Immer größere Datenraten

Payload-Auswertung: effiziente Ethernet-Qualifizierung auf bittransparenten Kupfer- oder Glasfaserstrecken

Dennis Zoppke

Wie erkennt man Übertragungsfehler auf der letzten Meile? Das ist eine Frage, die Spezialisten für Telekommunikationsmesstechnik immer wieder beschäftigt. Für DSL wurde in den letzten zwanzig Jahren von den Messtechnikherstellern eine Vielzahl von Mechanismen, Zählern und Grafiken eingeführt, um Fehler besser und schneller sichtbar zu machen. Hier stand bisher im Vordergrund, auf dem DSL-Streckenabschnitt keine Pakete zu verlieren. Das darauffolgende Ethernet, das prinzipiell auch zur letzten Meile zählt, war mit anfangs 100 Mbit/s bisher nie das Nadelöhr einer Verbindung – doch diese Zeiten ändern sich jetzt.

Dennis Zoppke ist Produktmanager bei der Intec Gesellschaft für Informationstechnik mbH in Lüdenscheid

Die bei Privatkunden eingesetzten Ethernet-Endgeräte verfügen heute über eine 1000-BaseT-Schnittstelle, und moderne DSL-, G.fast- und FTTx-Anschlüsse liefern inzwischen 500 Mbit/s und mehr, je nach Länge der Leitung. Leistungsfähige VDSL2-Anschlüsse, die mit Vectoring und Supervectoring (VDSL-Profil 35b) mehrere hundert Mbit/s anbieten, werden bereits in ganz Europa ausgerollt. Durch das Bündeln dieser Anschlüsse, das sogenannte VDSL-Bonding, soll die Datenrate noch einmal nahezu verdoppelt werden. Selbst für G.fast gibt es solche Pläne, und erste Chipsatzhersteller bieten bereits Lösungen an.

Im Geschäftskundenbereich existiert dagegen immer noch eine Reihe von Anwendungen, die nicht so hohe Datenraten erfordern. Dafür werden von den Netzbetreibern neben DSL- auch immer noch reine Ethernet-Anschlüsse mit einer garantierten Datenrate von 5, 10, 50 oder 100 Mbit/s angeboten – oft über große Distanzen und daher mithilfe anderer Techniken, bei denen die Ethernet-Rahmen bittransparent über lange Strecken übertragen werden können. Beispiele dafür sind SHDSL- und SDH-Strecken; hier werden kleine Datenströme zu größeren Datenströmen zusammengefasst (Multiplexing) und über große Entfernungen synchron übertragen. Das geschieht heute im Normalfall optisch über Glasfaser.

Dies bedeutet, dass in Zukunft eine Überprüfung des Durchsatzes allein an der DSL-Schnittstelle nicht mehr ausreichend ist. Um zu gewährleisten, dass die benötigte und vertraglich zugesicherte Datenrate den verschiedensten Anwendungen dauerhaft und sicher zur Verfügung steht, muss eine Überprüfung der gesamten letzten Meile inklusive des Ethernet-Abschnittes erfolgen, im Geschäftskundenbereich eben auch inklusive der bittransparenten Übertragungsstrecken.

Prüfen in drei Schritten

Bei Inbetriebnahme, Wartung und im Fehlerfall ist eine möglichst frühzeitige Erkennung möglicher Bitfehler, die häufig während der Übertragung auf der Strecke entstehen, besonders wichtig. Bei solchen Bitfehlern handelt es sich in der Regel um sogenannte gekippte Bits, also Bits, die während der Übertragung ungewollt ihren Zustand von 0 nach 1 (oder umgekehrt) geändert haben. Ursachen dafür sind oft Rauschen oder Übersprechen.

Bei zeitkritischen UDP- oder RTP-Übertragungen wie Fernsehen (IPTV) und Telefonie (VoIP) führen diese Bitfehler zu Paketverlusten und Qualitätseinbußen, bei einfachen Datenübertragungen (TCP) zu durchsatzreduzierendem Overhead (Zusatzdaten) durch wiederholt zu sendende Pakete. Um diese Bitfehler frühzeitig zu erkennen, muss eine Überprüfung schon auf tieferen Ebenen des ISO/OSI-Modells – am besten auf Layer 2 – erfolgen.

