Network Monitoring Technology

Statseeker
every port. every minute. everywhere.

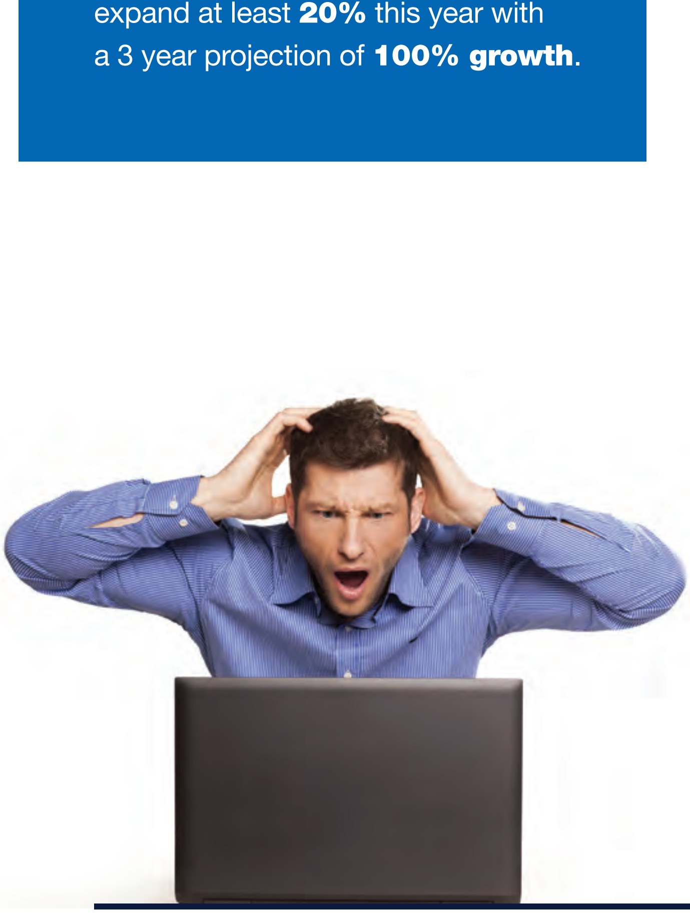
Three Key Challenges

facing today's professional Network Managers | *By Frank Williams*

Is this you?

You manage a small-to-midsize network of about 5,000 physical devices connected across multiple locations. Lately, you experience even greater demand for both physical and virtual connections to the network, and increased performance expectations by Users.

Your total network is expected to expand at least **20%** this year with a 3 year projection of **100% growth**.



It's early Monday morning and you are finishing up breakfast at your home. Suddenly, your smart phone begins to ring constantly. A steady stream of messages arrives from various Users at work claiming the network is slow, or not functioning properly. The next thing you know your manager is on the phone asking you what's going on and how fast will you be able to return service to normal – in other words ***FIX IT!***

After 3 hours of analysis, 5 hours from your first alert; and 10 more urgent calls from your manager, you determine that a User on the network created a broadcast storm by connecting through a poorly configured switch.

Bang! Once again you find yourself in a purely reactive mode.

Perhaps daunting, but the above scenario is becoming the norm. What to do?

Unplanned disruption to the network, even short outages, become problematic and may have a potential financial or security impact on your business.

Let's face it. Today's fast paced, ever-changing and connected business environment is pressing the ability for you and your IT team to pro-actively manage network uptime and balance User availability, cyber security risk and ever-escalating scaling and maintenance costs (CAPEX & OPEX).

Technologies such as the Internet of Things (IoT), BYOD & BYOA (bring your own device, bring your own application) and The Cloud appear in the market with lightning speed and disrupt current network practices; as a network manager you desperately try to keep pace.

Networks are an integral part of any well run business these days. As business owners translate the benefits of a well-connected business into cost, productivity and efficiency gains for the business, the more important network performance and availability become.

