Gigamon®

WHITEPAPER

So funktionieren Netzwerk-TAPs – Der erste Schritt zu mehr Sichtbarkeit

Einleitung

Ein Netzwerk-TAP ist ein einfaches Gerät, das eine direkte Verbindung zur Infrastruktur der Netzwerkkabel herstellt, um Datenpakete zur Verwendung bei der Analyse, der Security oder dem allgemeinen Netzwerkmanagement zu teilen oder zu kopieren. Im Englischen steht das Wort „Tap“ unter anderem für „anzapfen“ oder „abhören“. In der IT wurde der Begriff „TAP“ für „Test Access Point“ eingeführt. TAP ist in diesem Fall also ein Akronym. In diesem Whitepaper finden Sie:

- Hintergrundinformationen
- TAP vs. SPAN
- Überblick zu Netzwerk-TAPs
- Verschiedene Arten von TAPs und wie sie funktionieren
  - Passive TAPs
    - Arten von optischen Splittern
    - Spezialisierter 40Gbit BiDi TAP
    - Teilungsverhältnisse
    - Arten von Glasfasern und deren Geschwindigkeiten
    - Energiebudgets und Lichtverlust
  - Aktive TAPs
  - Weitere TAPs
    - Bypass-Technologie
    - Aggregations-TAP vs. Aggregationsknoten
    - Standalone vs. Embedded TAPs
- 10GBASE-T
- TAP Best Practices
- Zusammenfassung

Hintergrund

Für eine gute Vernetzung sind gemeinsame Kommunikationsprotokolle entscheidend. Einfache Verbindungen funktionieren unabhängig von den in der Nutzlast mitgeführten Informationen. Dank des einfachen Systems konnte das Internet in seiner heutigen Form entstehen, wodurch zahlreiche Anwendungen vom Online-Banking bis hin zu internationalen Telefongesprächen ermöglicht wurden.

Aber eben weil das System so einfach gestrickt ist, führt das auch zu einigen Herausforderungen.

Denn wenn jedes Datenpaket von außen betrachtet gleich aussieht, wie können Sie sich dann sicher sein, dass das Paket (oder ein Frame) auch die richtigen Informationen enthält? Wurde eine bestimmte Banktransaktion oder ein Online-Verkauf tatsächlich mit dem korrekten Betrag abgeschlossen? Wurde eine Krankenakte gemäß den Vorschriften zur Einhaltung der Compliance und der Nachverfolgbarkeit ordnungsgemäß abgelegt? War der Kunde auch wirklich dazu autorisiert, auf die Datenbank zuzugreifen?

Um solche Fragen beantworten zu können, braucht es Sichtbarkeit sowie eine detaillierte Analyse der Datenpakete. Dort befinden sich alle übermittelten Informationen. Heutzutage sind unzählige Analyse-Tools im Umlauf. Diese sind auf die Informationen in den Datenpaketen angewiesen. Deshalb sind Netzwerk-Monitoring und IT-Sicherheit eine zentrale Voraussetzung für jede Branche.

TAP vs. SPAN

Um den Traffic direkt vom System zu erfassen, gibt es zwei gängige Vorgehensweisen: entweder mit TAPs oder mit SPANs. Ein Netzwerk-TAP ist eine Hardware-Komponente, die direkt in die Netzwerk-Verkabelung integriert wird und Pakete für Monitoringzwecke kopiert. Ein SPAN (Switch Port Analyzer) bezeichnet eine Softwarefunktion eines Switches oder Routers, die den Verkehr von eingehenden oder ausgehenden Ports dupliziert und den kopierten Verkehr an einen speziellen SPAN-Port (auch Spiegel- oder Mirror-Port) weiterleitet. Grundsätzlich verwendet man aus den folgenden Gründen eher TAPs statt SPANs:

- SPAN-Ports können sehr leicht überbelegt werden und erhalten bei der Datenweiterleitung die niedrigste Priorität. Das kann in manchen Fällen zu Paketverlusten führen.
- Eine SPAN-Anwendung ist zudem sehr rechenintensiv und kann sich deshalb negativ auf die Performance des Switches auswirken und so möglicherweise den Netzwerk-Traffic beeinträchtigen.
- Da der SPAN-Verkehr leicht umkonfiguriert werden kann, kann sich auch der Output des SPANs jederzeit verändern — das führt zu inadäquatem Reporting.

Es gibt jedoch einige Situationen, bei denen ein TAP nicht unbedingt praktikabel ist. Beispielsweise wenn der Traffic auf einer physischen Infrastruktur läuft, die sich Ihrer direkten Kontrolle entzieht, oder es einfach nicht möglich ist, ein Zeitfenster für eine TAP-Installation einzurichten. Auch bei Remote-Standorten, die wenig Traffic haben und eine dauerhafte TAP-Lösung nicht notwendig ist, können SPANs meist die sporadische Fehlerbehebung gewährleisten, ohne dabei die Verbindung abzubrechen. Zudem gibt es diverse Geschwindigkeits- oder Schnittstellentypen, bei denen nur ein SPAN kompatibel ist. Daher ist eine Kombination aus TAP und SPAN weit verbreitet. Um an der Stelle eine Netzwerk-Weisheit zu zitieren: TAPen Sie, wo Sie können und SPANen Sie, wo Sie müssen.

Überblick zu Netzwerk-TAPs

Da ein Netzwerk-TAP den Traffic eines Systems am effektivsten kopiert, erläutert dieses Whitepaper die verschiedenen Arten von TAPs, wie sie funktionieren und wie sie verwendet werden. Hier sollte erwähnt werden, dass TAPs für zahlreiche Netzwerkgeschwindigkeiten und Kabeltypen verfügbar sind. Statt zwei Switches oder Router direkt miteinander zu verknüpfen, sitzt der Netzwerk-TAP dazwischen und ist direkt mit den beiden Endgeräten verbunden. Der Traffic wird erkannt und kopiert, wodurch eine genaue Sichtbarkeit auf den Netzwerk-Traffic entsteht (siehe Abbildung 1).

