



Verkabelung

**Alien-Crosstalk-Schutz
per Design**

**Neuer Standard für
Glasfaser-Feldmessung
mit Marktübersicht
Steckersysteme**

Sonderdruck für Network Instruments

Mobiles und stationäres Monitoring

Netzwerkanalyse und Monitoring bleiben trotz zuverlässiger und redundanter Netzwerke ein wichtiges Thema, da sie in komplexer werdenden Netzwerkstrukturen den nötigen Einblick bieten. Es liegt auf der Hand, dass sich mit entsprechender Messtechnik Ausfallzeiten oder Leistungseinbußen und die damit verbundenen Kosten minimieren lassen. Außerdem kann der Verantwortliche das Netzwerk sowie die darauf basierenden Applikationen besser planen und optimieren, wenn bekannt ist, wie die derzeitige Auslastung aussieht.

Bei der Wahl der richtigen Strategie für eine Netzwerkanalyse spielen viele Faktoren eine Rolle. Ein wesentlicher Punkt dabei ist, welche Techniken zur Verfügung stehen, zum Beispiel SNMP, RMON, Netflow oder Paketanalyse. Zusätzlich ist die richtige Wahl der Messpunkte und der Anschlussart eines Analysators wichtig und schließlich, ob man sich für eine eher reaktive oder proaktive Art der Analyse entscheidet. Das Konzept der so genannten retrospektiven Analyse ist eine neue Art der Vorgehensweise: Dabei zeichnet das System alle relevanten Parameter laufend auf und sorgt dafür, dass sie bereits im Störfall mit den historischen Daten zur Verfügung stehen. Dies kann dem Anwender bei intermittierenden Problemen eine große Zeitersparnis bringen.

Bei der richtigen Wahl der Mess- und Analysensysteme ist es wichtig, exakt zu beachten, welche der genannten Techniken unterstützt werden. Dies gibt Aufschluss darüber, in welchen Bereichen und bei welchen Problemen diese Systeme weiterhelfen. Die einzelnen Ansätze schließen sich dabei nicht gegenseitig aus, sondern ergänzen sich und sollten parallel zum Einsatz kommen. Der Netzwerkanalysator Observer von Network Instruments kann als Beispiel dafür dienen, wie Hersteller mehrere Funktionen in einem Gerät zusammenfassen.

Der Observer beherrscht SNMP, RMON, Netflow/Sflow und Paketanalyse mit einem entsprechenden automatisierten Expertensystem, das die Auswertung und Analyse vereinfacht.

Switches und Router liefern erste Ansätze bei der Fehlersuche

Über das SNMP-Protokoll empfängt der Observer durch Fernabfragen eines Switches oder Routers wichtige Netzwerkparameter wie Auslastung, Broadcast und Fehler auf OSI-Ebene 2 – beispielsweise defekte, zu lange oder zu kurze Pakete und Kollisionen. Mithilfe der SNMP-Managementkonsole, die solche Statistiken sam-

melt, erhält der Administrator eine schnelle Übersicht über Netzwerkengpässe, zu hohen Broadcast-Level oder Broadcast-Stürme, defekte Netzwerkkarten oder Schnittstellen und Hinweise auf „Auto-Negotiation“-Probleme im Netzwerk. Dabei handelt es sich nur um Netzwerkeckdaten. Er erhält diese allerdings mühe-los aus der vorhandenen Infrastruktur von einem zentralen Punkt aus, und daher sollte eine solche übersichtliche SNMP- und RMON-Konsole im Analysekonzept niemals fehlen.

Gefundene Engpässe werfen gleich weitere Fragen nach deren Verursacher auf. Durch welche Nutzer und welche Applikationen wurden diese verursacht? Antwort auf diese Frage liefern auf die einfache Art und Weise neuere Techniken wie Netflow und Sflow. Dabei werden solche Informationen über eine Observer-Probe direkt aus dem Switch oder Router gesammelt. Außer einer Konsole ist keine zusätzliche Hardware erforderlich, was die die bereits vorhandene Infrastruktur nur effizienter ausnutzt.

