



A Multifunctional Approach to Improve Monitoring Access in High-Performance Networks

Executive Brief



The Director™ data monitoring switch brought a new level of port density and functionality to the monitoring access market. Net Optics now raises the bar to an even higher level by introducing Director Pro™, a new line of data monitoring switches that adds new capabilities to the Director family. By integrating a custom, high-performance packet processor called the Pro Engine, Director Pro provides five key functions:

- Dynamic load balancing on a flow or packet basis
- Deep packet inspection by pattern matching anywhere in the payload
- Real time traffic statistics by port and filter
- Granular filters
- MPLS filtering

The benefits of these functions are summarized in the table. A detailed discussion of each feature follows.

New Director Pro Capabilities

| Feature | Benefit |
|--------------------------------|--|
| Dynamic load balancing | <ul style="list-style-type: none">• Spread the load to multiple tools when it exceeds the capacity of a single tool• Use 1 Gigabit tools on 10 Gigabit links• Facilitates analysis by keeping flows intact• More even load distribution compared to static load balancing |
| Deep packet inspection | <ul style="list-style-type: none">• Filter on the payload, not just the packet header• Facilitate troubleshooting by identifying packets by content• Detect leaks of confidential information• Identify email and chat traffic by keywords and user names• Identify VoIP traffic by phone number• Improve monitoring tool efficiency by sending tools the exact data streams they need to inspect |
| Centralized traffic statistics | <ul style="list-style-type: none">• Easily check effectiveness of load balancing• Examine traffic volume by protocol, port, VLAN• See integrated view of traffic from multiple Director Pro, Director, and other iTap devices• Real-time statistics based on one-second analysis of traffic |

A Multifunctional Approach to Improve Monitoring Access in High-Performance Networks

Executive Brief

| Feature | Benefit |
|------------------|--|
| Granular filters | <ul style="list-style-type: none">• Eliminates false-positive data passed by approximate range filters implemented with masking• Use monitoring tools more efficiently by eliminating unwanted traffic• Ease trouble-shooting network issues with more accurate drill-down• Extended filtering• Filter on Ethertype to identify L2/L3 protocols• Filter on MPLS label to analyze MPLS traffic |

Dynamic Load Balancing

This section discusses the problem of tool oversubscription, several current approaches for mitigating the problem, and why dynamic load balancing is the best solution. Finally, the dynamic load balancing capabilities of Director Pro are described.

The Problem: Tool Oversubscription

As the volume of network traffic continues to skyrocket, it sometimes outstrips the bandwidth of the monitoring tool's interface or the tool's processing speed. This condition is called tool oversubscription. When tools are oversubscribed, packets are dropped and analysis is hampered. Traffic recording systems miss vital messages, performance analyzers have difficulty finding the root causes of issues, and security systems give intruders and harmful malware an opportunity to invade the network. In short, monitoring tools cannot do their jobs when they are oversubscribed.

Solution 1: Pre-Filtering

It may be possible to solve an oversubscription problem by pre-filtering the traffic that is passed from the network to the monitoring tools using an access switch such as Net Optics Director. For example, the Director can pass Web Application firewalls just the HTTP traffic they need to monitor while passing all other traffic to an IPS. Or Director can drop all packets except for TCP traffic, if TCP traffic is sufficient for the monitoring purpose. But sometimes pre-filtering is not an option because the application requires all of the traffic, or because the time and effort to set up pre-filters is too costly.

Solution 2: Static Load Balancing

Another way to relieve tool oversubscription is to split the traffic and have multiple tools operate on different parts of it. For example, when traffic in a 10G pipe grows to the point where it regularly exceeds 1G, it may be more cost-effective to apply two existing 1G tools to the traffic rather than upgrade to expensive 10G tools. The function of splitting the traffic into multiple, evenly balanced streams is called load balancing.

