NEOX NETWORKS

WATCH YOUR NETWORK!

www.neox-networks.com

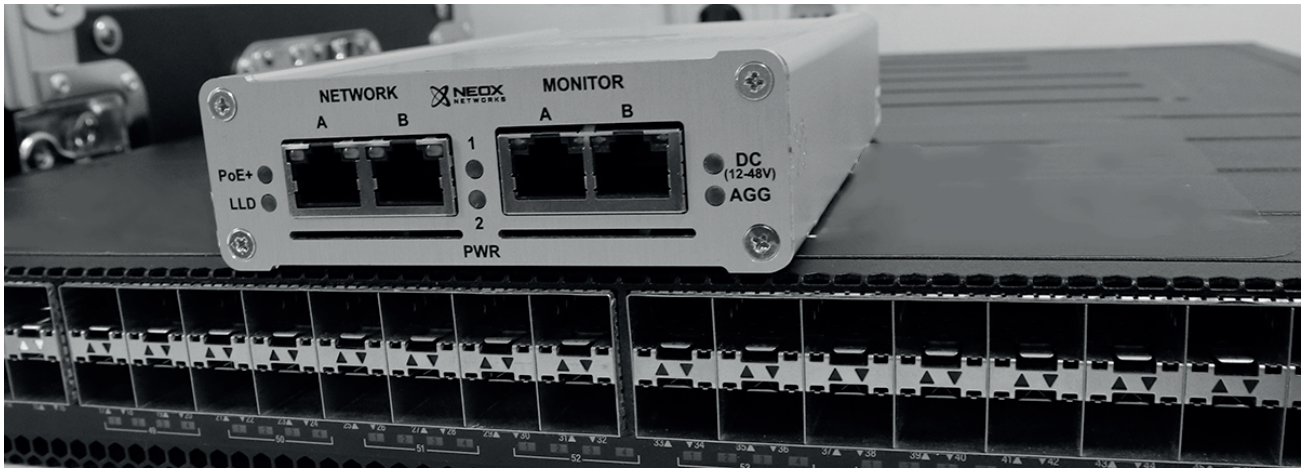
WHITEPAPER

NETZWERK-TAP GEGEN SPAN/MIRROR-PORT

PROFESSIONELLE AUSLEITUNG DER NETZWERKDATEN FÜR MONITORING-, ANALYSE- UND SECURITY-TOOLS

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig



1. Einleitung

Monitoring-, Analyse- und Out-of-Band-Security-Tools haben alle eines gemeinsam: Sie benötigen eine zuverlässige Datenquelle, aus der sie die Netzwerkdaten beziehen können, und sind auf diese Quelle angewiesen, damit sie funktionieren können. Wie aber führt man die Netzwerkdaten am besten diesen Tools zu?

Viele sind der Ansicht, dass sie zur Ausleitung der Netzwerkdaten einfach einen SPAN-Port, auch Mirror-Port genannt, auf bestehenden Switches konfigurieren können. Auf diesem Port wird dann je nach Konfiguration eine Kopie der Netzwerkdaten, die über den Switch laufen, ausgegeben.

Andere setzen lieber auf Netzwerk-TAPs (TAP steht für Test Access Point oder auch Test Access Port), also auf spezielle Geräte, die in eine Netzwerkleitung eingeschleift werden und eine Kopie der über diese Leitung gesendeten Netzwerkdaten aus dem produktiven Netzwerk ausleiten.

Welche dieser beiden Möglichkeiten man wählen sollte und welche Gründe dies hat, wollen wir uns auf den folgenden Seiten näher betrachten.

2. Funktionsweise eines SPAN/Mirror-Ports

Um die Vor- und Nachteile eines SPAN-Ports zu kennen, muss man zuerst verstehen, wie dieser funktioniert.

Das Konzept selbst ist sehr simpel. Nachdem vom Nutzer ein freier Port auf einem Switch als SPAN-Port definiert wurde, werden ankommende Datenpakete vom Betriebssystem des Switches entsprechend dupliziert und auf eben jenem SPAN-Port als Duplikat ausgegeben.

