty cables, addressing interference, or reconfiguring network settings.
- 5. Update Firmware and Software:** Keep networking equipment and devices updated with the latest firmware and software patches. This can address known issues and improve overall network stability.
- 6. Reduce Network Noise:** Minimize unnecessary network traffic and applications that may contribute to congestion. Background downloads, updates, or other



... good quality cables and connectors. Ensure that your network cables and connectors are of good quality and properly shielded to minimize interference and signal degradation.

8. **Implement Jitter Buffering:** Jitter buffering is a technique used in networking equipment and software to temporarily store and reorder incoming packets. This helps smooth out variations in packet arrival times before delivering them to the receiving application.
9. **Adjust Buffer Sizes:** Network devices may have adjustable buffer settings. Optimizing buffer sizes can help manage variations in packet arrival times and reduce jitter.
10. **Prioritize Traffic:** Use Quality of Service (QoS) settings to give priority to real-time traffic like VoIP and video conferencing over other types of data.
11. **Use VPNs Wisely:** Virtual Private Networks (VPNs) can introduce additional latency and jitter. If using a VPN, choose a service with optimized routing and low-latency servers.
12. **Monitor and Analyze:** Regularly monitor your network's performance using Obkio's network monitoring tool. Analyze jitter metrics and performance data to identify trends and take proactive measures.
13. **Contact Your Internet Service Provider (ISP):** If the issue persists and you've exhausted local troubleshooting options, consider reaching out to your ISP. They can help diagnose and address issues affecting your network connection.

Remember that fixing jitter might involve a combination of these steps, and it's important to approach the process systematically. Identifying and addressing the root causes of jitter will contribute to a more stable and reliable network for real-time applications.



## II. How to Reduce Jitter in Networking?

Reducing jitter in networking involves implementing various strategies to minimize the variation in packet delay and ensure a more consistent and predictable network performance. Here are several steps you can take to reduce jitter:

- 1. Use Quality of Service (QoS):** Implement QoS settings on your network devices to prioritize real-time traffic, such as VoIP and video conferencing, over other types of data. QoS ensures that time-sensitive applications receive sufficient bandwidth and lower latency.
- 2. Optimize Network Configuration:** Configure your network devices, such as routers and switches, to operate efficiently. Adjust buffer sizes, queue management algorithms, and other settings to minimize packet delay and jitter.
- 3. Upgrade Network Hardware:** If your current networking equipment is outdated or unable to handle your network's demands, consider upgrading to hardware with better processing power and improved packet handling capabilities.



5. **Use Wired Connections:** Whenever possible, use wired Ethernet connections instead of wireless connections. Wired connections offer lower latency and more stable performance.
6. **Optimize Wi-Fi Setup:** If you must use Wi-Fi, optimize your Wi-Fi setup by selecting appropriate channels, using the 5 GHz band, and minimizing interference from other devices.
7. **Monitor Network Performance:** Regularly use network monitoring tools to track packet delay, jitter, and other performance metrics. This helps you identify patterns and address issues promptly.
8. **Implement Jitter Buffering:** Use jitter buffers in network devices or software applications to temporarily store and reorder packets. This helps smooth out variations in packet arrival times before delivering them to the destination.
9. **Minimize Interference:** Identify and mitigate sources of electromagnetic interference that can disrupt your network signal, such as electronic devices and appliances.
10. **Use Quality Cables and Connectors:** Ensure that you use high-quality, shielded cables and connectors to minimize signal degradation and interference.
11. **Upgrade Internet Service Plan:** If your current internet plan doesn't provide sufficient bandwidth for your needs, consider upgrading to a higher-speed plan to accommodate real-time applications better.
12. **Prioritize Network Traffic:** Use traffic shaping techniques to prioritize time-sensitive traffic like VoIP over less critical data traffic.



**14. Test and Optimize:** Continuously test and fine-tune your network setup.

Experiment with different configurations and settings to find the optimal setup that reduces jitter.

**15. Consult with Experts:** If jitter persists despite your efforts, consider seeking

assistance from network professionals or your internet service provider to diagnose and address more complex issues.

Just like how the Jitterbug dance requires continuous monitoring and adjustment to ensure smooth moves, reducing network jitter also requires ongoing monitoring and adjustment to ensure optimal network performance. By taking the steps mentioned above, you can minimize jitter and ensure your network applications dance to a jitter-free beat. So, put on your dancing shoes and keep on monitoring to maintain the jitterbug rhythm of your network!

## Step 10: Continuous Network Jitter Monitoring

So, you've got your jitter monitoring and network monitoring all set up with Obkio, and you've tackled those annoying high jitter events like a champ. Well done! But hold up, don't close that monitoring dashboard just yet. Continuous jitter monitoring is still a must-do, even after conquering those initial jitter headaches. Why, you ask? Because keeping a watchful eye on jitter is key to maintaining a smooth-sailing network.

