



Netzwerküberwachung – Voll im Trend liegt derzeit die Tap-Technologie. Sie nutzt nicht nur passive Messpunkte für eine störungsfreie Analyse und das Monitoring im Netz, sondern auch für nachgeschaltete IDS- und IPS-Security-Lösungen.

Test-Access-Ports – kurz Tap oder Taps genannt – stellen einen passiven Messpunkt für die Analyse von Hochgeschwindigkeits-Netzen im Halb- oder Voll duplex-Modus zur Verfügung. Dadurch ermöglichen sie es, den Datenstrom permanent analysieren und überwachen zu können, ohne ihn zu stören oder gar zu unterbrechen. An Taps angeschlossene Messgeräte verhalten sich so, als wären sie inline. Das allein bringt entscheidende Vorteile gegenüber Span- beziehungsweise Mirror-Ports, da die Messung nicht durch unerwünschte oder unentdeckte Fehlerquellen mehr beeinträchtigt werden kann. Außerdem wird über die störungsfreien Messpunkte der Einsatz nachgeschalteter Sicherheits-Technologien möglich.

Taps sind für genaueste Messergebnisse deshalb so zuverlässig, weil die passive Verbindung den Datenstrom niemals unterbricht. Zero-Delay-Technology nennt dieses Prinzip beispielsweise der Hersteller Net Optics, den Systematic, eine Business-Division der Systeam, in Deutschland vertritt. So können Netzwerkadministratoren ein Analysegerät der gängigen Hersteller wie Network Generals Sniffer, Agilent's Internet-Advisor oder Cisco's Switchprobe sofort in den Datenstrom einklinken und mit der Messung beginnen, indem sie ihr Messgerät einfach über ein Patchkabel mit dem Analyse-Port am Tap verbinden. Ebenso störungsfrei werden Intrusion-Detection- beziehungsweise Intrusion-Prevention-Systeme über Taps implementiert. Im Gegensatz dazu sieht ein Monitoring-Device, das am SPAN-Port eines Switch angeschlossen ist,

nicht einmal den gesamten Traffic, weil korrupte Pakete verworfen werden.

Vorteile gegenüber Span-Ports

Um eine Überwachung oder eine Intrusion-Detection zu ermöglichen, unterstützen Switch-Hersteller üblicherweise einen Span- oder Mirror-Port. Darüber wird der Datenstrom eins zu eins an einen Analyse-Port gespiegelt, jedoch mit drei entscheidenden Nachteilen. Zum einen wird der Switch durch den zusätzlichen Datenstrom stärker belastet. Dadurch kann die CPU-Leistung oder Speicherkapazität überfordert und ein Upgrade erforderlich werden. Zum anderen werden bei vielen Geräten die Low-Level-Fehler vom Datenstrom entfernt, was eine Fehlersuche unmöglich macht.

Falls drittens ein Full-Duplex-Link untersucht wird, der am maximalen Datendurchsatz arbeitet, wird meist stillschweigend vorausgesetzt, dass auch der Span-Port mit entsprechender Performance arbeiten kann. Doch wenn er ohne Non-Blocking-Funktion auskommen muss, können viele Daten verloren gehen, da ein Span-Port niedrige Priorität hat. Taps hingegen arbeiten auch hier fehlerfrei. Eine Tap-Lösung nutzt zur Netzwerküberwachung und Intrusion-Detection passive Fiber- oder Kupfer-Splitter-Taps an den wichtigen Netzwerklinks. Dieser Ansatz vermindert den Aufwand und entschärft die oben genannten Schwierigkeiten.

In der Praxis ist es allgemein üblich, das Analysegerät für die Netzwerküberwachung oder Intrusion-Detection direkt anzuschließen. Aber

diese Vorgehensweise hat zwei große Nachteile. Erstens sind Messgeräte meist sehr teuer und können deshalb nicht permanent angeschlossen bleiben. Falls ein anderer Messpunkt erforderlich wird, muss die derzeit aktuelle Verbindung getrennt werden. Zweitens sind die meisten Messgeräte nicht passiv, so dass damit eine zusätzliche Fehlerquelle im Netz vorhanden ist. Durch den Einsatz von passiven Taps hingegen werden die Risiken, die beim direkten Verbinden des Messgerätes mit dem Netzwerk entstehen, umgangen und nebenbei auch eine viel höhere Kosteneffizienz erzielt. Die Taps geben dem Administrator größtmögliche Flexibilität, um ein Hochverfügbarkeitsnetz rund um die Uhr zu überwachen. Darüber hinaus sind alle über ein Tap angeschlossenen Geräte vom Netz aus unsichtbar und damit auch unangreifbar.