Paketanalyse geht ins Detail

Bei vielen anderen Fragen sowie bei Netzwerkstrukturen, die Netflow/Sflow nicht unterstützen, hilft ein direkt an die zu analysierende Verbindung oder an den jeweiligen Switch angeschlossener Analysator weiter. Dabei spiegelt der Switch die zu analysierenden Daten auf den Port, an dem etwa der Observer angeschlossen ist. Da es wegen Kosten und vermehrtem Verwal-

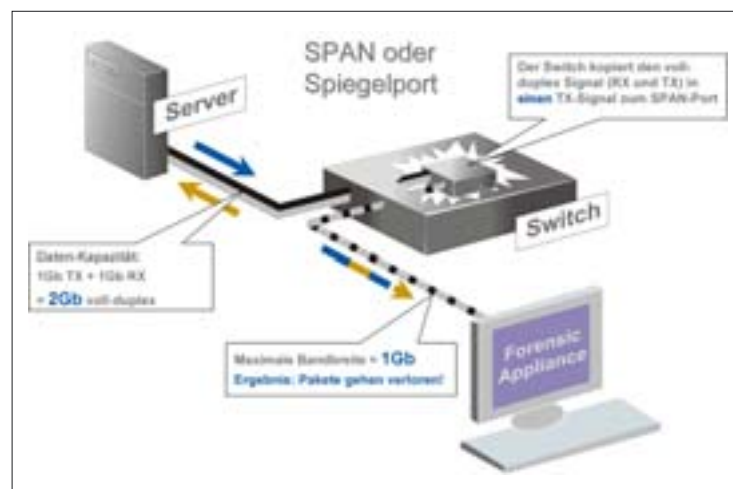


Bild 1. Port-Spiegelung einer Gigabit-Verbindung

tungsaufwand nicht überall und an jeder Verbindung möglich ist, eine Detailanalyse mit einem dedizierten Gerät vorzunehmen, ist ein durchdachtes Konzept notwendig, das die Aufstellung und Anzahl der Messpunkte und deren Anschlussart berücksichtigt. Ein direkt an den jeweiligen Datenstrom angeschlossener Analysator kann die Daten der OSI-Schichten 2 bis 7 auswerten und eignet sich daher für die verschiedensten Aufgaben. Dazu zählen die Protokollanalyse, Laufzeit-, Applikations- und Applikations-Performane-Analyse, forensische Analyse sowie neuerdings auch die Qualitätsuntersuchung von VoIP.

Reaktiver Ansatz scheitert oft

Der oft noch praktizierte reaktive Ansatz, ausschließlich mit portablen Messmitteln auf Netzwerkfehler zu reagieren, nachdem ein Problem bereits entstanden ist, scheitert in der Praxis sehr oft. Einmal liegt es am Faktor Zeit, an der es durch Personaleinsparungen mehr denn je mangelt – vor allem jedoch auch am fehlenden Wissen und Können, globale Abläufe im Netzwerk zu erfassen und zu verstehen.

Ein permanent installiertes Analyse- und Monitoring-System ermöglicht eine viel proaktivere Arbeitsweise und fördert das Verständnis der netzwerkinternen Abläufe. Viele Applikationen sind in heutigen Netzwerken zentralisiert. Daher können die Messpunkte auf einige wichtige Verbindungen beschränkt werden, ohne den Überblick auf das Wesentliche zu verlieren. Dabei sollte der Administrator das Augenmerk auf wichtige Server- und zentrale Backbone- und Router-Verbindungen legen. Dort laufen die Daten des gesamten Unternehmens zusammen, und er kann die verschiedensten Störungen erkennen oder sogar proaktiv auf diese reagieren, bevor sie sich zu echten Problemfällen entwickeln. Das Expertensystem überwacht das Netzwerk permanent auf Fehler und durchsucht die Datenströme auf Anomalien. Portable Messmittel sind zwar auch weiterhin nötig, jedoch ist deren Einsatz nur dort notwendig, wo mit den zentral installierten Systemen keine

Untersuchung möglich ist. Falls die portablen und verteilten Messmittel aus einer Hand kommen, ermöglicht die gleiche Benutzeroberfläche und die vertraute Arbeitsweise, Probleme viel schneller und geübter anzugehen und die Schulungszeit deutlich zu verkürzen.

Port spiegeln oder TAP?

Ebenso ausschlaggebend ist die Frage, wie man einen Analysator an die zu überwachende Verbindung anschließt. Der Observer lässt sich sowohl über eine Port-Spiegelung (SPAN-Port) als auch über einen in die Verbindung eingelagerten TAP

eignet sich diese Methode nicht für höher ausgelastete Voll-Duplex-Verbindungen. Ab spätestens 50 Prozent Link-Auslastung, das heißt 1000 MBit/s bei Gigabit Ethernet und 10.000 MBit/s bei 10 Gigabit Ethernet, kommt es unweigerlich zum Paketverlust, was die Messdaten verfälscht.

