ACCEDIAN

Guide

10 Things to Look For When Troubleshooting Slow Network Performance

Slow network and application performance are much more than technical bottlenecks: they are productivity and bottom-line killers

If you communicate, collaborate, and do business on the web, you've probably experienced your network come to a grinding halt, freezing, or moving at a snail's pace. While we can all speculate on the reasons why, most networking professionals know that these interruptions are usually due to one of the following reasons:

- **Increases in latency,** which can cause serious bottlenecks in the network. Latency is often defined as the length of time it takes for one data packet to go from one part of the network (e.g. user workstation) to another (e.g., back-end server). High latency, such as required in a SCADA environment, demands slower processing times. Slower processing times, especially in a busy network, can cause significant bottlenecks, slowing down the overall speed of transmission
- **Outages** often impede network performance. These outages could be for a variety of reasons including: router or switch failures; planned or unplanned software upgrades; security breaches (e.g. distributed-denial-of-service attacks); and service maintenance issues. Any of these factors can slow down a network or even bring it to a crashing halt. Recovery time can vary depending on the complexity of the problem
- **Lost connections** are frequently a cause of networks not performing at the desired levels. A simple reason for lost connections may be completely physical, such as faulty cabling or an unplugged network cord. Another primary reason for lost connections could be that network capacity has been reached, causing the connection to be dropped as there is no available queue for a packet. TCP sessions are not terminated properly or sessions may be time out due to TTL being exceeded

The consequences of these issues are sometimes minor, with the user just logging back in again or reconnecting to the network. But when the downtime is more significant, the cost to the enterprise can be incredibly high, from lost revenue and irate customers and users, to diminished productivity or financial penalties tied to contractually mandated availability, and to impact on brand or other potentially catastrophic situations (i.e. in the case of a public utility or medical facility).

Additionally, help desks and IT skills are often pushed to their limits trying to manage the influx of calls, emails, etc. from irate users. Instead of focusing on important tasks, projects, or initiatives, networking administrators and support teams have to analyze a myriad of requests regarding network and application performance, whether it be the occasional interruption of an application process or the habitual slow response times during peak work hours. No matter the cause, the result is ineffective utilization of valuable, and often costly, organizational resources.

With all those possible outcomes impacting an enterprise or organization, it is important to use all the available monitoring tools such as SNMP polling platforms or network protocol analyzers (e.g. Wireshark) as they can provide the microscopic insights necessary to effectively monitor and manage network performance.

Besides those tools, which are essential components of the Skylight™ solution, here are ten things you should look for when managing and monitoring your network. More importantly, they validate why unified network and application monitoring helps minimize and/or eliminate the negative impacts these issues can have on your organization and end users.

1. Hardware failure

While degradations and downtime often occur due to structural issues around processing and response times, traffic load, or unfulfilled handshakes between servers, sometimes the issue is simply a hardware malfunction or fault. It could be a defect in the cable or a bad cable patch. Always make sure to check the cables to ensure that the hardware is properly connected and is functioning correctly.

2. Network switch configuration

One possible problem may be that there is a defective configuration in the network switch. This will cause degradations in network performance. Some of the outcomes of a defective configuration can include packet loss, bad interface negotiation, and physical errors (e.g. damaged or unplugged cables, improper cabling configuration, device bad network interface card, etc.)

Many times network switch issues can be related to speed or duplex mismatches. In this scenario, one device may be connecting at a higher gigabyte speed than the other device. Or it may be that one device is hard-coded and the the other device is set to autonegotiate, causing a duplex mismatch. Switch or port configuration issues are very common so performing a switch port command can help ascertain if the switches have been configured correctly.

3. Network loop problem

A switching loop occurs in a network when there is more than one Layer 2 path between two endpoint devices (i.e. two ports on the same switch connected together or multiple connections between two network switches.)

When there is a switching loop, the destination will generally be unreachable (i.e. until the switching loop disappears) for at least a couple of minutes depending on routing protocol. It can also create broadcast storms that cause broadcast messages to flood the network. The result of switching loops is that users will lose their ability to communicate until the loop is broken.

A well-designed network performance monitoring (NPM) solution, such as Skylight, can pinpoint where these switching loops are occuring and disrupting user experience, so they can be removed.

4. Bandwidth congestion

Bandwidth congestion happens when the quantity of data sent to or from a given destination exceeds the capacity of the network. The business application involved may have capacity requirements that are greater than the capacity of the network. Another reason may be that there is network usage, such as web browsing, that is not within the scope of the network requirements. Additionally, defective configurations such as back-ups and updates being run outside of the normal time windows can also cause bandwidth congestion. No matter the reason, the network will slow down considerably as the increase in data severely impacts network performance.

5. Increase in network latency

It is important to understand network latency as it impacts the delivery of applications throughout the network. Network latency is the time required to send a packet over a network. These are the components:

- **Propagation,** which is a constant based on the time data moves from one network device interface over a physical cable. The only way to shorten this time is to reduce the actual physical connections on the route
- **Processing and serialization,** which is fairly constant and often negligible
- **Queueing,** which is the time a data packet spends in the router queue. As a packet spends more time in the queue, the queue becomes larger, which negatively impacts performance

When latency increases, whether it is due to a change in the data's path or a defective network device, data takes longer to move through the network. This creates performance issues, especially with applications that require speedy response times.