Die Tap-Technologie unterstützt das Monitoring und die Überwachung von Netzwerken aller Topologien, ob Kupfer oder Glasfaser mit Single- oder Multimode, von Fast- und Gigabit-Ethernet über ATM, DS3 und T1 bis hin zu Sonet- und 10-Gigabit-Ethernet-Netzen. Taps wie die von Net Optics sind von allen führenden IDS- und IPS-Herstellern zertifiziert und haben sich in sensiblen Sicherheitsbereichen bewährt. Taps können problemlos in 19-Zoll-Racks eingebaut werden und zeichnen sich durch einfache Installation und hohe Kompatibilität aus. Das verfügbare Tap-Portfolio für Messung und Security-Maßnahmen ist weit gespannt und sehr differenziert. Es kennt Stan-

TEST-ACCESS-PORTS

Key-Features und Vorteile

- ◆ passive Netzwerküberwachung für Glasfaser- und Kupfer,
- ◆ störungsfreie Messpunkte für Analyzer, IPS und IDS,
- ◆ kosteneffizient, weil multifunktional,
- ◆ bewährt im Maximum-Security-Bereich,
- ◆ zertifiziert von IDS- und IPS-Herstellern,
- ◆ in 19-Zoll-Racks einbaubar,
- ◆ einfache Installation, hohe Kompatibilität

dard-Taps zur Überwachung einer Verbindung mit einem Analyzer, aber auch so genannte Station-Taps, die die Funktionalität von bis zu 20 dieser Standard-Taps auf geringstem Raum vereinen. Aggregation-Taps dienen indessen dem Monitoring einer Verbindung mit einem Analyzer mit nur einer einzigen NIC. Während bei Port-Aggregation-Taps der RX- und TX-Stream zusammengefasst wird, um die Verbindung mit einer einzigen NIC zu überwachen, werden bei Link-Aggregation-Taps die RX- und TX-Streams mehrerer Ethernet/Fast-Ethernet-Verbindungen aggregiert, um einen einzigen Stream mit nur einem Gigabit-Ethernet-Adapter monitoren zu können. Darüber hinaus sind Link-Aggregation-Taps zum Anschluss an Span-Ports erhältlich. Diese bündeln zum selben Zweck die verschiedenen Mirror-Ports zu einem Stream.

Line-Analyzing

Demgegenüber helfen sogenannte Dual-Port-Link-Aggregation-Taps, bis zu vier Verbindungen mit einem oder zwei Analyzern zu überwachen. Ist mehr gefordert, so kommen Regeneration-Taps zum Einsatz, die die Kontrolle einer Verbindung mit bis zu acht Analysegeräten erlauben. Darüber hinaus hat beispielsweise Net Optics Matrix-Switches im Programm, die zur Überwachung einer Matrix bis zu 32 Verbindungen mit einem oder zwei Analyzern dienen. Sie erhöhen die Effizienz der Leitungsüberwachung und verringern zugleich die Ausgaben für teure Analysegeräte. Mit »SpyderSwitches« besteht sogar die Möglichkeit, bei Einsatz eines einzigen Distributed-Device bis zu 64 Verbindungen oder Span-Ports nach Wahl in Echtzeit passiv zu überwachen. Über die mitgelieferte Software können die Administratoren anhand vordefinierter oder selbst zusammengestellter Überwachungsmuster ihre Netze 24/7 überwachen.

Die aktuelle Weiterentwicklung der Produkte zielt unter anderem auf Fernwartung. Beispielsweise stellte systematic zu Jahresbeginn mit dem »iTap« von Net Optics erstmals auch einen Gigabit-Port-Aggregator mit Auslastungsdisplay und Fernwartungsoptionen vor. Der iTap liefert eine permanente Echtzeit-Anzeige der Netzwerkauslastung zur raschen Intervention bei Spitzenlasten oder DOS-Angriffen. Dies geschieht

sowohl durch eingebaute Displays als auch durch die Übermittlung der Anzeige an einen vom zu überwachenden Netz völlig getrennten Monitoring-Port.

Ein solches Gerät versorgt die Administratoren auf einen Blick mit allen Informationen über die Netzwerkauslastung. Ein Auslastungsdisplay lässt Echtzeitbewertungen von Netzwerkperformance-Proble-

men zu. Sichtanzeigen geben einen sofortigen Überblick über die Leistung kritischer Netzwerkverbindungen. Auf dem Front-Panel kann der Administrator sofort die aktuelle Bandbreitenauslastung jeder der beiden Halbduplex-Verbindungen ablesen, ebenso die Höhe und das zeitliche Auftreten von Spitzenwerten. Es bedarf keiner zusätzlichen Überwachungstools mehr, um erforder-

liche Gegenmaßnahmen sofort zu ergreifen. Da Sicherheit und Zuverlässigkeit des Netzwerkes unabdingbar sind, bieten die Test-Access-Ports in all ihren Ausdifferenzierungen für Mess- und Sicherheitstechnik eine umfassende Lösung für jedes Netzwerk.

**Bück Heinz, freier Publizist,
Riba BusinessTalk,
hbueck@riba.de**