Gleichzeitig verliert der SPAN-Port seine Funktion als Switch-Port, da alle ankommenden Pakete vom Switch verworfen werden.

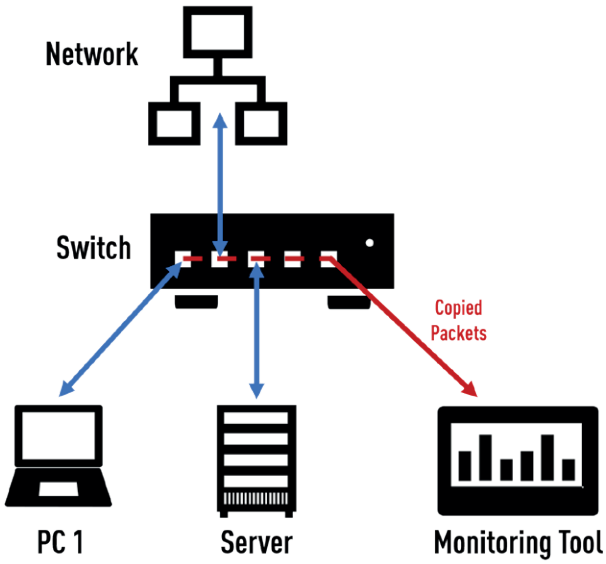


Abbildung 1: Funktionsweise eines SPAN/Mirror-Ports

3. Funktionsweise eines Netzwerk-TAPs

Anders als bei einem SPAN-Port, welcher die Duplikate in Software erstellen muss, arbeitet ein Netzwerk-TAP mittels dediziertem FPGA auf OSI Layer 1, sprich Signalebene.

Aber Achtung! Wirklich jeder TAP? Mitnichten! Bitte beachten Sie, dass wir uns im Folgenden auf einen Netzwerk-TAP beziehen, welcher wie unsere PacketRaven Modelle auf einen entsprechenden FPGA-Chipsatz setzt.
Der Begriff TAP ist bis dato weder geschützt noch entsprechend standardisiert. Manche Hersteller setzen bei ihren Netzwerk-TAPs weiterhin reguläre Switche ein und bieten die TAP-Funktionalität mittels fest eingestellter SPAN-Session an. Auf diese und ähnliche Ansätze treffen die folgenden Vorteile, die ein TAP bringen kann, natürlich NICHT zu!

Ein TAP wird typischerweise zwischen 2 Endgeräte gesetzt und die Verbindung dieser beiden Geräte durch die Netzwerk-Ports A und B durchgeschliffen. Somit sitzt der TAP transparent in der zu überwachenden Leitung und kann, insofern es sich um einen FPGA-basierten TAP handelt, sämtliche Pakete, welche die Endgeräte austauschen, auf Signalebene duplizieren.

Dies ist auch ein wichtiger Unterschied zum SPAN-Port, welcher aufgrund seiner Funktionsweise nur valide Ethernet Pakete während des Verarbeitens duplizieren kann, ein TAP jedoch greift auf der niedrigsten OSI-Schicht die Daten ab und wird immer und grundsätzlich alle ausgetauschten Informationen dem angeschlossenen System zur Verfügung stellen. Solange es ein Ethernet-Paket ist, wird es dupliziert, egal welche Größe es hat und wie viele Tunnel oder Enkapsulierungen vorhanden sind. Selbst defekte Pakete, die ein Switch ohne Ausnahme verwirft, werden verlustfrei unter Beibehaltung der Datenintegrität dupliziert.

