dacoso

Vor dem Verschlüsseln: Transparenz und Stabilität auf Layer 2 sicherstellen

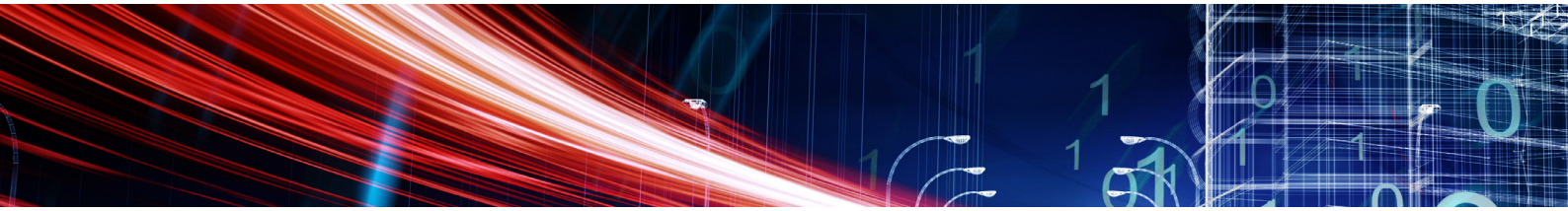
Sie haben für ein neues Projekt gerade eine „transparente Layer-2-Punkt-zu-Punkt-Leitung“ von einem Drittanbieter gekauft. Anschließend haben Sie an den Endpunkten dieser Leitung Layer-2-fähige Verschlüsselungsgeräte installiert – doch Frames gehen verloren, die Verschlüsselung funktioniert nicht und Ihre Kunden sind unzufrieden. Jetzt beginnt die mühsame Fehlersuche unter Zeitdruck. Es kann vieles schieflaufen: defekte Geräte, falsche Konfigurationen, Inkompatibilitäten oder Einschränkungen an irgendeiner Stelle. In diesem Moment wird die Situation schnell unübersichtlich.

Wer verschlüsselte Layer-2-Services für Endkunden bereitstellt, muss die Infrastruktur vorher sauber vorbereiten. Je nachdem, wie viel Kontrolle Sie über die Strecke dazwischen haben, wird das einfacher oder deutlich komplexer. In jedem Fall haben Sie Möglichkeiten, die Infrastruktur fit zu machen, damit Sie Ihre Kunden vertragsgemäß bedienen können. Eine gute Planung ist kaum zu überschätzen – sie verhindert unnötige Kosten und Verzögerungen.

Verstehen, was dazwischen liegt

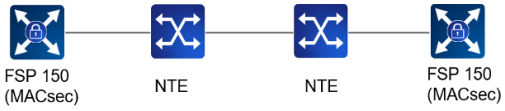
Warum ist das Gesamtbild so wichtig? Es ist verlockend zu glauben: Wenn „ein paar Dinge funktionieren“ und „die Tests gut waren“, wird am Ende schon alles wie erwartet laufen. Besonders dann, wenn eine „transparente Leitung“ zugesagt wurde – oft nur mündlich. Aber: Je mehr Komponenten zwischen den Endpunkten liegen oder je weniger Kontrolle Sie über diesen mittleren Abschnitt haben, desto höher ist das Ausfallrisiko. Funktionen wie QoS werden Hop für Hop konfiguriert. Deshalb ist es sinnvoll, die Anzahl der Hops so gering wie wirtschaftlich und technisch möglich zu halten. Typische Probleme bei Layer-2-Leitungen sind Engpässe, Filter oder schlicht nicht zueinander passende Parameter. Hinzu kommt der zusätzliche Overhead, der meist mit weiteren Netzsegmenten entsteht. Auch die Suche nach der minimalen L2-MTU kann in komplexen Umgebungen schwierig werden.

dacoso

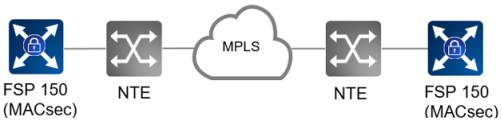


Bei Punkt-zu-Punkt-Verbindungen auf Layer 2 gibt es mehrere Arten von Zwischennetzen, die häufig vorkommen. In den folgenden Beispielen dienen Geräte der Adtran-FSP150-Familie als MACsec-Verschlüsselungsgeräte.

