White Paper

Selecting a Network Recorder for back-in-time analysis to solve intermittent problems and unexpected events

Often, the only way to get to the root cause of unwelcome or intermittent events that occur on your network is to use a Network Recorder. This is a device that can capture and store packets at full line speed without dropping any packets, and without resorting to packet slicing.

In this white paper you will learn when it is important to use a Network Recorder, and key considerations when selecting a network recorder for back-in-time forensics analysis.

Table of contents

FLUKE networks

Introduction

Network managers often rely on basic protocol analyzers (such as Wireshark) or monitoring devices (such as RMON probes) to keep track of what is happening on their networks. Even sophisticated analyzers and probes, however useful, are still limited by the fact that they are basically traffic sampling devices that provide statistical KPI's. Such devices may sometimes indicate that a persistent problem has occurred, but they cannot go back and investigate the problem in depth, because they have not captured and stored all of the packets related to the problem. The root cause of the problem may remain elusive resulting in finger-pointing and continuing loss of productivity.

Shortcomings of traditional protocol analyzers

Protocol analyzers on the market today are typically software-based, and are designed to be installed on an ordinary PC. They tend to have one or more of the following limitations:

- The small size of the capture buffer means that they can only capture a small number of packets, and then it becomes full and either has to stop capturing, or the buffer has to wrap, which often causes important data to be lost.
- If slicing is used to increase the number of packets that the buffer can hold, the visibility into the payload data is compromised. This often makes it difficult to analyze security problems, compliance problems, and certain kinds of application problems.
- Ability to monitor multiple locations simultaneously and to correlate the data is often quite limited. This makes it hard to get the full picture when there are redundant paths, load-balancing, or asymmetric flows.
- There is often a lack of sufficient analysis capability at remote locations. An operator might need to bring the contents of an entire buffer across the network before it can be analyzed.
- The protocol analyzer may be unable to open a large trace file, or may run very slowly when it tries to open one.

When do you need a Network Recorder?

It is getting ever more important to have the whole picture that includes the payload of packets to resolve problems. Here are a few situations that especially need the help of a good Network Recorder:

- During data center consolidation or virtualization. Less servers or data centers will be handling more traffic. There will be increased traffic going into fewer network segments that operate at very high speeds, up to 10 Gbps with high rates of utilization. The traffic from such segments quickly overwhelms the traditional analyzer's capture buffer, and very little traffic is kept for later in-depth analysis.
- Networks are more stable but there are more problems that occur intermittently and can occur at any time. The only way to be sure of finding the offending packet(s) is to capture and store all of them.
- When new applications are deployed, unexpected behavior happens because of interoperability issues between different application tiers or incompatibility with configuration of network interconnecting equipment: packet partition by gateway, delay expectation from tier to tier and IP port blocked by the firewall. Root cause analysis of these problems require not only response time measurement but detailed analysis of the payload.
- There are attempts to gain unauthorized access to the network. Even the best IDS/IPS will miss some of the intrusion. These often occur outside of normal working hours, and might only come to light if all the packets are captured and stored. Network security and operation teams need to understand the methods used by the intruder by reviewing the traffic payload so that proper countermeasures can be made to block future unauthorized access.
- Other unexpected events such as application performance problems caused by moving assets across VM which starts a broadcast storm and cripples the application and even the network.
- Some employees are making inappropriate use of your company's network by downloading and watching streaming video.

You need to assess whether this excess bandwidth consumption is impacting productivity or placing unacceptable strains on the network. Being able to reconstruct the actual video content would help deliver impact answers and provide evidence for corrective actions.

A simple analogy

There is a difference between simply knowing that a problem exists and actually finding the root cause of that problem. Consider this situation. You park your car in the parking lot of a shopping center and go inside to make a few purchases. When you return to your car, you find that one of the doors has been severely dented and there is no note left behind. You know that you have a problem, but that's all you know. Now consider how the situation might be different if there were one or more security cameras covering the area. By replaying the video from the security cameras, you are able to see that a truck has backed into the door, and you have the license number of the truck. You now have enough information to pass on to your insurance company, who can track down the driver and work out a settlement. The security cameras in this situation are analogous to the Network Recorders on your network.

Risks that arise from not having the right Network Recorder

Not having a Network Recorder, or having one that lacks certain key features, can result in these problems:

- **False positive –** there appears to be a problem, but it would turn out to be benign if you could only reconstruct the full transaction in detail.
- **False negative –** a problem goes undetected because some of the evidence is lost.
- Functional teams engage in finger pointing ***("it's not us, it's them")*** because there is not enough evidence to pinpoint the cause of a problem.
- **Intermittent problem –** a problem is detected, but by the time a portable analyzer is brought to the offending network segment, the problem is not happening.
- **No user friendly analysis capability –** there are enough packets stored, but the desired information cannot be found because the Network Recorder does not provide a quick and easy way to retrieve the desired information from the huge quantity of stored packets.

Key points to consider when choosing a Network Recorder

Visibility	How many links can one recorder connect to and what kind of topology can it link to?
Performance	What is the throughput to disk (not to memory) with no packet loss? How much will turning on real-time monitoring or data analysis affect the throughput?
Capacity	Is the storage specified based on raw storage or real data storage available? Is there a way to filter or slice traffic so that only relevant data is stored?
Redundancy	Is RAID 5 or 10 used? If not, what happens when the hard disk fails? Will data be lost? How much work does it take to recover the system and/or the data?
Ease of use	How difficult is it to analyze the data captured? Can data collected from different parts of the network be easily aggregated, segmented and analyzed to get to the root cause?