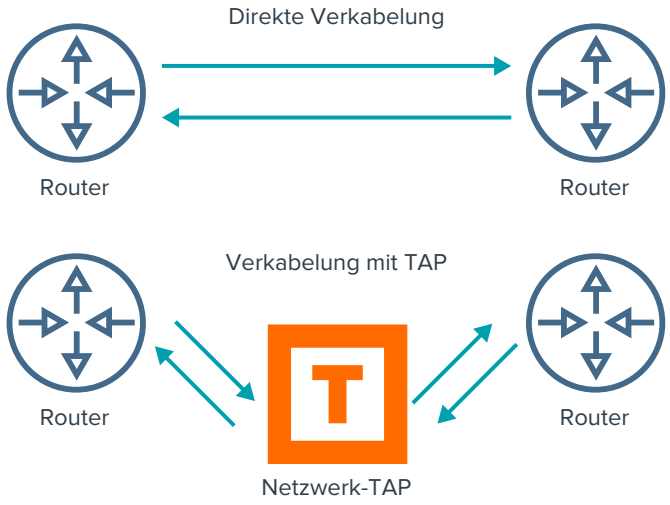

Abbildung 1: Direkte Verkabelung vs. TAP-Verkabelung

TAPs sind einfach zu handhabende Geräte, die in der Regel in gesicherten Bereichen platziert werden und über Jahre hinweg laufen. Sobald der Traffic mit Hilfe der TAPs abgerufen wurde, kann die Kopie für jede Art von Monitoring-, Security- und Analyse-Zweck verwendet werden. Deshalb sind TAPs zentrale Bestandteile eines jeden Visibility-Systems.

Verschiedene Arten von TAPs und wie sie funktionieren

Es gibt viele unterschiedliche Arten von TAPs. Die zwei wichtigsten Arten von Netzwerk-TAPs sind:

- Passive TAPs
- Aktive TAPs

Passive TAPs

Passive TAPs benötigen keine eigene Stromversorgung und interagieren nicht aktiv mit anderen Netzwerkkomponenten. Sie verwenden optische Splitter, um eine Kopie des Signals zu erzeugen. Daher werden sie oft auch als „photonische“ TAPs bezeichnet. Die meisten passiven TAPs besitzen keine beweglichen Teile, sind äußerst zuverlässig und erfordern keine Konfiguration.

ZU EINER TYPISCHEN TAP-INSTALLATION GEHÖRT:

1. **Den TAP auf einem Shelf oder Rack platzieren.**
2. **Die Kabel verbinden.**
3. **Sicherstellen, dass alles funktioniert.**

Ja, es ist wirklich so einfach. Sollte ein TAP nicht funktionieren, liegt das Problem höchstwahrscheinlich an der Verkabelung oder einer schlechten Verbindung. Bedenken Sie bitte, dass die Installation oder der Austausch eines TAPs in einer bestehenden Netzwerk-Umgebung die Verbindung unterbricht, bis die Kabel wieder angeschlossen werden. Die Installation von TAPs wird deshalb in der Regel in einem vordefinierten Wartungszeitraum oder während der Planungsphase des Netzwerks durchgeführt, bevor Live-Traffic entsteht.

Glasfaser sendet Licht von einem Transceiver durch ein dünnes Glaskabel zu einem Empfänger am anderen Ende der Leitung. Statt einer direkten Verbindung ist jeder der beiden End-Knoten (Switches, Router, Datenbank usw.) mit Netzwerk-Ports auf dem TAP verbunden. Diese besonderen Ports sind paarweise verkabelt, sodass der Traffic permanent über sie läuft. Zusätzlich zu den Netzwerk-Ports gibt es Monitoring-Ports. Wie auf Abbildung 2 zu sehen ist, senden die Monitoring-Ports vollstandige Kopien des Traffics aus.

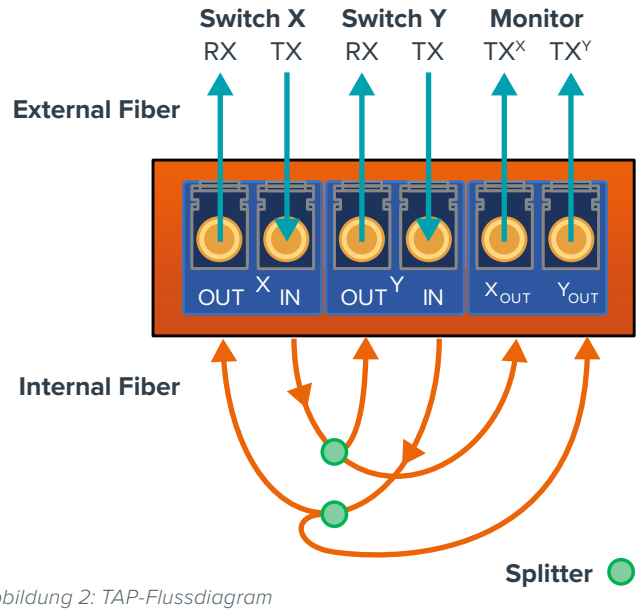

Abbildung 2: TAP-Flussdiagram

Im Gegensatz zu Netzwerk-Ports, die Traffic sowohl senden (Tx) als auch empfangen (Rx), können Monitoring-Ports nur senden, da sie unidirektional sind. Sie können keinen Traffic empfangen und geben den Traffic auch nicht in das System zurück. In der Abbildung sehen Sie zwei Monitoring-Ports. Da jeder Netzwerk-Port sowohl Traffic sendet als auch empfängt, können folglich auf einer 10-Gbit-Verbindung ganze 20 Gbit laufen. Würde der gesamte Traffic in ein einziges Monitoring-Kabel geleitet, könnte die Verbindung schnell überbelegt werden. Werden zwei separate Monitoring-Verbindungen verwendet, ist eine Überbelegung ausgeschlossen. Der überwachte Traffic wird somit in zwei Sendesignale (nur TX) aufgeteilt, sprich in eine Kopie von Endpunkt A (Switch X) und eine Kopie von Endpunkt B (Switch Y).

Wie in Abbildung 2 dargestellt, ist ein passiver optischer Netzwerk-TAP innen einfach aufgebaut. Die externen Anschlüsse führen zu Sets aus Glasfasern, Splittern und weiteren Glasfasern, die wiederum zurück zu den externen Anschlüssen führen. Bei jedem Splitter führt eine Faser rein und zwei Fasern raus.

