Best Practices for Network Monitoring Switch Automation
# Table of Contents

Executive Summary .................................................................................... 4  
What Is Adaptive Monitoring? .................................................................. 4  
Adaptive Monitoring Applications ............................................................ 6  
Best Practice Monitoring Switch Examples for IT Operations............... 7  
Best Practice Monitoring Switch Examples for IT Security and Tool Groups........................................................... 9  
Extended Solutions.................................................................................. 13  
Conclusion.............................................................................................. 13
Executive Summary

Network monitoring switches continue to advance in both technical capabilities and usefulness. New features (like automation) drive to the core need for network monitoring – delivering the right data at the right time to the right destination. These advances increase the efficiency of the IT operations group and provide real-time responsiveness to help eliminate network problems as fast as possible. Ixia believes that network monitoring should be as big as the problem, not as big as the network.

This whitepaper will focus on providing best practices for using automation to achieve adaptive monitoring within enterprise and service provider organizations. Automation capability allows for a tight integration with your automated data center provisioning systems (NMS, OSS, or other orchestration system) and your existing tools (whether the tools are for network monitoring, application monitoring, or security analysis).

What Is Adaptive Monitoring?

So what do we mean by adaptive monitoring? Adaptive monitoring is an advanced feature that many of the common network monitoring switches don’t have. Adaptive monitoring allows switches to be automated to initiate functions (e.g., apply filters, add connections to more tools, etc.) in response to external commands. This automation is akin to SDN (software defined network) capabilities, which allow a switch/controller to make real-time adjustments to suspicious activities 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.

Automation for network monitoring will become critical over the next several years, especially as more of the data center is automated. The reasons for this are plain: how do you monitor your whole network at one time? How do you make it scale? You don’t have enough budget to put monitoring tools on every SPAN in your network, yet you are being asked to ensure that the network be 100% functional 100% of the time. In addition, your network is dynamic and constantly changing. The days of static programming are over. You need automation to align your tools to those dynamic changes to increase operational efficiencies and create an adaptive monitoring environment. This is possible if you choose a network monitoring switch that can adapt to network changes to provide the monitoring functions you need, where you need them, when you need them. Incorporating adaptive monitoring into your network monitoring practices is a cost effective way to solve many of your problems.
Your problems are similar to most other IT departments. You are being hit with lots of change and it’s coming from all directions. The most common sources of change are the following:

- Provisioning of new services and customers
- Network traffic changes due to the addition of new customers and new services
- Security threats (both external and internal)
- Troubleshooting needs that are constantly changing
- New tools for monitoring and security applications
- Infrastructure additions, upgrades, and removals

There are typically two main groups within IT (depending upon your organizational structure) that need adaptive monitoring – the IT operations group and the tools group. The main driver of automation for the operations group is achieving operational efficiency to reduce manual processes and the delays/errors that those processes introduce. For the tools group, the main driver is increasing the monitoring capability for the whole network because most IT departments usually don’t have enough money to provision multiple sets of tools across the whole network.

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. It’s a proactive approach used to efficiently minimize security threats and dramatically decrease the mean time to repair (MTTR) for your network. Faster responses to problems result in a shorter mean time to diagnosis and a corresponding faster mean time to repair.

Let’s look at a quick example of how adaptive monitoring can help you. You have a security information and event management (SIEM) tool that spots some anomalous traffic on your network. The SIEM then sends a message to the monitoring switch instructing it to capture the anomalous traffic and send it to an IPS to analyze the anomaly. The packet captures are analyzed and this is identified as a threat by your IPS tool. Since you’ve previously connected your network monitoring switch in-line after your tap, the SIEM instructs the monitoring tool to divert this anomalous packet stream to a Honeypot. From this Honeypot you can now control the access that the intruder has and begin to understand better where the threat is coming from (e.g., who and where geographically), the threat attack used to gain entry into your system, and the nature of the attack the intruder had intended (e.g., defacement of the web site, crashing of the website, theft of corporate intellectual property, etc.).

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

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 increase 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**
- 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 and protection systems.
- Improved flow of information to redirect 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 (which is a problem with several monitoring systems).
- 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 filter features to isolate violations and filter them directly to discover source ports.
Best Practice Monitoring Switch Examples for IT Operations

While automation takes a little effort to configure initially, the benefits are dramatic. IT operations groups need to automate their data centers to maintain current levels of productivity. 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, with limited interaction with the operations group. Removing dependencies upon 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 been trying to implement internal SLA’s to speed up intergroup dependencies. Automation helps you sidestep this whole SLA conversation and make life easier within the IT department.

There are three fundamental use cases for adaptive monitoring and automation that benefit the core IT Operations group:

1. Provisioning network monitoring for new services
2. Provisioning network monitoring for new users
3. Integration to a network management system for centralized management

Let’s dive further into each use case with specific examples using the Ixia Net Tool Optimizer (NTO) as the network monitoring switch. These examples illustrate potential applications that your IT department may want to deploy.