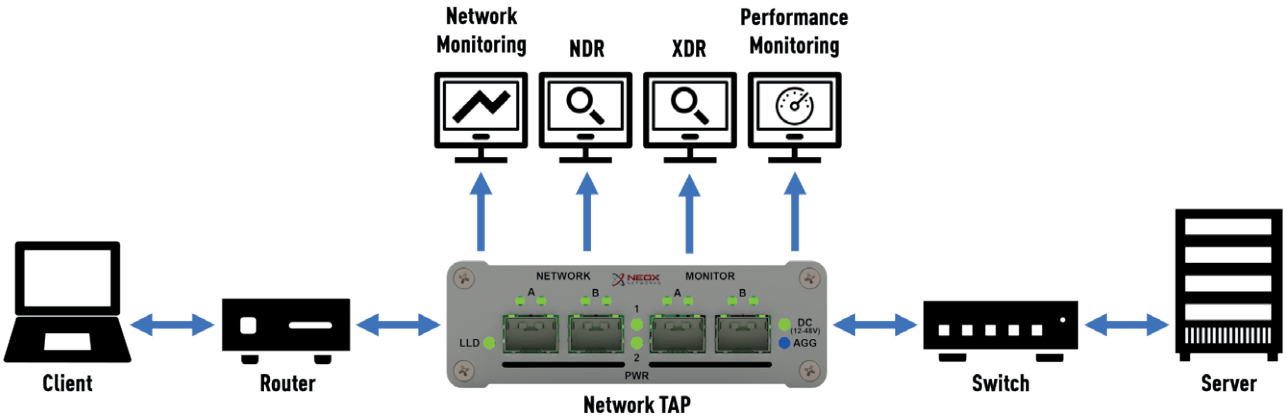


Abbildung 2: Funktionsweise eines Netzwerk-TAPs

4. Konfigurationsaufwand und Risiko einer Fehlkonfiguration

Wie bereits oben angemerkt, muss ein SPAN-Port manuell ausgewählt und definiert werden. Hierfür wird natürlich erstmal ein freier Port benötigt, welcher die duplizierten Daten vom System ausgeben soll. Dies allein kann je nach Szenario schon bereits zu den ersten Problemen führen, da freie Ports auf Switches je nach Umgebung gerne auch mal Mangelware sind.

Der Benutzer muss sich weiterhin auch im Klaren darüber sein, welche Verbindungen genau er überwachen möchte, da ein Switch nur eingangsseitig Pakete duplizieren kann, Daten welche den Switch verlassen, können hier von der Software nicht mehr erreicht/dupliziert werden.

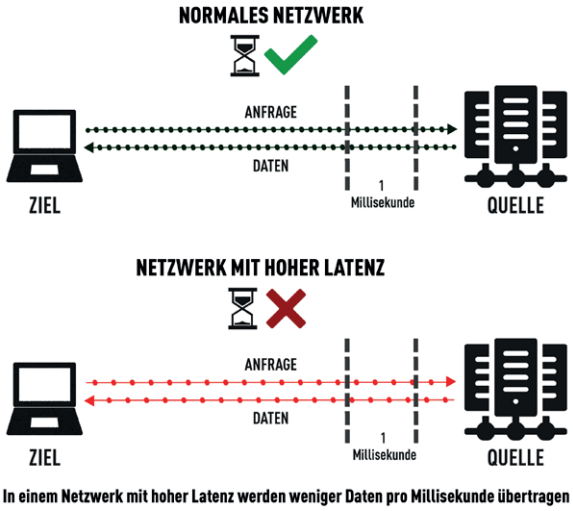
Ein großer Teil des Risikos eines SPAN-Ports jedoch liegt in der Gefahr einer falschen Konfiguration. Da ein SPAN-Port keine ankommenden Daten verarbeitet und versucht vollständig zu verwerfen, kann eine Fehlkonfiguration dazu führen, das der Administrator sich selbst vom System aussperrt, sollte es dazu kommen, das er ausversehen den einzigen Port mit der MGMT IP als SPAN-Port definiert.

Ein wichtiges Gut in der Paketanalyse ist die Reihenfolge der Pakete selbst! Wenn die Daten beispielsweise in Ihrem Monitoring in der falschen Reihenfolge eintreffen, kann dieses keinerlei Auswertungen mehr anstellen. Da der Switch jedes Paket, bildlich gesprochen, „anfassen" muss, besteht immer Raum zum fehlerhaften Handling der Pakete, u.a. mit dem Best-Effort-Prinzip begründet, welches wir weiter unten noch einmal extra behandeln.

