ComConsult GmbH
BERATUNG + PLANUNG + SCHULUNG

Der Netzwerk Insider

April 2019

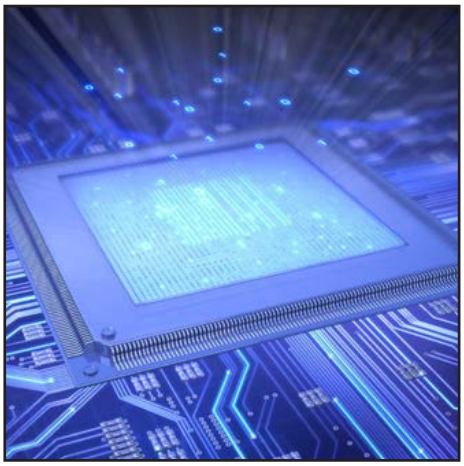
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Neue Prozessoren braucht das Land – die Entwicklungen des letzten Jahres

Neue Lücken, neue Gegenmaßnahmen und die Auswirkungen im realen Leben

von Dr. Markus Ermes

Spectre und Meltdown – ein Synonym für den Fokus auf Leistungsfähigkeit bei der Entwicklung von Prozessoren und die mangelnde Berücksichtigung von Sicherheitsaspekten. Was zu den Anfangszeiten des Internets noch wenig Relevanz hatte, ist in Zeiten von Cloud und gemeinsamer Nutzung von Infrastruktur umso kritischer. Innerhalb von etwas mehr als einem Jahr hat sich aus zwei Sicherheitslücken mittlerweile ein ganzer Zoo entwickelt, der in wenige Gattungen unterteilt werden kann. Was gibt es Neues? Welche Auswirkungen haben die Lücken? Was sagen Experten dazu?



Im Juni letzten Jahres erschien ein erster Artikel zum Thema „CPU-Sicherheit“ im Netzwerk-Insider. Darin wurde bereits darauf hingewiesen, dass auf Basis von Spectre und Meltdown neue architekturbedingte Sicherheitslücken entdeckt wurden, aber Details waren noch nicht bekannt. In den vergangenen 10 Monaten sind diese (und weitere) Sicherheitslücken veröffentlicht und im Detail beschrieben worden. Außerdem konnten in dieser Zeit die Auswirkungen auf den realen Betrieb von IT-Systemen beobachtet werden. Dieser Artikel soll eine Übersicht über die wichtigsten neuen Informationen geben, speziell über die neuen Sicherheitslücken, wobei diese technisch detailliert behandelt werden müssen. Außerdem werden neue Informationen zu den Auswirkungen von Gegenmaßnahmen betrachtet sowie eine Einschätzung zur aktuellen Gefährdungslage dargestellt.

weiter auf Seite 6

Ethernet im Takt

von Markus Geller

Dieser Beitrag befasst sich mit Time Sensitive Networking (TSN). TSN soll auf der Basis von Ethernet die Vorteile bieten, die zum Beispiel mit klassischen Zeit-Multiplex-Techniken verbunden sind, vor allem was die Synchronizität betrifft.

Relevanz bekommt TSN in allen Bereichen mit Echtzeitanforderungen an die Datenübertragung. Während verhältnismäßig moderate Echtzeitanforderungen wie beispielsweise in den Bereichen Audio- und Videoübertragung von den bisherigen Paketnetzen erfüllt werden, gilt das nicht für striktere Zeitvorgaben in der Größenordnung weniger Millisekunden (geschweige denn Mikro- und Nanosekunden). Solche strikten Anforderungen hat vor allem industrielle Kommunikation. Aber auch das Basisnetz für 5G muss Echtzeitübertragung unterstützen. Ultra Reliable Low Latency Communications (URLLC) ist eines der drei Nutzungsprofile, die in 5G möglich sein müssen.

weiter ab Seite 17

Geleit

Wireless: Technologievielfalt bleibt

auf Seite 2

Standpunkt

Moderne Zonenkonzepte erfordern Mikrosegmentierung

auf Seite 15

Aktuelles Seminar

Sommerschule - Neueste Trends der IT-Infrastruktur

ab Seite 4

Top Veranstaltungen im Sommer

Storage – aktuelle Technologien und ihr Einsatz im Unternehmen

Trouble-Shooting-Praxis für Netzwerk und Anwendungen

auf Seite 14

Geleit

Wireless: Technologievielfalt bleibt

Das erste Geleit aus dieser Feder sollte mit einer guten Nachricht beginnen: Das Wurmtal ist gerettet. Was diese Nachricht mit dem Netzwerk Insider zu tun hat, werden Sie beim Weiterlesen erfahren.