- **Dark-Fiber-Verbindung mit NTEs (Network Terminating Equipment) unter eigener Kontrolle**
  Das ist die einfachste – und teuerste – Variante. Alle L2-Geräte im Netz werden von Ihnen kontrolliert, sodass sich die konfigurierten Parameter einfach abstimmen lassen. Mögliche Varianten:
  - Carrier-Ethernet-Switches als NTEs, an die L2-Verschlüsselungsgeräte angeschlossen sind
  - ausschließlich L2-Verschlüsselungsgeräte dienen als NTEs für die Dark Fiber

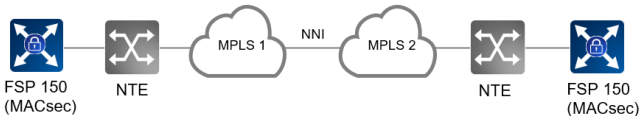


- **MPLS-Core des Providers in der Mitte**
  Hier wird es häufig kompliziert, und Designprobleme werden leicht übersehen. Wholesale-Provider überwachen den vertraglich vereinbarten Traffic in der Regel sehr streng und ändern konfigurierte Parameter normalerweise nicht einfach auf Zuruf. Ihre Services sind meist klar definiert und nicht flexibel anpassbar. Der Vorteil: Auf den zuverlässigen Betrieb des Provider-Core-Netzes können Sie sich in der Regel verlassen, ohne dort selbst auf Fehlersuche gehen zu müssen.



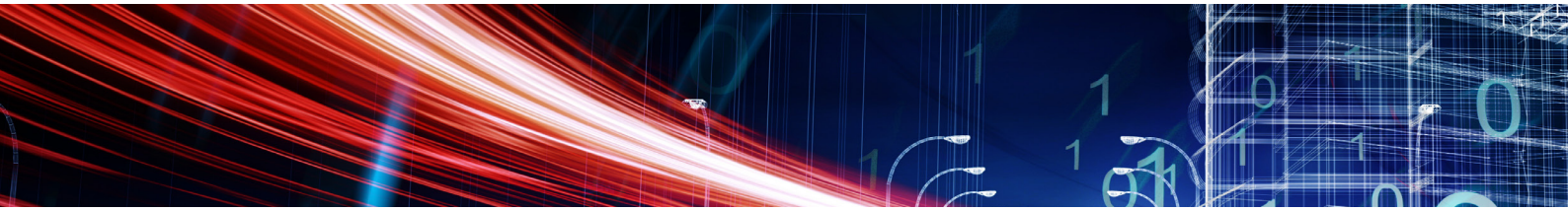
- **Dark-Fiber-Verbindung mit NTEs unter Kontrolle des Providers**
  Dieses Szenario ist etwas komplexer. Bevor Sie Verschlüsselungsgeräte kaufen und installieren, müssen Sie beim Provider erfragen, welche Funktionen die Carrier-Ethernet-Switches als NTEs unterstützen und welche Parameter dort konfiguriert sind.

- **Gemischte Umgebung**
  Natürlich kann es auch deutlich komplexer werden. Zum Beispiel ist eine MPLS-Cloud nur eines von mehreren Netzsegmenten, während der restliche L2-Pfad über Tunnel durch weitere MPLS-Clouds aufgebaut wird.



- **DWDM-Core des Providers in der Mitte**
  Dieses Szenario ähnelt der Dark-Fiber-Variante oben. Entscheidend ist weiterhin vor allem, wer die L2-NTEs kontrolliert. Potentielle L1-Probleme werden hier nicht weiter thematisiert.

