

Network Monitoring

RMON-Based vs. Localized
Analysis

White paper



www.niksun.com

NetVCR and NIKSUN are registered trademarks of NIKSUN, Inc.
NetReporter, NetDetector, and NetX are trademarks of NIKSUN, Inc.

Copyright © 2002 NIKSUN, Inc.

This publication is protected by International Copyright Law. No part of this publication may be reproduced, stored in a retrieval system, translated, transcribed, or transmitted in any form, or by any means manual, electric, electronic, electromagnetic, mechanical, chemical, optical, or otherwise, without prior written permission from NIKSUN, Inc. NIKSUN makes no warranty of any kind with respect to this material and disclaims any implied warranty of merchantability or fitness for a particular purpose.

NIK SUN, Inc.
1100 Cornwall Road
Monmouth Junction, NJ 08852
USA
Telephone: (732) 821-5000
Fax: (732) 821-6000
Customer Support: (888) 821-2003
E-mail: info@niksun.com

Table of Contents

Introduction	4
Remote Monitoring.....	4
Localized Analysis.....	4
RMON-based vs. Localized Analysis	5
Accuracy and Reliability	5
Third Party Management	5
Data Storage and Analysis Capability	6
The NetVCR Solution	7
Scenario 1	7
Scenario 2	8

Introduction

As enterprise networks grow larger, the network becomes more complex. Network management becomes more crucial and network bandwidth becomes a premium. In order to maintain and deliver high quality of service to end users, network performance and usage must be monitored constantly and potential faults must be dealt with proactively. As network administrators face the challenge of allocating scarce resources across the network and ensuring efficient, cost-effective usage, they need state-of-the-art network performance monitoring technologies and tools for confronting these issues. Two approaches for dealing with network monitoring can be utilized: Remote Monitoring Based (RMON based), aid in establishing centralized management and analysis of network data and Localized Analysis, where network-monitoring devices perform their own local, in-depth analysis of network data. A few key issues differentiating the two methods are discussed. We will also demonstrate how NIKSUN[®] NetVCR[®], a localized analysis with RMON support, offers a unique solution to network monitoring

Remote Monitoring

RMON is a standard Management Information Base (MIB) that defines a set of statistics and functions that can be exchanged, via Simple Network Management Protocol (SNMP), amongst the various probes and console systems deployed across the network. SNMP facilitates communication between console managers and probes in order to provide network fault diagnosis, planning and performance tuning information. The more recent RMON II provides statistics about the traffic for layers above the MAC layer so end-to-end network application layer traffic can be monitored. There are nine RMON groups of monitoring elements (statistics, history, alarm, etc.) with each one providing specific information to meet typical network-monitoring requirements. Typically, various probes support all RMON MIB groups. However each of the RMON groups is optional so network administrators have increased freedom in selecting specific probes and consoles that meet their particular needs. The NetScout probe is one of the well-known RMON based network monitoring devices.

Localized Analysis

In localized analysis, devices retrieve data from the network but do not export it to a centralized manager. Consoles strategically distributed across the network non-intrusively tap traffic passing through each network “checkpoint” gathering and storing information in its database. With network monitoring data stored locally, performance analysis and troubleshooting can be done immediately. Therefore network administrators can quickly detect, isolate and diagnose potential and actual network problems before they escalate to critical situations. NIKSUN NetVCR is one of the most popular localized analyzers.

RMON-based vs. Localized Analysis

Accuracy and Reliability

RMON-based monitoring systems derive their network data from periodic polling of the network. In this scenario, the centralized console manager basically requests data at set intervals from each of the probes dispersed throughout the network. Essentially, RMON-based systems retrieve and analyze their data external to the source due to the necessary export from probe to console. Certain probes do not perform well with frequent polling, so the administrator must increase the duration between polls. A longer duration between polls means short network aberrations may go unnoticed. Basically, RMON-based systems may not account for all the packets going across the link due to their smaller capacity. RMON values are stored in 32 bit registers that limit the count value. For example a 100 Mbps Fast Ethernet Network running at 10 percent load will reset to zero after an hour of activity. Consequently, there exists the possibility that the data being obtained may not provide an accurate assessment of actual network health. Furthermore, RMON-based systems mainly report statistical information and may not support full packet capture due to its design nature. Therefore, more in-depth analysis cannot be performed when trying to identify the specific causes of network outages.

