Gigamon®

WHITEPAPER

TAP oder SPAN?

Einleitung

TAP- und SPAN-Technologien bieten einen direkten Zugang zu den Datenpaketen, die durch Netzwerke laufen. Aber welche Vorgehensweise ist bei den heutigen Infrastrukturen besser? Wenn beide Varianten geeignet sind, wann sollte dann welche Technologie eingesetzt werden? TAP oder SPAN? Das ist hier die Frage.

Die heutigen Netzwerke werden immer größer und komplexer und transportieren noch nie dagewesene Datenmengen mit zunehmender Geschwindigkeit. Beispielsweise werden 400-Gbit/s- und 1-Tbit/s-Ethernet entwickelt, das Internet of Things (IoT) und Cloud Computing schaffen zusätzliche Komplexität. All das macht den durchgängigen Zugriff auf die Paketebene deutlich schwieriger. Gleichzeitig werden auch Cyber-Bedrohungen immer anspruchsvoller. Deshalb ist Netzwerksichtbarkeit für das Monitoring, das Management und den Schutz Ihres Netzwerks essenziell.

Um Sichtbarkeit zu erlangen, ist es wichtig, dass Sie auf die Data-in-Motion bis hin zur Paketebene zugreifen können. Keine andere Maßnahme bietet Ihnen einen vergleichbaren Grad an Tiefe und Granularität. SPAN- und TAP-Technologien sind dabei die gebräuchlichsten Methoden. Wie entscheiden Sie, welche Methode verwendet werden sollte?

Dieses Whitepaper befasst sich bis ins Detail mit den beiden Technologien, um klar zu definieren, welche der beiden bei den heutigen modernen Infrastrukturen am besten zum Einsatz kommen sollte.

Abbildung 1: TAP versus SPAN

Technische Grundlagen von TAP und SPAN

Ein Netzwerk-TAP (Test Access Point) ist ein einfaches Gerät, das direkt mit der Kabelinfrastruktur verbunden wird. Anstelle von zwei Switches oder Routern, die direkt miteinander verbunden sind, sitzt der Netzwerk-TAP zwischen den beiden Geräten, wodurch alle Daten auch durch den TAP fließen. Mithilfe eines internen Splitters erstellt der TAP eine Kopie der Daten für das Monitoring, während die Originaldaten ungehindert durch das Netzwerk weiterlaufen.

Daten aus einem Netzwerk werden von Gerät A übertragen (Tx), um von Gerät B empfangen (Rx) zu werden. Gleichzeitig können Daten in umgekehrter Richtung laufen, wobei Gerät B Daten an Gerät A überträgt. Die meisten TAPs kopieren die Sendesignale von A und B getrennt und senden sie an separate Monitoring-Ports (TxA und TxB).

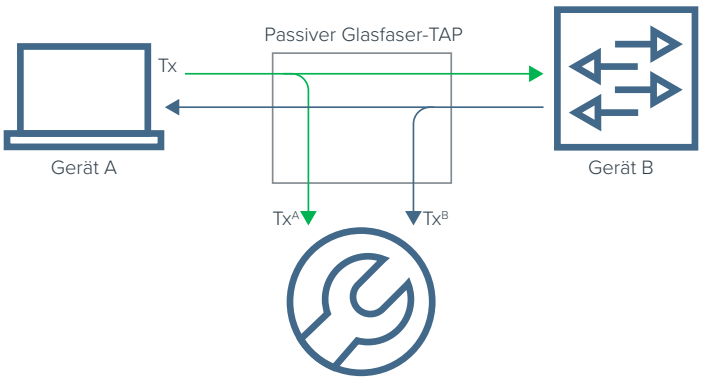

Abbildung 2: TAP-Flussdiagramm

Damit wird sichergestellt, dass jedes Paket unabhängig von der Größe kopiert wird. Diese Technik verhindert zudem eine Überbelegung. Wurden die Daten kopiert (TAPed), kann das Duplikat für jede Art von Monitoring-, Sicherheits- oder Analysezweck verwendet werden. Deshalb sind TAPs zentraler Bestandteil eines Visibility-Systems.