Arten von optischen Splittern

Im Inneren des TAPs liegt zwischen den Netzwerk-Port-Paaren ein kleines Stück Hardware, das optischer Splitter genannt wird. Das englische „split" steht für „teilen". Der Splitter macht also das, was der Name schon sagt: Er teilt einen optischen Strahl in zwei Pfade auf. Ein Teil des Lichtes wandert zum eigentlichen Bestimmungsort; während der Rest auf einen Monitoring-Port geleitet wird.

Um das Licht aufzuteilen, verknüpft oder verschmilzt man meist zwei Kabel miteinander, sodass ein Teil des Lichts in einen zweiten Strahl geschleust wird. Diese Technologie wird Fused Biconical Taper (FBT) genannt (siehe Abbildung 3). Im Prinzip läuft es genau so ab wie bei einem Fluss, der auf eine Gabelung trifft. Ein Teil des Wassers läuft weiterhin mit dem eigentlichen Strom, während der Rest einen anderen Weg nimmt. Die Flussarme fließen weiterhin stromabwärts. Wie Wasser ist auch das Licht lenkbar. Deshalb neigt der FBT dazu, den Traffic in eine Richtung zu leiten. FBTs sind in der Regel kostengünstig und eignen sich gut für Verkabelungen mit niedrigeren Geschwindigkeiten.

Abbildung 3: Fused Biconical Taper (FBT)

Eine andere Art von Splitter basiert auf der Dünnschichttechnik. Hier kann man das Konzept mit einer Taschenlampe vergleichen, die durch ein klares Glasfenster scheint. Obwohl der größte Teil des Lichts durch das Fenster strahlt, wird ein Teil des Lichts vom Glas zurückreflektiert. Im richtigen Winkel kopiert eine halbdurchlässige Membran, die die Faser durchdringt, einen Teil des optischen Signals zum Monitoring-Port (siehe Abbildung 4). Die reflektierende Dünnschichttechnik weist eine geringere Verlustrate auf, wenn sie mit High-Speed-Verbindungen arbeitet. Beispielsweise entstehen bei Geschwindigkeiten von 100 Gbit Hot Spots aufgrund der ungleichmäßigen Lichtverteilung auf der Faser. Der FBT-Anteil sieht nur den Teil des Lichts, der miteinander verschmolzen ist. Dünnschichttechnik kann die Verteilung gleichmäßig durchführen, da sie das reflektierte Licht über den gesamten Durchmesser des Kabels erkennt.

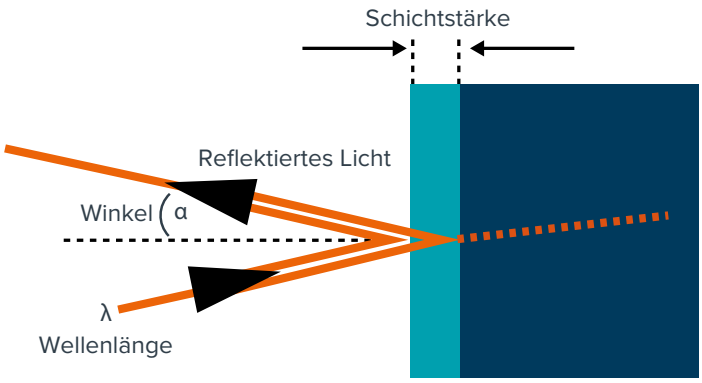

Abbildung 4: Dünnschicht-Splitter-Technologie

Spezialisierter 40 Gbit BiDi TAP

Dünnschichttechnik wird außerdem auch für bidirektionale TAP-Verbindungen bevorzugt, wie zum Beispiel für 40 Gbit Cisco BiDi. Hier werden mehrere Wellenlängen gleichzeitig reflektiert, um jedes Lambda (bzw. jede Wellenlänge) des Lichts zu brechen. Cisco BiDi nutzt die 40-Gbit-Technologie unter Verwendung von Standard-LC-basierter Verkabelung, um die Gesamtkosten für die Bereitstellung von 40-Gbit-Verbindungen zu reduzieren. Dieser Trend nimmt aktuell zu – besonders in Hinblick auf die Cisco Spine-Leaf-Konfigurationen. Abbildung 5 zeigt exemplarisch wie Reflektions-Technologie innerhalb der hochspezialisierten passiven TAPs verwendet wird.

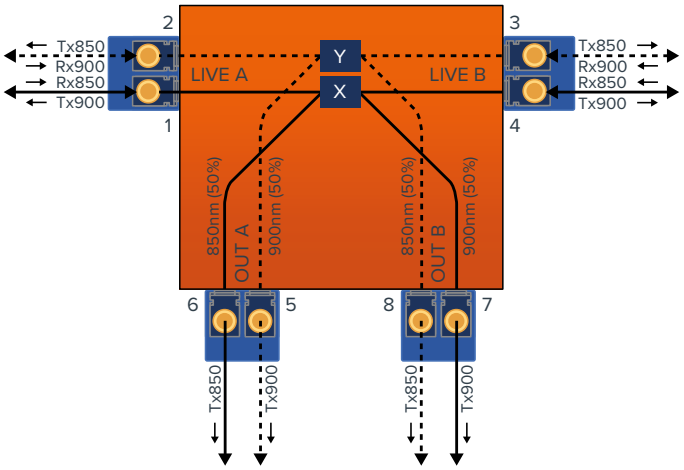

Abbildung 5: Dünnschichttechnologie in bidirektionaler Implementierung

Teilungsverhältnisse

Unabhängig von der gewählten Methode lenkt der passive Splitter physisch einen Teil des Lichts von seiner ursprünglichen Quelle ab. Der proportionale Anteil des Lichts für jeden Pfad wird als Teilungsverhältnis (Split Ratio) bezeichnet. Das Teilungsverhältnis wird als Kombination von zwei Prozentsätzen angegeben. Die erste Zahl wird als Netzwerk-Prozentsatz bezeichnet, die zweite Zahl ist der Monitoring-Prozentsatz. Zusammen ergeben sie immer 100 Prozent. Üblicherweise beträgt das Teilungsverhältnis bei 1-Gbit-Kurzstreckenverbindungen 70/30, wobei siebzig Prozent des Lichts zum Netzwerk- und dreißig Prozent zum Monitoring-Port geleitet werden.

