WHITE PAPER

Automation: The Future of Network Visibility

Table of Contents

Executive Summary

Data center automation is increasing in importance. In fact, Gartner identified it as one of the key pieces of technology for cloud and data centers in their June 2013 IT Infrastructure & Operations Management Summit. However, what about automation for your adaptive monitoring needs? This is one of the most neglected pieces of automation. At the same time, it's one of the most important. Automation drives the core need for network visibility – delivering the right data to the right destination at the right time.

This whitepaper will illustrate two fundamental scenarios for adaptive monitoring automation – data center provisioning within large enterprises and service providers, and maximizing monitoring tool investments within the enterprise. Both scenarios demand the real-time responsiveness of adaptive monitoring.

You can't be everywhere at one time, and neither can your monitoring tools. Adaptive monitoring lets you virtually move the monitoring switch wherever it needs to be, allowing you to control your capital expenditures while capturing the network information you need. In addition, you can right-size the data that you capture to be only what you need. Basically, the data captures should be as big as the problem, not as big as your network – if you want to control data center costs as you scale your network.

You can't be everywhere at one time, and neither can your monitoring tools.

The Need for Monitoring Switch Automation in the Data Center

Network monitoring switches are fast becoming an important component for enterprise and service provider networks. The reason is simple – how do you monitor your whole network at one time? How do you make it scale? Most IT managers don't have nearly enough money to spend on monitoring tools to cover every segment of this network. This means lack of coverage. Lack of coverage means lack of visibility. Lack of visibility means blind spots. Blind spots usually mean ulcers.

Additionally, if you're a large enterprise with network orchestration systems, the last thing you want is to have your staff manually programming monitoring switches to cover new services and customers. The OPEX for those kinds of tasks is excruciating. Wouldn't it be great if the monitoring system automatically spun up the requisite network monitoring functions as the services and users were set up?

One of the most powerful, but often overlooked features for data center automation is automating the network monitoring switch. In this case automation means monitoring switches can initiate functions (e.g., apply filters, add connections to more tools, etc.) in response to external commands. This data center automation is akin to software defined network (SDN) capabilities, which allow a switch/controller to make real-time adjustments in response to events or problems within the data network. However, the source of the command doesn't have to be an SDN controller. It could be a network management system (NMS), provisioning system, security information and event management (SIEM) tool, or some other management tool on your network.

Let's look at one quick example. It's 3:00 am and a hacker has just attacked your corporate network – how does you network behave? Does it understand who's attacking the network? Once the attack has begun, what exactly happens? Maybe you've purchase a SIEM and just like you hoped, it spots the problem. What will the SIEM do next? Is there an intrusion detection and prevention system that just happens to be connected to the right SPAN that the SIEM can spin up? What about starting a packet capture? How about starting the forensic recorder? Do those tools just happen to be on the same SPAN that this threat vector is coming from? Now – going for the gold medal here – can your current network divert this threat to a honeypot so that you can actually stop the theft of intellectual property as fast as possible, capture more information about the intruder, determine the nature of the threat vector being used so you can prevent it in the future, and discover the exact information the intruder is after and purpose of the attack?

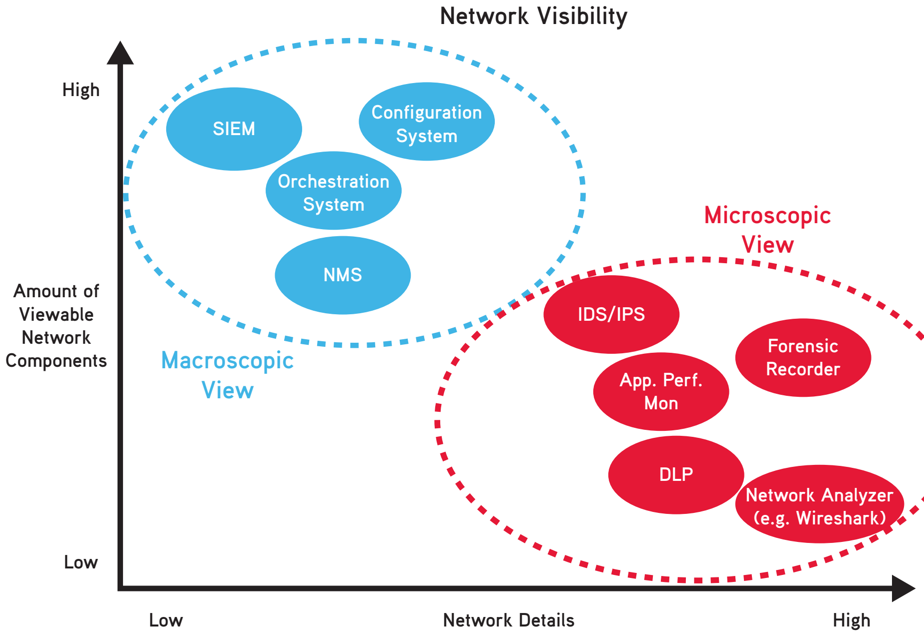
Final question: if you answered no to any of the questions above, will this be you?

