2026 Guide to network performance monitoring.

Statseeker.

How and why network monitoring plays a crucial role in maintaining uptime and enhancing service capability

Remote working, BYOD (bring your own device), cloud and distributed computing have transformed the network monitoring landscape.

Not being in control of every device connecting to your network makes managing it even more challenging - network managers can now be responsible for networks spanning hundreds of physical locations and thousands of unique users and devices.

Effective network monitoring has now become more important than ever: you need **complete visibility** of exactly what's happening how and where, in order to maximise uptime, improve performance, manage costs and plan for evolving capacity requirements.

This guide covers some of the fundamentals of network monitoring, and features four recommended activities for network managers:

- **Creating a network baseline**
- **Determining KPIs for your network**
- **Adopting best practice principles**
- **Future-proof your network**

Network monitoring – the basics

For your network to be functioning smoothly, each device needs to be fully functioning and available; its interfaces (or ports) need to be functioning correctly; you need to have enough bandwidth available for all your data traffic (especially at peak times); and you need sufficient storage space and support from system-level services to avoid any issues occurring within critical applications.

For example, interfaces (or ports) are the entry and exit points for 'packets' of data. If an interface fails, is overloaded or discards packets, you're likely to see a poor network experience for the user. And if hardware devices (such as switches and routers) fail or experience errors, then network availability will be at risk.

Network monitoring uses two information gathering technologies, ping and SNMP.

Ping is a utility that tests availability by sending a message using internet control message protocol (ICMP). From the reply received, it can report on response times, errors, packet loss and standard deviation. (And yes, it really is named after sonar technology.)

SNMP stands for simple network management protocol, which is used to record and organize device information, such as availability, status, CPU temperature, fan speed and power supply.

One of the significant benefits of an effective network monitoring solution is not just its 'find and fix' function that helps you stay on top of what's happening in the here and now – it's the ability to pick up any **early warning signs and anomalies** that enable you to anticipate and identify problems before they happen. And with detailed analytics, you can use your network history to identify trends and forecast future requirements.

Why you need a network baseline – and how to create one

How well can you spot irregularities in your network?

If you're responsible for your organisation's network monitoring and management, you'll always be on the lookout for unusual or suspicious activity. This means comparing what you expect to see against what's actually happening.

You need an accurate baseline to work from.

You need to know what 'normal' looks like for your network if you're to successfully identify problems and anomalies, and effectively monitoring your network requires a clear picture of how it functions under everyday working conditions.

This means you need to create a benchmark – or baseline – against which you can measure performance.

Your baseline provides a clear picture of everything on the network, including both hardware and software. It maps your network as it exists and provides you with the configuration of every single network node.

Creating a network baseline

First, make sure that you can see your whole network, so that your network monitoring solution can provide you with a complete inventory of physical and virtual devices and nodes (including virtual switches and virtualized application accelerators). This should be an automated process the last thing you'll want to do is manually collate your inventory.

Once you have your inventory, you can then analyze traffic to obtain an overall measure of the health of your network, and a deeper understanding of how it is being used. Tools such Netflow and sFlow will provide much of the information that packet sniffers are able to, but without the overhead that they require. You'll want data granularity to be as fine as possible, so that you can accurately determine application usage.

Finally, you should allow this data capture to take place over an entire network cycle (for example, a week for a B2B network, or a season for a retail network). This is so that you can capture the normal variations within your business over a period of time. If you have regular seasonal peaks and troughs that make a significant difference to the volume and type of traffic, it's a good idea to run baseline reports then, too, as part of the process of capturing what 'business as usual' looks like for your network.

Set your metrics

You can use this baseline to determine network performance metrics moving forward. Since there are no universal standards for the kind of performance you should expect, you need to review the specifications of all the devices in your network to determine what best performance for that specific device is. This will allow you to develop your own appropriate set of metrics to work to.

Keep your baseline up to date

It is essential that you keep this baseline upto-date to take into account organizational or network changes. This requires regular network audits to look for alterations, additions and dramatic fluctuations in usage. We'd recommend these audits were conducted monthly, however for stable or under-utilized networks quarterly may be appropriate.

Your baseline provides a clear picture of everything on the network, including both hardware and software.

Determining KPIs for your network

Which KPIs do you use to measure network performance?

Managing, updating and scaling your network is pretty much impossible unless you can visualize what it's doing – and this is especially true with software defined networks (SDNs).

Key performance indicators (KPIs) aren't just for evidencing performance levels to others; they're an invaluable tool for you, enabling measurement and assessment of the network's quality and capability. Below are the most common KPI categories.

Device health

The most common KPIs are CPU and memory allocation, memory utilization, temperature and fan status. You should be able to obtain these values (or similar) from every physical device on your network.

