

## Best Practices Guide



This guide has recommendations of best practices for designing a Monitoring Access Platform (MAP) into your network before problems occur. Permanent monitoring access points designed into the network architecture increase network security and uptime because they provide the flexibility to attach and remove needed monitoring tools at any time, without disrupting traffic or entailing network reconfiguration.

The practices discussed here represent the accumulated wisdom acquired by Net Optics engineers and customer service personnel working for 12 years with more than 5,000 customers in all industries. Following the best practices presented here will enable you to get maximum value from your monitoring solutions and keep your network running smoothly.

### MAP Basics

- Plan monitoring access as part of the network architecture, before installing the network. A MAP speeds problem resolution by enabling monitoring tools to be connected immediately, as soon as a problem is detected, without waiting to reconfigure switches or install Taps.
- Install monitoring access at the same time the rest of the network is installed. In parts of the network that are already deployed, install the MAP now, *before* problems occur.
- Baseline network behavior before problems occur.

### MAP Architecture

- Include monitoring access for all critical network links at the edge, in the data center, and at the core.
- At the edge:
  - Use **Bypass Switches** to create a fail-safe connection for in-line devices such as Intrusion Protection Systems (IPS), WAN optimization devices, and threat management appliances. A Bypass Switch sends link traffic through the attached in-line device as long as the device is operating normally; but if the device fails or is removed, the Bypass Switch keeps the link up by automatically routing traffic around the in-line device. In addition, when traffic is being routed around the in-line device, it is also copied to the monitoring ports like a Tap, so link traffic can be monitored without difficulty.
  - Use **Regeneration Taps** to enable multiple security and performance-analysis tools to monitor the same traffic simultaneously, or when multiple groups may want to monitor the same information. Regeneration Taps duplicate the same traffic stream on multiple monitoring ports so multiple tools can be used at the same time without conflict.
  - Use **Network Taps** to directly monitor DS3 and E3 links to optimize traffic on expensive WAN links. Unnecessary traffic destined for remote and distributed campus environments can be captured and eliminated without reconfiguring switches or taking down links to deploy in-line tools.

**Best Practices Guide**

- In the data center:
  - o Use in-line **Link Aggregators** to combine the traffic from up to ten network links and send the resulting data stream to as many as four separate monitoring tools, greatly increasing the efficiency of tool usage. However, if the traffic load is such that aggregated traffic from all links may exceed 100 percent of the monitor port bandwidth, be sure the Link Aggregator has enough buffering to accommodate bursts of high bandwidth traffic; otherwise packets may be dropped.
  - o Span ports can be a cost-effective monitoring access method when switches have low enough utilization that they can service the Span ports without dropping packets. If you elect to rely on Span ports, then use **Span Link Aggregators** to combine the traffic from up to ten Span ports and send the resulting data stream to as many as four separate monitoring tools. In addition, don't forget to consider the impact on problem resolution speed if switches must be reconfigured for Span when trouble-shooting; it is best if Span ports have a pre-configured, fixed function in the MAP.
  - o If high link utilization makes use of Link Aggregators problematic, even with buffering, then use a **Director Data Monitoring Switch** to enable a pool of up to 10 tools to be instantly switched across as many as 28 selected network links. More tools and links can be accommodated by daisy-chaining multiple Director chassis into a larger logical system.
  - o Select intelligent **iTap** devices for increased visibility, with or without external monitoring tools attached. **iTap** devices measure and display peak utilization rates, packet counts, and user-configurable alarms through both front panel interfaces and software management utilities.
  - o Use **Converter Taps** for connectivity when monitoring tools are mismatched to link media types. For example, an LR-to-SR Media Converter Tap can be attached to an LR monitoring port to enable it to be used with an SR-based tool. For a complete list of Net Optics Media Converter Taps, see [http://www.netoptics.com/products/product\\_family.asp?cid=5&Section=products&sid=&menuitem=5&network=Connectivity](http://www.netoptics.com/products/product_family.asp?cid=5&Section=products&sid=&menuitem=5&network=Connectivity).
  - o **Converter Taps** can also be used to extend the reach of network links for horizontal distribution and riser cables by converting copper to fiber, or multi-mode fiber to long-reach single-mode fiber.
- Within the core:
  - o Use **1 and 10 GigaBit Fiber Taps** to provide line-rate data capture of the core's high-speed network links.
  - o Use **Link Aggregators** to combine the traffic from multiple outputs of a load balancer so all requests are captured by the same tool regardless of which server the load balancer distributes the requests.
  - o Use **Link Aggregators** in meshed network environments so asymmetrical traffic can be captured and replayed for essential compliance and trouble-shooting requirements.