Dem Netzwerk wird mehr Licht zugewiesen, um den Netzwerk-Traffic nicht zu verlangsamen. Geschwindigkeiten wie 10 Gbit, 40 Gbit und 100 Gbit haben unterschiedliche technische Anforderungen und verwenden meist ein eher gleichmäßiges Teilungsverhältnis von beispielsweise 50/50 oder 60/40. Das heute gängigste Teilungsverhältnis liegt bei 50/50, vorausgesetzt die vorhandenen Lichtverhältnisse sind angemessen. Wenn das Lichtniveau niedrig ist, sollte man zu besseren Optiken wechseln, die einen höheren Sicherheitspielraum bieten.

Gigamon testet jeden hergestellten TAP und liefert zu jedem Gigamon TAP die tatsächlich geprüften Verlustwerte. Darüber hinaus beschreiben Gigamon Datenblätter für TAPs die maximal akzeptablen Netzwerk- und Monitoring-Verlustwerte (einschließlich der Verbindungen) für jedes Teilungsverhältnis wie folgt:

Arten von Glasfasern und deren Geschwindigkeiten

Glasfaser-TAPs sind für diverse Geschwindigkeiten und Kabeltypen erhältlich. Die meisten Netzwerke setzen auf IEEE 802.x standardbasierte Lichtwellenleiter. Die Geschwindigkeit wird in Gigabit pro Sekunde, auch Gbit/s, angegeben. Die Bezeichnung Gigabit wird oft auch als Gbit oder Gb abgekürzt. Die heute gebräuchlichsten Geschwindigkeiten sind 1 Gbit, 10 Gbit und 40 Gbit. Der Trend geht aber aktuell in Richtung 100 Gbit. Geschwindigkeiten von 400 Gbit werden wohl erst in den kommenden Jahren verfügbar sein. Da für jede Geschwindigkeit unterschiedliche Transceiver-Technologien eingesetzt werden, verändern passive Glasfaser-TAPs zwischenzeitlich nicht die Geschwindigkeit. Wenn Traffic bei 10 Gbit mit einer Wellenlänge von 1550 nm eintrifft, besitzt der Traffic auch nach dem Split die gleiche Geschwindigkeit und Wellenlänge.

Um beste Ergebnisse zu erzielen, sollte die Art der Kabel über die gesamte Infrastruktur konsistent sein. Passen Sie die Kabel Ihrem Bedarf an. Im Allgemeinen werden Glasfaserkabel in zwei Kategorien unterteilt:

- Multimode-Fasern
- Singlemode-Fasern

Multimode Passive TAPs			
Teilungsverhältnis	50/50	60/40	70/30
Maximaler Netzwerkverlust	3,9 dB	3,15 dB	2,2 dB
Maximaler Monitoring-Verlust	3,9 dB	5,15 dB	6,2 dB
Singlemode Passive TAPs			
Teilungsverhältnis	50/50	60/40	70/30
Maximaler Netzwerkverlust	3,7 dB	3,05 dB	2,0 dB
Maximaler Monitoring-Verlust	3,7 dB	4,95 dB	6,1 dB

Abbildung 6: Gigamon veröffentlichte Höchstverlustraten (einschließlich der Verbindungen) für verschiedene Teilungsverhältnisse

Verbindungen über kürzere Distanzen laufen häufig über Multimode-Kabel, während bei Verbindungen über größere Entfernungen eher Singlemode-Kabel verwendet werden. Der entscheidende Unterschied zwischen den beiden Faserarten ist, dass Multimode einen größeren Kerndurchmesser besitzt (bis zu 62,5 µm), was eine breitere Streuung des Lichts ermöglicht. So können kostengünstigere optische Transmitter auf LED-Basis verwendet werden, und folglich sinken auch die Gesamtkosten.

Da das Licht auf einem größeren Kern über mehrere Modi gestreut wird, kann es auf dem Weg durch das Kabel stark hin und her springen. Und weil verschiedene Licht-Modi unterschiedlich lange Distanzen zurücklegen, kommen die Signale nicht gleichzeitig an. Es ist also schwierig, einen Impuls von einem anderen zu unterscheiden. Das kann das Signal massiv dämpfen oder sogar zum Signalverlust führen. Aus diesem Grund sind Multimode-Fasern je nach Kabeltyp nur für kürzere Strecken von ein paar hundert Metern ausgelegt. Außerdem ist es wichtig, dass die größere Multimode-Coreverkabelung (62.5 µm) nur bis 1 Gbit verwendet werden sollte.

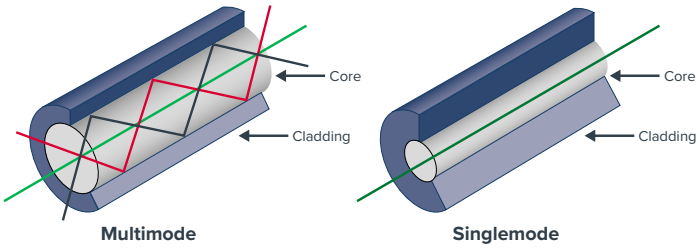

Abbildung 7: Multimode- und Singlemode-Kabel

Singlemode-Fasern laufen mit höheren Bandbreiten über kleinere Kerne. Dies erfordert präzisere Messgeräte und teurere Laserdioden zur Übertragung des Signals. Vertical-Cavity Surface-Emitting Laser (VCSEL) sind kleine, flache Impulsgeber, die häufig für kurze und mittlere Distanzen verwendet werden. Längere Distanzen von 40 km oder mehr erfordern Fabry-Pérot-Laser, die präziser (und mit höheren Temperaturen) arbeiten. Abbildung 8 zeigt gängige Kabeltypen.

Energiebudgets und Lichtverlust

Wenn Sie in den Nachthimmel schauen, sehen Sie Sterne. Es gibt aber viele Sterne, die Sie mit bloßem Auge nicht erfassen können. Das Licht wird nämlich entweder durch Wolken oder durch Luftverschmutzung verdeckt. Ob Sie die Sterne sehen können, hängt zudem auch von Ihrer Sehkraft und von der Helligkeit (oder Energie) des Sterns selbst ab. Das Sternenlicht legt Milliarden von Kilometern in einer relativ geraden Linie durch das Vakuum des Weltraums bis zu Ihrem Auge zurück. Im Gegensatz dazu prallt Licht mit geringer Leistung in einem optischen Kabel an der Kabelwand ab und muss durch mehrere Verbindungen übertragen werden. Das führt zu Lichtverlusten. Deshalb nimmt der Lichtpegel im Kabel recht schnell ab.

