

SOLUTION NOTE

Solution Benefits:

- Optimize capital expenditure on switch purchases by reducing port wastage and increasing the utilization of existing switch ports
- Increase network security by quickly pinpointing the location of offending devices
- Maintain audit trails of end point connections for security audits
- Identify network ports accidentally left open to minimize unauthorized access
- Locate where devices are connected for easy troubleshooting

Stop Flying Blind—Quickly Discover Switch Ports and Intelligently Optimize Your Infrastructure

Network port drops are everywhere, from the datacenters and employee offices to the meeting rooms and other common areas. Employees and visitors alike access these ports to perform their jobs. This ubiquity has provided the switch ports a commodity status. Everyone expects to find one when they need one. In some ways switch ports are treated as any other office supplies: more are ordered when we sense supplies are depleting and no one keeps a close track of who is using it and for what. With a data center switch port costing in excess of \$600 per port and access ports \$200 per port and with a potential for serious security breaches by malicious parties using these, switch ports are no ordinary office supplies. IT departments need to keep a close eye on how switches are getting used and which devices are connected where, in order to control capital expenditures on switch purchases and to increase security and ease troubleshooting.



The Infoblox PortIQ™ appliance provides complete visibility into switch port usage for port capacity planning, security audits and ease of troubleshooting.

- Eliminate port wastage, saving CapEx;
- Enhance security with vital port intelligence; and
- Improve visibility for faster troubleshooting.

The remainder of this paper details how to tell if your organization needs visibility into your network infrastructure and describes how the PortIQ appliance from Infoblox provides unparalleled visibility into switch port usage—essential for port capacity planning, security investigations, and ease of troubleshooting.

How Do You Know If You are Flying Blind?

Try answering some of the following questions and see how you fare.

- You are about to sign an expensive switch purchase order to meet the demands of the next year; do you know how many switch ports on your network are under-utilized?
- A firewall has just alerted you about malicious traffic coming from an IP address; can you quickly locate the switch/port this device is connected to and disable it?
- Your IPAM system indicates you have an unauthorized wireless router plugged into your network; can you locate the switch port to unplug it?
- You are troubleshooting a network issue on a device, can you find out the port speed (full duplex/half duplex etc.) without manually tracing the cable to the switch port?
- Do you know how many open network ports are in common areas and meeting rooms that may pose a security threat if an outsider gets access to these?

If you answered “No” to any of these questions you might need help with your switch port visibility. But worry not, you are not alone. An independent survey of network professionals revealed that 90% of the respondents would like better tools and technologies to keep a track of their switch port usage. The following chart indicates that a majority of networking professionals feel they spend too much on purchasing and managing switch ports.

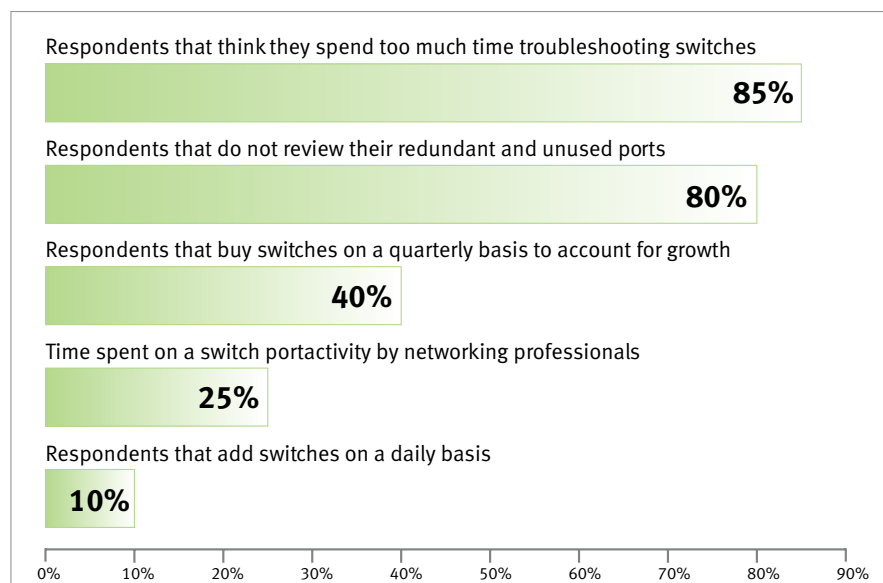


Figure 1: Results of an independent survey of network professionals.

Perils of Flying Blind

Flying blind is dangerous. Lack of a comprehensive, enterprise wide view of network port usage and end device identification leads to the following challenges:

SOLUTION NOTE

- Switch port capacity wastage—With no visibility into port usage patterns, IT departments routinely overestimate capacity requirements making unnecessary capital expenditures on switch purchases. The high costs of purchasing and managing switch ports can significantly increase the network TCO.
- Security enforcement and audits are difficult—Lack of location information for end point devices makes it hard to enforce security when an offending device is identified. In addition, there is no audit trail for where a device connects on the network. This makes it difficult and expensive to investigate security incidents.
- Troubleshooting requires locating devices manually—Troubleshooting network incidents require identifying and locating devices on the network. Manual locating procedures are labor intensive and may reduce IT effectiveness by increasing resolution times. A recent survey revealed that average time taken to trace a device to its switch port is approximately 30 minutes.

PortIQ Appliances to the Rescue

The Infoblox PortIQ appliance provides complete visibility into switch port usage for port capacity planning, security audits and ease of troubleshooting. With PortIQ appliances, network administrators can instantly identify the location of all connected devices and get reports on how often network ports are used. With this kind of unparalleled visibility, IT departments can make more intelligent switch purchase decisions. In addition, the ability to quickly locate where devices are connected increases security and eases troubleshooting efforts.