Eine falsche Reihenfolge ist daher nicht unüblich in stark ausgelasteten Netzen. Doch nicht nur die Reihenfolge selbst kann davon betroffen sein, auch das sogenannte Timing der Daten, sichergestellt durch den Inter Frame Gap (IFG), kann sich ändern, was die Akkuratheit jeder Analyse fraglich erscheinen lässt.

Doch selbst wenn keine der obigen Nebenwirkungen auftreten, sind zeitlich akkurate Messungen mit einem SPAN-Port nur schwer möglich, allein aufgrund der hinzugefügten Latenz (*Abbildung 3.*) zu den duplizierten Daten. Während ein FPGA-basierter Netzwerk-TAP gerne mal eine zusätzliche Latenz im nur einstelligen Nanosekundenbereich zu den duplizierten Daten hinzufügen mag, lässt sich solch eine Aussage für Switche gar nicht erst tätigen, da wir hier um viele Faktoren höher liegen und noch zusätzlich gewaltigen Schwankungen unterliegen können.

Ein weiteres Risiko der Fehlkonfiguration steckt in der Gefahr zu doppelten Paketen, auch hier kann es sehr schnell passieren, dass fälschlich vorgenommene Konfigurationen an der SPAN-Session und daraus resultierenden doppelten Datensätzen eine Überbuchung Ihres SPAN-Ports oder aber sogar Ihrer angeschlossenen Lösung selbst hervorrufen können.



In einem Netzwerk mit hoher Latenz werden weniger Daten pro Millisekunde übertragen

Abbildung 3: Unterschied von normaler und hoher Latenz. Jeder Punkt im obig illustrierten Netzwerkverkehr stellt einen Ethernet-Frame dar!

Hierzu ein Beispiel (*Abbildung 4.*) anhand einer auf VLAN basierten SPAN-Session: Möchte man die Daten von VLAN 100 und VLAN 200 auf einem SPAN-Port ausgegeben bekommen, wird der Switch die Daten, welche er mit VLAN 100 empfängt, auf dem SPAN-Port ausgeben und danach die selben Daten, diesmal jedoch mit VLAN 200 gestempelt, ebenfalls auf dem SPAN-Port ausgeben. Das Resultat sind dann doppelte Pakete in Richtung Ihres Monitoring-Systems.

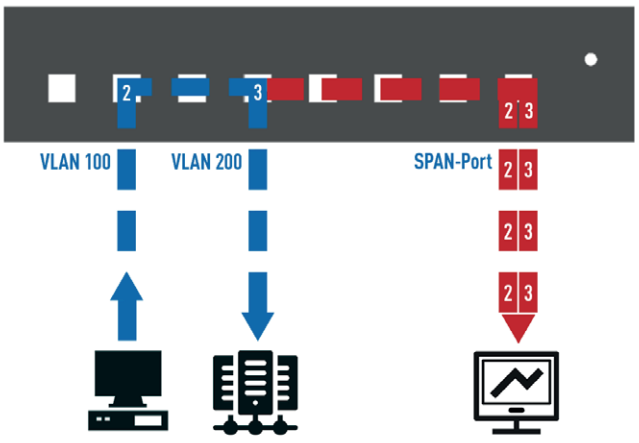


Abbildung 4: Problem - doppelte Pakete

Auch die Nutzung des Parameters „Both" bei der Einrichtung einer SPAN-Session kann solch ein Verhalten provozieren. „Both" bezieht sich hierbei auf die Sende- und Empfangsrichtung der übertragenen Daten, in Kombination mit einem VLAN wird der Switch dementsprechend alle Daten duplizieren, welche das VLAN betreten und jene die es wieder verlassen, auch hier sind doppelte Pakete das Resultat, welches auf Ihrem Monitoring-System sichtbar wird.