Der optische Energieverlust eines Glasfaserkabels wird in Dezibel (dB) gemessen. Damit der Lichtempfänger das Signal korrekt erfassen kann, muss die Lichtquelle hochwertig sein. Ist das Signal zu schwach, wird die Nachricht nicht richtig interpretiert, und Pakete gehen verloren.

Das optische Energiebudget bezeichnet die Differenz zwischen der ursprünglichen Leistung des Senders und der Empfindlichkeit des Empfängers (siehe Abbildung 8). Passive TAPs lenken einen Teil des Lichts um, ohne das Signal dabei zu verstärken. Deshalb muss klar sein, wie viel Lichtverlust im Prozess entsteht, um später die richtigen Lichtmargen zu erhalten. Wichtig ist auch, dass die Sender und Empfänger außerhalb des TAPs liegen und alle ihren eigenen Grad der Abweichung haben. Die meisten Hersteller von Optiken stellen spezifische Informationen zur Leistung und Empfängerempfindlichkeit ihrer Produkte zur Verfügung, die von den Branchenspezifikationen erheblich abweichen können. In vielen Fällen sind die tatsächlichen Zahlen viel besser als das Institute of Electrical and Electronic Engineers (IEEE) sie in ihrem Standard 802.3 ausweist.

Es ist wichtig zu verstehen, was das Licht auf dem Weg von A nach B negativ beeinflussen kann. Einige Beeinträchtigungen wie zum Beispiel die Signaldämpfung lassen sich schon rein rechnerisch nicht vermeiden. Solche Beeinträchtigungen sind tendenziell linear und relativ gering im Vergleich zu anderen Verlustfaktoren. Dazu zählen fehlerhafte Verbindungen, schlechte Spleißstellen oder das Mischen verschiedener Kabeltypen, die negative Folgen haben und dringend vermieden werden sollten. Zur Prüfung von Kabelanlagen stehen tragbare optische Time-Domain Reflectometer (OTDR) zur Verfügung, bei denen eine Reihe von optischen Impulsen eingespeist und daraufhin das Licht gemessen wird, während es von Punkten entlang der Glasfaser zurückreflektiert wird. Obwohl diese oft zur Fehlerbehebung verwendet werden, können sie einige Ihrer Berechnungen schnell validieren.

	Kabeltyp	Durchmesser (µm)	Farbe	Anschluss	Allgemeine Anwendung
OM1	Multimode	62.5/125	Slate	LC	FE/1 Gb/10 Gb
OM2	Multimode	50/125	Orange	LC	FE/1 Gb/10 Gb
OM3/OM4	Multimode	50/125	Aqua	LC/MPO	FE/1 Gb/10 Gb/40 Gb/100 Gb
OS1/OS2	Singlemode	9	Gelb	LC	FE/1 Gb/10 Gb
Cat 5e/Cat 6A	Twisted-Pair-Kupferkabel	n/a	Diverse	RJ45	FE/1Gb

Abbildung 8: Gängige Kabeltypen

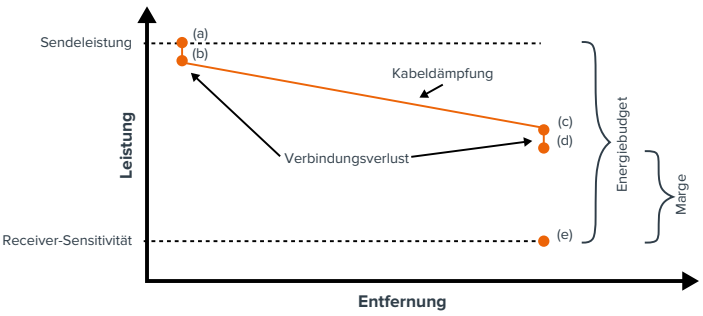

Abbildung 9: Theoretisches Verlustdiagramm

Das Diagramm (siehe oben) zeigt den voraussichtlichen Verlust zwischen zwei Endpunkten mit einem Sender an einem Ende und einem Empfänger am anderen Ende mit je zwei Anschlüssen (an jedem Ende). Die folgenden Formeln können hier angewandt werden:

Energiebudget = Sendestärke – Empfangsempfindlichkeit = a – e

Kabeldämpfung = Abnahme der Signalstärke aufgrund von Absorption und Streuung pro Kilometer eines bestimmten Kabeltyps = b – c

Signalverlust = Signalbeeinträchtigung durch Anschlüsse im System = (a - b) + (c - d)

Gesamtverlust der Verkabelung = Kabeldämpfung + Verbindungsverlust = (a – b) + (b – c) + (c – d)

Energiemarge = Zusätzliche Energie, die verbraucht werden könnte und dennoch ein wertvolles Signal liefert = Energiebudget – Gesamtverlust der Kabelanlage

Die beste Option ist, sofern möglich, die Berechnungen mit den tatsächlichen Zahlen der verwendeten Sendeempfänger und Kabel durchzuführen. Alternativ kann das Worst-Case-Szenario mit den nach IEEE-Spezifikationen festgelegten Mindestzahlen herangezogen werden. Wenn wir die Zahlen für eine 10 Meter lange OM2-Multimode-Faser mit 1 Gbit (gemäß den Spezifikationen von IEEE 802.3-2012 Abschnitt 3) nehmen, kämen wir zu folgendem Ergebnis:

1000BASE-SX-Transceiver mit durchschnittlicher Startleistung (Min.) = -9,5 dBm

1000BASE-SX-Empfängerempfindlichkeit = -17 dBm

Dämpfungsraten von Multimode-Kabel (für 10 Meter) = 3,5 dB/km = 0,035 dB/10m

Signalverlust von Multimode-Steckverbindern = 0,5 dB

Wenn man die Worst-Case-Zahlen in die ursprünglichen Gleichungen einfügt, kommt man zu den folgenden Ergebnissen:

Energiebudget = (-9,5) – (-17) = 7,5 dBm

Kabeldämpfung (10 Meter) = 3,5/100 = 0,035 dB

Signalverlust = 0,5 x 2 Anschlüsse = 1 dB

Gesamtverlust der Verkabelung= Kabeldämpfung + Verbindungsverlust = 0,035 + 1 = 1,035