6. Quality of service settings

Because there is a constant demand for voice and video streaming in both the consumer and enterprise space, quality of service (QoS) across all networks, especially IP networks, is a given in the digital age. Many applications, such as video gaming, are negatively impacted by any network delay or slowdown. A momentary or constant bottleneck can reduce network capacity for any given application. For example, a filtering device can decrease network optimization by resetting or blocking network connections.

If a network is designed to handle bursts or has adequate bandwidth levels, then QoS won't be impacted by packet loss, delays, or even jitters. But if the network experiences bottlenecks or significant congestion, and packets are dropped, then QoS is affected.

That's why it's important for network administrators to establish processes and procedures that prioritize applications. For example, class of service (CoS) allows you to mark traffic in a way that assigns those data packets priority over data. This priority system can reduce network downtime and minimize packet loss, especially for critical applications.

Some additional causes of network slowness may not be related to the network itself.

7. Host resource outages

While this may not be a network-related issue, a resource problem may negatively impact data transfer speeds on either (or both) servers. One example of this is a client or server that runs out of system resources and sends out "0-Windows" to slow down the transfer.

8. Application server processing times

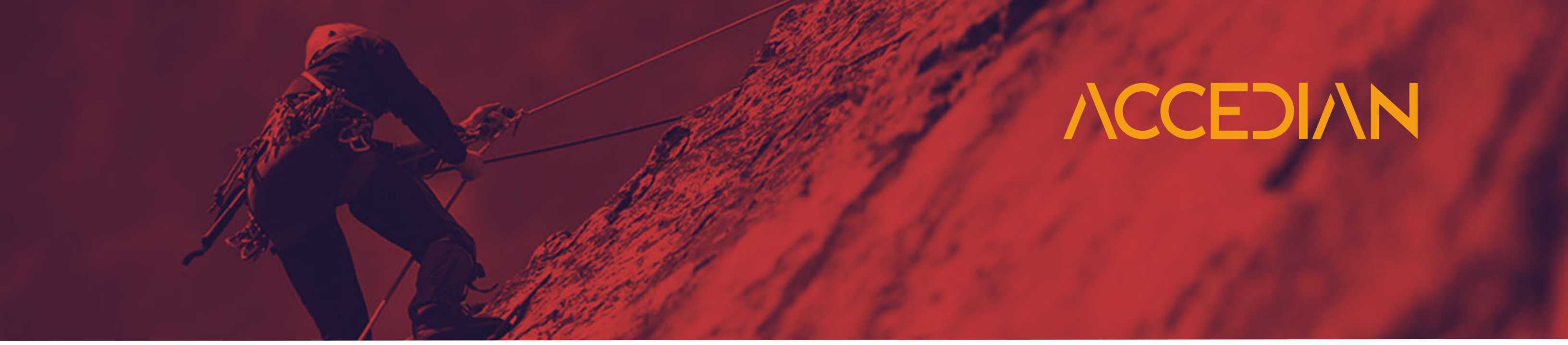
Again, this may not be network-specific; nevertheless, it causes slowdowns as the application server takes too long to respond to specific requests or all requests. This causes some of the requests to generate application errors.

9. Quantity of data

When the quantity of data sent and received by an application is too large and takes too much time to move through the network, this slows down the network considerably. One of the reasons for this may be a configuration or application defect. To reduce mean time to resolution (MTTR), there are a number of steps that can be taken, such as defining and implementing a traffic capture method or checking the network layer, to resolve this issue.

10. Common services

Final reason the network performance may not be optimal may have to do with specific services and servers responding too slowly or encountering errors. For example, a DNS server may have requested an incorrect server name before querying the right server. Or the authentication server may be responding too slowly.



Conclusion

In today's digital world, organizations and businesses around the world are highly dependent on constant communication, commerce, and collaboration between users, with consumers, and with the general public. As witnessed with data breaches and much-publicized websites being down for extended periods of time, a single of second of downtime can costs millions of dollars in lost revenue, brand reputation, and productivity. It can also, in the case of a public emergency or natural disaster, lead to more dire consequences.

By proactively monitoring and managing network and application performance in real time, organizations can more efficiently and effectively identify, troubleshoot, mitigate, and resolve issues. The ten reasons listed above (i.e. specific to why a network is slow or not performing at optimal levels) are meant as a guidepost by which proper procedures and processes are documented and implemented.

Skylight has the real-time analytics engine to capture network performance, application performance, and end-user experience on the fly, from a wide-angle perspective. It reports on everything it sees happening on the network: all devices and applications, for all users, across all transactions. This visibility and functionality is essential when performance degradations or slowdowns hinder users ability to access mission-critical applications. By seeing what is happening at all times, Skylight quickly identifies the root causes impacting performance, resulting in expedited resolution. Happy users, happy network administrators.

About Accedian

Accedian is the leader in performance analytics and end user experience solutions, dedicated to providing our customers with the ability to assure their digital infrastructure, while helping them to unlock the full productivity of their users.

Learn more at accedian.com

Accedian | 2351 Blvd. Alfred Nobel, N-410 | Saint-Laurent, QC H4S 2A9 | 1 866-685-8181 | **accedian.com**