Bis hierhin haben wir ausschließlich über mögliche Fehler bei der Software-seitigen Einrichtung des Switches gesprochen. Nicht außer Acht zu lassen ist jedoch auch die physikalische Komponente. Sollte eine SPAN-Session für bestimmte Ports eingerichtet worden sein, jedoch ein Kollege/Mitarbeiter, entweder unwissentlich ob der SPAN-Session oder aus anderen Gründen die zu überwachenden Geräte einfach an einen anderen Port auflegen, verlieren Sie das gesamte Monitoring, solange die SPAN-Session nicht entsprechend angepasst wurde. Ein Umpatchen von Geräten auf andere Ports kann hier ganz schnell zum Abbau von wichtiger Netzwerktransparenz führen.

5. Sichtbarkeit im Netzwerk

Ein Netzwerk-TAP ist, wie bereits erwähnt, aufgrund seiner FPGA-basierten Bauweise immer und grundsätzlich zu 100% unsichtbar im Netzwerk! Da er auf OSI Schicht 1 arbeitet, besitzt er auch keine MAC- oder IP-Adresse und kann weder gehackt noch kompromittiert werden.

Fairerweise ist jedoch festzuhalten, dass auch ein SPAN-Port unsichtbar im Netz ist, jedoch nicht gefeit vor Angriffen. Der Switch selbst bietet große Angriffsflächen für Eindringlinge, welche Mittel und Wege haben, einen SPAN-Port außer Betrieb zu setzen, dies ist bei einem Netzwerk-TAP unmöglich.

Während also ein TAP immer unsichtbar und unangreifbar ist, ist ein SPAN-Port zwar ebenfalls per se unsichtbar, jedoch nicht unangreifbar.

6. Gefahr einer Kompromittierung

Ein TAP bietet keinerlei Angriffsfläche für jedwede Art der Kompromittierung, er kann weder erkannt noch gehackt werden, dies lässt seine Bauweise aufgrund des FPGAs auch gar nicht zu.

Ein SPAN-Port selbst bietet erstmal auch keine Angriffsfläche, das Betriebssystem des Switches, welche auch für die Duplizierung und Bereitstellung der Daten für den SPAN-Port zuständig ist, jedoch schon!

Überprüfen und Einspielen regelmäßiger Updates auf den Switch sind hier, je nach Umgebung, absolute Pflicht!

Ein Netzwerk-TAP bietet weder die angesprochene Angriffsfläche, noch benötigt er irgendwelche Updates.

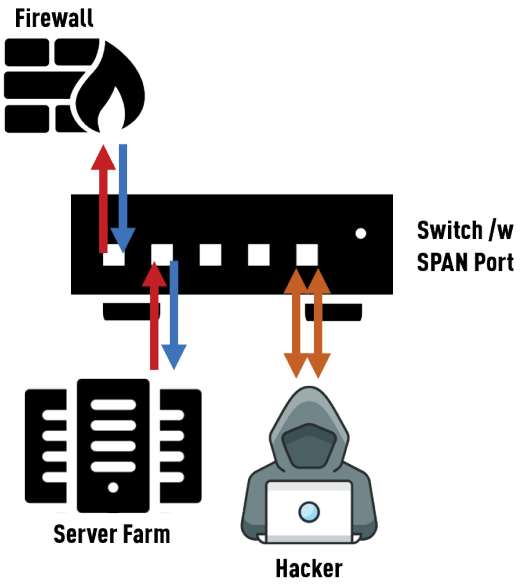


Abbildung 5: SPAN-Port Kompromitierung

7. Potentielle Überbuchung

Die Gefahr einer Überbuchung des SPAN-Ports ist imminent. Ein SPAN-Port hat mehrere Limitierungen was den Durchsatz betrifft, eine davon ist natürlich erst einmal die maximale theoretische Bandbreite des Ports, bei einer Link-Aushandlung mit 1000Base-T sind das theoretisch 1000 Mbit/s. Dieser Wert wird jedoch schwerlich erreicht, da die „Quelle" der Daten ein Softwarebestandteil des Systems ist, welcher die Duplizierung zusätzlich zu seiner regulären Aufgabe, dem Switching, erledigten muss.