Energiemarge = 7,5 – 1,035 = 6,465

Bei einer Energiemarge von 6,465 dB passt ein TAP sehr gut in dieses Netz. Der TAP mit dem höchsten Maximalverlust (siehe Abbildung 6) ist 6,2 dB (einschließlich Verbindungen zum TAP). Es gibt genügend Spielraum, um einen TAP mit einem Teilungsverhältnis von 50/50, 60/40 oder 70/30 anzuschließen. Nutzer sollten sich allerdings darüber im Klaren sein, dass jede Umgebung anders ist. Das oben gezeigte Beispiel mit einer 1-Gbit-Leitung bietet einen deutlich größeren Spielraum als schnellere Leitungen mit 10 Gbit, 40 Gbit oder 100 Gbit. Beispielsweise beträgt das gesamte Energiebudget, das für einige 40-Gbit-Transceiver mit kurzer Reichweite bereitgestellt wird, weniger als 2 dBm. Best Practices schreiben die richtigen Zahlen für jede Installation vor. Gigamon empfiehlt in der Regel nicht die Verwendung eines 70/30-Teilungsverhältnisses für 10-Gbit-Multimode-Infrastrukturen, da die Lichtmargen für den zum Monitoring vorgesehenen Traffic zu gering sind.

Um die Lichtverhältnisse für die richtige Platzierung eines passiven TAPs schnell zu ermitteln, sind die folgenden vier Faktoren wichtig:

1. Sendestärke (das anfängliche Lichtsignal)
2. Empfängerempfindlichkeit (Restlicht das am anderen Ende ankommt)
3. Lichtverlust innerhalb der Verkabelung (vor dem Einfügen des TAPs)
4. Auswirkungen des TAPs (der tatsächliche TAP-Signalverlust)

Aktive TAPs

Aktive TAPs sind nicht passiv. Sie benötigen eine eigene Stromquelle, um die Signale zu regenerieren. Das Teilungsverhältnis wird dabei nicht berücksichtigt, da der TAP die Nachricht empfängt und sie dann sowohl an die Netzwerk- als auch an die Monitoring-Zielpunkte weiterleitet. So betrachtet scheint das durchaus eine positive Funktion zu sein. Und trotzdem werden passive TAPs bevorzugt. Während eines Stromausfalls kann ein aktiver TAP das Signal nicht regenerieren und wird so selbst zur Fehlerquelle. Da ein passiver TAP nicht selbst mit Strom versorgt werden muss, wäre er bei einem Stromausfall nicht betroffen und die Pakete (die aus einer Quelle stammen, die noch mit Strom läuft) werden weitertransportiert. Einige aktive TAPs enthalten Bypass- oder Failover-Technologien, um dieses Problem zu umgehen. Dazu später mehr.

Wann werden aktive TAPs bevorzugt? Aktive TAPs werden häufig für die folgenden Anwendungen eingesetzt, bei denen passive TAPs keine gute Alternative sind:

1. Wenn nicht genügend Licht für einen Splitter vorhanden ist ➜ die Regeneration ist hier eine praktikable Lösung
2. Kupfer-basierte Infrastrukturen ➜ bei denen Elektrizität zur Bewegung von Elektronen verwendet wird (statt Photonen)
3. Signalkonvertierungen ➜ da ein aktiver TAP das Signal ohnehin regeneriert, kann er auch so programmiert werden, dass er ein anderes Signal erzeugt (z.B. 10 Gbit SR konvertiert in 10 Gbit LR)
4. SFP-basierte Verbindungen die anderweitig nicht unterbrochen werden können (wie z.B. eine TwinAX-Verkabelung) ➜ auch hier funktioniert die Regeneration

Solange die Nachteile eines Stromausfalls voll und ganz verstanden werden, bieten aktive TAPs einen ausgezeichneten Nutzen und erweitern die Sichtbarkeit auf Bereiche des Netzwerks, die sonst dem Monitoring verborgen blieben. Hochentwickelte aktive TAPs haben eine eigene, integrierte Batterieversorgung, um bei Stromausfällen für eine gewisse Zeit weiterlaufen zu können. Einige TAPs bieten zusätzliche Failover-Funktionen, wenn die Batterie zuneige geht. Ein Beispiel: Verlieren aktive TAPs aus Kupfer an Leistung, werden elektromagnetische Relais eingesetzt, die die Verbindung physisch schließen. So kann der Traffic weiterhin durch das Netzwerk fließen. Zwar wird so der Monitoring-Traffic gestoppt, aber der Durchfluss des Netzwerk-Traffics ist weiterhin gewährleistet. Wenn das Relais geschlossen wird, werden die Eigenschaften der Verbindung neu verhandelt. Das kann sich auf einige Pakete auswirken. Die TCP-Übertragung würde einen solchen Verlust in der Regel ausgleichen. Dennoch besteht hier für Netzwerke mit höherer Geschwindigkeit eine Gefahr. Denn diese sind unter anderem anfälliger für Änderungen der Routing-Tabelle.

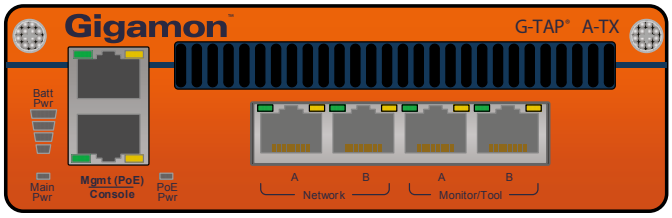

Abbildung 10: Ein Beispiel für einen G-TAP® ATX always-on Active TAP aus Kupfer mit mehreren Stromversorgungsoptionen, Batterie-Backup und Failover-Funktionen

Weitere TAPs

Bypass-Technologie

Mit der Bypass-Technologie kann Traffic aufgenommen und schnell umgeleitet werden. So kann man einen bestimmten Prozess „umgehen". Aus Hardwareperspektive ist die Bypass-Technologie die Weiterentwicklung eines TAPs. Sie verwendet ähnliche paarweise Querverbindungen für Ports wie ein TAP, um die für sicherheitsbasierte Inline-Tools typischen Verbindungsschutzfunktionen bereitzustellen.

