Monitor the core and troubleshoot the access layer with integrated network analysis solutions

Network change is constant. New technologies and applications require infrastructure changes and affect performance. In this constant state of change, you need to deliver a high level of network performance and quickly solve problems.

In this white paper, you'll learn how to plan for new application deployment, manage against internal security threats, diagnose network problems, prove it's not the network, and analyze application problems.

Table of contents

FLUKE networks

Introduction

Today's networks are typically very stable. The problem is they aren't static. Management and users are constantly demanding new technologies, new services, and better performance, which inevitably require changing infrastructure, deploying new applications, and dealing with security. All these, together with the need to troubleshoot network and application performance issues when they arise means you need to be able to clearly see all aspects of your network to accurately assess the impact of adding new technologies and services and to make sure it is delivering maximum performance with what you already have.

As an IT professional, you need to keep your finger on the pulse of the network 24/7 and this task can be made easier by:

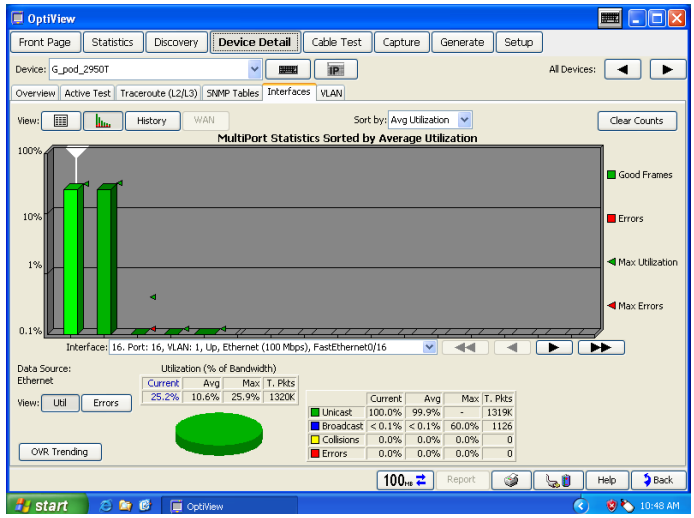
- Knowing the "normal" operating conditions for your network. This should be monitored in the core and must include information on:
  - Traffic levels
  - Protocols in use
  - Number of hosts and where they are connected
  - Switch performance including port utilization and error rates
  - Router and WAN link performance
- Establishing alert thresholds to warn you of potential problems
- Being able to identify anomalous network events such as a device losing connectivity and be notified of such an event

In addition to core network monitoring, you also need to be able to diagnose network problems, including the elusive intermittent problems, prove its not the network and analyze application problems at the same time ensuring network integrity from internal security threats and plan for new application deployment.

Baseline information

The initial baseline information is essential as it can be used as a reference for future comparisons and allows network professionals to potentially detect problems before they significantly impact network performance. Whether a problem is detected before network performance is degraded, or, whether the users report it, network professionals need to quickly identify the source of the problem and subsequently correct that problem.

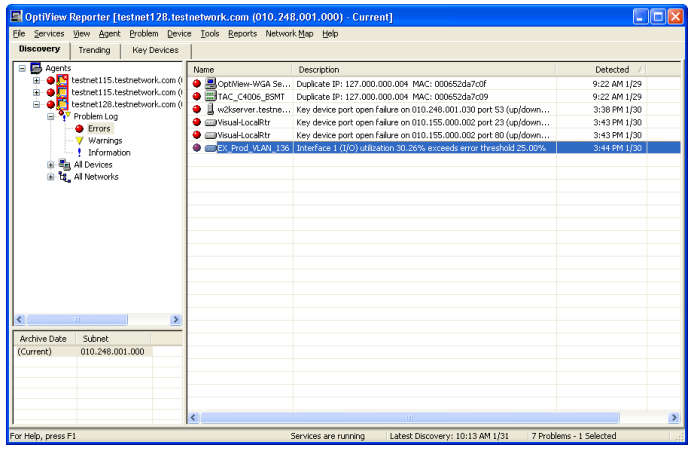
In order to perform this task efficiently, it is necessary to understand the network and also the applications running on it. When troubleshooting problems, you need not only to understand what symptoms you are observing on the network, but sometimes what you are not observing. The fact that you do not see something you expect in the traffic pattern can provide indicators to the source of the problem, and, more importantly, the ability to observe what is occurring in the network core and the performance at the access layer can often speed problem resolution. This is where an integrated approach is required, an "always-on, always available" analysis appliance in the core to monitor critical parameters, and a portable analyzer with the same capabilities as the core appliance, to deploy for troubleshooting access layer problems.