Access switch solutions such as Director can perform static load balancing by applying filters on, for example, a few bits of an address or port field. For instance, all packets with odd IP source addresses can be sent to one tool, and all packets with even IP source address to a second tool. The load will be balanced fairly evenly if the distribution of IP source addresses between odd and even is random. The key to achieving an even balance with static load balancing is to identify a field in the target traffic which has a random distribution. To take another example, if RTP traffic is being analyzed, the SSRC ID field may be a good candidate for static load balancing.

A Multifunctional Approach to Improve Monitoring Access in High-Performance Networks

Executive Brief

Static load balancing may not be an adequate solution when an appropriate filtering field cannot be identified, either because traffic is not evenly distributed relative to any chosen field, or because analysis of the traffic to find such a field is impractical or undesirable.

The Best Solution: Dynamic Load Balancing

What is needed is a dynamic load balancing capability in which the load levels on the output channels are actively monitored and packet distribution is adjusted to keep the loads as even as possible. But this task is not as easy as it sounds, because it is usually not acceptable to send packets randomly to multiple tools. In order for the tools to make sense of the traffic, they usually need to see entire flows of packets, where a flow is all of the packets involved in a particular conversation between two endpoints.

Dynamic Load Balancing in Director Pro

Director Pro satisfies the need for dynamic, flow-based load balancing. Operating at line speed up to 10 Gbps, the Pro Engine can load balance an input load to anywhere from 2 to 32 output ports, while guaranteeing that each tool receives complete flows. Flows can be identified in three ways: by IP address pairs, by IP source address only, and by IP destination address only. A fourth load-balancing mode is provided for times when keeping the flows intact is not important; this mode uses a packet-by-packet round-robin algorithm, sending each successive packet to the next output in order, looping back to the first output after the last one.

Dynamic load balancing can be used in conjunction with all of the other Director functions including filtering, aggregation, and daisy-chain expansion. For example, traffic from network port n1.1 in each unit of a ten-unit daisy-chain can be aggregated, filtered for TCP protocol, and load balanced to eight selected monitor ports. Furthermore, load balancer outputs can be weighted, sending, for example, two or three times as much traffic to a particular tool. Weighting the outputs is useful for matching loads to tools that have differing capacities.

Overflow-based Load Balancing

Director Pro's dynamic load balancing can optionally be configured in an overflow-based balancing mode. When overflow-based balancing is selected, all traffic flows are sent to the first monitoring tool until the bandwidth utilization of the monitor port exceeds a configurable level, for example, 80 percent. At that point, new flows begin being directed to the second tool. When the second tool's bandwidth utilization exceeds the threshold, new flows are diverted to the third tool, and so on, up to 32 tools.

Consider the usefulness of overflow-based balancing when the application is forensic recording, that is, capturing all of the traffic on a link. Say the link is a 10G pipe and 1G traffic recorders are available. Initially, the traffic load may be low and a single recorder can capture it all. As the network administrator sees the traffic load growing, she can attach a second traffic recorder to Director Pro. When the traffic exceeds 800 Mbps, Director Pro automatically begins sending traffic to the second recorder. When the administrator notices traffic approaching 1.6 Gbps, a third traffic recorder can be prepared; and so on, as the 10G pipe fills up over the ensuing weeks and months.

Link State Awareness and Tool Sparing

The Director Pro load balancer is link-state aware: If a tool in the load balance set fails, Director Pro responds to the link down condition by redistributing the traffic to the remaining tools. When the failed tool is repaired or replaced and the link comes back up, Director Pro puts it back into the load balance set so it receives a balanced portion of traffic. Link-state aware load balancing works for any number of failed tools, all the way down to all of the traffic going to a single tool if only one link is up. In addition to link-state awareness, the dynamic load balancer offers an N+1 redundancy tool sparing feature.

A Multifunctional Approach to Improve Monitoring Access in High-Performance Networks

Executive Brief

With this feature, a spare monitoring port can be specified for the load balancing set. Then, when a tool loses power, is removed, or otherwise fails, Director Pro responds to the link down condition by switching the traffic flows that were going to that port over to the spare port. The monitoring operation continues uninterrupted, with the spare tool replacing the down tool.