Es ist zu beachten, dass beim Einsetzen eines TAPs in eine bestehende Netzwerkverbindung eine kurze Abtrennung der Kabel erfolgt, sodass TAPs normalerweise während eines Wartungsintervalls installiert werden.

Ein SPAN-Port (auch Spiegel- oder Mirror-Port) ist eine Softwarefunktion, die in einen Switch oder Router eingebaut wird. Dieser erstellt eine Kopie von ausgewählten Paketen, die das Gerät passieren, und sendet sie an einen ausgewiesenen SPAN-Port. Mithilfe von Software können Administratoren die Art der zu überwachenden Daten leicht einstellen oder anpassen.

Da die wichtigste Aufgabe eines Switches oder Routers die Weiterleitung von Produktionspaketen ist, erhalten SPAN-Daten auf dem Gerät eine geringere Priorität. Der SPAN verwendet auch einen einzigen Egress-Port, um mehrere Links zu sammeln, sodass er leicht überbelegt sein kann. In beiden Fälle kann es zu Paketverlusten kommen. SPANs waren nie für ein langfristiges Monitoring vorgesehen.

Sie eignen sich vielmehr für ein Ad-hoc-Monitoring von geringen Datenmengen in Bereichen, wo keine TAPs installiert sind. SPANs stellen nach wie vor die einzige Möglichkeit dar, auf einige Datentypen zuzugreifen, wie z.B. Daten, die auf demselben Switch von Port zu Port laufen.

Ein historischer Rückblick

In den Anfangszeiten von Netzwerken waren diese noch langsam, und es war einfach, Pakete zu erfassen. Netzwerke nutzten 10-Mbit/s-Ethernet über Koaxialkabel und teilten sich Media-Hubs, um Daten zu übertragen. Da jeder Port eines Hubs alle Daten innerhalb der Domain enthielt, konnte ein Protokoll-Analysetool an jedem Datenport eines Hubs angeschlossen werden, um alle ein- und ausgehenden Daten jedes lokalen Geräts anzeigen zu lassen.

Mit der zunehmenden Nutzung von LANs und WANs entstanden Skalierungsprobleme sowie ernstzunehmende Sicherheitsrisiken. Im Jahr 1995 standardisierte das IEEE das Fast Ethernet, womit die Ära der Switches eingeläutet wurde. Die Switch-Technologie leitet Daten an Ports weiter, an denen sich bestimmte Adressen befinden. So erhalten die Stationen nicht alle Daten, während sie nach ihrer eigenen Adresse suchen. Die Switch-Skalierbarkeit ist deutlich stabiler. Zeitgleich mit der Einführung der Switches nahm die Nutzung des Internets explosionsartig zu.

Da die Switches Pakete jedoch nur an den entsprechenden Port weiterleiten, wurde es schwieriger, auf alle Daten zuzugreifen. Dadurch wurden Netzwerk-TAPs zur Standardausrüstung, um alle Daten zu sehen, die über bestimmte Verbindungen geleitet werden. Das führte dann zu einem öffentlichen Aufschrei von Netzwerkadministratoren. Die großen Switch- und Router-Hersteller (wie zum Beispiel Cisco) reagierten darauf und fügten ihren Geräten eine Software hinzu, um Daten auf die Monitoring-Ports von SPANs zu spiegeln. Da diese Funktion nur für die gelegentliche Fehlerbehebung gedacht war und ihre Implementierung sich auf die Performance des Switches auswirkte, mussten Anbieter den Produktionsdaten eine Priorisierung gegenüber den gespiegelten Paketen einräumen.

Viele Jahre konkurrierten TAP- und SPAN-Technologien direkt miteinander. Netzwerkexperten ergriffen je nach Perspektive auf Netzwerke und Security unterschiedliche Positionen, was mitunter religiöse Züge annahm. Einige IT-Betriebe setzten ausschließlich TAPs ein, während andere sie innerhalb ihrer Infrastruktur vollständig verboten.

