The 5 Most Common Network Performance Issues

Devolutions

TO HELP YOU IDENTIFY AND RESOLVE THE PROBLEM WHEN YOUR NETWORK PERFORMANCE IS LAGGING BEHIND.

There are many causes of poor network performance. Some network problems can arise from faulty hardware, such as routers, switches, firewalls, and even from unexpected usage patterns, like network bandwidth spikes, changes in app configuration, or security breaches. Today, we're running you through five of the most common network performance issues to help you identify and resolve the problem when your network performance is lagging behind.

Experiencing a network problem is frustrating, and left unattended, it can be disastrous for your business network. That's why it's important to understand what can go wrong with your network and to continuously monitor network performance to quickly identify and fix network problems as soon as they arise.

Now, let's go through some of the network issues that have left many users pulling their hair out in frustration.

5 Network Performance Problems

1. High CPU Usage

CPU, or "Central Processing Unit", is the primary component of a computer that receives and processes instructions for operating systems and applications. With such a big job on its shoulders, the signs of high CPU usage on a network device are troubling for many of us.

As your network device continues to work harder to perform tasks, there is a greater chance that things can go wrong.

The most common cause of high CPU usage is when your network becomes bogged down by enormous amounts of traffic. CPU usage can increase drastically when processes require more time to execute or when a larger number of network packets are sent and received throughout your network.

There are network devices such as switches that have hardware components (ASICs or NPUs) that take charge and process packets super quickly. For this equipment, the CPU usage is not linked to the amount of traffic.

For equipment that analyzes or manipulates traffic, like firewalls, that's another story. Depending on the enabled features, the CPU may be in the critical path of packet routing or forwarding. If overused, latency, jitter, and packet loss will increase, which will in turn degrade performance.

2. High Bandwidth Usage

Bandwidth refers to a network's capacity to transfer data between devices or the internet within a given span of time. Higher bandwidth allows data to be transferred at a faster rate and allows more devices to connect at once.

When someone or something on your network is monopolizing your bandwidth by downloading gigabytes worth of data, possibly by video, it creates a congestion in your network.

When there's congestion in your network due to high bandwidth usage, it leaves not enough bandwidth for other parts of your network — which is when you can start experiencing problems like slow download speed over the internet.

3. Poor Physical Connectivity

It may seem obvious, but when the time comes to troubleshoot network problems, our instinct is often to think about the most complex cases first, when sometimes the problem is actually very simple.

Testing all your cables one by one in search of that one cable that may be damaged can be a nightmare. We don't always have the equipment to do it and changing the cables one by one is sometimes not an option. Nevertheless, when a cable or connector is defective, the interface of the network equipment to which it is connected will typically generate errors.

This is also the case outside of the LAN. A copper, cable, or fiber-optic cable can be damaged, which will likely reduce the amount of data that can go through it without packet loss.

A simple way to monitor cables on a defective connector is to have a network monitoring solution that will measure errors on all network interfaces and warn you in case of problems.

4. Malfunctioning Devices

Another common network performance problem is when devices or hardware are not functioning properly, perhaps because they have been misconfigured or disabled.

You need to pay attention to all the switches and devices on your network to ensure that they're always working as they should be — and so you can react quickly if they aren't.

Long story short, all devices on your network need to be configured correctly in order for your network to function properly. Whenever you install or reconfigure a device, or upgrade equipment firmware on your network, you need to test that device to ensure that it's been configured correctly. Many performance issues are caused by misconfigurations that can turn into major problems down the line.

5. DNS Problems

DNS, which stands for Domain Name System, is basically a directory for the Internet (and every internet-

connected device) that matches domain names with IP addresses. Every single website has its own IP address on the web, and computers can connect to other computers via the Internet and look up websites using their IP address.

DNS errors essentially happen because you're unable to connect to an IP address, signalling that you may have lost network or internet access. For example, your site can simultaneously appear online for you, but offline to your visitors.

The inability to access the internet or particular sites can have a very immediate and negative impact on your business. Just a few hours offline can cost your company or website in both revenue and reputation.

That's why it's important to find and fix DNS problems as soon as possible.

How to Identify Network Problems

Now that we've run you through the five most common network performance issues, I think it's safe to say that most of you are thinking you'd really like to avoid experiencing these problems yourself.

The easiest and most accurate way to identify network problems is to continuously monitor network performance using an end-to-end solution. End-to-end performance monitoring is the practice of monitoring the performance of your whole network, from LAN to WAN. This gives you full visibility so you can easily identify any of the problems mentioned earlier. Some problems may occur elsewhere than in your own network (ex: in your ISP's network), but such issues can still affect your end users.

There are an array of reasons why you should monitor network performance, all of which are geared towards helping you improve your network performance and avoid issues in the future.

Essentially, continuous network monitoring helps you:

1. **Create a network performance baseline to easily identify poor performance.**
2. **Quickly identify any sign of performance degradation.**
3. **Pinpoint the cause and location of network problems.**
4. **Collect the data you need to find quick fixes.**
5. **Get a 360-view of your network at all times.**

You can also identify these network problems by testing and measuring different operating parameters based on a variety of network performance metrics, such as:

- Latency
- Jitter
- Packet Loss
- Throughput
- Packet Duplication
- Packet Reordering

There are a number of network performance monitoring tools out there that will do all the work for you, so you don't have to do it all manually.

So the next time your network starts bugging or slowing down on you, refer back to these five common network problems to find and fix your issue as soon as it happens!