In this paper we'll examine the challenges associated with running and maintaining today's expanding network. We'll break the challenges into three main areas – Uptime, network costs (CAPEX & OPEX as you scale), and cyber security.

Uptime - pro-actively keeping your network healthy

Unplanned disruption to the network, even short outages, become problematic and may hold financial or safety related impact. Maintaining the availability of the network infrastructure is becoming a key focal business strategy.

The interpretation of uptime is a relative term in the networking world. It all depends on the operational risk. Uptime of 90% can be classed as acceptable in certain defined use cases, such as email or web browsing access. Other industries hold the need for 99% (or even 99.9999%) uptime, such as Telco, service providers, oil & gas or financial institutions where network disruption can cause significant revenue or safety impact.

Network downtime is a real issue and can result in financial costs to the business organization:

- Revenue or Safety/Insurance
- Damaged reputation/Customer loyalty
- Regulatory/Contract compliance – e.g. SLA penalties
- Remedial – e.g. what is cost to repair damage

You may find it interesting that in a recent Gartner survey the single highest cause for network downtime was human error – almost 32%. Downtime cost the average organization a minimum of roughly $140K/hour. And the average resolution time per outage is around 200 minutes. Consider these numbers and apply them to your business to see the hidden impact (read: cost) of network downtime.

What can be done? Monitor your network of course, but be selective, not all monitoring software is designed the same with the ability to deliver the needed visibility from-end-to-end in a timely manner – typically you should look for polling performance of under 60 seconds for > 35,000 devices or up to 600,000 ports. Remember, your network is expanding. The more devices, the longer it will take to find potential problems, so efficient (fast!) polling time will be even more critical going forward.

Networks are becoming more complex. Retaining your data in its original granular form, not averaged, will be even more important in making improved decisions to head off potential downtime issues as well as provide the increased ability to fine tune the network to a consistent peak performance.

You should evaluate technology such as Statseeker's Network Infrastructure Monitor that delivers strong performance value. You should expect to get value from the software within the first hour of deployment. The software should be able to highlight visibly: slow devices, ports/interfaces that are showing errors or discards, highlight and alert on congested parts of the network and identify key utilization metrics. It should be checking for SLA performance and looking for congestion. It should also provide information on the health of each device. And it should be scalable with minimal additional CAPEX expenditure.

Costs - Scalability and managing CAPEX & OPEX expense

IT professionals and their counterpart on the OT (operational technology) side of things face the continual challenge of providing a high network service level (QoS) at a reasonable cost. Cost savings will be key in the exploding world of the network of things (NoT).

However, it is not unusual for IT management to deal with flat, and in some cases reduced budgets, while at the same time have demand for increased service levels.

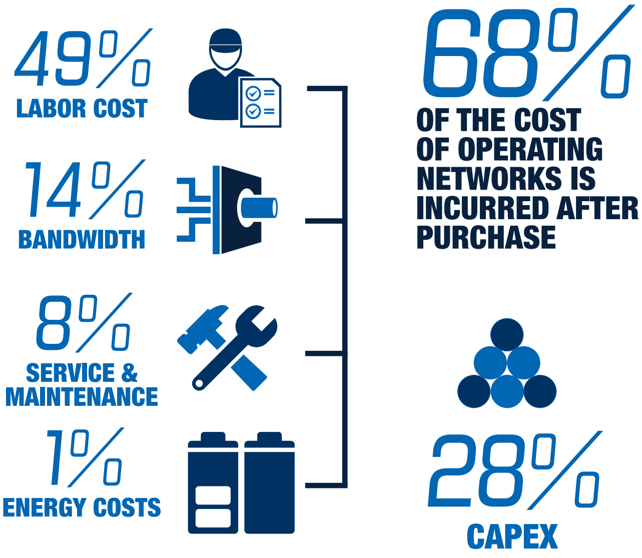
Let's face it, CAPEX and OPEX expenditures get closer scrutiny by financial managers and Company owners. While demand for increased User levels continue, doing so in a more cost-effective manner is necessary.