Though most localized analyzers, such as NetVCR, support RMON-based polling, they can function independently without connecting to a central management device. Network traffic can be retrieved and analyzed locally at the source of the localized analyzer. Without the need for periodic polling, network diagnostics are based on real-time network traffic rather than time-delayed information. More intermittent network deviations can be detected and alarms and traps would be sent to the network administrator for appropriate action.

Third Party Management

The need for third party management tools is intrinsic to the design of RMON based network monitoring systems. A centralized third party manager is essential to analyze the data collected from the various probes deployed throughout the network. In general, RMON probes do not possess the capability to perform in-depth analysis of the data collected from the network. Statistical data must be sent to some control console from the probes in order to extract any meaningful statistics from the traffic passing through the network. On one hand this is beneficial because data can be aggregated to provide a full view of the network landscape. Each probe provides its data to contribute to the overall outlook of the network. However, there is also an additional layer (delay - approximately 1 polling interval, i.e. 15 minutes) between the network administrator and network data before any analysis can be conducted. In essence, the RMON probes act in a similar fashion to "dummy" terminals lacking the ability to execute complex operations independently.

Although network-monitoring probes that locally analyze data are generally capable of working with third party management tools, they do not rely on third party management tools for performance analysis and troubleshooting. Instead the probes across the network each act as controllers for their own segment of the network. In this system,

devices have the capability to perform their own independent and immediate analysis of network traffic. Without the need to export network data to a third party management console, analysis can be done more quickly. Network administrators can isolate problems to specific regions of the network, but will have more difficulty defining network wide operations.

Data Storage and Analysis Capability

RMON-based monitoring systems do not have (or need) extraordinary data storage capacity. With the periodic export of data to a console manager, it is unnecessary to maintain sizable storage at each probe. Relaying large amounts of data to a centralized console would not only use valuable network bandwidth but also add to the overall network traffic when sent in-band. RMON-based systems support short-term storage of data to provide primarily statistical information about the network.

On the other hand, increased data storage is a possibility in local analysis. Since vast amounts of data do not need to be sent to any other console there is no concern for impeding network performance. Having large data storage capacity can also facilitate the implementation of full packet capture for a more refined analysis of network data. Additionally, large storage allows for historical analysis to facilitate network trending and performance tuning.

The NetVCR Solution

RMON-based systems and devices that locally analyze network data offer administrators two distinct options for monitoring network traffic. NIKSUN's NetVCR straddles the line between these two approaches and offers a hybrid solution that maximizes the benefits of both.

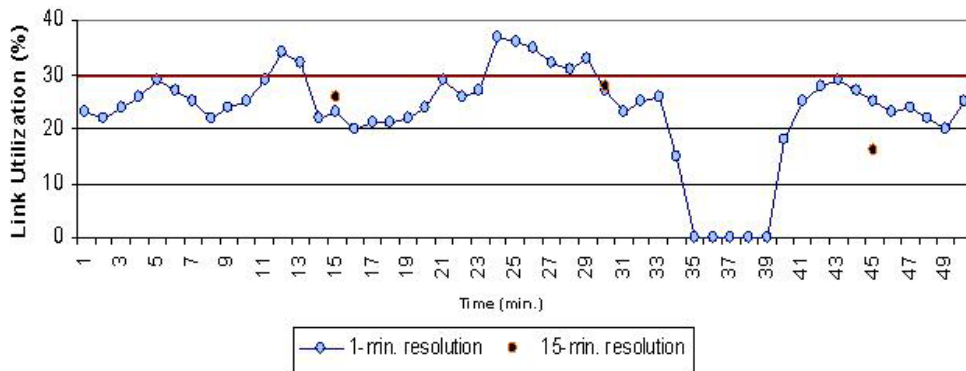
NetVCR functions primarily as a localized analysis device, but has the versatility to act in the role of an RMON probe. In contrast to other RMON based-monitoring systems, NetVCR efficiently handles short polling intervals to provide a more precise image of the network and generates RMON data from real-time network traffic as opposed to time-delayed information retrieved only at each lengthier polling interval. This enhanced efficiency allows more frequent polling and better utilization of RMON data. Ephemeral deviations from regular network conditions can be caught and dealt with appropriately by the network administrator.