Device availability

You need to be able to view device availability on your network, in as near to real-time as possible. If you only become aware that a router or a managed switch isn't working when someone calls you to complain, that's too late.

Latency and packet loss

Measuring device latency and packet loss gives you an early warning of any problems and can tell you a lot about the health of a device. If latency is increasing, you'll know that you have a problem. If you can see packet loss, then something unacceptable is going on. Time to investigate.

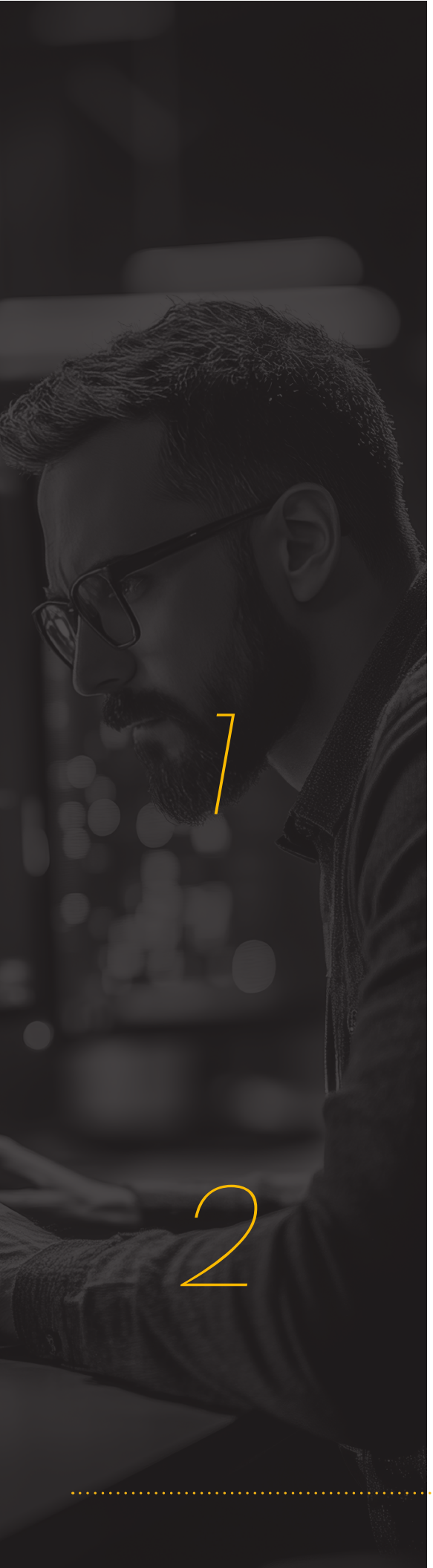
Network interface

Using SNMP polling you can see common KPIs, such as volume of network traffic. You can also see errors and discards per interface, inbound and outbound. You can poll an interface for availability and – like a device – if it doesn't answer its ping, you can assume that it is down or broken.

You can also use link bandwidth data to assess the capacity of the network and predict the need for capacity upgrades.

Link statistics

Link statistics tell you what is occurring on the link itself – particularly important when you use the cloud for some portions of your network or lease a network segment from a vendor. Running tests will tell you if the link is working; and using link latency and packet loss jitter as KPIs will give you a real-time view into that segment of your network.



Seven best practice principles for network monitoring management

Whether you're dealing with the day-to-day, implementing change or planning for future network development, use this checklist to make sure that you're following all the fundamental principles that play a positive part in optimizing network performance.

1 Know your network and what's needed for the near future

You can't begin to improve your network until you've established the status quo and determined what you're going to need from your network in the future. You've probably already audited your network, so how does this compare with what your company actually needs?

- Is your company growing?
- Are you getting ready for – or already using – cloud or wireless integration?
- How are you handling big data?
- What mobility solutions are already in place or being planned?