dacoso



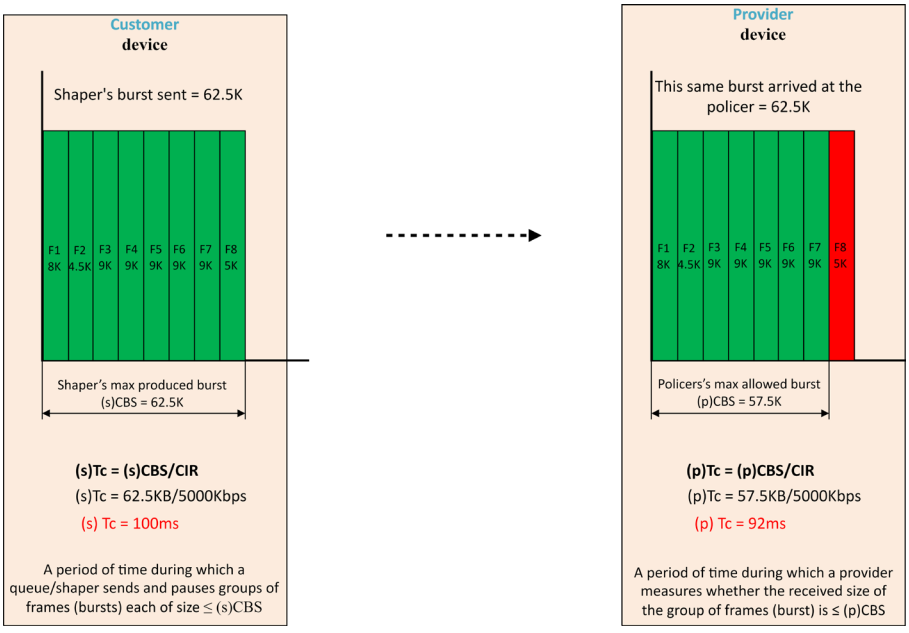
Die wichtigsten Parameter im Partnernetz verstehen

Auf die Aussage „transparente 10G-Leitung“ allein sollten Sie sich keinesfalls verlassen. Wichtig ist zu verstehen, wie die vorgeschalteten Geräte konfiguriert sind – und ob sie wirklich den transparenten Service liefern können, den Sie brauchen.

- **Leiten die Zwischengeräte MACsec-Frames durch?** Vielleicht heißt es, die Switches seien „MACsec-fähig“. Aber können sie MACsec-Frames auch durchleiten – oder in der Terminologie mancher Hersteller „tunneln“? Verschlüsseln und Entschlüsseln ist das Eine; MACsec-Frames transparent weiterzuleiten, ist etwas Anderes. Nicht alle Switches können das. Ist MACsec-Pass-through Teil Ihres Vertrags mit dem Provider? Falls nicht, riskieren Sie plötzlich zusätzliche Investitionen in ein Leitungs-Upgrade.

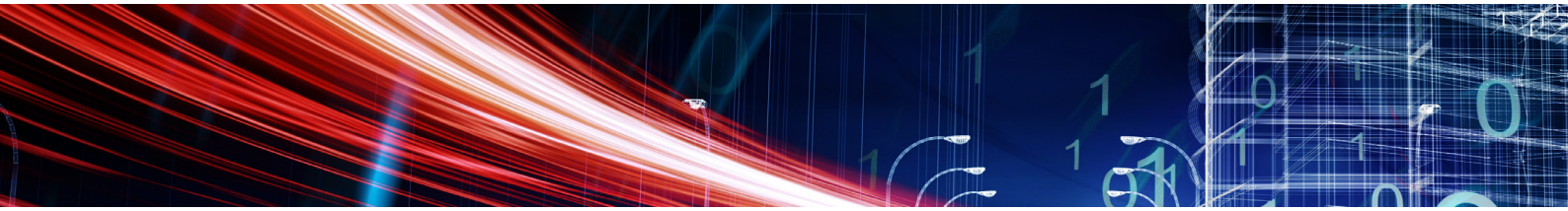
- **Die Zwischengeräte sind „Carrier Grade“, und Verschlüsselungs-Frames sollten eigentlich durchgehen – tun es aber nicht?** Dann stellt sich die Frage: Gibt es Filter auf Basis der Ziel-MAC-Adresse oder des Ethertype-Werts? Idealerweise wäre das ein Provider-Thema. Nehmen wir aber an, Ihr Provider
  - ist nicht daran gewöhnt, Leitungen für Verschlüsselungsservices bereitzustellen
  - hat dennoch geprüft und sogar gezeigt, dass L2-Verschlüsselung auf genau dieser Leitung grundsätzlich funktioniert

  Mit den Testgeräten des Providers funktioniert es – mit Ihren Geräten aber nicht. Genau hier unterscheiden sich Hersteller manchmal. Ethertype-Werte und Ziel-MAC-Adressen, die MACsec nutzt – Multicast oder Unicast –, können dabei eine Rolle spielen. Und leider kann das auch zu Ihrem Problem werden, wenn diese Details nicht ausdrücklich im Vertrag festgehalten wurden. Das ist in der Praxis natürlich nicht immer einfach.