The following two scenarios illustrate how shorter polling intervals can provide a network administrator the most accurate statistics about the network. These cases demonstrate examples of link utilization and network throughput.

Scenario 1

An organization seeks to maintain the link utilization less than 30%. With data collected on 15-minute intervals using a RMON-based device, there are no exceptions detected. However, when NetVCR polls the data every minute, there are two aberrations detected with 8 minutes or 16% of the monitored time outside the desired profile.

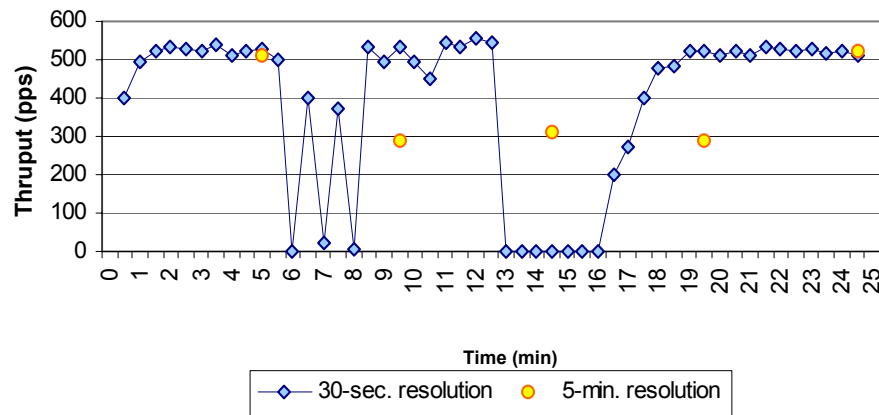
Figure 1: Link Utilization plotted over Time



Scenario 2

The network administrators are keen to ensure that their links are not flapping (rapidly changing from an up state to a down state and vice versa). As such, they establish a delta alarm is to be triggered when the lower threshold of the mean throughput is -300 pps or the upper threshold is 200 pps. When data is collected every 5 minutes from a traditional RMON-based probe, no alarms are triggered since the deltas were -224 , 26 , -24 and 223 . However, data derived every 30 seconds by NetVCR triggered 8 alarms, four falling alarms (at 6, 7, 8, and 13 minutes) and four rising alarms (at 6.5, 7.5, 8.5 and 16.5 minutes).

Figure 2: Thrupt plotted over Time



Furthermore, NetVCR supports full packet capture for increased granularity in analysis of network outage. Network administrators can determine which packets caused the problem and their content. Additionally, NetVCR allows access to the data that initiates alarm conditions by sending trap messages with a link to the NetVCR analysis screen. This allows network administrators to more rapidly analyze alarms, dismiss false-positives and to fine-tune the alarm configuration. NetVCR is designed in such a way as to provide network administrators with the most complete and accurate statistics in an efficient manner.

In addition, NetVCR also accommodates exporting data to third party network management tools supporting the RMON protocol, including HP OpenView, Concord eHealth and NetScout's nGenius Real Time Monitor. Combined with its increased efficiency for utilizing RMON data, NetVCR can provide network wide analysis without concerns of less accurate data. Moreover, NetVCR technology can also operate independently of third party analysis tools. NetVCR has its own detailed analysis and troubleshooting tools so problems can be narrowed down to specific segments of the network quickly. NetVCR demonstrates the scalability for larger networks and the flexibility to independently analyze network data or operate as an RMON probe.

With regards to storage capacity, NetVCR is unparalleled in the market. Most network monitoring systems support data capture in the megabyte range, where NetVCR far exceeds that amount by supporting full packet capture up to 1TB. Having this large storage allows for historical analysis of network traffic. NetVCR can go back days, weeks or even months for post event analysis and future network trending. Current

network anomalies can be compared against past network traffic for a thorough and complete analysis.

Overall, NIKSUN's NetVCR offers one of the most comprehensive solutions available. With network landscapes perpetually changing and companies having a myriad of needs, it becomes essential to have a product flexible enough to meet the challenges presented. NetVCR can either utilize RMON or perform local, independent analysis in an efficient manner to achieve peak network performance. Whether it be localized or centralized management, NetVCR's robust design affords it the ability to adjust to the different specifications of multiple networks and provide all the necessary information to manage service levels and enforce quality of service.

Disclaimer

All the data was generated to the best of our knowledge as of March 19th, 2002. Conditions may have changed since that date.