Als sich Netzwerke bei der Geschwindigkeit von 10Mbit/s zu 10Gbit/s entwickelten, fand eine weitere Verschiebung statt. Das enorme Datenvolumen überlastete SPAN-Ports häufig. Anbieter zeigten deutlich auf, dass SPAN-Ports nur für Daten mit geringem Volumen bestimmt waren und bei falscher Konfiguration den Produktions-Traffic negativ beeinflussen konnten. Einige Highspeed-Switches wurden lediglich ohne SPAN-Fähigkeit entwickelt, während andere ganz davon abrieten. Bei einer Geschwindigkeit von 10 Gbit/s implementierten einige Hersteller sogar eine Geschwindigkeitsbegrenzung am SPAN-Ausgangsport als Standardeinstellung, um negative Auswirkungen zu reduzieren. So konnten sich TAPs als die bessere Access-Technologie für moderne Netzwerke durchsetzen.

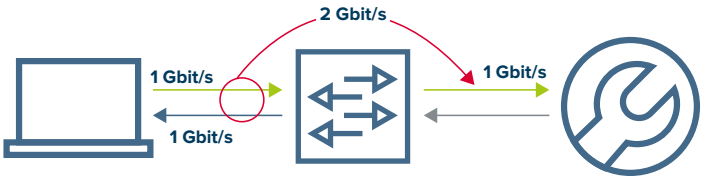

Abbildung 3: Warum SPAN-Ports leicht überbelegt werden

Warum werden Netzwerk-TAPs gegenüber SPAN-Ports bevorzugt?

In modernen Netzwerken wird ein TAP aus verschiedenen Gründen einem SPAN-Port vorgezogen. Passive TAPs werden ohne Strom betrieben und laufen über Jahre hinweg ausfallfrei. Ihre Hardware erfasst jedes Paket in der richtigen Reihenfolge und verhindert Überbelegungen. Obwohl SPAN-Ports bei niedriger Auslastung einwandfrei funktionieren, werden sowohl gesendete (Tx) als auch empfangene (Rx) Datenströme an einen einzigen SPAN-Ausgangsport weitergeleitet. Das bedeutet, dass ein einziger Switch-Port bei bidirektionalem Datenverkehr von 60 Prozent Auslastung Daten an den SPAN-Port mit 120 Prozent Auslastung sendet. Da ein Ethernet-Anschluss nie über 100 Prozent hinausgehen kann, würden mindestens 20 Prozent der Daten verloren gehen. Wenn etwa ein Dutzend ähnlicher Ports zu einem einzigen SPAN-Port zusammengefasst werden, würde nur ein Bruchteil der Daten jemals zu den Monitoring-Tools gelangen. Das folgende von einem Kunden erstellte Diagramm zeigt ein reales Netzwerk an dem Punkt, an dem die ExtraHop-Quelle von SPAN in TAP konvertiert wurde. Sobald die Änderung vorgenommen wird, kommt es zu einer sofortigen Datenspitze. Wichtig ist: Sowohl vor als auch nach der Konvertierung wurden die gleichen Daten gesammelt. Allerdings wurde die ursprüngliche SPAN-Konfiguration dabei überbelegt, wodurch Pakete verloren gingen.