Ein Inline-Tool leitet und verarbeitet den Live-Traffic durch ein Tool, bevor er an seinen tatsächlichen Bestimmungsort weitergeleitet wird. Die meisten Out-of-Band-Analyse-Tools haben keinen Einfluss auf den Live-Traffic. Ein Inline-Tool wie ein Intrusion Prevention System (IPS) kann hingegen Pakete im Produktionsnetzwerk ablegen oder sogar hinzufügen. Da es als Inline-Anwendung läuft, würde ein Ausfall des Tools sich dramatisch auf das gesamte System auswirken und es sogar ganz zum Absturz bringen. Die Bypass-Technologie wurde entwickelt, um genau das zu verhindern. Diese Tools können ein beeinträchtigtes oder ausgefallenes Tool umgehen. Beispielsweise bei einem Stromausfall oder sogar bei einer Überbelegung. Der Bypass überwacht dabei das Tool kontinuierlich durch Heartbeats. Durchläuft ein Heartbeat das Tool nicht korrekt, schließt es automatisch die Verbindung und stellt eine Bypass-Verbindung her.

Aggregations-TAP vs. Aggregationsknoten

Wie bereits erwähnt, gibt es bei TAPs getrennte Monitoring-Ports für den Ingress- als auch für den Egress-Datenverkehr. Das ist einer der Vorteile von TAPs. Es gibt aber auch einige TAPs, die beide Feeds in einem einzigen Monitoring-Port kombinieren. Das wird oft als Aggregations-TAP bezeichnet. Der Vorteil ist, dass die Anzahl der Monitoring-Ports dadurch reduziert wird. Allerdings besteht der Nachteil darin, dass es zu Überbelegungen oder verlorenen Paketen kommen kann. Deshalb werden diese Devices nicht unbedingt immer empfohlen. Bei Verbindungen mit geringer Auslastung (<5 - 10 %) ist es meist besser, den Edge-Traffic von mehreren TAPs mit Hilfe eines Aggregationsknotens zu kombinieren. Diese Geräte, wie die Gigamon GigaVUE-TA Serie, bieten Filterregeln, um den Datenverkehr zu aggregieren, bevor er an intelligentere Komponenten der Visibility-Plattform gesendet wird.

Standalone vs. Embedded TAPs

TAPs werden normalerweise als eigenständige Geräte über das gesamte Netzwerk hinweg eingesetzt, je nachdem, wo der Traffic angezeigt werden muss. Die Monitoring-Ports können entweder direkt mit dem Analyse-Tool oder mit den Visibility-Knoten verbunden werden, um den Datenverkehr effizient zu filtern und dann auf mehrere Tools zu verteilen. Der Trend geht mittlerweile aber mehr und mehr in Richtung TAP-Hardware als integriertes Modul innerhalb eines Visibility-Knotens. Ein wesentlicher Unterschied zwischen eigenständigen (Standalone) TAPs und integrierten (Embedded) TAPs sind die offenliegenden Ports. Standalone TAPs verfügen sowohl über Ports für Netzwerk- als auch für Monitoring-Verbindungen, während Embedded TAPs nur die Netzwerk-Ports freigeben. Die Monitoring-Ports sind direkt mit der Backplane des Systems verbunden und entsprechend geroutet. Dadurch wird die Verkabelung insgesamt vereinfacht und die Effizienz des operativen Betriebs gesteigert. Da es keine offenen Monitoring-Ports gibt, kann weder ein Sniffer noch ein anderes Erfassungsgerät ohne eine ordnungsgemäße Konfiguration angeschlossen werden. Das schafft eine sicherere Umgebung.

10GBASE-T

10GBASE-T ist eine Ethernet-Technologie für eine 10 Gbit/s-Datenübertragung über Kupferkabel mit kurzer Reichweite. Sie wird hauptsächlich für Top-of-Rack-Switches, Server oder andere Geräte in Rechenzentren eingesetzt, um die Kosten für Infrastruktur und Konnektivität zu senken. Moderne 10GBASE-T SFP+-Transceiver übersteigen den in der SFP+-Spezifikation (SFF-8431) geforderten maximalen Energieverlust. Darüber hinaus sind Verbindungen von 10 Gbit/s nicht für TAPs geeignet, da bei solchen Geschwindigkeiten auf einer Kupferdraht-Verbindung ein Rauschen auftritt. Empfohlen wird daher:

- Die beste Option: Verwenden Sie kein 10GBASE-T, wenn sie TAPs verwenden müssen. Stattdessen sollten Sie auf eine 10G Short-Reach (SR)-Schnittstelle zurückgreifen, die sich leichter monitoren lässt.
- Alternative 1: Sie können auch einen SPAN-Port bzw. Mirror-Port auf dem Switch verwenden, der den 10GBASE-T-Link hostet. Bei dieser Option sollten Sie allerdings darauf achten, dass SPAN-Sessions gewisse Einschränkungen mit sich bringen, wie in Kapitel „TAP vs. SPAN" erläutert.
- Alternative 2: Verwenden Sie Back-to-Back-Medienkonverter mit einem TAP oder Port-Paar. Beachten Sie, dass dies kein Fail-to-Wire ist und dass eine 10GBASE-T PHY wichtige Signale verarbeitet und eine höhere Latenz aufweist als die entsprechende 10G optical PHY. Vor allem bei latenzempfindlichen Anwendungen müssen die Auswirkungen der beiden Medienkonverter berücksichtigt werden.

TAP Best Practices

Ein TAP ist einer der Grundbausteine für jedes Visibility-System. Für eine lückenlose Erfassung haben viele Unternehmen eine TAP-ALL-Strategie eingeführt. Das bedeutet, dass alle kritischen Verbindungen mit TAPs (und/oder SPANs) eingerichtet werden, auch wenn der Traffic nicht ständig überwacht wird. Da der TAP aber bereits vorhanden ist, sind die Daten im Falle einer Sicherheitslücke oder bei der Fehleranalyse leicht zugänglich.

Bestenfalls implementiert man einen TAP direkt bei der Einrichtung der gesamten Infrastruktur, denn eine nachträgliche Aufrüstung ist immer teurer. Für eine TAP-Installation muss die Netzwerkverbindung unterbrochen werden. Deshalb sollte ein Zeitfenster für die Wartung eingeplant werden.