Doch wie genau kann man einen SPAN-Port überbuchen? Wenn man sich noch einmal anschaut, wie genau ein SPAN-Port eingerichtet wird, erkennt man, das es sehr schnell passieren kann, das man zu viele Quell-Ports zu der SPAN-Session hinzufügt und diese dann die maximale Bandbreite des SPAN-Ports übersteigt.

Dazu ein Beispiel: An einem Switch sind 2 Server und 4 Clients angeschlossen. Möchte man nun sämtliche Daten, welche zwischen Server und Clients ausgetauscht werden, mitlesen und auswerten, werden alle 6 Ports zu der SPAN-Session hinzugefügt. Man könnte nun denken, dass es reicht, die 2 Ports mit dem angeschlossenen Server zu überwachen.

Einer der Nachteile einer SPAN-Session liegt jedoch darin, das nur ankommende Pakete dupliziert werden, keine ausgehenden.

Möchte man nun eine Full-Duplex Analyse des Verkehrs zwischen Clients und Servern machen, müssen auch die Clients in die SPAN-Session mit aufgenommen werden und somit auch sämtlicher Datenverkehr der Clients, welcher nicht für die Server bestimmt ist, da ein Switch hier keine Unterscheidung vornehmen kann.
Somit kann die Summe der duplizierten Pakete sehr schnell die theoretische Bandbreite eines SPAN-Ports übersteigen, ganz zu schweigen von der eigentlichen Bandbreite jenes Ports, welche durch die Software des Switches limitiert wird. Das Resultat ist dann, dass Ihrer angeschlossenen Lösung nicht alle Datenpakete zugeleitet werden.

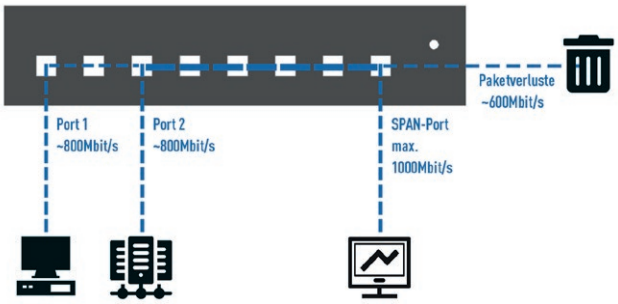


Abbildung 6: SPAN-Port Überbuchung/Oversubscription

Auch hier kann ein Netzwerk-TAP helfen! Ein TAP arbeitet immer mit der maximalen theoretischen Bandbreite und kann nie überbucht werden, selbst Microbursts, egal welcher Größenordnung, werden regulär verarbeitet und als Duplikat ausgegeben, die einzige Limitierung ist das Netzwerk selbst!

8. Best-Effort-Prinzip und hohe Netzlast

Dies bringt uns direkt zum nächsten Problem welches je nach Blickwinkel aber auch gewollt ist! Die primäre Aufgabe eines Switches ist das Switching, hierfür wurde das Gerät entwickelt, produziert und schlussendlich auch vom Kunden eingekauft.
Die Möglichkeit der Einrichtung einer SPAN-Session ist nur eine zusätzliche Dreingabe der Hersteller. Damit einhergehend ist das sogenannte Best-Effort-Prinzip, welches dafür sorgt, dass im Falle einer hohen Netzlast der reguläre Betrieb und damit das Switching immer und zu jeder Zeit Vorrang vor anderen möglichen Aufgaben des Switches hat, wie z.B. dem Generieren von Netflow Daten oder aber auch eine SPAN-Session.

Diese Eigenschaft, welche alle Switches gemein haben, könnte ein potentieller Angreifer ausnutzen, indem er künstlich eine hohe Last im Netzwerk erzeugt und damit den Switch zwingt, Pakete für die SPAN-Session nicht mehr duplizieren zu können, da dieser mit seiner grundsätzlichen Arbeit zu beschäftigt ist. Das Best-Effort-Prinzip erlaubt es somit dem Switch, die SPAN-Session mit einer niedrigen Priorität zu versehen.