Erster Prüfschritt: Ethernet FCS

Will man nun Ethernet auf einem bestimmten Streckenabschnitt testen, so ist das Generieren von Ethernet-Rahmen (*Bild 1*) das einfachste Mittel (Traffic-Generator). Um dabei aber eine qualitative Aussage treffen zu können, müssen diese Rahmen am Ende der zu testenden Strecke in einer Schleife (Loop) an den Sender zurückgeschickt werden, so dass der Sender wieder zum Empfänger wird.

Dabei reicht es aus, wenn die Loop über gerade so viel Intelligenz verfügt,

dass sie die Ziel- und Quell-MAC-Adressen gegeneinander austauschen kann. Oft reicht hier ein Switch mit Loop-Funktion oder eine einfache Loop-Box aus. Natürlich kann auch ein zweites Testgerät herangezogen werden (*Bild 2*).

Bei der Übertragung der Rahmen vom Sender zur Loop wird eine Prüfsumme (Eth CRC im Bild 1), auch Ethernet FCS genannt (im Beispiel im Bild 2 FCS A), berechnet und mitübertragen, während in der Layer-2-Loop eine eigene Ethernet FCS über die ankommenden Rahmen gebildet wird. Im Idealfall ist diese mit der empfangenen Ethernet FCS (FCS A) identisch, der angekommene Rahmen wird für „OK" (*Bild 3*) befunden und weiterverarbeitet. Bei einer echten Layer-2-Loop werden nur Ziel- und Quell-MAC-Adresse miteinander vertauscht, so dass sich prinzipiell für die zurückgesendeten Rahmen die gleiche Ethernet FCS (im Beispiel im Bild 2 FCS A') ergibt.

Mit Start des Traffic-Generators erzeugt das Testgerät permanent Rahmen mit einer vorher zu konfigurierenden Rahmengröße. Prinzipiell ist jede Rahmengröße zwischen 64 und 10.232 byte möglich. Im Idealfall wird die Größe jedoch so gewählt, dass sie in etwa der späteren Anwendung entspricht. Sollte diese unklar sein, empfiehlt es sich, unterschiedliche Größen zu generieren. Erwartet man „ganz

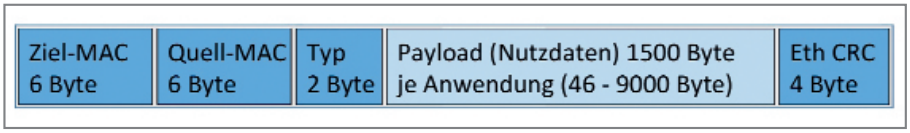

Bild 1: Typischer Ethernet-Rahmen (vereinfacht)

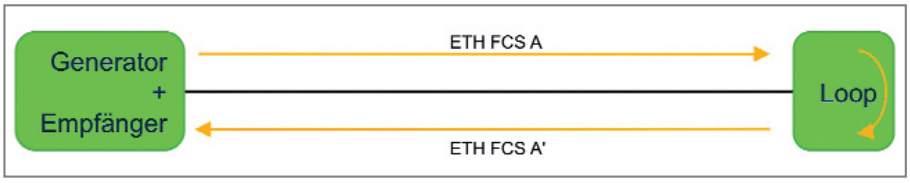

Bild 2: Skizze von Traffic-Generator und Loop, in beide Richtungen mit gleicher ETH FCS

normalen" Internet-Traffic, typisch für die Anwendung im Privatbereich, ist eine Größe von 1.518 byte ideal.