Switch port statistics

Core device interface trending, alarms and notifications

A network analyzer, when monitoring the core, in addition to generating statistics, and being able to trend performance of critical interfaces, must be capable of recognizing events that may indicate a potential problem. The analyzer should enable configuration of alarm thresholds on utilization and error rates for both warnings and severe error conditions and then generate notifications (Email, pager or SNMP traps) dependent upon which conditions have been exceeded. These alarms need to be set for individual switch ports and router interfaces to provide early warning signals for network performance degradation.



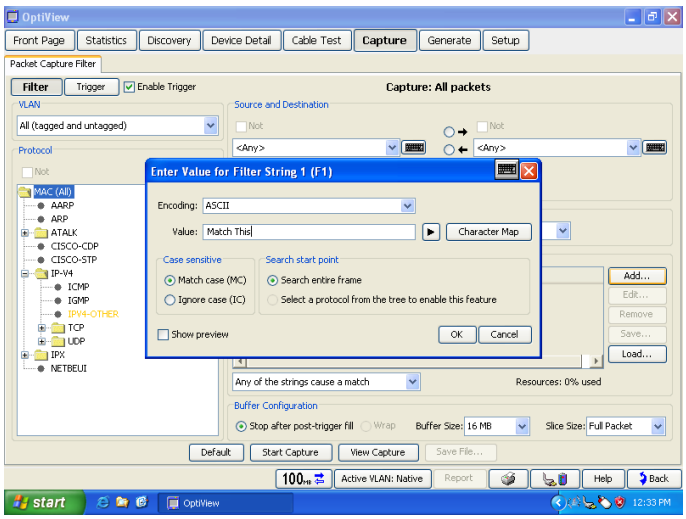
Event notification

Core to remote site connectivity

Monitoring at the core also allows IT professionals to ensure that connectivity and acceptable response times are available over WAN links to remote sites or branch offices. The analyzer can be set up to ping key devices at remote sites and again provide notification to IT staff when there is no ping response. However, since ICMP pings are not treated in the same way as other traffic – routers may be configured to forward them at a lower priority than other traffic or even block them completely – the ping packets can easily be lost in transit and therefore trigger false notifications. A better method of determining remote site connectivity and transit time is to configure the analyzer to open a specific TCP port on a remote device and then report success or failure of the port opening together with the response time which will include network round trip time and the time taken to open the port on the host device.

Intermittent problems

When intermittent problems occur, most IT professionals turn to packet capture to diagnose the problem therefore the analyzer must provide advanced triggering and filtering to capture the traffic before, after or around the event occurrence and ensure the event is captured the first time to avoid doing random traffic captures that may not contain anything of interest. To capture a specific event the analyzer must inspect the contents of each packet to see if it matches a pattern or error message string which is indicative of the event occurring. The key to success is that string matching has to be performed in hardware in real-time with line-rate gigabit capture to ensure all the relevant packets are captured – after all, you can't analyze packets that were never captured.