Am 12.03.2019, nach Starkregen und Sturm, führte die Wurm (einer der indirekten Zuflüsse des Rheins in der Aachener Region) so viel Wasser, Baumstämme und Geäst, dass durch die Verlagerung des Flussbetts eine Umweltkatastrophe drohte. Ein Steilhang an der Wurm und damit auch der Untergrund einer Abwasserleitung wurden unterspült. Ein Rohrbruch hätte einen wesentlichen Teil des Abwassers von tausenden Haushalten in die Wurm fließen lassen.

Dem Katastrophenschutz der Städte-Region Aachen gelang aber die Rettung des Wurmtals. 130 Personen haben zwei Tage und Nächte lang ununterbrochen mit 35.000 Sandsäcken den weggespülten Hang wiederhergestellt.

Mir sind aber bei der Betrachtung des Werks der unermüdlichen Katastrophenhelfer zwei Fragen in den Sinn gekommen:

- Was wäre, wenn sich die drohende Katastrophe in einer abgelegenen Region anbahnte und unbemerkt bliebe?
- Hätte man den teuren Einsatz durch Früherkennung vermeiden können, zum Beispiel durch eine Erkennung der darin bestehenden Anomalie, dass Baumstämme und ungewöhnlich viel Geäst im reißenden Strom mitschwammen?

Und hier kommt die Technologie ins Spiel. Wir in der IT-Gemeinde sprechen viel über IoT, Aktoren, Sensoren und deren Anbindung. Eine sinnvolle Anwendung ist eben Umwelt- und Katastrophenschutz. Bereits heute werden hierfür verschiedenste Technologien genutzt. Ich spreche nicht nur von Satellitenbildern und deren Auswertung. Der Zustand von Bäumen wird bereits in Pilotprojekten mit einfachen Sensoren beobachtet. Solche Sensoren entlang des Verlaufs von Flüssen oder Rohren können wertvolle Dienste leisten. Sie brauchen nicht viel Energie und kämen zum Beispiel mit kleinen Solarpanelen aus, oder mit jahrelang haltenden Batterien.

Abbildung 1: Was haben diese 35.000 Sandsäcke 500 m von meinem Wohnort mit Wireless zu tun?

Alle Welt spricht von 5G. Dabei wird die drahtlose Welt auch in Zukunft von Vielfalt geprägt sein. Wie an dieser Stelle im letzten Geleit meines geschätzten Vorgängers zu lesen war, werden weder 5G noch WiFi die eierlegende Wollmilchsau sein. Dafür sind die dringend benötigten Anwendungen drahtloser Technik zu vielfältig. Dr. Suppan hat in der letzten Ausgabe seiner Verwunderung Ausdruck verliehen, warum solchen Technologien wie Sigfox so wenig Beachtung zuteilwird. Dabei sind Sigfox und LoRa nur zwei Beispiele für das sogenannte LPWAN (Low-Power Wide Area Network). Ich empfehle wärmstens den Beitrag von Dr. Wetzlar in der Insider-Ausgabe vom September 2018, mit dem Titel „Funktechniken für das ‚Internet der Dinge'". Von den Ausführungen meines Kollegen habe ich vor allem gelernt, dass es in der drahtlosen Welt bei der Technologievielfalt bleiben wird. Es ist weder technisch noch wirtschaftlich sinnvoll, so unterschiedliche Applikationen wie Anschauen von Youtube-Videos und Monitoring von Wasserständen, Telefonieren und Steuerung von Gabelstaplern, Messdatenerfassung und E-Mail auf Teufel komm raus im selben Netz betreiben zu wollen.