Tool sparing is an important capability when the monitoring function is mission-critical. For example, if recording all of the network traffic is imperative for compliance or forensic reasons, the traffic can be load balanced to a sufficient number of traffic recorders to capture all the traffic without oversubscribing the recorders. Then, an additional recorder can be connected as a warm standby spare in case one of the active recorders fails. Recording of all of the traffic can continue while the failed recorder is repaired or replaced. Traffic can be switched back from the spare tool to the original channel once a functioning recorder is present.

Deep Packet Inspection

This section discusses the need for deep packet inspection (DPI) and describes the DPI capabilities of Director Pro..

The Need for DPI

Net Optics Director provides basic packet filtering capabilities based on L2 through L4 header information including IP addresses, TCP/UDP ports, MAC addresses, and VLANs, as well as user-defined fields. But sometimes it is useful to look deeper into the packets, at L5 through L7 information. These protocol layers carry the application protocols such as HTTP (Web traffic), FTP (file transfers), NTP (time synchronization), RTP (audio and video streams), and SNMP (system and network management traffic). They also carry the payloads or actual data of the applications.

Often L5-L7 protocols are identified by the TCP/UDP ports they operate over. For example, Port 80 is the standard port for HTTP, and Port 161 is for SNMP. However, sometimes the protocols run over non-standard ports, and sometimes malware sneaks in on standard ports. By examining L5-L7 information with DPI, it is possible to find application traffic on non-standard ports and to identify unwanted traffic on standard ports. The result is more thorough application performance analysis and more secure systems.

DPI in Director Pro

Director Pro offers a DPI capability with a pattern-matching engine that is capable of examining the entire packet payload at full line speed. Key characteristics of Director Pro DPI are:

- Each pattern is from 1 to 64 bytes long
- A bitwise mask enables “don’t care” bits
- Patterns may be specified as ASCII strings, hex digits, or a mix of both
- Case sensitivity can be on or off for ASCII string matching
- A single filter can include two patterns along with header filter parameters (such as `ip4_src=10.30.2.8 AND i4_src_port=80 AND “John”` followed by “Mary”), or three patterns exclusive of other parameters (such as “John” followed by “Mary” followed by “Tim”).
- An offset can be defined for each pattern; the offset is a number of bytes to skip before pattern matching begins; the offsets are independent for all patterns and all filters
- Each pattern can be anchored or unanchored; when anchored, the pattern must be found

A Multifunctional Approach to Improve Monitoring Access in High-Performance Networks

Executive Brief

immediately following the offset; when unanchored, the pattern can occur anywhere after the offset (sliding search)

- When two patterns are included in a filter, they are matched sequentially: a match on Pattern 1 must be found before the offset and search for Pattern 2 begins.

Director Pro DPI can locate packets by keywords such as user names and phone numbers. Certain types of traffic classification by application can be accomplished by searching for tags like “HTTP” or “Excel” in the packet payloads. Data leaks can be detected by looking for keywords such as “Confidential” and “Proprietary.”

Accurate and thorough L5-L7 traffic analysis demands complex, intelligent software algorithms; processing traffic at 1 Gbps or 10 Gbps line speeds with these algorithms requires powerful hardware that is often prohibitively expensive. Director Pro’s DPI pattern-matching capability, which operates at full line speed up to 10 Gbps. can be used as an L5-L7 pre-filter to limit the amount of traffic sent to the more sophisticated DPI tools, or as a fast and easy-to-use drill-down tool when NOC professionals trouble-shoot network issues. Other applications for this line-speed DPI capability are as wide as the user’s imagination.

Centralized traffic statistics

Web Manager, the browser-based Director GUI, displays RMON statistics for the traffic through each of Director’s network and monitor ports. Director Pro takes this monitoring function one step further, emitting traffic statistics over the management interface to an external collection server. Net Optics Indigo Pro™ can collect the statistics from multiple Director Pro units, as well as from other Net Optics products that will support this capability in the future. A browser is used to view the data collected by Indigo Pro, displaying real-time graphs of the monitored traffic. Each Director Pro unit supports up to five Indigo Pro appliances.