Free string match

Application problems

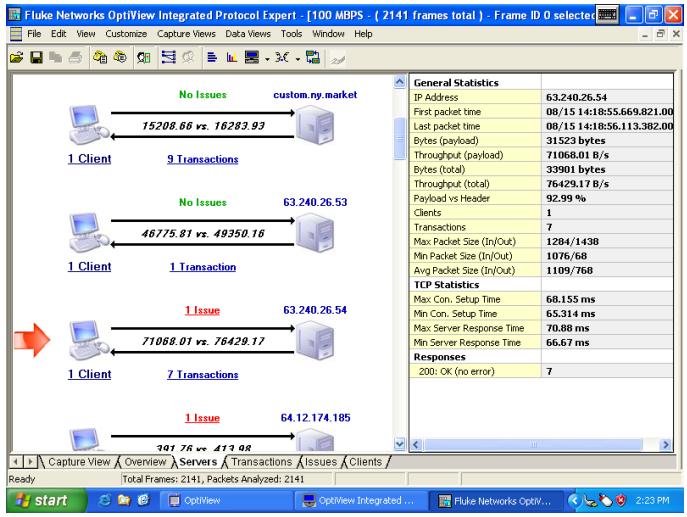
As every network professional knows, users complain about a slow network when it's often an application that's sluggish. Yet because it's initially perceived to be a network problem, it's the IT professional who is charged with determining the actual source of the slowdown. Some companies report that up to 90% of their troubleshooting time is spent proving a problem is not the network. And the two are often intertwined: Network issues can affect application performance, for example, making diagnosis that much more complex.

The challenge isn't only determining the source of the slowdown, however. Since poor performance impacts user satisfaction and even business productivity, IT professionals must deal with any issues rapidly and efficiently. The faster you can find the root cause of problem, the faster it can be fixed – whether it's the network or not.

When it comes to performance issues, there are two steps you can take to make diagnosis easier, faster and more accurate: First, understand the common causes of problems, and, second, use the right tool to diagnose them.

When isolating performance problems you need the right tools to provide insight into the entire network, that is where the OptiView Series III Network Analyzers can help – with a fixed appliance at the core and a portable analyzer at the access layer, when you're troubleshooting, you're at an advantage if you know whether you're going after the network or an application. Even if the problem originates with the way an application is designed, the OptiView Analyzers can help determine the problem.

Additionally, the move towards web-based applications has driven many companies towards implementing server farms for their web based and client server applications at the headquarters core. This transition results in breaking up the processing of the data by sharing the load among multiple severs therefore increasing the number of application servers that are available, resulting in faster response times and increased end user satisfaction.



Application connectivity

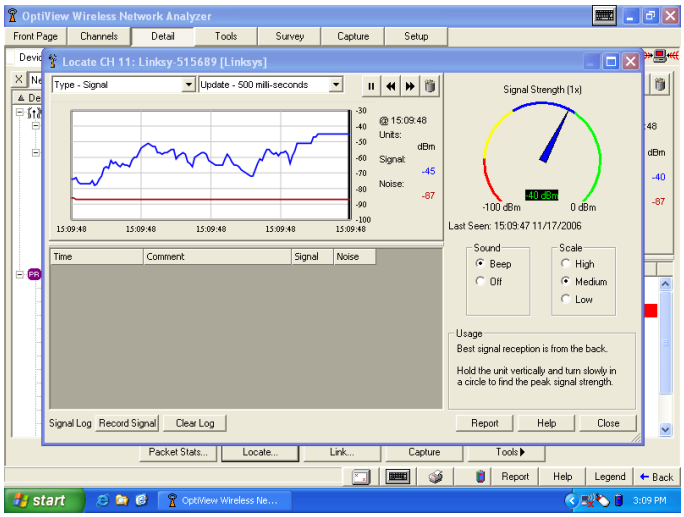
Consequently, this consolidation now makes it essential for IT professionals to know exactly how many, and which servers are involved in application transactions when attemting to diagnose the cause of reported application problems. Again, with a fixed analysis appliance at the core and a portable analyzer at the access layer, with the ability of controlling and viewing data from the core analyzer, diagnosing performance problems is made easier because you have access to client side performance on the portable analyzer and server side performance from the analyzer at the network core.

Securing the network from the inside

With the rise of instant messaging, peer-to-peer applications and an increasing amount of company business being done through remote access, network engineers now must address security threats generated on the inside. Even the strongest firewall can't keep out a growing problem: employees using unauthorized devices and applications that inadvertently create security threats. Whether it's a wireless access point brought in from home or a seemingly innocuous exchange of instant messages, employees are inadvertently compromising security.

The new challenge for network engineers is twofold: monitoring the network for unauthorized access points that could cause a breach in security and focusing attention on suspected trouble spots on a case-by-case basis. Security is a never-ending battle. But it's one of many demands on a network engineer's time and resources. What's needed are analyzers that provide flexibility in addressing both routine maintenance as well as security breaches. Such analyzers add another layer of security protection, while providing other mission-critical functions.