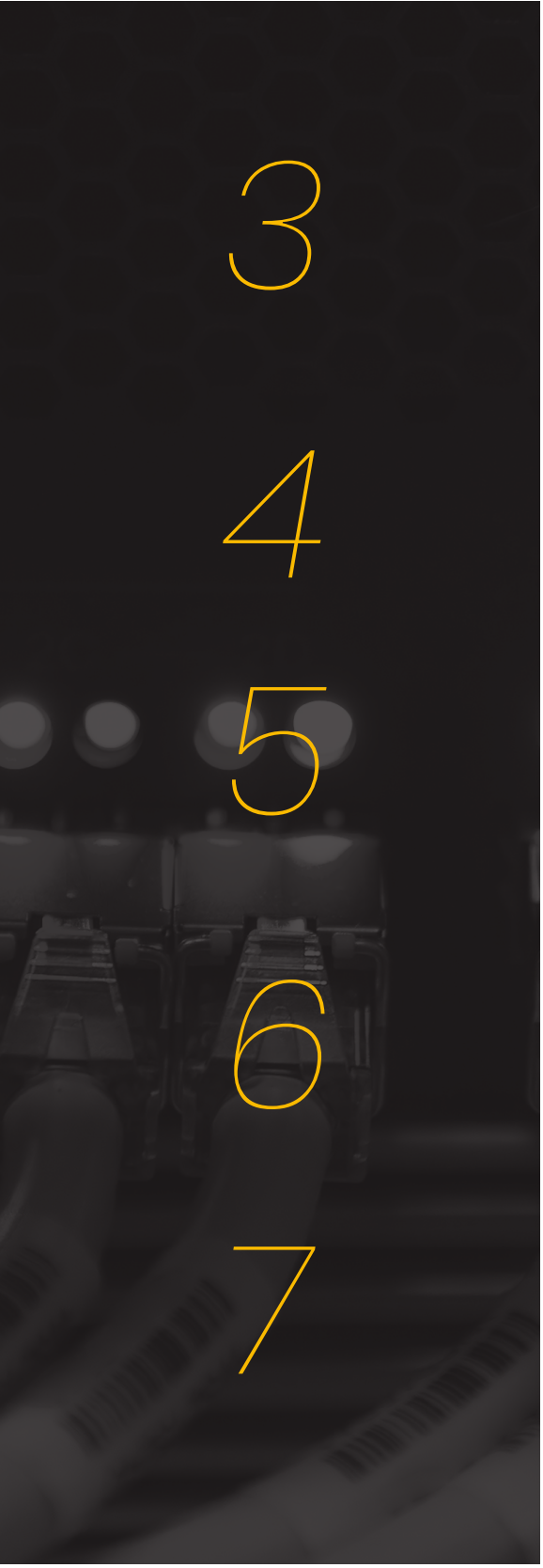
By leveraging the network data you have access to, you can predict areas of expansion, remove blockages and slowdowns, and prevent duplication of design effort. How will your network support current and future business strategy? Remove anything that has become redundant following the evolution of organizational needs.

2 Establish standards, policies and procedures

As in any discipline, it's good business practice to define a 'business as usual' operating framework. This will also prove invaluable if or when you need to design a new network.

Your standards should record technical specifications for equipment, wire, cable, connectors, and all the other hardware, firmware and software that have, or that you will be acquiring.

Create a formal record of policies and procedures for network operators and users. This should be revisited, audited and revised on a regular basis, and can make your life a whole lot easier in the future.



Design for future growth and flexibility

You need to clean up your existing network before looking at SDNs, virtualization and other application-based technologies. Identify 'configuration sprawl' and standardize your network architecture, removing any abandoned virtual local area networks (VLANs) and mismatched network segments. Then, as and when you're required to suddenly expand your network, you will be ready to respond swiftly.

Think outside the network

Don't limit your view to your own network – consider its impact on other networks connected to it. You need to be able to see and analyze traffic to and from your host, so you can identify any developing issues long before they become a problem.

Apply the 80/20 rule

Our advice is to target the 20% of the problems that lead to 80% of the disruption first. Leverage the network management solutions that resolve your most common, most disruptive and most expensive problems the quickest. Find and fix the bad actors first, and then deal with the small stuff later.

Use a network monitoring solution that properly serves your needs

You can't manage what you can't see. Use a network monitoring package that not only gives you complete visibility of your network, but also provides you with anomaly detection, accurate future predictions and intelligent realtime information – not just a pile of data – that empowers you to swiftly and accurately make meaningful business decisions.

Security comes first

You want to be confident that you've implemented the best security practices available, so make sure you consult with the relevant experts to make sure you get it right. It isn't enough to implement firewalls if they are not configured correctly, and it isn't enough to only make sure that your antivirus software and patches are up to date and clear.

You need to be able to see and analyze traffic to and from your host, so you can identify any developing issues long before they become a problem.

Finally, future-proof your network

Networks have never been more critical to an organization's success, yet pressure on performance continues to increase, thanks to factors such as the growing usage of rich media, proliferation of the IoT, the rapid adoption of cloud-based applications and the advent of 5G.

Here are three things you've probably already got well in hand, but as all network managers know, it never hurts to check. And re-check.

- Ensure you have a complete asset inventory. What equipment constitutes the network? What devices are connecting to it? What is its current capacity and future scalability?
- Consider software defined (virtual) networking, if you haven't already.
- Implement an effective and scalable network monitoring solution that provides you with total network visualization in real time, and provides you with anomaly detection, forecasting and analytics based on detailed and accurate data.

Statseeker.

Statseeker was developed by network engineers who understood the importance of proactive monitoring. Statseeker now has active deployments in over 22 countries, and many Fortune 100 firms consider Statseeker to be an integral part of their day-to-day operations.

Start a free 30-day trial now:

statseeker.com/free-trial