In addition to Director’s port-based RMON statistics, Director Pro also breaks down traffic by protocol and filter. Director Pro emits traffic statistics for the following data streams:

- The traffic through each network and monitor port
- The load balancer outputs
- The traffic passed by each filter implemented in the Pro Engine (up to 16 filters)
- Overall traffic into and out of the Pro Engine
- Total IPv4 traffic entering the Pro Engine
- Total IPv6 traffic entering the Pro Engine
- Total ARP traffic entering the Pro Engine
- Total ICMP traffic entering the Pro Engine
- Total TCP traffic entering the Pro Engine
- Total UDP traffic entering the Pro Engine

A centralized Indigo Pro device can monitor the entire network, using Director Pro units to tap the links in network concentration points such as the data center and wiring closets. A glance at an Indigo Pro display can quickly verify that load balancing is achieving an even load, and how many tools have been engaged in overflow-based load balancing. The mix of traffic by protocol is easily observed, and traffic of particular interest can be monitored by creating Pro Engine filters to select the traffic.

A Multifunctional Approach to Improve Monitoring Access in High-Performance Networks

Executive Brief

Granular filters

Filter definitions in some data monitoring switches accept ranges for IP addresses and VLANs. However, they implement the ranges with simple masking, resulting in significantly wider capture ranges than were specified. The result is that unwanted and irrelevant traffic is sent to the monitoring tool, wasting tool resources and complicating analysis.

Director Pro eliminates this inefficiency by implementing accurate range filters for IP addresses, MAC addresses, UDP/TCP ports, and VLANs. If vlan=1-5 is requested, that's exactly what you get – not 0-7. With accurate filter ranges, Director Pro saves time and money by reducing confusing, unwanted data and increasing monitoring tool efficiency.

Extended Filtering

Director Pro extends Director's packet header filtering by adding support for the Ethertype field and the outer MPLS label. Filtering on the Ethertype field is an easy way to exclude non-IP traffic, which can often be an annoyance in trouble-shooting. It also improves visibility of special traffic types such as AppleTalk, PPPoE, and FCoE. In addition, the Ethertype field identifies MPLS unicast and multicast packets, which, in conjunction with the MPLS label field filter, can be used for analysis of increasingly common MPLS traffic.

Director Pro supports all of the same Director Network Modules (DNMs) as Director. DNMs are cards with twelve 1G network ports in fiber or copper, with both in-line and Span models available.

The DIR-6400P models can be daisy-chained with DIR-7400 and DIR-5400 units. However, the Director Pro units have only a single 10G expansion port on the rear panel, so they can only occupy end positions on the daisy-chain.

Models

Director Pro is offered in four models:

- DIR-6400P Main chassis with 10 SFP monitor ports, 3 XFP 10G ports, 2 DNM slots
- DIR-6400P-DC -48VDC power version of DIR-6400P
- DIR-3400P Main chassis with 10 SFP monitor ports, 2 DNM slots
- DIR-3400P-DC -48VDC power version of DIR-3400P

Summary

With dynamic load balancing, deep packet inspection, and other capabilities never before available in the monitoring layer, Director Pro gives network professionals an important new tool for their monitoring toolboxes. Whether tuning network performance, tracking down troublesome issues, collecting forensic data, ensuring compliance, or securing the information infrastructure, network professionals and their tools operate faster and more efficiently—saving time and money—when the functionality of Director Pro is at their fingertips.



A Multifunctional Approach to Improve Monitoring Access in High-Performance Networks

Executive Brief

For further information about Load Balancing with Director Pro:

<http://www.netoptics.com>

Net Optics, Inc.

5303 Betsy Ross Drive

Santa Clara, CA 95054

(408) 737-7777

info@netoptics.com

Customer First!