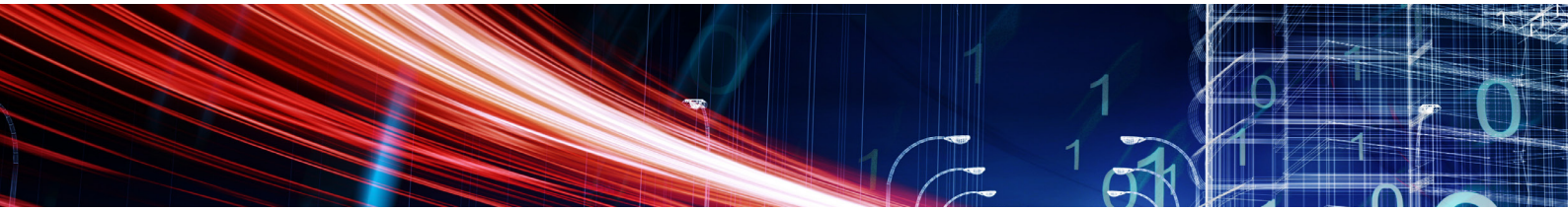
Was passiert, wenn eine Gruppe von Frames an einen Provider-Router gesendet wird? Das sendende Gerät erzeugt Gruppen solcher Frames bis zu einer bestimmten Größe, dem sogenannten CBS (Committed Burst Size). Beim empfangenden Gerät – dem Router des Providers – ist im Policing ein eigener CBS-Wert konfiguriert. Damit keine Frames verworfen werden, muss der CBS des Providers mindestens etwas höher liegen als der CBS des sendenden Geräts. Provider ändern solche Einstellungen bekanntermaßen nur ungern.

dacoso



- **Können Sie den CBS Ihres Queuers auf den Verschlüsselungsgeräten wirklich so beeinflussen, dass er niedriger ist als der Wert auf Provider-Seite?** Dieser Parameter definiert die maximale Größe eines „Bursts“ – also einer Gruppe von Frames, die ohne Pause an den Provider gesendet wird. Angenommen, der CBS Ihres Queuers beträgt 62,5 KB und der CBS des Provider-Policers 57,5 KB. In bestimmten Fällen – etwa wenn eine Anwendung burstigen Traffic erzeugt – führt das zu verworfenen Frames, selbst wenn die Bandbreitenauslastung auf einer 10G-Leitung nur bei etwa 3 bis 5 Gbit/s liegt.
- **Unterstützt Ihr Provider EBS oder nur CBS?** EBS (Excess Burst Size) gibt Ihnen mehr Flexibilität, wenn die vertraglich vereinbarte Bandbreite kurzfristig überschritten wird. CBS und EBS sind normalerweise entweder Teil des Vertrags oder der Servicebeschreibung. Deshalb ist es wichtig, die Policer-Einstellungen des Providers zu kennen.
- **Die Layer-2-MTU kann sogar wichtiger sein als die Layer-3-MTU. Warum?** Weil Ethernet-Frames im Gegensatz zu IP-Paketen nicht fragmentiert werden können. Wird die MTU überschritten, werden Frames unmittelbar verworfen.
- **Welche Art von Tagging erwartet das vorgeschaltete Gerät?** Kein Tagging, C-Tagging oder S-Tagging? Der Unterschied liegt im TPID-Feld von Ethernet-Frames mit C- oder S-Tags. Das hat nicht direkt mit Verschlüsselung zu tun, entscheidet aber darüber, ob Ihre Frames im Provider-Netz korrekt weitergeleitet werden.
- **Außerdem lässt sich der MACsec-bezogene Teil eines Ethernet-Frames – der „SEC“-Tag – nicht vollständig hinter VLAN-bezogenen Feldern wie S- oder C-Tag „verstecken“.** Ein Provider leitet einen Frame zwar anhand von VLAN-ID und TPID-Feldern weiter, der Switch des Providers muss den Ethernet-Frame aber trotzdem parsen und den Ethertype-Wert des SEC-Tags verarbeiten. Genau darum ging es oben bereits: Die MACsec-Ethertype-Werte müssen von den Provider-Geräten zugelassen und verarbeitet werden.
- **Wichtig ist auch, die effektive Bandbreite zu verstehen, die Sie vom Provider tatsächlich erhalten. Sind es 9,9 Gbit/s oder 9,0 Gbit/s?** Wenn Sie später eigene Performancetests mit aktiviertem MACsec und gesetzten VLAN-Tags durchführen, kann es zu Oversubscription kommen – und die Verschlüsselung kann ab bestimmten Auslastungswerten beeinträchtigt werden.