Ein Netzwerk-TAP hingegen hat keine dieser Einschränkungen. Weder unterliegt er einem Best-Effort-Prinzip, noch lässt er sich von einer hohen Netzlast aus der Ruhe bringen, der FPGA sorgt jederzeit dafür, dass sämtliche Signale immer und jederzeit dupliziert werden. Wichtig hierbei ist, noch einmal zu verdeutlichen, dass ein TAP auf Signal-Ebene arbeitet und nicht auf MAC- oder gar IP-Ebene, er besitzt daher auch kein Konzept für Best-Effort oder dergleichen, alle Signale werden bei Full-Line-Rate ohne Engpässe verarbeitet.

9. Vollständigkeit der übertragenen Daten

Auch hier können wir direkt an dem oben aufgeführten Punkt anknüpfen und über ein weiteres wichtiges Thema sprechen, namentlich die Vollständigkeit der Daten. Zusammengefasst kann man hier sagen, dass diese nicht jederzeit gegeben ist, eben aufgrund des bereits angesprochenem Best-Effort-Prinzips unter welchem der SPAN-Port arbeitet.
Leider gibt es keine Zähler oder Speicher, welche die nicht duplizierten Pakete zwischenspeichern oder wenigstens zählen. Daraus leitet sich dann sehr schnell ab, dass ein SPAN-Port keine verlässliche Datenquelle für Ihr Monitoring, geschweige denn Ihre Security-Installation ist.
Es sollte sich daher schon abzeichnen können, dass ein Netzwerk-TAP, eben aufgrund des Fehlens jeglicher Nachteile eines SPAN-Ports die Vollständigkeit als auch die Integrität der Daten zu jeder Zeit garantiert!

10. Integrität der übertragenen Daten

Speziell im Hinblick auf Security und vielleicht sogar etwaige Cyber-Versicherungen ist die Datenintegrität von unumstößlicher Wichtigkeit!

Gerichtsverwertbarkeit ist hier das Zauberwort. Leider kann ein SPAN-Port Daten dieser Güte niemals liefern, da z. B. etwaige VLANs, welche der Switch auf ausgehende Datenpakete stempelt, nicht dupliziert werden können.

Somit gehen wichtige Informationen verloren und die Software-basierte Duplizierung der Daten tut ihr Übriges bei einer möglichen Manipulation der Daten.

Es kann daher nie wirklich sichergestellt werden, dass die duplizierten Daten eine exakte Kopie des eigentlichen Netzwerkverkehrs sind.

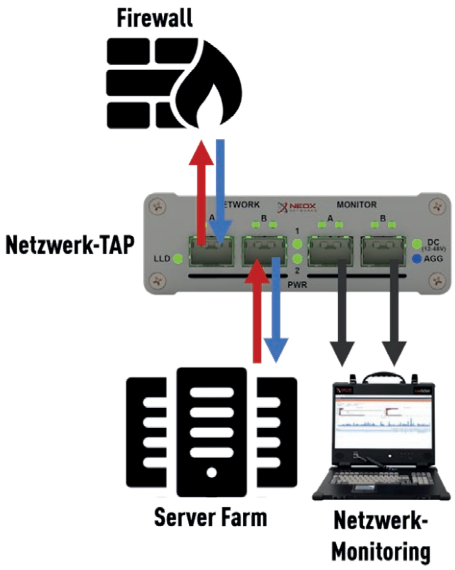


Abbildung 7: Portabler TAP für das Netzwerk-Monitoring

11. Rückwirkungsfreiheit auf das produktive Netzwerk

Auch in diesem Punkt hat der Netzwerk-TAP wieder die Nase vorn: Nicht nur dass ein Switch aufgrund einer eingeschalteten SPAN-Session möglicherweise höhere Latenzen im Netzwerk verursacht, auch das Blockieren von ankommenden Daten am SPAN-Port ist eine Software-seitige Funktion.
Eine offene Sicherheitslücke, ein nicht eingespielter Patch o. ä. könnten dafür sorgen, dass ein Angreifer über ein kompromittiertes Monitoring-System Zugriff auf den Switch und somit auf Ihr Netzwerk erhält.