Example 1: Provisioning of Network Monitoring for New Services and Users

In this example, the network has a centralized system, which includes not only using an NMS to control the NTO but includes a larger strategy for services management. These customers see and understand the value of a monitoring switch but they also want it integrated into their pre-existing business processes. This allows customers to have a visibility network that mirrors their production network. Service providers are an excellent example of this customer type.

As part of this use case, automation is used to bridge the new monitoring equipment with your pre-existing network strategies for virtualization (like SDN and ITIL). Basically, the new visibility switch can “plug in” to your existing infrastructure. The system controller or SDN controller can use the Ixia REST API to communicate with the NTO. The NTO then becomes an extension of the centralized control structure and can be utilized by various IT groups (core networking, configuration management, IT security, compliance, etc.) which are often the “internal” customers of the IT Operations 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. Not only can the different groups have task permissions but permissions are granular all the way down to filter aspects of each specific filter. This provides further confidence that the monitoring switch capability will perform as needed, when needed.
A good example of this use case could be integration to your provisioning system (e.g. IBM Netcool® or other provisioning tool). Once new services are implemented, you’ll want a way to monitor the services to make sure they are functioning correctly and, if not, change the service as needed. For instance, you may have a customer service that is using VLAN 55 but someone in the IT department doesn’t know this and they make changes to VLAN 55, or eliminate it altogether. This can cause your service serious problems. But if you have a filter that is monitoring the VLAN continuously (or periodically), you can fix the problem as soon as it happens; possibly even before the customer notices.

Example 2 – Integration to A Network Management System

In this example, customers typically have a centralized management environment that usually contains a network management system at its heart. The NMS is the de facto command center. By using automation, the NTO can slide into this environment very easily. Once the NMS and NTO are integrated, the NMS can monitor and control the NTO like any other devices using a single pane of glass to see all of the pertinent information. The difference between this use case and example 1 is that an orchestration system is not included. Basically, the enterprise is big enough to use an NMS but not as large as a service provider and hasn’t, or doesn’t want to, invest in an orchestration system.

With an NMS integration, the relationship typically focusses on a fault, configuration, accounting, performance, security (FCAPS) deployment, where the NMS is constantly monitoring the NTO for alarms and incidents. The NMS can also provide SNMP and SYSLOG data to the NMS. When an NTO system event/alarm is generated (packet loss, high percentage of change for a specific parameter, or something else), the NMS can trigger a filter that starts the flow of specific traffic to one or more network, or application monitoring, tools for further analysis and processing of packet information.

In addition, policies can be created that send the same traffic stream through multiple analysis points. At the same time, triggers can be placed within an NMS to launch more processes should certain criteria be met. Maybe there is an increase in SYSLOG traffic which passes a pre-defined threshold, traffic from that SPAN can be diverted by a network monitoring switch to monitoring tools for further analysis.

In another situation, an NMS could also be used to apply filters across multiple NTO’s at one time to collect data. This could be the same filter, or different filters, that need to be initiated across multiple monitoring switches in either an ad-hoc situation (based upon external stimulus) or as part of a scheduled activity. Customers that have 10 or more monitoring switches tend to find this use case extremely appealing.

A third use case is to automate routine activities. For instance, maybe you want to periodically pull data to get the information that you need – from either a business intelligence perspective or from a trend analysis perspective. Once a specific filter is created for your data needs, you can have an NMS or other device send commands to the NTO to run the filter at specified times, or in response to thresholds (e.g. usage), for specified durations so that you can collect the data you need.
Best Practice Monitoring Switch Examples for IT Security and Tool Groups

Smaller IT organizations typically don’t have a core IT operations group. They tend to have more dedicated functionalities. The person or team 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.

There are typically three fundamental use cases for automation by IT tool groups:

1. Fast response to network problems and anomalies to minimize downtime
2. Real-time response to security threats
3. Documentation of compliance initiatives

Let’s dive further into each use case with specific examples using the Ixia Net Tool Optimizer as the network monitoring switch.

Example 1 – Fast Response to Network Problems

In this example, the monitoring switch is used to help collect troubleshooting data for the IT department so they can troubleshoot a failure or other network impairment as fast as possible. These situations are obviously unscheduled tasks that demand immediate attention. At the same time, staff support is usually limited and the problems often occur after normal business hours.

Once a problem is observed by an external device (an NMS, OSS, SIEM, or some other device), a request is sent to the Ixia NTO to send data to a packet capture tool. Depending upon how the NTO is programmed, a floating filter (basically a pre-programmed filter) could be connected to a network port and then activated based upon the external command. The floating filter should already be connected to a specified tool based upon the initial use case created for the filter. In a different instance, a new filter could be created and populated with critical information (like IP address, filter criteria, VLAN, etc.) to start the packet capture. For either instance, the packet capture process is started and data is sent to a specific, pre-defined monitoring tool such as packet recorder. Once the IT person logs on, they can view the data capture file created so far to analyze the traffic to determine what has caused the problem.