Darüber hinaus muss man über den Wert „Bandbreite" die Geschwindigkeit festlegen, mit der die Rahmen zyklisch erzeugt und auf die Leitung gegeben werden. Hier wählt man genau die Geschwindigkeit, die später auch im Realbetrieb dem Kunden oder der Gegenstelle zugesichert werden soll. In der Regel handelt es sich dabei um 10, 100 oder 1.000 Mbit/s, aber nicht selten werden auch „krumme" Geschwindigkeiten von 5, 25 oder auch 50 Mbit/s angeboten.

Bei Bedarf lässt sich auch der Übertragungsmodus festlegen. Er bestimmt, ob der Traffic über eine gewisse Zeit oder endlos erzeugt wird oder ob man eine vorher festgelegte Menge von Rahmen senden will. Die Nachlaufzeit definiert, wie lange das System noch auf verspätete Rahmen wartet. Hier hat sich eine Zeit von 3 s bewährt.

Mithilfe dieser Einstellungen und der Loop zeigt der Schnelltest mit dem Traffic-Generator auf Schicht 2 umgehend eventuelle Probleme auf. Im Display des Testgeräts lässt sich während und nach dem Test die erreichte Datenrate ablesen (siehe Line Rate im Bild 3). So erkennt man sofort, ob die gewünschte Geschwindigkeit erreicht wurde. Darüber hinaus zeigt ein Zähler an, wie viele Rahmen insgesamt OK waren – im Idealfall gilt das für alle gesendeten und empfangenen Rahmen.

Im gezeigten Beispiel im Bild 3 waren zwar 100 % der gesendeten Rahmen (Tx) OK, allerdings wurden keine OK-Rahmen empfangen (Rx). Das bedeutet, dass 100 % aller Rahmen während der Übertragung als defekt oder fehlerhaft erkannt und verworfen wurden.

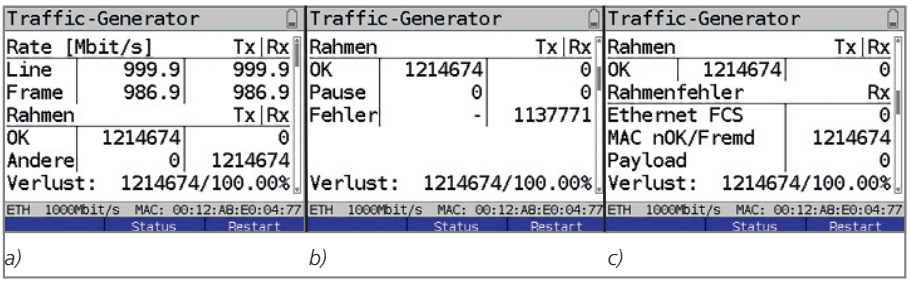

Bild 3: Beispielhafte Darstellung eines Testergebnisses mit Fehlern im Display des Testgeräts

Was genau ist hier passiert? An den Zählern im Gerätedisplay ist zu erkennen, dass die Anzahl der gesendeten Rahmen (Tx) mit der Anzahl der „anderen" Rahmen identisch ist (Bild 3a). Ein zweiter Blick (Bild 3b) zeigt, dass es sich nicht um Pauserahmen handelt, die dafür sorgen, dass nicht zu schnell gesendet wird, sondern zu 100 % um fehlerhafte Rahmen, sogenannte Rahmenfehler.

Zweiter Prüfschritt: MAC-Adresse

Diese Rahmenfehler werden im weiteren Verlauf der Anzeige (Bild 3c) genau aufgeschlüsselt. So lassen sich die Anzahl der Rahmen mit fehlerhafter Ethernet FCS sowie der Rahmen mit einer MAC-Adresse, die entweder nicht OK oder sogar fremd war, leicht ablesen. Im Beispiel sind also alle Rahmen, die gesendet wurden (Tx), mit einer fehlerhaften MAC-Adresse empfangen worden (Rx).

Am einfachsten lässt sich der Fehler damit erklären, dass die Loop nicht die MAC-Adressen getauscht hat und daher alle gesendeten Rahmen (Tx) mit einer fremden Adresse zurückgekommen sind. Vermutlich handelt es sich hier um eine Layer-1-Loop, die die ankommenden Bits 1:1 durchschiebt, oder um eine Layer-2-Loop, bei der der Tausch der MAC-Adressen unterdrückt wurde.