The Infoblox PortIQ appliance replaces time consuming and unreliable, manual procedures by tracking where devices connect to your network. The Infoblox PortIQ appliance scans your network infrastructure and quickly collates and displays information to provide comprehensive insight into what is connected to your network and where. This insight enables network managers to make informed business decisions and reduce operational overhead and port wastage while enhancing network availability and security.

As a standalone system, the PortIQ appliance can automatically inventory routers and switches and gather data to provide detailed reports on ports in use, activity level and other information that enables better use of existing capacity and saves money.

Connected to an Infoblox Grid, the PortIQ appliance adds valuable data about device location, switch, port, VLAN etc. into the Infoblox IPAM system. Armed with this additional information, network engineers can quickly associate an IP address with a VLAN and switch port to pinpoint trouble spots and resolve problems. This has many applications, including quickly shutting infected devices off the network when virus or worm attacks occur and quickly locating and removing an unauthorized device from the network when discovered by the Infoblox discovery process.

The PortIQ Appliance is Available with the following Software Options

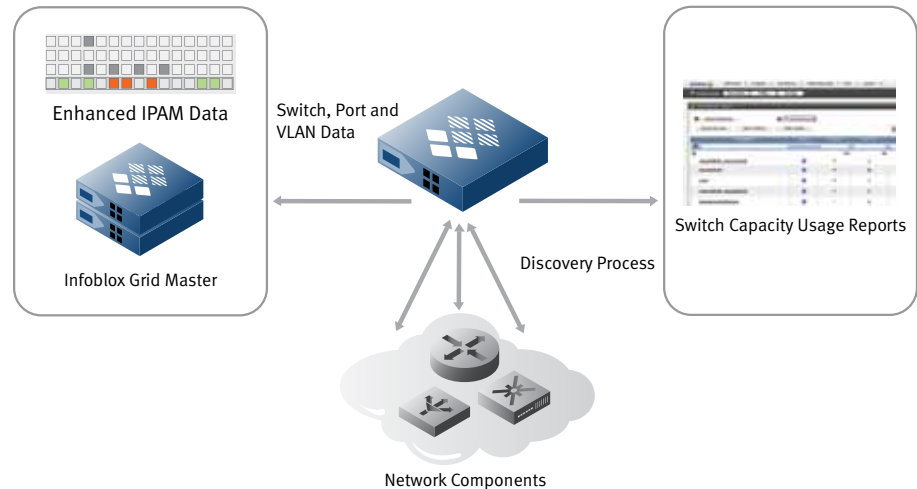


Figure 2: PortIQ appliance enhances Infoblox IPAM data and reports on switch capacity utilization.

PortIQ Appliance with IPAM Connector

With the IPAM Connector version, the PortIQ appliance can be used for port-discovery to enhance the IPAM database in an Infoblox Grid by associating discovered switch and port information with IP, MAC and other IPAM data. This additional information helps network administrators to secure and troubleshoot networks faster.

The PortIQ appliance associates the following information for each IP and MAC address in the Infoblox IPAM database:

Switch Name, Switch Port, Switch Description, VLAN Name, VLAN Number, Switch status, Port Speed/Duplex, Link status, First seen and Last seen times.

PortIQ with Capacity Management

The Capacity Management version of the PortIQ appliance includes a powerful software application that provides switch and port utilization, historical data and capacity reports. The reports provide a comprehensive inventory of network infrastructure and enable network managers to spot potential port exhaustion, identify devices with low utilization and re-balance their infrastructure to match capacity with needs and avoid unnecessary purchases. This results in a very fast ROI. The Capacity Management version of the PortIQ appliance can be used as a standalone system, and also includes the capabilities of the IPAM Connector, which means that it can be connected to an Infoblox Grid to enhance IPAM data with switch, port, VLAN and other data.

SOLUTION NOTE



Figure 3: Infoblox IPAM data showing PortIQ discovered fields e.g. switch, port and VLAN.

Conclusion

Visibility into port usage is a must for controlling costs and securing networks properly. Most IT departments do not have this visibility due to a lack of tools and technologies for this purpose. The Infoblox PortIQ appliances fill this void by providing unparalleled visibility into switch port usage—essential for port capacity planning, security investigations, and ease of troubleshooting.

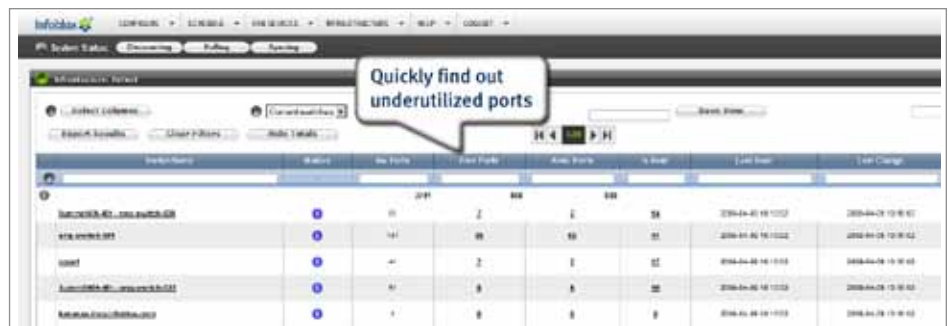


Figure 4: PortIQ switch view report shows discovered switches and utilization levels for a specified period.

Infoblox Product Warranty and Services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that will meet published specifications. Optional service products are also available that extend the hardware and software warranty. These products are recommended to ensure the appliance is kept updated with the latest software enhancements and to ensure the security and availability of the system. Professional services and training courses are also available from Infoblox. Information in this document is subject to change without notice. Infoblox Inc. assumes no responsibility for errors that appear in this document.