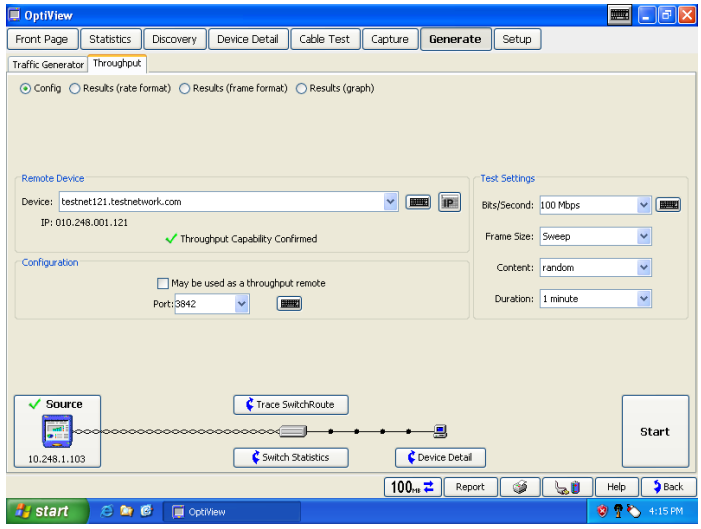
The best way to address the problem of unintended security breaches is to analyze the network on a routine basis. That requires deep packet inspection at the core to identify peer-to-peer applications, Instant Messengers and other unauthorized applications together with the use of a portable wired/wireless network analyzer to walk the campus to identify rogue access points – all which must be performed on a regular schedule.



Locating rogues

Network performance validation for new application deployment

Deployments of new applications can provide major challenge to IT professionals since even the most seemingly simple changes could significantly affect the network performance. Assessment of the current network performance is sometimes forgotten the deployment of a new application could affect the stability and integrity of the network and potentially disrupt communication and critical network services. By using both the OptiView Series III Integrated Network Analyzer and the OptiView Series III Workgroup Analyzer, you can easily assess your network readiness for new application deployment and be confident that the new project deployment will be successful.



Throughput testing

Prior to deploying new applications, it is essential to determine that your current infrastructure is capable of handling the additional traffic. To accurately measure existing infrastructure performance and determine if there is the possibility of packet loss and also the direction of the loss, the OptiView Network Analyzers may be used to execute an Internetwork Throughput Test. For example with an OptiView Workgroup located at the core and the OptiView Integrated Network Analyzer located at the client side end point of the application, a throughput test can be initiated – at gigabit line rate if necessary – to determine the actual achievable throughput between the two devices and, in the event of packet loss, determine the direction of that loss. Parameters that may be controlled are traffic rate, packet size, packet content and duration of the test. If packet loss is detected, the vendor independent infrastructure analysis capabilities of the analyzers may be used to determine the cause of the packet loss.

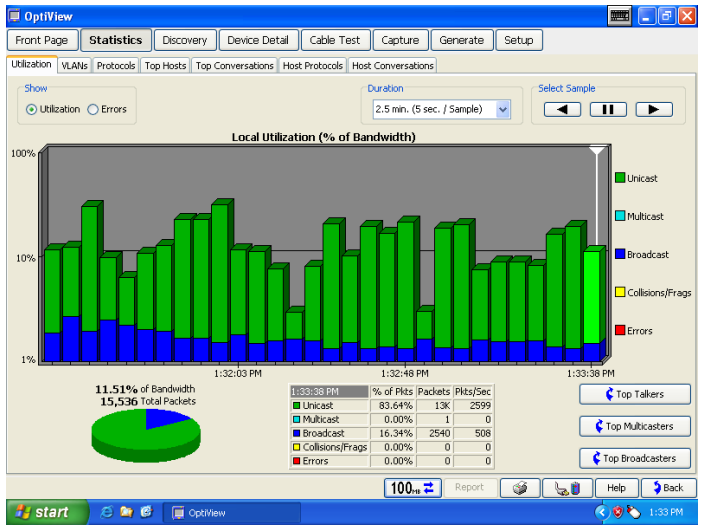
Access layer troubleshooting

The initial step in resolving the problem is to identify and interpret the symptoms:

- Has the event occurred previously?
- Does the problem interfere with critical network operations?
- Does the problem affect a single user or many users?