Hätte ein Bitfehler zufälligerweise bei der Übertragung mehrerer tausend Rahmen die verwendete MAC-Adresse beispielsweise durch Rauschen, Übersprechen oder Dämpfung verfälscht, würde der Zähler „MAC nOK/Fremd" lediglich eine 1 anzeigen, nicht aber wie im gezeigten Beispiel die Summe aller gesendeten Rahmen (Tx).

Um sicherzustellen, dass Fehler in der MAC-Adresse stets erkannt und angezeigt werden, ist es wichtig, dass das Testgerät eine MAC-Prüfung ermöglicht. Hierbei sucht es aus Gründen der Vereinfachung gezielt nur seine eigene MAC-Adresse in Quelle, Ziel oder in beiden Feldern, falls gegen einen Schleifenstecker (100BT) Layer-2-Traffic generiert wird oder der Anwender nicht genau weiß, gegen welche Art Loop (Layer 1 oder 2) gearbeitet wird.

Prinzipiell kann sich die MAC-Adresse bei Tests auf höheren Schichten durch die Streckenführung ändern, so dass man nicht davon ausgehen kann, dass die Ziel-MAC-Adresse beim Senden (Tx) auch tatsächlich der Quell-MAC-Adresse beim Empfangen (Rx) entspricht. Deshalb wird die Adresse der Gegenstelle grundsätzlich nicht überprüft. Treten hier Fehler auf, werden diese durch die Ethernet FCS erkannt.

Besonderheit: Bittransparenz

Bei den oben bereits erwähnten bittransparenten Übertragungen, zum Beispiel über SHDSL-Strecken, gibt es jedoch eine Besonderheit, die eine weitere Prüfung erforderlich macht. Die Bits werden bei einer bittransparenten Übertragungsstrecke unverändert als eine Art Bitstrom ohne definierten Anfang oder Ende übertragen. Der Strecke ist es sozusagen egal, was sie überträgt – am Ende sind es nur Nullen und Einsen.

Oft kommen hierbei Techniken zum Einsatz, die Übertragungen über große Entfernungen ermöglichen. Zwar verfügen diese auch über Sicherungsmechanismen, in der Regel können diese aber kein gekipptes Bit erkennen und wieder korrigieren.

Kommt es also bei diesen Übertragungsstrecken wegen hoher Leitungslängen (Dämpfung) oder Störungen von außen (Rauschen) durch Nachbaradern oder Geräte zu einem Bitfehler im Payload, also bei den Nutzdaten, wird dieser nicht von den beiden oben genannten Prüfungen erkannt.

Der Grund dafür ist relativ einfach: Zur Reduzierung von Redundanz wird die Ethernet FCS (im Beispiel FCS A) nicht über die bittransparente Strecke mitübertragen, die 4 Byte werden vor der Übertragung einfach entfernt und am Ende der Übertragungsstrecke neu berechnet und ergänzt (*Bild 4*). Auch die Präambel sowie das SFD-Byte und die Inter Packet Gap (IPG) werden technikbedingt nicht mitübertragen.

Wenn jetzt ein Bit bei der Übertragung gekippt ist, wird dies am Ende der bittransparenten Strecke nicht erkannt. Die neu erstellte Prüfsumme, die jetzt den Fehler miteinschließt, wird als die richtige Prüfsumme angesehen und die Übertragung mit ihr fortgesetzt. Eine Gegenstelle, beispielsweise eine Layer-2-Loop, erhält nun die Rahmen mit korrekter Prüfsumme (FCS B) und loopt diese zurück. Die Rahmen werden erneut über die bittransparente Strecke übertragen, wo sie wiederum durch Bitfehler verfälscht werden könnten, und am Ende der Strecke wieder mit einer neuberechneten FCS (jetzt FCS C) versehen. Der auswertende Empfänger, hier identisch mit dem sendenden Traffic-Generator, erhält diese geloopten Rahmen zurück, prüft die Ethernet FCS und sucht die eigene MAC-Adresse. Im gezeigten Beispiel befindet er das Paket für in Ordnung und führt es der Weiterverarbeitung zu – und der Bitfehler bleibt unbemerkt.