- **Early Detection of Jitter Issues:** Continuous monitoring allows for the early detection of jitter problems as they arise. Jitter refers to the variation in the delay of packet delivery, and it can lead to inconsistent and choppy audio or video streams, degraded call quality, or disruptions in real-time applications. By continuously monitoring jitter metrics, network administrators can identify sudden increases or sustained high levels of jitter, enabling them to take proactive measures to address the issue promptly and minimize its impact on communication quality.



performance by tracking jitter fluctuations and identifying their sources. By proactively addressing jitter-related issues, organizations can deliver smooth, uninterrupted communication experiences, leading to increased productivity, customer satisfaction, and user engagement.

- **Troubleshooting and Root Cause Analysis:** Continuous network jitter monitoring provides valuable data for troubleshooting and root cause analysis. By monitoring jitter levels over time, administrators can correlate jitter events with other network parameters such as latency, packet loss, or congestion. This helps in identifying underlying network issues or specific devices causing the jitter. Armed with this information, administrators can take targeted actions to resolve the problem, whether it involves adjusting network configurations, upgrading hardware, or optimizing traffic management.
- **Quality of Service (QoS) Management:** Continuous jitter monitoring is essential for organizations that have committed to meeting specific quality of service (QoS) requirements or service level agreements (SLAs). By continuously monitoring jitter metrics, administrators can ensure compliance with performance standards and take proactive steps to maintain the agreed-upon quality levels. This helps in building trust with customers, reducing service disruptions, and upholding the reputation of the organization.
- **Capacity Planning and Network Optimization:** Continuous monitoring of network jitter provides insights into long-term performance trends and patterns. By analyzing historical jitter data, administrators can identify capacity limitations, anticipate future demands, and optimize network resources accordingly. This enables organizations to plan for network upgrades, allocate bandwidth effectively, and make informed decisions to enhance overall network performance.

## Performing A VoIP Jitter Test: Measure Jitter for VoIP Applications

A VoIP (Voice over Internet Protocol) jitter test is a diagnostic tool used to measure the variation in the delay of VoIP packets as they travel across a network. Jitter can



## Here's how a VoIP jitter test works:

- **Test Setup:** The test involves two key components: the sender and the receiver. The sender generates a continuous stream of VoIP packets and sends them over the network to the receiver. Both the sender and receiver are typically software-based applications or devices designed to simulate VoIP traffic.
- **Packet Transmission:** The sender sends packets at a regular interval, simulating real-time VoIP traffic. Each packet contains a timestamp indicating when it was sent.
- **Packet Reception:** The receiver receives the packets and measures the time it takes for each packet to arrive. It then calculates the difference between the expected arrival time (based on the sender's timestamp) and the actual arrival time.
- **Jitter Calculation:** The jitter is calculated by measuring the variation in the arrival times of packets. Specifically, it's the average of the absolute differences between the expected arrival time of each packet and its actual arrival time. Jitter is usually expressed in milliseconds (ms).
- **Jitter Reporting:** Once the test is complete, the jitter value is reported. A low jitter value indicates that the network is delivering VoIP packets consistently and predictably, while a high jitter value suggests that there is significant variation in packet delivery times.

## Interpreting the Results:

- **Low Jitter:** Jitter values of around 1-10 ms are generally considered low and indicate good network conditions for VoIP. VoIP calls are likely to have clear audio quality and minimal disruptions.
- **Moderate Jitter:** Jitter values between 10 ms and 30 ms may still be acceptable for many VoIP applications, though some minor audio artifacts or delays might be noticed in certain cases.



VoIP jitter tests are useful for diagnosing network issues and optimizing network settings to ensure a smoother VoIP experience. Network administrators can use the results of jitter tests to identify and address potential problems, such as network congestion, improper QoS settings, or other issues affecting VoIP traffic.

## Performing An Internet Jitter Test

An Internet jitter test is a diagnostic tool used to measure the variability in delay (jitter) of data packets as they travel across the internet. Jitter can impact the performance of various online applications, including real-time communication tools like VoIP, video conferencing, and online gaming. An internet jitter test helps assess the quality and consistency of your internet connection for such applications.

**Here's how an internet jitter test typically works:**

- **Test Setup:** Similar to other network tests, an internet jitter test involves a sender and a receiver. The sender generates a stream of data packets and sends them over the internet to the receiver. Both the sender and receiver can be software-based tools or services designed for this purpose.
- **Packet Transmission:** The sender sends data packets at regular intervals, emulating typical internet traffic. Each packet contains a timestamp indicating when it was sent.
- **Packet Reception:** The receiver receives the data packets and measures the time it takes for each packet to arrive. Just like in a VoIP jitter test, the receiver calculates the difference between the expected arrival time (based on the sender's timestamp) and the actual arrival time.
- **Jitter Calculation:** The jitter value is calculated by measuring the variation in the arrival times of data packets. It's usually calculated as the average of the absolute differences between the expected arrival time of each packet and its actual arrival time. The result is typically expressed in milliseconds (ms).