In another situation, it’s common for tier one IT personnel to escalate trouble tickets to tier two network engineers with little or no troubleshooting data attached to the tickets. The network engineers then have to manually log into devices to capture the required information. Using automation can save time and money. In addition, the network engineering department can have automated filters that run to capture data at specified periods, or in response to pre-defined thresholds. This allows the network engineering group to have a baseline history of network activity to compare against and can help speed up the resolution of anomalies.
Network engineers can get good diagnostic information from data backups when trying to troubleshoot network problems. This can provide dramatic improvements for customers. One customer, which is a large financial institution, was able to reduce their average mean time to diagnosis from three weeks to minutes. The significant source for time savings was the inclusion of the data capture information when the trouble ticket was sent to the tier two engineer.

Automated backups are another topic of interest to this customer type. Network engineers can get good diagnostic information from data backups when trying to troubleshoot network problems. With automation, periodic snapshots can be taken of the monitoring switch configuration and network traffic processing speeds and capabilities. When coupled with trouble ticket data, this can result in faster time to resolution.

Capturing random and intermittent anomalies is always a difficult challenge. By nature, these events are random and dynamic. Even in the best scenarios, the end result is that your MTTR can drag on for days or weeks. By using extensive and granular filtering criteria, you can create a "dynamic" filter that specifically captures the conditions that you have noted so far about the problem. When you combine this with automation and a specialized monitoring tool (like CA Spectrum) to look for the specific conditions, you can create a solution that delivers intelligent packet capture that gives you only the relevant data you need to find and fix the problem the next time it occurs.

This example is similar to the debugging example mentioned earlier, except that this automated process may have to lie dormant for days/weeks until the incident happens again. In the debugging example, the packet captures were implemented instantaneously.

**Example 2 – Real-time Response to Security Threats**

A second example is to use the NTO with a security information and event management tool. This is the same example presented earlier on in the whitepaper but we’ll dive into more of the details here.

In this example, the external equipment (e.g., ArcSight SIEM) sees an anomaly like a buffer overflow situation. The SIEM then sends a command to the NTO to start a packet capture. The filtered packet stream is then forwarded to another tool (like an IDS tool) to determine whether this is a security attack, some random anomaly that may require further...
investigation, or some mistake (corrupted packets due to network or component failures). See Figure 2 for an illustration.

Figure 2 – NTO Monitoring Switch Integration with an SIEM

Figure 3 illustrates a filter that is ready to capture and record the security data. The SIEM tool then requests the NTO to connect the floating filter to a network port to activate the flow of information.

Figure 3 – Forensic Recorder on Call for Incident Remediation
Automated routines may be constantly looking for generic route encapsulation tunnels or other parameters.

Figure 4 illustrates how the forensic tool triggers the intrusion detection system device so that it can analyze the data to characterize the threat.

Figure 4 – IDS Used to Automatically Identify Anomalies

Continuing with this example, IT could combine NTO automation with an IDS and use the NTO to divert traffic to a honeypot to further characterize the security attack. Basically, instead of killing the security attack once discovered, a network monitoring switch can divert the specific stream to a honeypot to capture more information about the intruder, the nature of the threat vector they are using and the information they are after (or purpose of the attack).

In a different example, a cloud environment needs increased security analysis due to its dynamic nature and the service level agreements that it has in place. Automated routines may be constantly looking for generic route encapsulation tunnels or other parameters. Once a condition is discovered by an IDS, a packet capture can be initiated by a monitoring switch that can provide more data. Based upon further analysis of this specific data, API calls can then be launched to throttle firewall traffic by opening or closing ports or moving traffic to other VLANs.

Example 3 – Documentation of Compliance Initiatives

Another example of using automation is for documentation of compliance initiatives. This could involve running a filter that checks for payment card industry (PCI) or other regulatory compliance or possibly for service level agreement (SLA) validation. In both cases, a specific floating filter is created. When instructed to by an outside source, the NTO can connect the filter to one or more network ports to check the status of those network ports. The specific filters would have the preconfigured criteria loaded into them. In the case of a PCI filter, the filter could check for traffic of various ports [such as 20 (FTP data), 21 (FTP control), 23 (Telnet), 69 (TFTP), 80 (HTTP CONNECT) and others] that should not be in use if PCI compliance is required. If traffic is captured on those ports, then further investigation could be performed to determine why. If no traffic is found during the specified interval, this could be logged as a pass by the external system initiating the service.
Network visibility will continue to increase in importance over the next several years as network complexity increases, and the deployment of SDN and data center automation becomes more prolific.

Conclusion

Network visibility will continue to increase in importance over the next several years as network complexity increases, and the deployment of SDN and data center automation becomes more prolific. Automation can be used to dramatically increase your network visibility and also increase your ability to reduce the MTTR for your network. 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 so that the monitoring switch adapts to changes in your network and provides adaptive monitoring. Adaptive 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.