Da bei diesem Test nicht der eigentliche Inhalt, also die Nutzdaten, weiterverarbeitet und durch nachfolgende Protokolle aufbereitet wird, bleibt auch unbemerkt, dass es bei der Übertragung über diese bittransparente Strecke zu Fehlern gekommen ist, das heißt, die Strecke wird für gut befunden, obwohl sie es nicht ist.

Sollte diese Strecke dann allerdings im Wirkbetrieb genutzt werden, können immer wieder Fehler und Übertragungsprobleme auftreten, die mit Datenverlust und reduzierter Bandbreite einhergehen.

Dritter Prüfschritt: Payload-Auswertung

Um den Payload nach der Übertragung über die bittransparente Strecke auf Richtigkeit untersuchen zu können, muss es also eine dritte, von der Ethernet FCS unabhängige Prüfung geben, um mögliche Fehler auszuschließen. Dafür wird der Payload mit einem eigenen Prüfmuster beschrieben, dessen Aufbau mit dem des Ethernet-Rahmens vergleichbar ist. Hierfür wird zunächst ein eigener Header eingeführt, der einen Zeitstempel und eine Paketnummer enthält. So kann das Empfängergerät (das auch Sender war, Bild 4) sofort erkennen, wie lange dieser Rahmen unterwegs war und ob alle Rahmen in der richtigen Reihenfolge eintreffen. Die letzten 4 Byte des Payload werden für eine Prüfsumme reserviert, die die letzten 4 Byte der Summe aller aufaddierten Bytes des Headers und den „Payload mit Muster" enthält.
Der Teil, der nicht für Header und Prüfsumme verwendet wird, wird mit folgendem Bitmuster gefüllt: „00 01 02 03 04 05 … FA FB FC FD FE FF". Das Muster wird so lange wiederholt, bis der gesamte verbliebene Payload („orangener Payload", *Bild 5*) gefüllt ist. Sollte nun auf einer bittransparenten Strecke ein Bit verändert werden, fällt dies sofort auf. Der Rahmen kann sofort als fehlerhaft erkannt und verworfen werden (Bild 3c).

Payload-Auswertung vs. BERT

Ein Bitfehlerratentest (Bit Error Rate Test – BERT), so wie man ihn von ISDN kennt, ist als Alternative nicht zielführender. Denn jeder BERT setzt einen kontinuierlichen Bitstrom voraus, was bei Ethernet grundsätzlich nicht gegeben ist. Zwar ließe sich ein kontinuierlicher Bitstrom mit einem typischen Bitmuster erzeugen, dieser würde jedoch keine realistische Ethernet-Übertragung simulieren. Ein BERT auf dieser Basis würde lediglich die Anzahl oder das Fehlen von Bitfehlern feststellen, nicht aber die Aussage treffen können, ob eine Ethernet-Übertragung mit einer gewählten Geschwindigkeit von zum Beispiels 1 Gbit/s und einer bestimmten Paketgröße auch fehlerfrei im Wirkbetrieb angewendet werden könnte. Wie viele Rahmen zu früh oder zu spät kommen, hat also für die Qualitätsbeurteilung keine Relevanz.
Anstatt die Frage zu beantworten, wie viele Bitfehler aufgetreten sind, ist es viel wichtiger zu erfahren, wie viele Rahmen über welchen Zeitraum verloren gegangen sind. Die Kombination aus den drei beschriebenen Prüfungen