Nichtsdestotrotz ist die Wireless-Diskussion in der Öffentlichkeit 5G-fixiert. Scheinbar dreht sich alles darum, ob die vier Teilnehmer an der Versteigerung der 5G-Frequenzen die sprichwörtliche Milchkanne in Hintertupfingen anbinden werden oder nicht. Sie werden es nicht tun, so viel steht fest. Und die für Forschung zuständige Bundesministerin bezweifelte offen die Sinnfälligkeit eines solchen Unterfangens.

Wenn die Milchkanne nicht angebunden wird, gilt das auch für die Flüsse und Abwasserrohre, und umso mehr für den Baumbestand. Die Provider, insbesondere wenn sie ihren milliardenschweren Beitrag zur Bewahrung der schwarzen Null im Bundeshaushalt geleistet haben, werden vor allem daran interessiert sein, (wie in der gesamten bisherigen Mobilfunk-xG-Historie) mit möglichst wenig Infrastruktur möglichst viel Umsatz zu erzielen. Das ist in Ballungszentren möglich. Es ist also zu vermuten, dass das 5G-gestützte autonome Fahren außerhalb der Großstädte ein Traum bleibt.

Nun werden die meisten von uns noch ein paar Jahre ohne autonomes Fahren überleben. Aber die anderen Anwendungsfälle drahtloser Technik warten nicht. Beispiel Produktion und Logistik: Hier sind unsere

Neue Prozessoren braucht das Land – die Entwicklungen des letzten Jahres

Fortsetzung von Seite 1

Dr. Markus Ermes hat im Bereich der optischen Simulationen promoviert und Artikel in verschiedenen Fachzeitschriften veröffentlicht. Teil seiner Promotion waren Planung, Aufbau und Nutzung von verteilten und Höchstleistungs-Rechenclustern (HPC). Bei der ComConsult Beratung und Planung GmbH berät er Kunden im Bereich Rechenzentren, wobei seine Hauptaufgaben bei Netzwerken, Storage und Cloud-basierten Diensten liegen. Seine Kenntnisse im HPC-Bereich geben zusätzlich Einblicke in modernste Hochleistungstechnologien (CPU, Storage, Netzwerke), die in Zukunft auch im Rechenzentrum Einzug erhalten können.

1. Sicherheitslücken in CPUs - eine kurze Wiederholung

Um zu verstehen, was die aktuellen Sicherheitslücken in CPUs ermöglicht und wo die Gefahren liegen, soll in diesem Kapitel noch einmal in Kurzform eine Übersicht über die Funktionen „Out-of-Order-Execution“ und „Speculative Execution“ in modernen CPUs dargestellt werden. Außerdem werden die ursprünglichen Versionen von Spectre und Meltdown erläutert. Für eine detaillierte Beschreibung dieser Themen sei auf den entsprechenden Artikel im Netzwerk Insider von Juni 2018 verwiesen [1].

1.1 CPU-Technologien

Bei den CPU-Technologien sind zum Verständnis der Sicherheitslücken drei Aspekte zu nennen: Caches, „Out-of-Order-Execution“ und „Speculative Execution“; alle drei sollen hier nur kurz angeschnitten werden, um ein grundlegendes Verständnis für die Funktionsweise von Spectre und Meltdown zu schaffen.

Wichtig ist zunächst im Hinterkopf zu behalten, dass CPUs sehr viel schneller sind als der Arbeitsspeicher, auf den sie zugreifen. Dadurch werden bei jedem Zugriff auf den Arbeitsspeicher viele Taktzyklen verschwendet. Heutzutage kann eine CPU in der Zeit, die ein Ladevorgang aus dem Arbeitsspeicher benötigt, bis zu 1000 Instruktionen abarbeiten. Um diese Diskrepanz zu maskieren, besitzen CPUs Cache-Stufen, die Daten aus dem Arbeitsspeicher zwischenspeichern und eine deutlich geringere Zugriffszeit besitzen als der Arbeitsspeicher. Es gibt, abgestuft nach Kosten, mehrere Cache-Stufen (sog. Level), die sich in Größe und Geschwindigkeit unterscheiden. Typischerweise gibt es drei Ebenen:

1. Extrem schneller, aber sehr kleiner (< 1 MB) Level-1-Cache (L1)
2. Sehr schneller, größerer L2-Cache (wenige MB)
3. Schneller L3-Cache (> 10 MB)

Eine Skizze der Technologien „Out-of-Order-Execution“ und „Speculative Execution“ ist in Abbildung 1 dargestellt.

