

Automating Port Intelligence

It is essential that IT managers know what each port in their network is being used for. Yet even understanding that individual ports are being used at all is beyond most IT departments, who have to conduct time-consuming, inefficient and risky manual processes in order to make decisions that affect the entire organisation.

Instead, when called upon to isolate security breaches, investigate outages or to scope the network prior to expansions and upgrades, organisations have the opportunity to automate port intelligence. This makes tasks far more cost-efficient, streamlined, responsive and less time consuming.

AUTOMATED IT RATING: 4.7

This advisory describes the process and impact of automating port intelligence.

- **Situation Analysis (Before & After Automation)**
- **The Business Criticality of Automating Port Intelligence**
- **Automation Impacts**
 - **Running Costs**
 - **Time/Labour**
 - **Space & Power**
 - **Decision Making**
 - **Uptime**
- **Implementing Automation**
- **Infoblox Solutions**

Situation Analysis

Before Automation

- IT professionals are unaware of the amount of available ports on the network, or their status/speed etc., so mistakenly purchase new switching equipment when extra capacity is not in fact required.
- Without visibility of ports and their status, opportunities are routinely missed to determine the performance of the network as a whole. Moreover, the potential impact of planned switch maintenance/upgrade is unknown. This makes measuring the success of such processes difficult, leading to inaccurate analysis that impacts on future spending decisions.
- Troubleshooting outages and other failures is ineffective and inefficient. The process of identifying the port in question likely involves manually researching logs that enable the conversion of IP address into MAC address, then into switch location, and finally switch port number. In many cases it will involve physically visiting the switch in question and sifting through cabling infrastructure.
- Shutting down urgent security issues takes too long, is time and labour intensive, and can provoke counterproductive errors. Attacks exploiting a specific port cannot be acted upon quickly enough, and occasionally the need to 'pull the plug' on a suspected port is done hastily and incorrectly.
- As the manual port intelligence processes in place are 'learned', only the most skilled and experienced IT professionals within the team are capable of supporting them.

After Automation

- Port wastage is eliminated, and the IT team is fully aware of how many ports are available, how many are in use, and what their individual status is. It is far easier to make informed capacity planning choices, reduce common configuration errors and predict the impact of IT infrastructure expansion and maintenance.
- With new ports costing between £100-300 each, the organisation is saving significant amounts of CAPEX and space/power by no longer procuring infrastructure it does not require, and instead making more efficient use of installed assets.
- The IT team can rapidly identify which ports need to be shut down in the event of a brute force attack, virus, security breach or DoS attacks, and take action with a simple keystroke.
- The organisation can seamlessly integrate its IP address management (IPAM) process with port intelligence to make overall network management as efficient as possible.

The Business Criticality of Port Intelligence

Access to real-time, granular information about the most fundamental elements of your network infrastructure means strategic and tactical decision making can be undertaken accurately and with confidence. Without automation, organisations run the risk of prolonged security attacks, serious configuration/connection errors and immense wastage of time, money, space and power.

Automation Impacts

Running Costs

HIGH 😊

According to Gartner, 30% of ports in a typical network are unused at any given time. When it comes to extending the size of the network, IT decision makers, unaware of the unused capacity, buy unnecessary new switches. Through automating port intelligence, the cost of operating the core network can be reduced by being able to correctly identify unused capacity, informing investment decisions accordingly.

Automation also lowers OPEX as well as CAPEX, by reducing the time and associated expense of maintaining inefficient manual processes for intelligence gathering and execution. Look out for tools which are vendor agnostic, enabling management of all network ports in a multi-vendor environment.

Time/Labour

HIGH 😊

The process of managing ports and securing them effectively is very time consuming if done manually. Consider the workload of an IT Manager having to go through this process, which will be not only multifaceted, but multi-platform and multi-departmental. Tasks are often fragmented and need information extrapolated from a number of different sources. In a network environment of potentially thousands of ports, it can often take days or weeks to carry out a simple assessment, yet with automation in place it takes just a fraction of that time.

Added to this, automated port intelligence reduces the frequency of helpdesk enquiries, with each enquiry also being solved more quickly and underlying issues identified more swiftly. Prior to automation, issues would have

involved a cross department response. Indeed, many organisations will either lack the in-house skills to carry this out, or will have to second a highly skilled member of the team to manually carry out these processes. Port intelligence automation lowers skills barriers, meaning it can be carried out by a number of people without the expertise needed to do it manually.

Space/Power

HIGH 😊

By more efficient utilisation of available ports, organisations only need invest in new switches they actually require. This avoids significant wastage of space and power on superfluous equipment. Moreover, by leveraging hitherto unused port capacity on existing switch infrastructure, the organisation can achieve a better utilisation per user/device/application while maintain the same density footprint.

Decision Making

MED 😐

Automated port intelligence provides IT decision makers with a platform for better visibility and faster troubleshooting. Automated port intelligence is a highly constructive 'housekeeping' initiative that supports system performance, enables more strategic decision making (particularly with regard to capital investments and switch upgrade/maintenance projects) and reduces the disruption and distraction of valuable IT personnel.

Port intelligence tools with 'historic' tracking and analysis capability can even track the connection activity of specific users, and determine the 'net usage' of specific ports over time rather than simply reporting a current snapshot.

Uptime

MED 😐

Automated port intelligence really comes into its own in a crisis; a faster and more granular security response will deliver better uptime. Added to this, threats are less likely to spread and inaccurate responses - such as pulling out the wrong port - are minimised.

An example of this is when a firewall sends an alert that the device at a given IP address is sending worm packets. Prior to automation, an IT manager would have to consult a myriad of manually stored logs, or else go and query all of the switches and routers in the network to find where the device is attached. With 3-6 commands per switch, this can take hours before an informed decision can even be taken. With automation in place IT Managers can immediately see the port that the device is on and take action. Added to this, an automated audit history can help identify the "mobile" offender. Note however, that only some automated solutions carry this 'historic port intelligence' capability.

Implementing Automation

Embracing automated port intelligence involves a rapid and pain-free implementation process, whereby the deployed system auto-discovers all the ports on the network and builds an immediate picture of the switch estate.

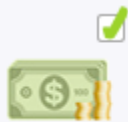
To maximise the investment in an automated port intelligence solution, it is advisable to invest some time determining which auditing and alerting commands are to be utilised and in a configuration that suits the IT team. In addition, organisations can further maximise the benefits of automated port intelligence by integrating this with an automated IP address management (IPAM) solution.

Infoblox Solutions

This advisory has been produced with support from Infoblox, pioneers of an appliance-based approach that controls and automates the core services that drive all networks and applications. For more information on how Infoblox successfully automates port intelligence for businesses of all sizes, visit www.infoblox.com.

[Click here](#) to read the Infoblox PortIQ solution note

[Click here](#) to watch the Infoblox PortIQ demo



SLASH COSTS

- Lower hardware TCO
- Better use of existing hardware
- Slash opex by over 50%
- Less hardware needed



SAVE MAN-HOURS

- Free up skills for innovation
- Typical 1,000 user organization can save 40 man-days per month



CUT SPACE/POWER

- Maximise virtualisation opportunities
- Use less infrastructure to manage network infrastructure



BETTER DECISION-MAKING

- Dramatically increase efficiency of IP address management
- Dedicate less resources to fire-fighting
- Platform for better business decision making



BOOST UPTIME

- Underwrite critical network services
- Mitigate unnecessary human error/intervention
- Improve security