Then you need to understand the problem:

- Is it a connectivity issue?
- Has a network infrastructure device failed?
- Are network services, DHCP and DNS available and operating correctly?
- Is it a logon problem – is 802.1x authentication operational?
- Are application servers available?



Local utilization

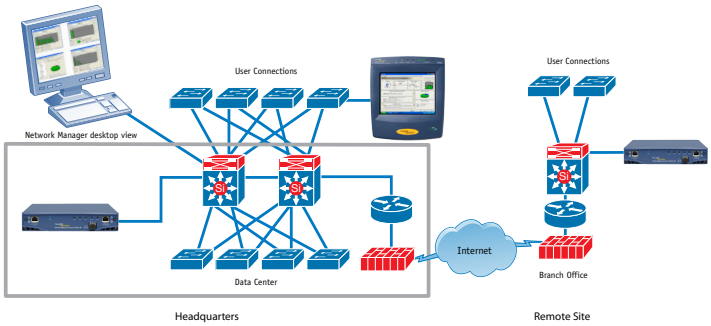
In order to quickly and efficiently troubleshoot these problems you need to be able to:

- Determine where the hosts are connected to the network
- Identify what protocols are being used by the hosts
- Determine whether the necessary application servers be reached from the host location

From here, you can identify whether the problem is with the network, the host or the server. Now if you suspect a network problem you can examine the path between the users and the server and investigate the performance of all the devices in the path using vendor independent infrastructure analysis. For suspected server problems, you can determine whether the server is accessible and the application port can be opened on the server and for a host problem, ensure it is configured correctly to communicate with network services and the relevant application server.

How the OptiView™ Series III Network Analyzers in the core and access layer make monitoring and troubleshooting easier

All the functionality of multiple tools is combined into one device, making core monitoring and access layer troubleshooting easier and faster when engineers no longer have to switch from tool to tool to conduct a full array of tests. In addition, network professionals can monitor critical interfaces in the core and analyze access layer problems with analyzers that have identical user interfaces, reducing training time and providing information – not just data. And more than one person can view the data, with the OptiView analyzer, network professionals can also work together when some staff members are off-site because data can be shared by launching multiple user interfaces on both the Workgroup and Integrated network analyzers for assisted analysis and collaboration during troubleshooting phases.



The OptiView analyzers provide discovery information on network and device problems and identifies protocols in seconds. It also speeds reporting for complete infrastructure documentation. With the OptiView analyzer, network professionals can conduct a complete inventory of all network devices, where they're connected, and which services are running on them. It can do automated mapping, creating maps of the network in its current state. An engineer can plug the OptiView into the network, let it run the discovery, then go through a simple, multi-step process for printing the map. The OptiView Reporter formats discovery data and exports that data to Microsoft® Visio®, so network professionals get the data in a familiar format which can easily be used when troubleshooting problems. Using the OptiView analyzer, network professionals can verify and prove network readiness for network expansions, mergers, consolidations, and upgrades. They can validate and document performance, and verify new configurations to ensure the stability of the network. And they can use the OptiView analyzer to identify VLAN configurations, validate network health, audit switch/router configurations and performance.

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

The business case for an integrated network analyzer

The OptiView Series III Network Analyzers helps network professionals manage IT projects, solve network problems and support IT initiatives, resulting in reduced IT costs and improved user satisfaction. It gives you a clear view of your entire enterprise – providing visibility into every piece of hardware, every application, and every connection on your network.

No other tool offers this much vision and all-in-one capability to help you:

- Deploy new technologies and applications
- Manage and validate infrastructure changes
- Solve network and application performance issues
- Secure the network from internal threats

You'll see where your network stands today and helps you accurately assess its readiness for the changes you need to make now and in the future. Leverage the power of OptiView to give you vision and control of your network. For more information about the OptiView Series III Workgroup Analyzer, visit **www.flukenetworks.com/optiview**.

NETWORKSUPERVISION

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. 2/2008 3276489 H-ENG-N Rev A