Obwohl TAPs meistens gegenüber SPAN-Ports bevorzugt werden, haben beide ihren Nutzen. Physische TAPs entsprechen Best Practice bei kritischen Verbindungen mit mittlerer bis hoher Auslastung. SPANs am besten in Bereichen einsetzen, in denen TAPs nicht geeignet sind. Dazu gehören beispielsweise Verbindungen mit eingeschränktem Energiebudget sowie Remote-Standorte mit niedrig ausgelasteten Verbindungen.

Wenn beide Optionen zur Verfügung stehen, werden in der Regel passive TAPs gegenüber aktiven TAPs bevorzugt. Hauptgrund dafür ist, dass passive TAPs bei Stromausfällen die Verlustrate kleinhalten. Das ändert sich allerdings: Aktive TAPs verstärken das Signal, um größere Entfernungen überbrücken zu können. Gleichzeitig besitzen viele aktive TAPS mittlerweile eine eigene Notstromversorgung mit Batterien, um einen ausfallsicheren Betrieb zu gewährleisten.

Sie müssen die vorhandenen Einschränkungen der Lichtverhältnisse genau kennen, bevor Sie Änderungen an Ihrer Infrastruktur vornehmen. Energiebudgets sind die Basis für einen ordnungsgemäßen Einsatz von TAPs. Sie werden zudem dazu verwendet, die geeigneten Teilungsverhältnisse für den Einsatz zu bestimmen. Als Risiko in Bezug auf Verluste zählen Entfernung (Dämpfung), Verbindungen, Teilungsverhältnisse, Spleiße und verschmutzte Umgebungen. Am besten verwenden Sie die Empfindlichkeits- und Leistungswerte Ihrer Glasfaserkabel. Wenn die tatsächlichen herstellerabhängigen Lichtwerte nicht verfügbar sind, können Sie auf die IEEE-Spezifikationen zurückgreifen. Ist das Energiebudget zu knapp bemessen, sollten Sie erwägen, ob für Sie ein aktiver TAP oder SPAN-Port in Frage kommt. Alternativ können Sie Ihre Glasfaser und deren Verkabelung so aufrüsten, dass diese sich auch für größere Entfernungen eignen. Glasfaserkabel für größere Entfernungen sind teurer, werden aber meist mit High-End-Lasern kombiniert. So entsteht ein deutlich stärkeres Signal. Dennoch sind die höheren Ausgaben an dieser Stelle meist sinnvoll, denn eine zusätzliche Energiemarge senkt bei einer kritischen Verbindung viele Risiken.

Wenn ein TAP ausfällt, liegt das meist an einer unsachgemäßen Verkabelung. Verwenden Sie deshalb immer neue Kabel und reinigen Sie alle Verbindungen ordnungsgemäß, bevor Sie TAPs anschließen. Kombinieren Sie auch niemals Kabeltypen innerhalb einer Ende-zu-Ende-Verbindung. Überprüfen Sie die Schaltpläne, um sicherzustellen, dass an jedem Port die richtigen Kabel angeschlossen sind. Passen Sie jeden TAP an den verwendeten Kabeltyp an, und biegen Sie die Kabel nie weiter als in den Kabeltyp-Angaben beschrieben. Verwenden Sie für neuere Technologien, wie z.B. Cisco BiDi-Implementierungen, ausschließlich TAPs, die für genau die verwendeten Wellenlängen ausgelegt sind.

Nicht alle TAPs sind gleich geschaffen. Erkundigen Sie sich bei Kollegen ihrer Branche nach Empfehlungen von Qualitätsanbietern und fragen Sie nach Hardware-Garantien. Wie bei Glasfaser-Transceivern können die Kilometerangaben ja nach Anbieter variieren. Gibt ein Anbieter nur eine kurze Garantie auf sein Produkt, sollten Sie unbedingt die Qualität der Produkte in Frage stellen. Außerdem kann es nicht schaden, nach der Mean Time Between Failure (MTBF) zu fragen.

Zwar kann ein TAP direkt mit einem Monitoring-Tool verbunden werden. Es ist es aber deutlich besser, den TAP direkt mit der Gigamon Visibility Platform zu verbinden. Die Visibility Platform ist eine Matrix aus Knoten, die über die gesamte Infrastruktur verteilt sind und als zusammenhängende Plattform funktionieren. Sie leitet Pakete aus jeder Quelle zu den richtigen Monitoring-, Analyse- oder Sicherheitstools weiter.
Die Konsolidierung Ihrer Tools ermöglicht es Ihnen, Ihre Monitoring-Lösungen zu optimieren und erhöht gleichzeitig die Sichtbarkeit Ihres gesamten Netzwerks für durchgängige Security und Analysen. Der Datenverkehr kann je nach Bedarf repliziert, aggregiert oder gefiltert werden. Auch höherwertige Sicherheits-Funktionen wie Paket-Deduplizierung, SSL/TLS-Entschlüsselung oder Header Stripping sind innerhalb der Plattform möglich. So werden einzelne Tools entlastet und Probleme können schneller gelöst werden. Verfügbar ist außerdem die NetFlow-Generierung. So können kritische Switches und Router effizienter genutzt werden.

Zusammenfassung

Ein TAP stellt den Verbindungspunkt dar, an dem der reale Datenverkehr direkt aus dem Netzwerk kopiert wird. Deshalb ist ein TAP der erste Schritt zu jeder Visibility-Lösung. TAPs können entweder Standalone-Geräte oder direkt als Modul innerhalb eines Visibility-Knotens integriert sein. Bei beiden Lösungen wird der Datenverkehr zu Monitoring-, Sicherheits- und Analysezwecken kopiert, während der Datenverkehr weiterhin das Netzwerk durchläuft.

Über Gigamon

Gigamon ist das weltweit erste Unternehmen, das eine einheitliche Sichtbarkeit und Analyse des gesamten Datenverkehrs von Rohpaketen bis zu Apps über physische, virtuelle und Cloud-Infrastrukturen hinweg bietet. Wir erfassen, verarbeiten und analysieren Netzwerk-Traffic, um kritische Performance- und Sicherheitsanforderungen zu erfüllen einschließlich einer schnellen Aufdeckung und Behandlung von Bedrohungen. So halten Sie Ihrer Organisation den Rücken frei, digitale Innovationen voranzutreiben. 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 Branche führenden Kundenzufriedenheit mit mehr als 3.500 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/.

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