Erfordernisse im Voll-Duplex-Betrieb

Die Ursache dafür ist, dass der Switch den Sende- und Empfangskanal nur über einen Sendekanal zum Analysator weiterleitet. Drittens sind bei einer Port-Spiegelung die zeitlichen Informationen verfälscht, da im

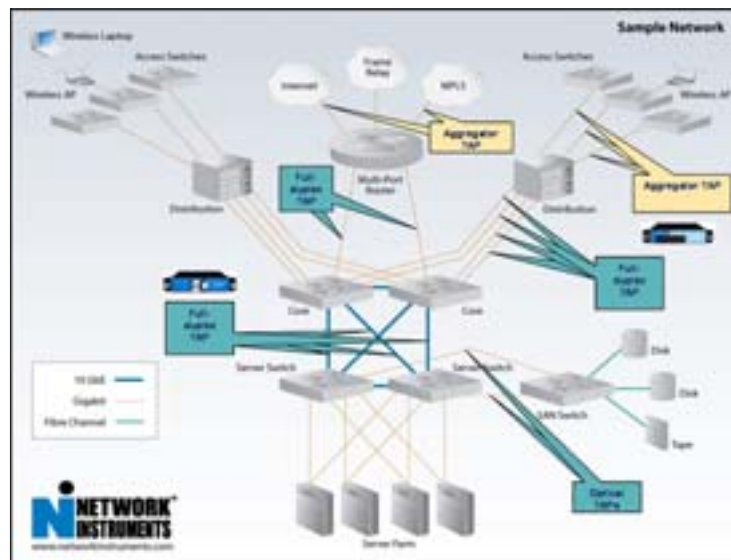


Bild 2. Wahl der Messpunkte mit Hilfe von Netzwerk-TAPs

(Test Access Port) anschließen. Dazu dienen mehrere Eingänge des Analysewerkzeugs, die auch Verbindungen mit Load Balancing unterstützen und bei denen der Datenstrom auf mehrere physikalische Verbindungen aufgeteilt wird.

Die Port-Spiegelung ist die einfachste Methode, die zudem fast jeder Switch unterstützt. Die Daten der zu beobachtenden Verbindung werden dabei auf den Port kopiert, an den der Analysator angeschlossen ist. Andernfalls würde der Analysator nichts außer Broadcast und Multicast erkennen. Die Port-Spiegelung kann jedoch schnell an ihre Eignungsgrenzen stoßen. Erstens filtert der Switch alle fehlerhaften Pakete heraus, bevor er sie zum Analysator leitet. Damit zeigt der Analysator keine Fehler auf der OSI Schicht 2 an. Zweitens

Voll-Duplex-Betrieb Pakete von beiden Seiten gleichzeitig ankommen und überlagernde Pakete gepuffert und geordnet werden müssen, bevor das System sie weiterleitet. Andererseits reduziert diese Analysemethode die Investitionskosten, da günstigere Halb-Duplex-Hardware oder Software-Probes ausreichen.

Benötigt der Administrator eine präzisere Analyse oder handelt es sich um eine höher ausgelastete Verbindung, bedient er sich eines TAPs (Test Access Port). Diese passiven Netzwerkkomponenten sind in die Verbindungen „eingeschleift“, sie verfügen also über einen Ein- und Ausgang für die Netzwerkverbindung und zwei Ausgänge zum Analysator. Durch diesen permanenten Messpunkt lässt sich der Observer zu jeder Zeit anschließen, ohne dass die Ver-

bindung beeinflusst wird. Auf die zwei Analyseausgänge sind ohne Paketverzögerung einmal der Empfangskanal und einmal der Sendekanal eins zu eins kopiert.

Arbeiten mit TAPs: eine Frage der Ports

Auch fehlerhafte Pakete leitet das System zur Analyse weiter. Da der TAP zwei Ausgänge zum Analysator hat, benötigt der Analysator zwei Eingänge. Eine handelsübliche Voll-Duplex-Netzwerkkarte kann bis zu 50 Prozent der Bandbreite empfangen (1000 MBit/s bei Gigabit Ethernet und

und auf nur einen Ausgangs-Port zusammenfasst. Lastspitzen speichert ein interner Puffer zwischen, und auch Layer-2-Fehler wandern an den Analysator weiter. Soll der Switch nicht durch zusätzliche Aufgaben wie Port-Spiegelung belastet sein, ist ein Aggregator-TAP jedenfalls eine sichere Alternative.