Out-of-Order-Execution

Bei der Out-of-Order-Execution moderner CPUs wird die Reihenfolge von Instruktionen innerhalb eines auszuführenden Programms modifiziert, um die einzelnen Bereiche einer CPU (Gleitkomma-Einheit, Fließkomma-Einheit, Vektor-Einheit etc.) optimal zu nutzen. Das ist natürlich nur möglich, sofern die Daten bereits in den Cache geladen wurden oder andere Teile des Programms lange genug brauchen, um einen Ladevorgang aus dem Arbeitsspeicher zu rechtfertigen. Komplexe Logik innerhalb der CPUs stellt sicher, dass Änderungen der Reihenfolge das Ergebnis der Ausführung nicht beeinflussen. Trotzdem kann es dazu kommen, dass Zugriffe erfolgen, die nicht erlaubt sind und sog. „Exceptions“ auslösen. In diesem Falle wird der ursprüngliche Zustand vor der Ausführung (theoretisch) wiederhergestellt. Allerdings kann, wie im Folgenden beschrieben, die CPU dazu gebracht werden, auch Instruktionen nach einem eigentlich unerlaubten Zugriff auszuführen.

Speculative Execution

In nahezu allen Programmen kommt es irgendwann zu Verzweigungen des Ausführungspfads. Ein typisches Beispiel ist hier ein „if-then“-Konstrukt, also eine „Wenn-Dann“-Abfrage. Hier wird die Performance normalerweise reduziert, da keine Instruktionen jenseits der Abfrage durch Out-of-Order-Execution ausgeführt werden können. Hier setzt „Speculative Execution“ an; es wird der wahrscheinlichste Pfad ermittelt oder durch vorherige Ausführungen gelernt und schon einmal „auf Verdacht“ ausgeführt. Diese Ausführung kann auf schon im Cache vorhandene Daten zugreifen oder schon im Voraus Daten

Abbildung 1: Schematische Darstellung von "Out-of-Oder-Execution" und "Speculative Execution" [1]

aus dem Arbeitsspeicher laden und diese verarbeiten. Sollte der Verdacht stimmen, gewinnt man viele Taktzyklen. Sollte der Verdacht nicht stimmen oder eine Exception auftreten, so wird – wie bei „Out-of-Order-Execution“ – der ursprüngliche Zustand (zumindest theoretisch) wiederhergestellt und die Applikation wie eigentlich geplant fortgesetzt.

1.2 Spectre und Meltdown

Die dargestellten Technologien wurden mit starkem Fokus auf Performance entwickelt. Etwaige Folgen für die Sicherheit wurden nur bedingt betrachtet. Dies liegt vor allem an der Zeit, in der diese Technologien entwickelt wurden und nicht am mangelnden Sicherheitsbewusstsein der Entwickler. Vor 20 Jahren war eine so stark parallele Nutzung von CPU-Ressourcen durch verschiedene User kaum denkbar wie sie im Zeitalter der Virtualisierung üblich ist. Diese wurde erst durch die Einführung von Multi-Core-CPUs sinnvoll. Ihren bisherigen Höhepunkt hat diese parallele Nutzung mit dem Aufstieg der Cloud gefunden. Gerade für die Wirtschaftlichkeit eines Cloud-Angebots ist eine gleichzeitige Nutzung von Ressourcen durch mehrere Kunden – unter Umständen sogar durch miteinander konkurrierende Firmen – eine Grundvoraussetzung.

Mit der Entdeckung von Spectre und Meltdown sowie deren verschiedenen Variationen wurden vergangene Versäumnisse beim Blick auf Sicherheitsaspekte von CPUs schmerzhaft verdeutlicht.

Dabei sei noch darauf hingewiesen, dass die Gefahr von Spectre und Meltdown darin liegen, dass die in Kapitel 1.1 erwähnte Wiederherstellung des Ursprungszustands der CPU nicht vollständig ist. Die bereits in den Cache der CPU geladenen Daten werden **nicht** wieder entfernt.