Adaptive monitoring is what you need to help you proactively secure a network that is dynamic and constantly changing.

Adaptive monitoring is what you need to help you proactively secure a network that is dynamic and constantly changing. You need automation to align your tools to those dynamic changes to increase operational efficiencies. The days of static programming are over. IT cannot sit back and be reactive anymore while internal and external customers force the network to change on a daily basis. There is a cost to doing nothing. Besides the cost of operational inefficiencies, various governments, organizations and even customers are assessing penalties for non-compliance to standards (SOX, PCI, HIPAA, Data Protection Act for Europe), security breaches due to negligence and failure to meet service level agreement criteria. Now you have the tool that lets IT adapt to network changes as soon as they happen.

Another way of looking at automation is as a way to help you "focus" the network monitoring switch to get either a macroscopic or microscopic view of the network. You need both – but achieving both at the same time would be unrealistic and cost prohibitive.

Using automation to connect to both your orchestration systems and/or your network tools provides you the visibility and actionable insight into your network that you need, when you need it. Figure 1 provides a visual illustration of the "network focus" concept.



Achieving Macroscopic and Microscopic Views of Your Network

Big Data (including internal and external sources) is also flooding the network with an enormous amount of data – too much data in fact.

Network changes are occurring in all directions. The most common sources of change are the following:

- Provisioning of new services and customer
- Network traffic changes associated with the addition of new customers and services
- Security threats (both external and internal)
- Troubleshooting equipment needs constantly vary according to the problem type
- New tools for monitoring and security applications
- Infrastructure additions, upgrades, and removals

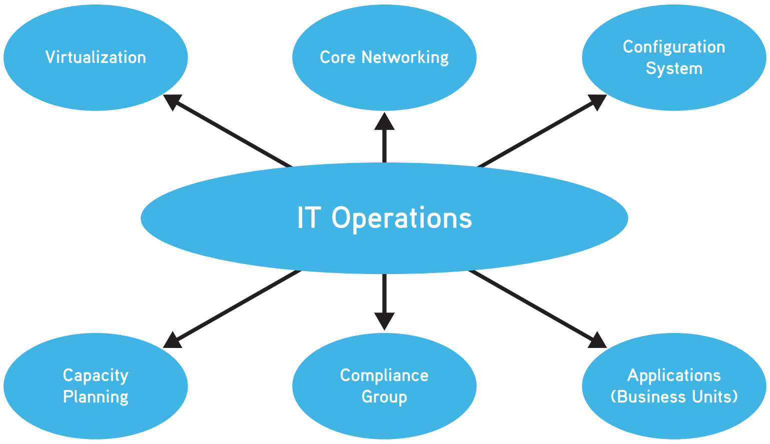
Big Data (including internal and external sources) is also flooding the network with an enormous amount of data – too much data in fact. With automation, you can monitor the pieces you need to when you need to because the right data is forwarded to the right destination for real time analysis.

When automation is combined with a network monitoring switch, near real-time responses can be achieved. This is because automation is a proactive approach that can be used to efficiently minimize security threats and dramatically decrease the mean time to repair (MTTR) for your network because faster responses to problems result in a shorter mean time to diagnosis and a corresponding faster mean time to repair.

If automation is implemented correctly within a network monitoring switch, the device will let you maximize the capabilities of your monitoring tools without specialization or changing your processes. Basically, a proper implementation of automation lets the monitoring switch conform to how you need to use it, not the other way round.

How Monitoring Switch Automation Fits Within Your Organization

There are two common IT user groups for monitoring switches – the IT Operations group and the Networking or Security Tools group. For businesses with a centralized IT Operations group responsible for IT service management, implementing network monitoring switches with automation is a Godsend. Once the automation is set, the IT group that owns the switch can basically set and forget about it. That group's internal customers (like the security group and core networking group) can then use the monitoring switch to perform the different functions they need it to, without further interaction with the Operations group. Figure 2 shows a typical set of customers for the IT Operations group.



IT Operations Group

Removing dependencies on other groups can have dramatic business consequences. Service and equipment turn up time can be decreased from hours/days to minutes. Some enterprises have also tried implementing internal SLA's to speed up intergroup dependencies. Automation helps to sidestep this whole SLA conversation and make life easier within the IT department.

Role-based access allows each of those internal customers to set filter customization and linkages to their respective tools (like provisioning systems, SIEM tools, etc.) without having to worry about another group affecting their access or automation linkages to the monitoring switch. This provides further confidence that the monitoring switch capability will perform as needed, when needed.