All dies ist mit einem TAP unmöglich, da hier auf eine Reihe an Sicherheitsmerkmalen gesetzt wurde, welche teilweise rein physikalischer Natur sind. Eine davon ist die Datendiodenfunktion (*Abbildung 9.*), welche alle unsere elektrifizierten TAPs gemeinsam haben. Daten, die das Monitoring-System an den TAP zurücksendet, werden entweder aufgrund einer galvanischen Trennung gar nicht erst zum FPGA durchgeleitet.
Im Falle unserer hybriden TAPs scheitert die Rückleitung von Daten über die Monitoring Ports an die Netzwerk Ports an der optisch-elektrisch-optischen Umwandlung, welche auch hier wieder mittels physikalisch nicht verdrahteten Komponenten ein Rückwirken ins Netzwerk verhindern.

Bei reinen Glasfaser TAPs können wir ebenfalls mittels spezieller Splitter (*Abbildung 8.*) eine solche Rückwirkungsfreiheit implementieren.

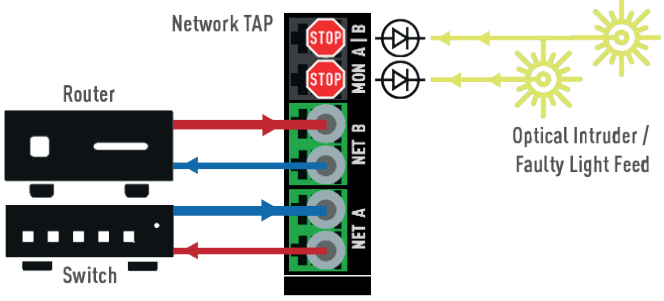


Abbildung 8: Modularer TAP mit optischem FIlter und Isolator

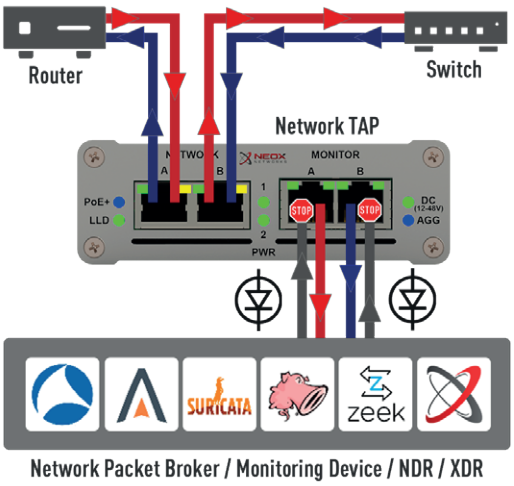


Abbildung 9: Portabler TAP mit Datendioden-Funktion

12. Fazit

Es bleibt festzuhalten: Das Abgreifen des Netzwerk-Verkehrs über ein Netzwerk-TAP hat viele Vorteile gegenüber dem Ausleiten über einen SPAN-Port. Netzwerk-TAPs sind die einzig zuverlässige Datenquelle, welche Ihnen 100% Transparenz, Sichtbarkeit und Sicherheit im Netzwerk garantieren!

Gerne beraten wir Sie zu unseren verschiedenen PacketRaven Netzwerk-TAPs und deren Eigenschaften, sowie zu Ihren individuellen Anforderungen. Unsere Kontaktdaten finden Sie untenstehend!

Abbildung 10: Modulare Glasfaser-Netzwerk-TAPs und Chassis

Abbildung 11: Portable und rackmontierbare Netzwerk-TAPs

NEOX NETWORKS GmbH
Monzastr. 4 · 63225 Langen · Germany
+49 6103 / 37 215 910
solutions@neox-networks.com
www.neox-networks.com