Retrospektive Analysen

In letzter Zeit entwickelt sich mehr und mehr ein neues Konzept bei der Netzwerkanalyse, das auch als retrospektive Analyse bekannt ist. Die bisher behandelten verteil-

Eine aufwändige Reproduktion entfällt

Ein Produktbeispiel ist Gigastor von Network Instruments. Das Ziel ist es, Probleme viel schneller lösen zu können, da deren aufwändige Reproduktion entfällt. Entscheidend bei dieser Art der Analyse ist, dass bereits wichtige Netzwerkparameter im ausgewählten Zeitbereich erkennbar sind, ohne dass man zunächst Gigabytes an erfassten Daten laden muss. Eine Protokollanalyse mit sehr großen Datenmengen ist zu zeitaufwändig und wird daher in den meisten Fällen gemieden. Der direkte Bezug zur Praxis muss auch an dieser Stelle im Vordergrund stehen. Beschwerdeträger im Vordergrund stehen. Beschwerdeträger nämlich etwa ein verärrter User über einen langsamen Datenbankzugriff oder Verbindungsabbrüche zwischen neun und zehn Uhr, kann der Administrator sehr schnell einen Überblick darüber bekommen, was in dieser Zeit vorgefallen ist und anschließend innerhalb von wenigen Sekunden nur die interessanten Daten für die Detailanalyse herausfiltern.

Fazit: Blick auf die wichtigsten Stellen ist notwendig

Durch Echtzeitapplikationen wie VoIP nimmt die Netzwerkanalyse einen neuen Stellenwert innerhalb einer modernen IT-Infrastruktur ein. War es in der Vergangenheit ausreichend, Analysen über eine Port-Spiegelung durchzuführen, ist zum Beispiel zur Analyse des Antwortzeitverhaltens einer Applikation eine Echtzeitmessung direkt im Link unabdingbar. Ein passendes Analysesystem bietet neben vertretbaren Kosten einen maximalen Einblick in die wichtigsten Stellen im Netzwerk und ist für die Zukunft skalierbar.

Aleš Mahler und David Eser/jos

Dipl.-Wirtschaftsingenieur Aleš Mahler ist Regional Sales Manager für Zentral- und Osteuropa bei Network Instruments. Dipl.-Ing. David Eser ist Sales Manager bei Psiber Data.

■ Info: Network Instruments
Tel. 08095/875858
www.networkinstruments.de



Bild 3. Zeitnavigierende Benutzeroberfläche zur Langzeitanalyse

10.000 MBit/s bei 10 Gigabit Ethernet) und 50 Prozent senden. Der Voll-Duplex-Observer verwendet daher keine handelsübliche Voll-Duplex-Karte, sondern basiert auf einer speziellen „Dual-Receive“-Erfassungskarte, die über mindestens zwei Ports auf einer Karte verfügt (auch mehrere Ports für Verbindungen mit Load Balancing). Dadurch ist es möglich, 100 Prozent der Bandbreite, also 2000 MBit/s beziehungsweise 20.000 MBit/s zu empfangen und zu analysieren.

Falls der Nutzer aus Kostengesichtspunkten nicht auf allen kritischen Verbindungen einen Hardwareanalysator einplant, sollte er zumindest diese Verbindungen mit einem TAP versehen, damit er im Problemfall einen Analysator anschließen kann, ohne diese Verbindung unterbrechen zu müssen. Eine interessante Alternative bietet der Aggregator-TAP, der ähnlich der Port-Spiegelung den Voll-Duplex-Datenstrom erfasst

ten Systeme ermöglichen es, in vielen Fällen proaktiv zu handeln und auf Probleme durch deren Expertensysteme hinzuweisen. Die gängige Praxis demonstriert allerdings, dass es durchaus nützlich sein kann, sich mit schnelleren Reaktionsoptionen auseinander zu setzen: Da der Techniker meist erst nach einer gewissen Zeit mit der detaillierten Suche nach der Ursache beginnt oder ein Anwender über sein Problem erst nach einigen Minuten oder Stunden berichtet, steht meist der gesamte Datenstrom nicht mehr zur Verfügung.

Dies ist aber auch gar nicht in jedem Fall sinnvoll: Lösungen, die es ermöglichen, Netzwerkdaten kritischer Verbindungen einer Gigabit- oder 10-Gigabit-Verbindung für Stunden, Tage oder sogar für Wochen aufzuzeichnen und bei Bedarf mithilfe eines zeitnavigierenden Dataming-Systems zu analysieren, sollen Abhilfe leisten.