dacoso



Anforderungen an den Provider vorbereiten

Um Ihre Erwartungen an eine bereitgestellte L2-Leitung für verschlüsselte Services zusammenzufassen, sollten Sie folgende Punkte berücksichtigen:

- gewünschte effektive Bandbreite
- Oversubscription-Optionen: möglichst hohe CBS- und EBS-Werte im Rahmen Ihres Budgets
- Switchover-Design: Wenn Sie ungetaggte und getaggte Frames parallel übertragen müssen, klären Sie mit dem Provider, ob das möglich ist.
- MACsec-Frames-Pass-through: Idealerweise nennen Sie den Hersteller für Ihre Verschlüsselungsservices oder definieren sogar die Ethertype-Werte, die MACsec für Schlüsselaustausch und Übertragung verschlüsselter Frames nutzt. Diese Werte sind den Herstellern bekannt und können dort erfragt werden.
- Pass-through von CCM-Frames für Connectivity Fault Management: MACsec stützt sich stark auf diesen klar definierten Mechanismus, um den Service nach einer Störung automatisch wiederherzustellen.

Den Service für Ihre Kunden beschreiben

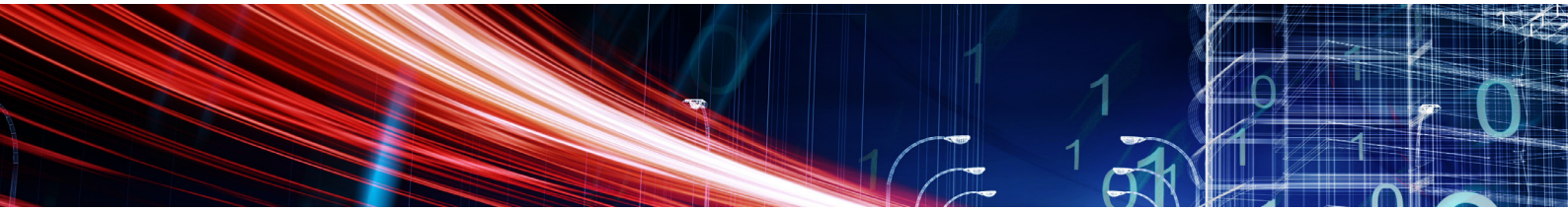
- Definieren und kommunizieren Sie die erwartete Bandbreite für Ihre Kunden nach Abzug aller Overheads: VLAN-Tags, MACsec-Tags, Service-Messages oder auch leicht abweichende CBS-Einstellungen, die Sie dazu zwingen, die effektive Bandbreite für Ihre Endkunden zu reduzieren. Der CIR (Committed Information Rate) sollte realistisch konfiguriert sein.
- Konfigurieren Sie das Policing in Richtung Ihrer eigenen Kunden oder Endnutzer bewusst – und machen Sie transparent, dass Sie Frames lieber verzögern als verwerfen. Anders als Ihr Upstream-Provider können Sie beim schwankenden Traffic-Profil Ihrer Kunden großzügiger sein und möglichst viel davon akzeptieren, etwa durch einen hohen Policer-CBS. Also: „Delay“ statt „Drop“. Ihr eingehender Policer misst den Kundentraffic über längere Zeiträume und erlaubt vertraglich vereinbarte Werte im Durchschnitt. Ihr Queuer puffert oder verzögert den Traffic anschließend, wenn er Ihr Verschlüsselungsgerät in Richtung Provider verlässt. Der Puffer des Queuers sollte groß genug sein, um den vom Policer zugelassenen Traffic aufzunehmen.