Role-based access allows each of those internal customers to set filter customization and linkages to their respective tools (like provisioning systems, SIEM tools, etc.) without having to worry about another group affecting their access or automation linkages to the monitoring switch.

The second fundamental user group for monitoring switches is the IT tools group. Smaller organizations typically don't have a core IT Operations group. They tend to have more dedicated functionalities. The person or group responsible for monitoring tools can take advantage of the monitoring switch capabilities to remove the need for "crash carts," and change board approvals for connecting monitoring tools to the network. Once the monitoring switch is inserted into the network, automation allows the network engineer to create real-time responsiveness to network changes to reduce MTTR, improve network operations with proactive scans, and respond faster to security threats.

Whether a business is large or small, automation can support your needs accordingly. Let's look at some example benefits broken down by functional group:

Services Management

- Allows the monitoring switch to be inserted into your existing processes so the visibility network can mirror your production environment
- Reduces operational costs and increases ease of use because you can create the integration with a monitoring switch once and then leave it alone
- Improves operational efficiencies with the easy application of consistent procedures
- Supports long term networking goals by allowing automation to bridge the new monitoring switch equipment with your network strategies for virtualization and SDN- basically, the monitoring switch "plugs in" to your existing infrastructure.
- Aids alignment of IT with company business processes to reduce costs

Security Tools

Whether a business is large or small, automation can support your needs accordingly.

- Real-time responses to mitigate/eliminate security anomalies and threats as they happen
- Faster responses to minimize the damage/cost to company
- Improved flow of information to/from intrusion detection & protection systems
- Improved flow of information to enable redirection of threats to Honeypots for better threat source isolation

Monitoring and Troubleshooting Tools

- Automated data captures and traces decrease Mean Time To Diagnosis (MTTD) and a corresponding Mean Time To Repair (MTTR) which in turn reduces downtime and troubleshooting costs
- Reduced operational costs and increased ease of use because the staff doesn't have to spend time constantly writing static filter rules
- Automated data captures can capture hard to trace spurious/intermittent anomalies
- Reduction of errors that are typically associated with programming complexity and changes are reduced
- Automation of data captures can reduce monitoring tool processing and storage requirements, thereby reducing costs

Compliance Initiatives

- Specific compliance filters can be created and automated to run and send results that can support your compliance initiatives
- Use features like "Tool Management View" to isolate violations and filter them directly to discover source ports
- Packet Payloads can be automatically stripped to remove sensitive information, such as customer records, before they reach a tool

Extended Solutions

In addition to the automation capabilities that are available directly through a monitoring switch – like the Ixia Net Tool Optimizer – Ixia has performed integrations with many of our technology partners to deliver fully integrated solutions based upon this technology. For instance, we have documented integrations with the following vendors:

- CA
- IBM
- SolarWinds
- HP
- LogMatrix
- LogRhythm
- Splunk

These solutions can be combined with the NTO to accomplish the real-time integrations that businesses need. For automation to work with the Ixia NTO product, the vendor tool can communicate to the Ixia web-based API based upon the IETF REST protocol, or an Ixia API based upon the TCL ("tickle") scripting language. Automation capabilities can be triggered in response to external events like SNMP Traps, SNMP Polls, Syslog messages, NMS events, SIEM events, etc.

Automation has been identified as a key feature for data centers to optimize productivity.

Conclusion

Automation has been identified as a key feature for data centers to optimize productivity. This includes network monitoring, where automation is critical to enabling adaptive monitoring capabilities and tactics to solve your visibility blind spots. Once the automation is configured, you can dramatically increase your network visibility – decreasing your OPEX, your provisioning cost, and the MTTR for your network. These benefits are due to the real-time capabilities that can be enabled within the data network. For example, network monitoring functions can be provisioned at the same time new services are set up and customers are added to the network. Another example is that adaptive network monitoring creates a proactive real-time solution to help you mitigate and/or eliminate problems and security threats as they occur, instead of at some point down the road.

If your network needs to work 24 x 7, you need the right tools and integration between those tools to allow the network to function at that level. You can't monitor your whole network at one time. Automation between your data center and your monitoring switch is the integration you need. This is because automation allows the network monitoring switch to route the flow of monitoring data to the correct monitoring tool at the correct time. Data captures should be as big as the problem, not as big as your network, to prevent overload situations.

WHITE PAPER

Ixia Worldwide Headquarters
26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

Ixia European Headquarters
Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom

Sales +44 1628 408750
(Fax) +44 1628 639916

Ixia Asia Pacific Headquarters
21 Serangoon North Avenue 5
#04-01
Singapore 554864

Sales +65.6332.0125
Fax +65.6332.0127