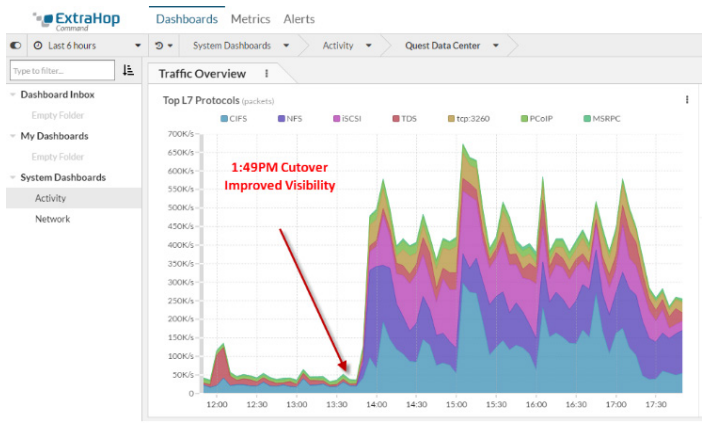

Abbildung 4: Umstellung von SPAN auf TAP

Es gibt noch weitere Gründe, warum TAPs gegenüber SPAN-Ports bevorzugt werden. Da Switches SPAN-Daten eine niedrige Priorität zuteilen, kann es nicht nur passieren, dass Pakete vollständig verloren gehen, sondern auch in der falschen Reihenfolge am Monitoring-Tool ankommen. Zudem können Latenzschwankungen auftreten, sodass SPAN-Daten früher oder später als Produktionsdaten geliefert werden. So etwas kann mit einem TAP nicht passieren, da jedes Paket in exakter Reihenfolge mit der Datenübertragungsrate weitergeleitet wird.

Das Fazit ist also, dass TAPs überall dort eingesetzt werden sollten, wo 100 Prozent Sichtbarkeit und Präzision beim Traffic erforderlich sind. Wenn Ihr Traffic-Volumen mittel bis hoch ist, sollten Sie auf Netzwerk-TAPs zurückgreifen. Best-Practice-Lösung: Installieren Sie TAPs schon während der frühen Designphase und leiten Sie den Datenverkehr direkt an einen Gigamon Visibility Node weiter. Selbst wenn Ihr Traffic noch nicht täglich auf Probleme überprüft werden muss, steht er innerhalb von Sekunden für Ad-hoc-Fehlerbehebungen oder Sicherheitsprüfungen bereit und erfordert keine Veränderungen im bestehenden System.

Zusammenfassung: Die 10 wichtigsten Gründe, warum Netzwerk-TAPs gegenüber SPAN-Ports bevorzugt werden:

1. TAPs erstellen eine exakte Kopie des bidirektionalen Netzwerk-Traffics bei voller Datenübertragungsrate und leisten daher präzise Arbeit im Bereich des Netzwerk-Monitorings, der Analyse und der Security.
2. Passive TAPs bieten kontinuierlichen Zugriff auf den Datenverkehr und erfordern nach der Installation weder Eingriff noch Konfiguration durch den Nutzer – eine richtige Set-and-Forget-Lösung.
3. SPAN-Ports werden leicht überbelegt – das führt zu Paketverlusten sowie ungenauen oder inkonsistenten Ergebnissen für Monitoring- und Sicherheitszwecke.
4. SPAN-Traffic besitzt bei der Weiterleitung die niedrigste Priorität und erreicht daher möglicherweise nicht die volle Datenübertragungsrate. In einigen Situationen kann diese niedrige Priorisierung sogar zu Paketverlusten führen, selbst dann, wenn der SPAN-Port mit einer Auslastung im einstelligen Bereich arbeitet.
5. Die Nutzung eines SPANs kann sich negativ auf die Performance des Switches auswirken und so den Netzwerk-Traffic beeinträchtigen.
6. Da sich der SPAN-Traffic leicht umkonfigurieren lässt, kann sich auch der Output des SPANs jederzeit verändern – das führt zu widersprüchlichen Ergebnissen.
7. Gesetzliche Vorschriften oder die Compliance des Unternehmens erfordern es manchmal, dass der gesamte Traffic eines bestimmten Bereichs überwacht werden muss. Das kann nur mit einem TAP gewährleistet werden.
8. Falsch konfigurierte SPAN-Ports können die Netzwerkleistung beeinträchtigen oder verursachen unter Umständen sogar Netzwerkausfälle.
9. Die Anzahl der SPAN-Ports ist im Vergleich zu den zu überwachenden Ports begrenzt. Zudem benötigen sie Ports, die eigentlich auch für den Produktions-Traffic benutzt werden könnten.
10. Für TAPs ist es egal, welches Protokoll im Datenverkehr genutzt wird oder ob es sich um IPv4 oder IPv6 handelt. Der gesamte Datenverkehr wird durch einen passiven TAP geleitet, auch fehlerhafte Pakete. Aktive TAPs blockieren in der Regel Fehler, leiten aber alles andere weiter.

