

## Fluke Optiview Integrated Network Analyzer

Universeller Spürhund für alle Layer

Der OptiView Integrated Network Analyzer vereint Analysetools für alle sieben Netzwerk-Layer in einem Gerät und verspricht schnelle Fehleranalyse ohne komplexe Bedienung. Network Computing hat das Spitzenmodell mit Gigabit-Schnittstelle und Protokoll-Analysator getestet.

### VON DIRK PELZER

Fehleranalyse und Problemeingrenzung in schnell wachsenden und immer komplexer werdenden Netzwerken sind mit der in vielen Unternehmen verfügbaren Personaldecke kaum noch zu bewältigen. Hinzu kommt, dass nur wenige ausgewählte Spezialisten in der Lage sind, komplexe Tools wie einen Paket-Sniffer zu bedienen und die von ihm dekodierten Datenpakete zu analysieren. Um die geplagten Netzwerkverwalter zu entlasten, hat Fluke mit dem OptiView Integrated Network Analyzer ein Gerät entwickelt, das nicht nur passiv Daten sammelt und analysiert, sondern auch aktiv bei der Fehlersuche unterstützt. So sind Funktionen wie Datenverkehrsanalyse, RMON2-Probe, Datenpaket-Dekodierung, Fernsteuerung über Web und aktive Fehlererkennung in dem mobilen Gerät integriert, das kleiner ist, als ein handelsübliches Notebook.

Je nach Modell findet der OptiView-Analyzer Anschluss an unterschiedliche Netztopologien. Das Standardmodell bietet hier lediglich einen kombinierten 10BASE-T/100-BASE-TX-Connector. Im Optiview Pro kommt noch ein 100BASE-FX-Anschluß hinzu und das Pro Gigabit-Modell verfügt darüber hinaus noch entweder über einen 1000BASE-SX oder einen 1000BASE-LX-Port.

### Autodiscovery sammelt Netzinformationen

Sofort nach dem Einschalten sammelt OptiView Daten aus einer Vielzahl von internen und externen Quellen, wie beispielsweise einem DNS-Server und zeigt die Ergebnisse auf dem integrierten Display an. Der Analyzer sucht automatisch nach allen in dem angeschlossenen Netzsegment vorhandenen Geräten und zeigt diese an. Für die gefundenen Geräte, stellt er darüber hinaus alles an Information dar, was zum jeweiligen Zeitpunkt ermittelbar ist. So versucht der OptiView den DNS-, den NetBIOS-, den IPX-

oder der SNMP-Namen zu ermitteln und anzuzeigen. Das Gerät identifiziert darüber hinaus Router, Switches, per SNMP managebare Hubs, Drucker und SNMP-Agenten.

Dargestellt werden die gesammelten Informationen über einen berührungssensitiven Farbbildschirm und eine graphische Benutzeroberfläche, die den Analysevorgang beschleunigen soll. Über dieselbe auf Java basierte Benutzerschnittstelle, die auf dem portablen OptiView-Analyzer zum Einsatz kommt, können auch bis zu sieben Remote-Benutzer gleichzeitig und voneinander unabhängig mit dem Gerät arbeiten.

### Umfangreiche Statistikfunktionen

Unter Zuhilfenahme der ermittelten Daten, stellt der OptiView-Analyzer zahlreiche Statistiken und Fehlerprotokolle zusammen, die Aufschluss über



## Fluke Optiview Integrated Network Analyzer

den Zustand eines Netzsegmentes geben. Die darstellbaren Statistiken können allerdings nicht nur auf den vom OptiView ermittelten Daten basieren, sondern auch aus Historien von Geräten mit RMON- oder RMON2-History-Funktion ermittelt werden. Der Administrator kann dabei das Betrachtungsintervall zwischen zwei Minuten und 24 Stunden frei wählen. Um herauszufinden, welche Stationen die meiste Last erzeugen, stellt der OptiView darüber hinaus auch noch Informationen über Top Talkers, Top Multicasters und Top Broadcasters zur Verfügung. Wenn der Administrator die Statistiken von der Auslastungssichtweise auf die Fehlersichtweise umschaltet, bekommt er Informationen über die gängigsten Netzwerkfehler, wie zum Beispiel CRC Alignment Errors, Pakete mit fehlerhafter Größe, fragmentierte Pakete und Jabbers. Auf Wunsch zeigt der Optiview auch wieder die Namen und Adressen der Stationen an, die für diese Fehler verantwortlich sind.