Typical IT budgets range in size from 2-5% as a percentage of total revenue. For the purpose of this paper, I don't intend to debate whether this type of KPI used to value IT, is best, it's used as a general reference understood by the market at large. However, I will mention that research is underway to better understand the value creation added to the business by IT, rather than treating IT as a necessary expense.

Determining what this ratio (IT spend to revenue) should be for your company requires knowledge of your industry, the nature of your company's IT division and an understanding of the ratio itself. Gartner, an IT research and consulting organization, suggests the average ratio for companies was 3.5% but for technology intensive industries such as financial services and software services, the ratio can range as high as 6%. Gartner has also found variations in this ratio depending on geography. In EMEA (Europe, Middle East and Africa), IT spending as a percentage of revenue is 4.4%. In North America, the figure drops to 3.5% and in Asia, the ratio is the lowest in the world at 2.9%.

More and more thought leaders in industry are now considering CAPEX ROI approach for IT expenditures as a one dimensional view of network costs.

What network and financial management should be reviewing is total cost of ownership (TCO). It may surprise you to know that 68% of the cost of operating networks is incurred after purchase.



What is total cost of ownership? Aside from bandwidth and service/energy related costs, the largest component is labor. Roughly 49% attributed to this category. It's a simple matter of head count. Expenses follow people, the less people you need, the lower the labor expense.

If you can deploy network monitoring software that allows a clear real-time view of your data – end-to-end; coupled with less hardware that delivers more scalability, then your total cost of ownership (TCO) will be reduced over time and much more predictable.

Cyber Security - Security is a journey not an event: remain vigilant

Open up any newspaper, or listen to your nightly news and there will be a segment or article on cyber security breaches within major organizations. The unintended consequence, driven by the demand to connect everything, is the persistent cyber security threat. The devaluation of a corporate brand, the loss of valuable IP or the revenue or safety impact of a cyber security attack can be devastating to any organization and in many cases unrecoverable.

The challenge for IT managers in cyber security is increasing and ever-changing. So called "actors and hactivist" attack at will, and connecting (networking) everything makes their exploit easier.

Over the past 5 years the hackers' model has changed from the once –*"I'll show them how smart and destructive I can be"*, to almost exclusively stealth mode, where stealing an organization's IP and selling it in the open market is the hackers' financial reward.

Consider this scenario – you're a large pharmaceutical organization that just spent 5 years and $500M on a new arthritis medicine. An unprotected network in the organization's manufacturing plant could expose the recipe to hackers lying dormant in the network waking up for only 30 seconds to send the captured IP to its controller. The recipe is then sold in the market and the value of the medicine is lost to the pharmaceutical company.

Implementing strong security policies, - e.g. password and access procedures, strategically placed firewalls (software and hardware), coupled with smart network architecture using a "Defense in Depth" strategy will help. Most of today's anti-virus software is a good place to start but IT teams must remain ever-vigilant.

As caretakers of the organization's network, you need to remain cyber ready. Choosing the correct network monitoring software coupled with change management alerts and threat intelligence software give you an edge to stay ahead of the hackers' game.

1 Gartner Blog – July 2014 – How much does down time cost?
2 CISCO Total Cost of Ownership - Slideshare
3 Gartner – "The Internet of Things, Worldwide Forecast, 2013"

Summary

One thing is for certain - Networks will continue to expand. Big data, the Internet of Things (IoT), etc all play into the accelerated growth of the networking of all things. In fact, there are a variety of market reports available on the growth of networks, but according to Gartner The Internet of Things (IoT), a main market driver for connecting things, will grow to 26 billion units installed in 2020 representing an almost 30-fold increase from 0.9 billion in 2009.

There is an old adage that should ring true for alert network managers - you can't manage what you can't see. Network engineers and managers that choose network monitoring tools wisely and find ways to provide consistent peak network performance that align with their organization's business goals; and do so, while containing CAPEX and OPEX expenditures will be highly rewarded.