## Interpreting the Results:

- **Low Jitter:** Jitter values in the range of 1-10 ms are generally considered low and indicate a stable and reliable internet connection for real-time applications. You can expect minimal disruption and smooth performance.
- **Moderate Jitter:** Jitter values between 10 ms and 30 ms might be acceptable for many applications, but some minor issues like occasional lags or delays could be noticeable, particularly in real-time applications.
- **High Jitter:** Jitter values exceeding 30 ms can lead to significant performance issues, including disruptions, delays, and potentially poor audio/video quality in real-time applications.

Internet jitter tests are valuable tools for assessing your internet connection's suitability for different types of online activities. They can help you diagnose and troubleshoot network problems, including issues related to network congestion, routing, or other factors affecting packet delivery. By understanding your network's jitter characteristics, you can make informed decisions about using real-time applications or optimizing your network settings to ensure a smoother online experience.

## All The Tools You Can Use Measure Jitter & Catch the Jitterbug

Measuring network jitter is like taking the pulse of your Jitterbug dance partner - it helps you understand their rhythm and timing. To measure network jitter, you can use a variety of tools and techniques. In the steps above, we showed you how to measure jitter using Network Performance monitoring tools, because they're the most complete and detailed.

But here are some common more methods:

- **Ping:** Ping is a command-line tool that sends a series of packets to a target device and measures the time it takes for them to travel back and forth. By comparing the time differences between packets, you can calculate the jitter.



- **Network performance monitoring tools:** There are many network performance monitoring tools available that can measure jitter, latency, packet loss, and other network metrics. Obkio sends packets every 500ms to catch jitter issues affecting VoIP, UC applications, and more. Just like how a skilled Jitterbug dancer can feel the pulse of their partner, [network monitoring tools](#) can measure the pulse of your network and identify any timing issues that may be causing jitter.
- **VoIP testing tools:** VoIP testing tools (or [VoIP Monitoring tools](#)) are specifically designed to measure jitter in real-time applications such as voice-over-IP (VoIP) calls. These tools simulate VoIP traffic and measure the quality of the connection, including jitter.

Overall, measuring network jitter requires a combination of tools and techniques to provide a comprehensive understanding of network performance. So, keep your network in rhythm by using the right tools to measure and monitor network jitter!

**The Ultimate Introduction to Obkio's Network Performance Monitoring Tool**

[Download the demo](#)



[Watch the free demo](#)

## Jitter Monitoring Tools vs. Network Monitoring Tools: Which Should You Use to Measure Jitter?

When it comes to measuring jitter in network communications, there are two primary approaches to consider: using a dedicated jitter monitoring tool and utilizing an end-to-end network monitoring tool. While both aim to assess and address jitter-related issues, they differ in their focus and scope.



## 1. Jitter Monitoring Tool:

A dedicated jitter monitoring tool is specifically designed to measure and analyze jitter in network communications. These tools focus on providing detailed insights into jitter metrics, such as variation, latency spikes, and packet delay. They typically employ specialized techniques, such as sending test packets and analyzing their timing, to accurately measure jitter.

### Pros:

- **Specialized focus:** Jitter monitoring tools are optimized for capturing and analyzing jitter metrics with precision.
- **Granular insights:** These tools offer detailed information about jitter fluctuations, enabling administrators to pinpoint jitter-related issues and take targeted actions to address them.
- **Real-time monitoring:** Jitter monitoring tools often provide real-time data updates and visualizations, allowing administrators to monitor jitter fluctuations as they occur.

### Cons:

- **Limited scope:** Jitter monitoring tools typically focus solely on jitter-related metrics and may not provide comprehensive information about other network performance parameters.
- **Potential fragmentation:** Using a dedicated jitter monitoring tool alongside other monitoring tools may result in fragmented data and require separate configurations.

## 2. End-to-End Network Monitoring Tool:



loss, device health, and application performance, in addition to jitter.

### Pros:

- **Holistic view:** End-to-end network monitoring tools offer a comprehensive perspective on network performance, including jitter, within a unified monitoring solution.
- **Contextual insights:** These tools analyze jitter in networking in relation to other network parameters, enabling administrators to identify potential correlations and root causes of jitter issues.
- **Scalability:** End-to-end network monitoring tools can handle large-scale networks and complex infrastructures.