How to mitigate the risks

You can mitigate these risks by having one or more Network Recorders installed. It is important, however, to scrutinize the Network Recorder specifications to ensure that the one(s) you buy are a good match to your needs. Here are some key questions to ask:

- How many points on the network are considered to be mission critical in the sense that poor performance at those points would have a serious adverse effect on the business? Consider installing enough Network Recorders to capture traffic at each such point.
- What is the bandwidth at each point? Make sure that the Network Recorder installed there can capture and store packets at full line rate without dropping any packets.
- How long would you need to capture packets in order to have a good representation of all the events that can occur? Multiply this time by a generous estimate of network utilization. Then make sure that the Network Recorder has at least that much storage capacity. Be sure to consider the capacity actually available for storing packets. Some Network Recorders use as much as 30% of the raw disk space for long operating system and other overhead.
- Is there a way to preserve critical data so that it will not be overwritten when the capture disk wraps? Data in a Network Recorder is typically organized in "records" (blocks of data defined by beginning and ending times). Does the Network Recorder have the ability to lock individual records so that they cannot be overwritten?
- Is capture performance vulnerable to conflicts with real-time monitoring or other features? Make sure that there is not an unsatisfactory tradeoff between monitoring and capture functions. This would defeat the main purpose of using a Network Recorder.
- Is there enough redundancy in the hard disk system to assure total capture in the event of a hard disk failure? For example, a RAID 5/10 disk system is much more reliable than a RAID 0 disk system. Are the individual hard disks easily swappable or need a service technician to replace? This may mean taking the risk of having sensitive data exposed.
- Is there an effective hardware filter capability that can restrict capture to specific kinds of packets that you may be watching for? When the tester is monitoring the network through a SPAN port, sometimes a packet may appear multiple times as it transverses in and out of the switch. Does the tester have the mechanism to de-duplicate the frame during capture – saving capacity and confusion?
- Are there display filters that can be applied to postcapture analysis, so that the screen is not full of irrelevant data that makes it hard to see your specific area of interest? For example, are there filters for specific kinds of VoIP traffic, specific caller and callee based on their ID, and/or VoIP-specific problems? Is there a pattern-matching capability that can isolate the flow that contains a pattern in one of the packets in the flow?
- Is there a user-friendly analysis capability that makes it easy to see results in a self-evident display? This is important, because it assures that you don't need a network expert to use the Network Recorder.
- Can multiple Network Recorders be accessed and controlled from one or more remote locations? This helps you get a complete picture when problems involve more than one network segment.
- Can information gathered from multiple network segments be merged and correlated? Look for a sophisticated multi-segment capability. Be sure that packets are stored with precise (nanosecond) timing information, so that data from different segments can be properly synchronized.
- Are there both rackmount and portable versions available? In general, you should have rackmounted Network Recorders installed on your mission-critical segments, and portable Network Recorders available to be connected to other segments when those segments become relevant to an investigation.

Summary

There can be serious problems that pose major risks to your network, but sometimes these problems occur rarely or are intermittent. A Network Recorder is the most valuable tool you can use for detecting and analyzing such problems. However, it is important to carefully scrutinize the specifications before buying one or more Network Recorders. This white paper is written to help you select the right Network Recorder for back-in-time analysis for identifying unexpected events and solving intermittent problems on your network.

Fluke Network provides a line of Network Time Machine™ products. These are Network Recorders with a variety of capture speeds and storage capacities. Both rackmount and portable versions are available.

For more information visit: **www.flukenetworks.com/ntm**

Back-in-Time Application-Centric Forensics Analysis from Fluke Networks

Using a unique, application-centric approach to network forensics, the Network Time Machine™ (NTM) and ClearSight™ Analyzer (CSA) from Fluke Networks simplify and expedite root cause identification. The Network Time Machine (NTM) is a best-in-class, stream-to-disk product that records network traffic, then indexes and categorizes the data. The NTM Atlas software lets you rewind and review the events and background information to extract the data you need to the built-in ClearSight Analyzer*. The ClearSight Analyzer is integrated with the Network Time Machine to provide an intuitive, easy-to-use interface for unparalleled application-centric analysis to provide quick answers.

With the NTM and CSA you can record, identify, and analyze current and past network traffic to view activity as it happens or go back days or weeks to quickly:

- Resolve application performance problems without looking at packets
- Back-in-time isolation of the root cause of intermittent application events
- Provide evidence to trace the sequence of events leading up to critical performance events, and security or compliance issues
- Troubleshoot issues anywhere from the application level to the packet level
- Debug equipment and application performance before rolling out new solutions

To learn more about Back-in-Time Network Forensics Analysis, visit: **www.flukenetworks.com/ntmresources**

*CSA software is integrated in NTM and is also available separately to install protocol analysis capabilities on a PC.

Contact Fluke Networks: Phone **800-283-5853** (US/Canada) or **425-446-4519** (other locations). **Email: info@flukenetworks.com**.

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.

Printed in U.S.A. 07/2010 3835642B D-ENG-N