



How to Detect, Diagnose, and Fix Issues with Network Bandwidth

E-book by

Adam Leeflang

General Manager - Products

How to Detect, Diagnose, and Fix Issues with Network Bandwidth

Network bandwidth has always been a precious commodity and given our current circumstances with so many people working from home, many companies have not had the bandwidth they need in the right places. This E-book will help you with some strategies on how to detect bandwidth issues, further diagnose those issues, and what actions you can take to relieve those bandwidth issues.

Table of Contents

Detecting Network Bandwidth Issues Through Congestion Management	3
Diagnosing Network Bandwidth Issues	4
Actions to Fix Network Bandwidth Problems	5
About the Author	6

Detecting Network Bandwidth Issues Through Congestion Management

Most issues related to network bandwidth will present as congestion, that is there is not enough bandwidth to satisfy the demands of the users and applications. Users will report that “some application” doesn’t work like it did yesterday. After you have confirmed the application is up, and the user reports are correct, where do you look next?

01

Monitor the helpdesk cases raised, in particular where users are reporting problems with applications across the network. Knowing whether this is from a branch, remote site or from home (will shorten troubleshooting), it is likely to indicate network congestion.

02

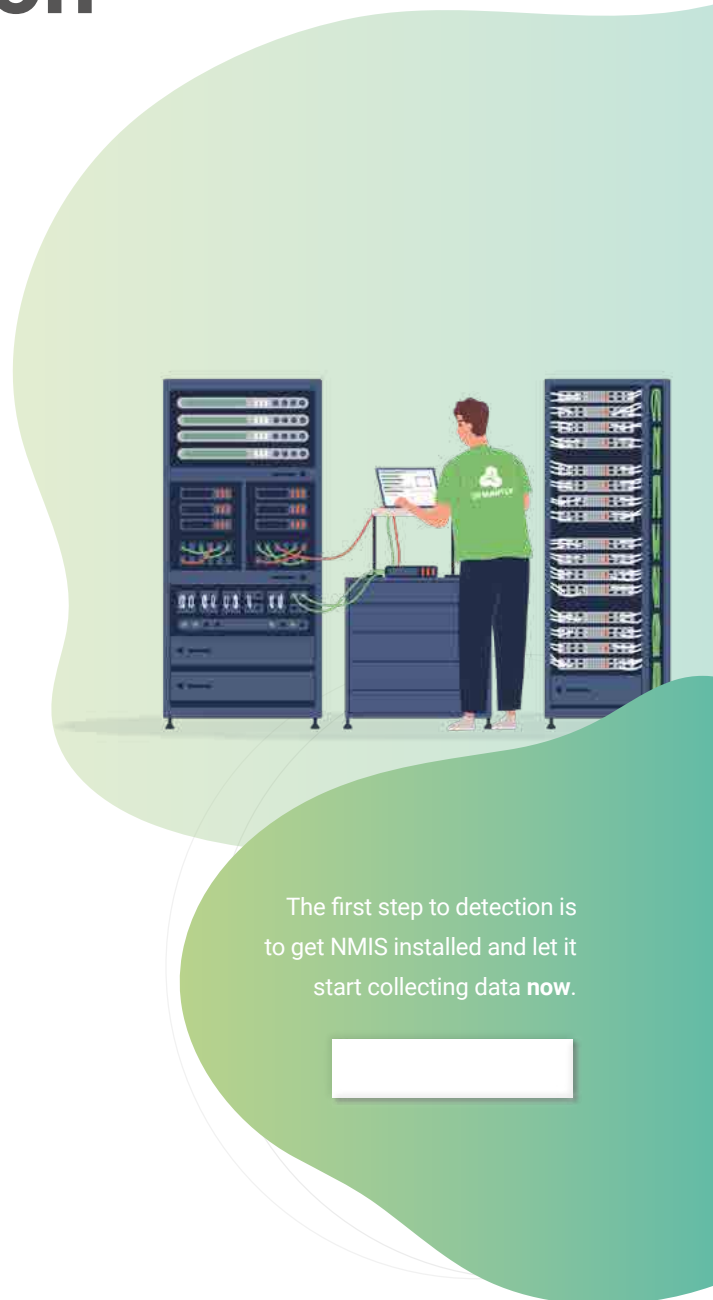
Monitor utilisation of network links and raise alerts when bandwidth becomes heavily utilised.

03

Make sure you monitor packet discards and errors.

04

Finally, monitor Quality of Service (QoS) parameters available in the network device; in particular, you are looking for where QoS caused packet loss.



Diagnosing Network Bandwidth Issues



What issues are being reported by users about the network, is the application slow or is it unusable? For example, is there a problem with voice over IP or video conferencing? Does it occur during file transfers? The more qualified information you get from your helpdesk, the faster you can get to work.

By monitoring the network for issues related to congestion, you are ready to start further diagnosis to determine what is causing those issues and look for possible solutions to avoid the congestion firstly or control it secondly.

Depending on the tools available to you, you should have an idea of those causes. For example, putting aside transmission, format errors, or device health issues packet discards will generally be caused by QoS classes dropping packets, so the solution is to refine the QoS configuration to prevent the desired traffic from being discarded.

Depending on the application, the dropped packets will be causing retransmissions if they are using TCP, while voice and video symptoms are voice clipping or slow refreshing video or video and voice not keeping sync.

Depending on the devices and operating systems being used, you should be able to see key performance indicators for this, which will be collected by your monitoring system, like NMIS. For example you could monitor for TCP retransmissions on servers, this would indicate issues with those applications.

Using systems like Cisco IPSLA are a great way to monitor for changes in latency or variability in latency (Jitter). NMIS can collect your IPSLA data, providing graphs as well as alerts when it detects issues.

Monitoring these metrics will guide where you need to look deeper, you might need to collect more detailed information from the devices to determine what the issues are, e.g. looking at command outputs for QoS or interface information to decide what changes are available to resolve the helpdesk reports.

If you identify the QoS Classes which are exceeding their configuration limits with resulting packet loss, you will need to consider changing the bandwidth allocations for those classes, increasing the available bandwidth for voice and video, for example.

Use **NMIS** and **opConfig** to collect data, which can then be analysed.

Here's how to use **opFlow** to look at the application mix on a link.

Actions to Fix Network Bandwidth Problems

Ultimately to fix a bandwidth issue, you should upgrade the overall capacity at the site. If you are not able to upgrade or need to buy time, then implementing QoS features to manage which traffic is less important to the business and have it shaped or dropped during times of congestion.

Contrary to popular belief, QoS does not create more throughput. It does create better “goodput,” with critical applications protected, and applications that are hogging bandwidth, controlled.

Two standard policy options for QoS are shape or police. Policing will ensure bandwidth is never exceeded and drop the offending traffic. Shaping will delay traffic to smooth out the traffic over time. Note that as shaping limits are exceeded, it may result in dropped traffic.



About the Author



Adam LeeFlang

General Manager - Products

Adam has over 25 years of experience in the IT and Telecommunications industries. Through his management of high-performance teams, he achieved success in multiple product evolutions and operational delivery excellence, most recently at IPSTAR Australia. He says this success came through driving clear and concise communication through the operation down to the customer delivery for every transaction and, “every customer interaction, with the business or product, should be simple and intuitive.”

Thank You

Start solving your network problems

Talk to us about how our solutions can give you the insight you need to make data-based decisions. You'll reduce helpdesk stress and own your infrastructure, all while improving the user experience.