### Cons:

- **Less specialized:** While end-to-end network monitoring tools provide jitter monitoring capabilities, they may not offer the same level of granularity and specialized focus as dedicated jitter monitoring tools.

In summary, a dedicated jitter monitoring tool excels in providing specific and detailed insights into jitter metrics, while an end-to-end network monitoring tool offers a broader perspective on network performance, including jitter, within a comprehensive monitoring framework. The choice between the two depends on the specific needs and priorities of network administrators, considering the level of granularity and comprehensive monitoring required.

## Why Should You Measure Jitter & Avoid Jitterbugs?

As we said above, jitter is one of the core network metrics which gives you an overview of your network performance and can also have a huge impact on the end user experience.



helps you understand the quality of your network performance, especially for time-critical applications such as VoIP and video conferencing.

2. **Identify network issues:** By measuring jitter, you can identify any timing issues that may be causing glitches or delays in your network traffic. This can help you proactively troubleshoot and address issues before they affect your applications or end-users.
3. **Optimize your network performance:** In addition, measuring network jitter can also help you optimize your network performance by identifying areas where network traffic can be prioritized or network hardware can be upgraded to reduce jitter. This can help ensure that your network is running efficiently and meeting the performance needs of your applications and users.

Ultimately, measuring network jitter is essential for maintaining optimal network performance and delivering a smooth user experience. By monitoring and addressing network jitter, you can minimize disruptions and ensure that your network is operating at its best.

Measuring key metrics like Jitter, along with [Packet Loss](#) and [Latency](#), also provide essential data for determining good or poor network performance.

## Don't Let the Jitterbugs Win - Measure Network Jitter Now!

Now that you know how to measure and reduce network jitter, you can keep your network Jitterbug-free and ensure smooth performance for all your time-critical applications. Just like how a skilled Jitterbug dancer knows the importance of timing and rhythm, monitoring and addressing network jitter is crucial for maintaining optimal network performance.

So, whether you're a network administrator or a Jitterbug enthusiast (or both!), don't let jitter slow you down. Keep your network in sync with these tips and [Obkio's Network Monitoring tool](#), and you'll be sure to impress your partners on the dance floor (and in the virtual meeting room)!



OBKIO NETWORK  
**Performance Monitoring**

Network monitoring & troubleshooting made easy.

[Start Your Free Trial](#)

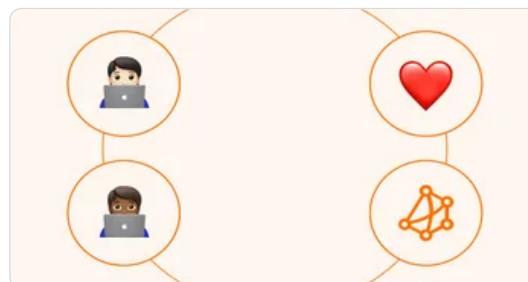
- 14-day free trial of all premium features
- Deploy in just 10 minutes
- Monitor performance in all key network locations
- Measure real-time network metrics
- Identify and troubleshoot live network problems

### Start measuring jitter!

Get started with Obkio's free trial!

Try Now!

### These might interest you



**HOW TO MEASURE NETWORK PERFORMANCE:**

Network Performance Metrics



## Say goodbye to network headaches.

Get a live demo of Obkio now!

[Get A Demo](#)

### Subscribe to our newsletter

A monthly digest of the latest Obkio news, articles, and resources.

Enter your business email\*

### Features

[Monitor All Network Segments](#)  
[Pinpoint Network Issues](#)  
[Measure Network Metrics](#)  
[Proactive Alerting](#)  
[Performance Reporting](#)

### Monitoring Solutions

[Cloud Network Monitoring](#)  
[VoIP Monitoring](#)  
[Remote Network Monitoring](#)  
[UC Monitoring](#)  
[SD-WAN Monitoring](#)  
[MPLS Monitoring](#)  
[Internet Monitoring](#)  
[Firewall Monitoring](#)

### Customers

[Testimonials](#)  
[Case Studies](#)  
[MSPs](#)  
  
**Blog Categories**  
[How To](#)  
[Network Monitoring Basics](#)  
[UC Monitoring](#)  
[Cloud Monitoring](#)  
[Traceroutes](#)  
[Network Troubleshooting](#)  
[SD-WAN Monitoring](#)

### Support

[Documentation Center](#)  
[Getting Started](#)  
[Getting Help](#)  
[White Papers](#)  
[Video Library](#)  
[System Status](#)  
[Community Forum](#)

### Useful Links

[Book a Demo](#)  
[Watch a Demo](#)  
[Screenshots](#)  
[Obkio Vision Demo](#)  
[About Us](#)  
[Contact Us](#)  
[Sign Up](#)  
[Network Audit](#)  
[Affiliate Program](#)  
[Public Monitoring Agents Directory](#)

