

## ANPASSUNG DES DATENVERKEHRS AUFGRUND GELÖSCHTER KOPFDATEN

### PROBLEM:

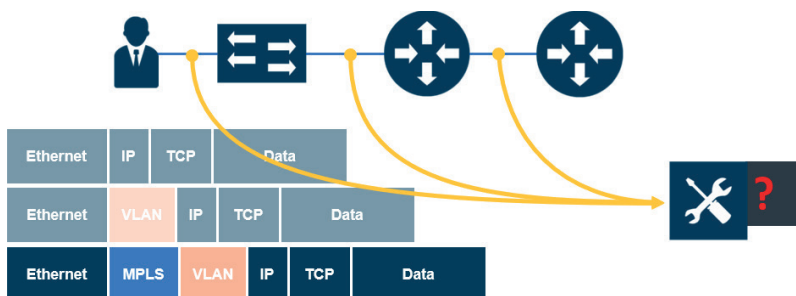
Oft muss der Datenverkehr für die Segmentierung etikettiert oder eingekapselt werden, um virtuelle oder geroutete Infrastrukturen zu durchqueren. Dafür werden Kopfdaten hinzugefügt, die diese Funktionen erfüllen, wie GRE, VxLAN, MPLS, VLAN, ERSPAN, Cisco FabricPath...

Wenn Erfassungen des Datenverkehrs durchgeführt werden, um sie an Sichtbarkeits- und Sicherheitstools zu senden, können die Kopfdaten nicht von diesen Geräten interpretiert werden, sodass sie mit Datenverkehr dieser Art nichts anzufangen wissen.

Wenn die Kopfdaten im Empfangsgerät selbst gelöscht werden, wirkt sich dies negativ auf die Leistung des-selben aus, da diese Geräte nicht auf diese aufwändige Aufgabe spezialisiert sind.

Zudem kann auch die bloße Löschung der Kopfdaten zum Problem werden, wenn die Rückverfolgbarkeit der Paketherkunft oder die Segmentierung, zu dem es gehörte, verloren geht.

### SCHEMA:



## ANPASSUNG DES DATENVERKEHRS AUFGRUND GELÖSCHTER KOPFDATEN

### LÖSUNG:

Die erweiterten Gigasmart-Dienste der Gigamon-Plattform unterstützen die Trunkierung von Paketen nativ auf verschiedene Weise:

- Löschung von Kopfdaten: ERSPAN, MPLS, MPLS+VLAN, VLAN (8021q und Q in Q), VN-Tag, VXLAN, GRE, markierte Pakete, Cisco FabricPath, FM6000
- Tunnel: ISL, GTP

Zudem besteht die Möglichkeit, generische Kopfdaten zu löschen, indem die Informationen bestimmt werden, die gelöscht werden sollen.

Die Funktion der Löschung von Kopfdaten kann mit der Aufnahme einer VLAN-Etikettierung kombiniert werden, um die Rückverfolgbarkeit der Pakete zu gewährleisten.

Ebenso werden die Ethertype- und CRC-Felder neu berechnet, um die Gültigkeit der Pakete sicherzustellen.

### LIZENZEN:

- Header Stripping