How the EndaceProbe® Intelligent Network Recorder Interacts with Your Network

EndaceProbe Intelligent Network Recorders (INRs) provide 100% capture technology with 0% network intrusion

At a Glance

The Endace Division of Emulex uses proven Data Acquisition and Generation (DAG®) technology in its EndaceProbe INRs to capture 100% of network traffic, ensuring data is available when needed to resolve an issue. This paper shows how the EndaceProbe INR interacts with the network, collecting network traffic data without causing any impact on your live network's traffic, and offers best practices for deploying capture technology.

Products

- EndaceProbe INR

Solution Benefits

- 100% capture of network data without impacting the live network's traffic

Overview

Securing and maintaining your data center network is essential to ensuring a great customer experience and avoiding network downtime and lost revenue streams. A network packet capture tool can help you discover problems that may negatively affect network and application performance as well as security intrusions. Network monitoring equipment deployed at various points in your network infrastructure should be non-obtrusive and should not cause any disruptions in network service. The EndaceProbe INR is built on proven DAG technology and is ideally suited for deployments where high throughput and high capture capability are required. It is designed to fit seamlessly into any network infrastructure.

Endace DAG Technology

The EndaceDAG™ Data Capture technology used to collect packet data off a network is very different from a standard Ethernet network interface card (NIC). The DAG technology, or interface, operates at the physical layer (Layer 1), not the Data Link Layer (Layer 2), in the Open Systems Interconnection (OSI) model. The operating system (OS) driver does not allow the DAG interface to participate in network traffic negotiations or conversations. Because it is not an addressable device on the network, it therefore is not susceptible to security threats.

Additionally, the DAG interface can be connected to a network using only the optical receive port connection if required. This ensures that there is no potential for a compromise of its capabilities.

Since the DAG technology operates at the physical layer, it will capture all traffic presented to it at wire speed for further processing. Incoming traffic can be sent to disk for storage or for processing by Endace Fusion Ecosystem™ connectors (i.e., on-board applications) or virtual machine (VM) hosted applications, such as Velocimetrics, Compuware and Splunk. For additional supported 3rd party applications visit the Emulex Fusion Alliance Ecosystem. As traffic is captured through the EndaceProbe INR, its path is easily tracked and managed, with status screens confirming its behavior. Furthermore, logging onto external systems, such as syslog, can provide an additional layer of auditing, if needed.

How the EndaceProbe® Intelligent Network Recorder Interacts with Your Network

EndaceProbe Intelligent Network Recorders (INRs) provide 100% capture technology with 0% network intrusion

Accessing Network Traffic

Ensuring complete visibility of network data is the first critical component of event analysis. As shown in Figure 1, there are three common ways for a monitoring device to access network traffic:

- Switched Port Analyzer (SPAN) session on a switch
- Network packet broker (NPB)
- Network Test Access Point (TAP)

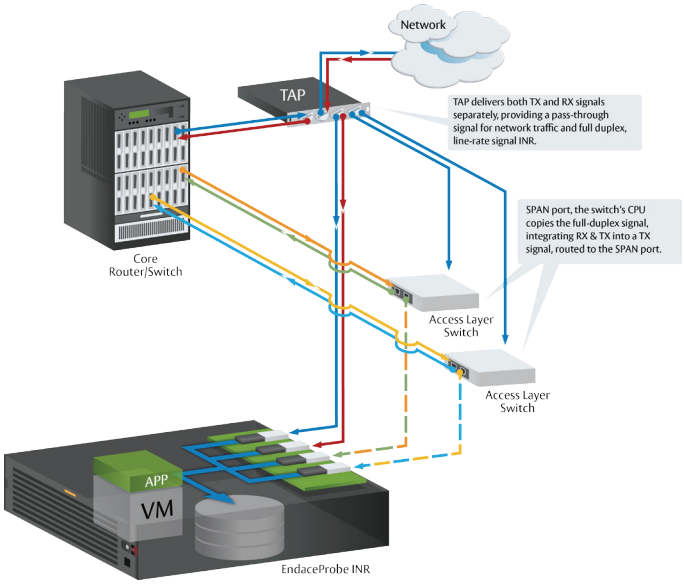

Figure 1: Accessing network traffic from the EndaceProbe INR.

The EndaceProbe INR is never an inline device on the network. It is fed a copy of a network's live traffic via SPANs, TAPs and/or NPBs and therefore cannot interfere in any way with the live network's traffic. Deploying an EndaceProbe INR will not cause any operational impact to the traffic it is monitoring.

Best Practices

It is recommended that when deploying any capture technology, the following precautions are taken into account:

1. The management interface of the capture appliance needs to be protected from direct access via internet (i.e., do not place the management interface directly on an internet facing network)
2. All the default passwords must be changed (for IPMI and Host Platform)
3. Only provide access to users on an as-needed basis. Do not provide free-for-all access.
4. Ensure that each user has the level of access that is relevant to their role (refer to role-based access control)
5. Enable syslog on the capture appliance to ensure all access to it is logged
6. Enable SNMP traps on the appliance for monitoring the events from the EndaceProbe INR
7. Enable HTTPS for managing the appliance via the web user interface

Conclusion

Complete and accurate network visibility is critical to resolving any network or security event. When selecting a network traffic capture tool, it is critical that it does not impact the live network traffic it is monitoring. The EndaceProbe INR is an ideal solution, offering complete network visibility across the data center, without causing any disruptions to the network core infrastructure.

For more information on the EndaceProbe INR, visit: **emulex.com**

For inquiries email: **inquiries@emulex.com**

endace EMULEX

www.emulex.com

Endace USA
2291 Wood Oak Drive, Suite 150
Herndon, VA 20171, USA
Phone +1 408 220 9051

Endace Limited (UK)
Davidson House, Forbury Square
Reading, Berkshire, RG1 3EU
United Kingdom
Phone +44 118 900 1436
Fax +44 118 900 1426

Endace Australia Pty. Ltd.
Level 32, 101 Miller Street
North Sydney, NSW 2060 Australia
Phone +1 800 196 594
Phone +61 2 8912 2157

Emulex Corporate Office
3333 Susan Street
Costa Mesa, CA 92626, USA
Phone +1 714 662 5600