- Ethernet FCS;
- MAC-Adressenauswertung;
- Payload-Auswertung

stellt jedoch sicher, dass jeder Fehler – und sei es auch nur ein einziger Bitfehler – bemerkt und angezeigt wird. Da es sich aber bei Ethernet um eine paketorientierte Übertragung handelt, ist nicht die Anzahl der Bitfehler entscheidend, sondern der Paketverlust, also die Anzahl der defekten oder verloren gegangenen Rahmen, da jeder fehlerhafte Rahmen verworfen wird.
Treten Bitfehler wie zum Beispiel ein sogenannter Burst auf, also viele Bitfehler auf einmal, können ein oder mehrere benachbarte Rahmen defekt sein. Kommen sie dagegen immer wieder regelmäßig vor, dann gehen über einen längeren Zeitraum immer wieder vereinzelte Rahmen verloren.
Ein Zähler, der die Sekunden mit Paketverlust zählt, erlaubt in Korrelation mit dem Gesamtverlust die Schlussfolgerung, ob die Störungen burstartig sind oder sich immer wiederholen. Damit ist ein Rückschluss auf die Ursache möglich. Ist die Anzahl der fehlerhaften Sekunden hoch und liegt gleichzeitig ein erheblicher Paketverlust vor, waren die Störungen wiederholend oder permanent. Ist die Anzahl der fehlerhaften Sekunden eher gering und liegt trotzdem ein erheblicher Paketverlust vor, war die Störung eher burstartig und daher nur kurzzeitig. Setzt man die Anzahl der fehlerhaften Sekunden nun noch ins Verhältnis zur Gesamtlaufzeit, dann erhält man eine „Errored Seconds Rate", also eine Rate in Prozent über die fehlerhaften Sekunden. So kann man schnell erkennen, ob eine Übertragung gut oder verlustbehaftet ist.
Ob eine Rate gut oder schlecht ist, hängt dagegen von der Dienstgütevereinbarung ab. Idealerweise sollte sie im Bereich Inbetriebnahme und Wartung immer Maximalwerte haben – und genau darum ist ein Traffic-Generator-Test mit Payload-Auswertung vor der Freigabe einer Ethernet-Strecke nicht nur sinnvoll, sondern immer empfehlenswert. *(bk)*

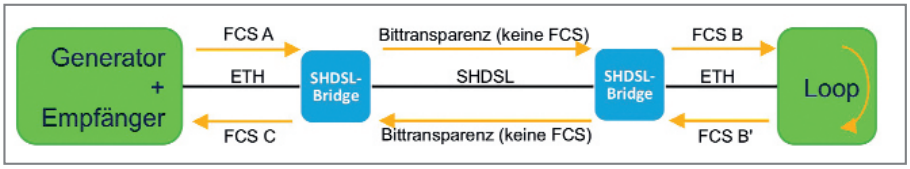

Bild 4: Ethernet-Übertragung über eine bittransparente Strecke ohne Ethernet FCS

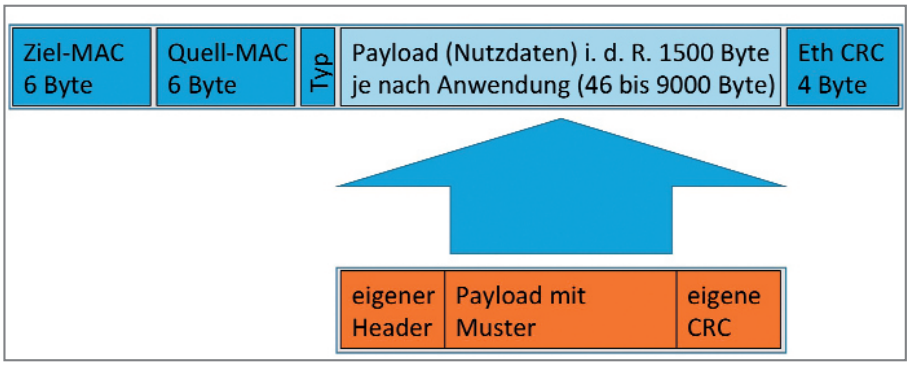

Bild 5: Der Payload der transferierten Rahmen wird mit eigenem Header, einem Muster und eigener CRC gefüllt