Wann sollten SPAN-Ports verwendet werden?

Wie bereits erwähnt, werden Netzwerk-TAPs bei modernen Netzwerken gegenüber SPAN-Ports klar bevorzugt. Es gibt jedoch noch immer Bereiche, bei denen ein TAP nicht unbedingt praktikabel ist. Sie sollten für folgende Ausnahmefälle eher SPAN-Ports verwenden:

- Ein begrenztes und Ad-hoc-Monitoring in Bereichen mit SPAN-Kapazitäten, wenn Sie aktuell noch keinen Netzwerk-TAP installiert haben.
- Bereiche mit begrenztem Lichtbudget, bei dem das Aufteilungsverhältnis eines TAPs möglicherweise zu viel Licht verbraucht. (Eine andere Möglichkeit wäre hier ein aktiver TAP oder ein leistungsfähigeres Glasfaserkabel, das für größere Entfernungen geeignet ist.)
- In dringenden Fällen, für die kein Wartungsfenster eingeräumt werden kann, um den TAP zu installieren.
- Remote-Bereiche, die wenig Traffic aufweisen und daher eine dauerhafte TAP-Lösung nicht notwendig ist.
- Wenn der Zugang zum Datenverkehr innerhalb eines Switches bleibt oder gar keine physische Verbindung erreicht, auf der der Datenverkehr aufgezeichnet (TAPed) werden kann.
- Als kostengünstige Alternative zur Fehlerbehebung bei Verbindungen mit geringer Auslastung.

Zusammenfassend lässt sich sagen, dass sowohl Netzwerk-TAPs als auch SPAN-Ports bei korrekter Verwendung einen zuverlässigen Zugriff auf Daten bieten.

Also: TAPen Sie, wo Sie können und SPANen Sie, wo Sie müssen.

Denken Sie daran, dass ein TAP und/oder SPAN nur der erste Schritt auf dem Weg zu einer durchgängigen Sichtbarkeit auf Ihre gesamte Netzwerkinfrastruktur sind. Sobald der Datenverkehr entweder über TAPs oder SPAN-Ports erfasst wurde, können Sie ihn an eine Gigamon Visibility Platform senden, um ihn zu monitoren, zu verwalten und zu sichern. Ihnen steht eine ganze Reihe an GigaSMART® Applikationen zur Verfügung, um Ihren Traffic zu optimieren und relevante Daten ausschließlich an bestimmte Tools zu senden, um die Performance und Effizienz dieser Tools zu verbessern.

Über Gigamon

Gigamon ist das weltweit erste Unternehmen, das eine einheitliche Sichtbarkeit und Analyse des Netzwerkes für den gesamten Datenverkehr von Rohpaketen bis zu Apps über physische, virtuelle und Cloud-Infrastrukturen hinweg bietet. Wir erfassen, verarbeiten und analysieren Netzwerk-Traffic, um kritische Anforderungen an Performance und Security zu erfüllen einschließlich einer schnellen Threat Detection – so können Sie digitale Innovationen vorantreiben. Kurz gesagt, wir ermöglichen es Ihnen, schnell, sicher und innovativ zu arbeiten. Gigamon hat bereits über 75 Technologiepatente erhalten und erfreut sich einer hohen, in der Industrie führenden Kundenzufriedenheit mit mehr als 3.000 Organisationen, darunter 80 Prozent der Fortune-100-Unternehmen. Gigamon hat seinen Hauptsitz im Silicon Valley und ist weltweit tätig. Für weitere Information und wie Gigamon Ihnen helfen kann, besuchen Sie www.gigamon.com/de/.

Besuchen Sie www.gigamon.com und fordern Sie eine kostenlose Demo an.

Hinweis: Weitere Informationen über die Funktionsweise von TAPs finden Sie unter:
https://www.gigamon.com/content/dam/resource-library/german/white-paper/wp-gigamon-understanding-network-de.pdf.

Gigamon®
Internationaler Hauptsitz
3300 Olcott Street, Santa Clara, CA 95054, USA
+1 (408) 831-4000 | www.gigamon.com/de/