### Best Practices Guide

- o It is especially important to plan monitoring access for links going to blade system chassis, because these systems make no provisions for Tapping into the network links that run through the blade system backplane from network blades to individual server blades. Use passive **Network Taps** or **Regeneration Taps** to provide monitoring access to external connections to blade switches.
- o A **Director Data Monitoring Switch** can provide all of the necessary 1- and 10-Gigabit Tapping, switching, aggregation, and regeneration capabilities in a single appliance. Its high port density—28 network ports and 10 monitor ports per 1U chassis—makes it ideal for deployment within the network core.

#### Centralized Data Monitoring

The advent of high-port density access devices such as Director has made it practical to centralize network monitoring for an entire building, campus, or small metro area in a single location.

- Place a Director chassis on each floor or in each building, daisy-chaining up to 10 chassis into a single logical system. SR, LR, and ER daisy-chain links have reaches of 300 meters (980 feet), 10 kilometers (6 miles), and 40 kilometers (25 miles) respectively, enabling even a small metro area to be covered by a single Director system.
- Use Net Optics **System Manager** software or a third-party SNMP-based management tools such as IBM Tivoli and HP OpenView to manage the entire multi-chassis Director system from a central location.
- To Tap into 1-Gigabit links, provision Director with one or two DNMs that support six in-line links each of the appropriate media type (fiber or copper). Or, for increased Tap density, use external Taps and provision Director with one or two DNMs that each support 12 Span ports or 12 external Taps.
- To Tap into 10-Gigabit links, use external Taps and connect to Director 10-Gigabit ports. Each Director chassis supports four 10-Gigabit ports that may be used as either network ports or monitor ports.
- When combining external Taps with Director:
  - o For lowest power, select all-optical Taps, which consume no power at all
  - o For increased Tap density, choose Port Aggregator Taps, which copy traffic from both directions of a full-duplex link to a single port
  - o For maximum Tap density, use Link Aggregator Taps to combine multiple low-utilization links into a single monitoring data stream
- Use your entire range of copper and fiber, 10-Megabit through 10-Gigabit monitoring tools by provisioning Director with appropriate XFP and SFP transceiver modules.
- Use Director's filtering capabilities to send tools only traffic of interest, increasing tool efficiency and preventing tools from becoming oversubscribed.



## Monitoring Access Platform

### Best Practices Guide

#### MAP Benefits

Deploying a monitoring access platform across the entire network infrastructure is cost effective because it improves network uptime and performance, enables network administrators to work more efficiently, decreases business risk by providing 100 percent visibility of mission-critical business applications, and multiplies the ROI of expensive monitoring tools. For organizations that rely on their networks, a Monitoring Access Platform is the key to optimal network performance, reliability, and security.

#### For further information:

[http://portal.netoptics.com/pdf/MAP\\_whitepaper.pdf](http://portal.netoptics.com/pdf/MAP_whitepaper.pdf)

<http://www.netoptics.com>

Net Optics, Inc.

5303 Betsy Ross Drive

Santa Clara, CA 95054

(408) 737-7777

[info@netoptics.com](mailto:info@netoptics.com)

*Customer First!*