Performance testen

Wie Sie den bereitgestellten Service testen – und wie Ihre Kunden die Performance ihres Services testen –, ist mindestens so wichtig wie die Konfiguration selbst. Entscheidend ist ein sauberer Testansatz, der keinen Interpretationsspielraum lässt. Einige zentrale Punkte zur Bewertung der Servicequalität:

- Unabhängig vom eingesetzten Testwerkzeug ist ein strukturierter Testansatz wichtig.
- Performancetests sollten durchgeführt werden, bevor der Service in den Produktivbetrieb übergeben wird.
- Schließen Sie Ihr Testgerät an die NTEs des Providers an und messen Sie die Performance-Parameter.
- Schließen Sie das Testgerät anschließend an den UNI-Port (Customer Port) der Verschlüsselungsgeräte an und messen Sie die Performance-Parameter auf die gleiche Weise. So lässt sich nachvollziehen,
  - ob der Provider geliefert hat, was zugesagt wurde
  - ob die Verschlüsselungsgeräte die Experience wesentlich verändert haben oder nicht

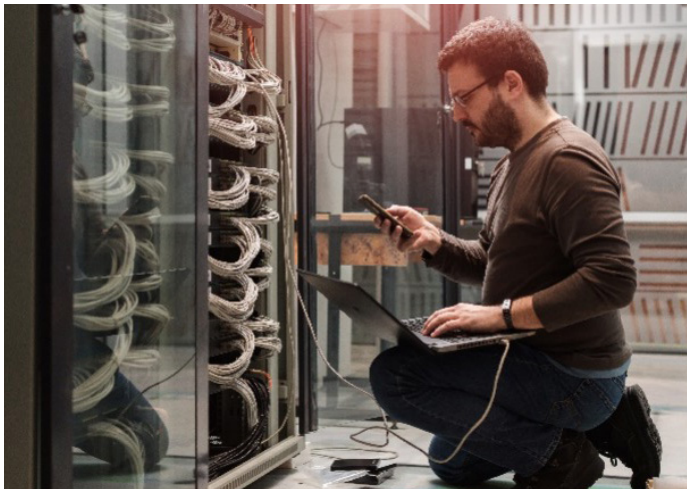
Die tatsächliche Experience der Endnutzer kann trotzdem abweichen. Nicht selten testen Engineers mit iperf und einem oder mehreren TCP-Streams. Frame- und Paketgrößen, Overheads und die verwendeten Testprotokolle beeinflussen die verfügbare Bandbreite. Wichtig ist, „Äpfel mit Äpfeln“ zu vergleichen – also Tests nah am Provider-Core und weiter davon entfernt mit derselben Messmethode durchzuführen. Unterschiedliche Methoden zu mischen, ist keine gute Idee und liefert kein repräsentatives Ergebnis, vor allem dann nicht, wenn Sie in der Bereitstellung nach einem Engpass suchen.



Unsere Expertise für Planung und Integration

Bei dacoso liefern wir mehr als vorkonfigurierte, MACsec-fähige Carrier-Ethernet-Geräte für 1G, 10G und 100G. Wir bringen tiefes Know-how ein und unterstützen Kunden dabei, sichere Lösungen zu planen und nahtlos in bestehende Netzlandschaften zu integrieren.

Adtran Carrier Ethernet FSP150 family



In unserem modernen Customer Briefing Center (CBC) zeigen wir ein breites Spektrum an Carrier-Ethernet-Lösungen für reale Herausforderungen unserer Kunden. Verschlüsselung in einer Multi-Vendor-Umgebung umzusetzen, kann schnell komplex werden – genau hier bringt unsere Erfahrung echten Mehrwert.

Buchen Sie hier Ihren Termin in unserem CBC in Langen bei Frankfurt: www.dacoso.com/customer-briefing-center

Sie haben Fragen oder wollen sich beraten lassen?
Dann kontaktieren Sie unsere Spezialisten für effizientes Netzwerk-Design.

Ihre Ansprechpartner

Dmitry Shkurko
Senior Solution Consultant
dmitry.shkurko@dacoso.com
+49 6103 404569891
+49 15118482567

Carl Josenhans
Manager Solution Consultancy Post Sales
carl.josenhans@dacoso.com
+49 711 12040646
+49 170 2205270