Auch für die in einem Netzsegment gefundenen Protokolle zeigt der Optiview interessante Informationen an. So stellt er nicht nur dar, welche Protokolle er ermittelt hat, sondern auch welche weiteren Protokolle beispielsweise in einem TCP-Paket enthalten waren. Das beginnt auf Schicht eins mit dem MAC-Layer und endet auf Schicht sieben mit dem Application-Layer. In Form eines Kuchen-

diagramms kann sich der Administrator zudem anzeigen lassen, welchen Anteil die gefundenen Protokoll am Gesamtverkehr während des Betrachtungszeitraumes hatten. Natürlich gibt es auch bei der Protokollstatistik eine Möglichkeit herauszufinden, welche Stationen im Netz die Top Talker für das jeweils betrachtete Protokoll waren.

### Gängige Probleme im Griff

Als hilfreich für das Troubleshooting erweist sich die Problem-Discovery-Funktion des OptiView. In einem Fenster der Bedienoberfläche des Tools werden dabei alle Stationen aufgelistet, die als problematisch erkannt wurden oder zumindest eine potentielle Fehlerquelle darstellen. Der OptiView unterscheidet hierbei nach drei Stufen, nämlich Errors, Warnings und Information. Unter die Kategorie Error fallen beispielsweise solche Dinge, wie doppelte IP-Adressen, falsche Subnetzmasken, eine mit der Subnetzmaske identische IP-Adresse oder eine vom DHCP-Server angebotene IP-Adresse, die bereits in Benutzung ist. Als Warning wird ein Router eingestuft, der nicht antwortet, oder ein Proxy-ARP-Reply für eine lokale IP-Adresse. Als bloße Information wird das Auffinden einer einzelnen Station in einer NetBIOS-Domäne registriert und angezeigt.



## Fluke Optiview Integrated Network Analyzer

Für weitergehende Troubleshooting-Maßnahmen bietet der Analyzer mit Ping, Trace Route und einem bei den Pro-Modellen integrierten Paket-Sniffer noch weitere interessante Werkzeuge. Ähnlich wie das bekannte Kommandozeilentool bietet Trace Route einen Überblick darüber, auf welchem Weg mit einer angegebenen Zielstation kommuniziert wird. Dabei liefert der OptiView Angaben über die Anzahl der Hops, Namen und IP-Adressen der Hops und die benötigte Zeit für jeden Hop. Auf Wunsch zeigt der Analyzer darüber hinaus die System Group, sowie die Routing- und ARP-Tabellen aller Router an, die zwischen zwei Hosts liegen. Als letzte Rettung bietet sich der integrierte Paket-Sniffer an, der in der Lage ist, auch im Gigabit-Ethernet Pakete mit Leitungsgeschwindigkeit einzusammeln und zu analysieren. Um die Zahl der zu sammelnden Pakete zu verringern, hat der Administrator die Option, Filter zu definieren, aufgrund derer etwa nur die Kommunikation zwischen zwei angegebenen IP-Adressen aufgezeichnet wird. Weiterhin einstellbar ist auch die Puffergröße, die zur Aufnahme der gesammelten Pakete dient. Wer nicht das gesamte Paket speichern möchte, sondern nur eine bestimmte Anzahl von Bytes, kann dies über den Parameter Slice Size einstellen. Die Dekodierung der gesammelten Pakete übernimmt entweder der mitgelieferte OptiView Packet Decoder, oder aber ein handelsübliches Netzwerkanalyse-Tool.

### Zur Person

DIPL. ING. DIRK PELZER arbeitet als freier Consultant und Journalist in München. Er betreibt ein Storage Labor für verschiedene namhafte Fachzeitschriften. Zudem beschäftigt er sich mit Speichernetzen und Hochverfügbarkeit.

### Fazit

Obwohl sich das OptiView zu Beginn unseres Tests etwas sträubte und Probleme hatte, konnte das Gerät insgesamt voll überzeugen. Die gebotenen Funktionalitäten sind sehr praxisorientiert und zeigen schnell und auf einen Blick welche Netzwerk-Komponenten tatsächliche oder potentielle Fehlerquellen darstellen. Mit dem OptiView hat es Fluke geschafft einen All-In-One Analysator zu schaffen, mit dem sich die überwiegende Mehrzahl aller Netzwerkprobleme erkennen und beseitigen lassen sollte. Damit ist der Preis von immerhin 31100 Euro für das Spitzenmodell durchaus zu rechtfertigen, insbesondere auch weil bis zu sieben Mitarbeiter gleichzeitig remote mit einem an das Netz angeschlossenen Analyzer arbeiten können.

### Produkt:

## OptiView Integrated Network Analyzer

### Charakteristik:

Netzwerk-Analyse-Tool für Layer eins bis sieben

### Kurzbeschreibung:

Einfach zu bedienender und umfassender Netzwerk-Analysator, der den Administrator bei der Suche nach Fehlern vom Kabel bis hin zum Applikationsprotokoll unterstützt.

Web: [www.flukenetworks.com](http://www.flukenetworks.com)

### Preis:

Von 16900 Euro (10/100 Mbit/s ohne Protokollanalysator) bis 31100 Euro (10/100/1000 Mbit/s inklusive Protokollanalysator)