Insgesamt ist das Ausnutzen von Spectre und Meltdown – auch in ihren neuen Versionen – sehr komplex. Ein Angriff in dieser Form muss sehr genau auf das geplante Ziel zugeschnitten werden und erfordert sehr viel Knowhow. Daher ist – zumindest momentan – davon auszugehen, dass diese Sicherheitslücken, wenn überhaupt, nur von staatlich finanzierten Hackergruppen ausgenutzt werden können. Wie in Kapitel 4 dargestellt wird, sind bisher aber noch keine Angriffe bekannt.

Im Folgenden soll kurz beschrieben werden, wie die ersten beiden Sicherheitslücken funktionieren.

Spectre

Spectre bedient sich der „Speculative Execution“, um eigentlich nicht zugängliche Daten auszuspähen. Dazu wird durch ein von einem Angreifer kontrolliertes Programm die CPU darauf trainiert, ein bestimmtes Abfrage-Ergebnis als wahrscheinlich anzusehen. Anschließend wird die Abfrage und ein innerhalb der Abfrage getätigter Speicherzugriff modifiziert. Zwar erkennt die CPU bei der Ausführung der Abfrage den Fehler und stellt den Ursprungszustand wieder her, doch die zuvor im Rahmen der spekulativen Ausführung geladenen Daten sind nach wie vor im CPU-Cache vorhanden und können über einen Seitenkanal ausgelesen werden. Dazu wird vor dem Angriff der CPU-Cache geleert und mit einem möglichen Wert der auszulesenden Daten gefüllt. Ein Beispiel hierfür wären die einzelnen Bytes eines Verschlüsselungs-Keys. Nach dem Angriff kann dann über Messungen der Zugriffszeit auf die auszuspähenden Daten ermittelt werden, ob diese aus dem Arbeitsspeicher geladen wurden oder ob der „geratene“ Wert im Cache stimmt. Es handelt sich dabei um einen langsamen Prozess mit geringen Übertragungsraten, aber bestimmte Daten, wie beispielsweise Verschlüsselungs-Keys oder Passwörter können trotzdem mit ausreichender Geschwindigkeit ausgelesen und an einen Angreifer übermittelt werden.

Meltdown

Bei Meltdown wird ebenfalls das Verhalten der CPU ausgenutzt, alle gelesenen Daten im Cache abzulegen. Doch statt einen bestimmten Ausführungspfad in einem Programm zu nutzen, wird die „Out-of-Order-Execution“ ausgenutzt. So wird eine Reihe von Instruktionen auf der CPU ausgeführt, die einen unzulässigen Speicherzugriff beinhaltet. Die Reihenfolge ist dabei so gewählt, dass der unzulässige Zugriff nach der Optimierung der Instruktionsreihenfolge zu einem früheren Zeitpunkt geschieht als im Programm eigentlich vorgesehen. Dadurch können auch hier – noch bevor die Exception verarbei-

Ethernet im Takt

Fortsetzung von Seite 1

Seit über 10 Jahren ist Markus Geller bei der ComConsult Research GmbH erster Ansprechpartner für die Themen VoIP und Lokale Netze. Der Schwerpunkt seiner Trainer Tätigkeit liegt dabei auf den Gebieten SIP, PSTN Migration, WebRTC sowie Layer 2 und 3 Techniken für MAN und LAN. Markus Geller verfügt über eine langjährige Erfahrung beim Aufbau und der Planung von Netzwerken im large Enterprise Umfeld, inkl. RZ-Netzwerken, WLAN und Multicastverfahren. In seiner über 20-jährigen IT-Laufbahn beschäftigt er sich mit der Evaluierung neuer Technologien und deren Einsatz in der Praxis. Zudem ist er als Autor diverser Fachartikel für den ComConsult Netzwerk Insider und das Wissensportal tätig.

Angesichts dieser Aktualität lohnt sich der genauere Blick auf TSN.

Moderne Kommunikations-Netzwerke unterscheiden sich ja bekanntlich grundlegend von der alt hergebrachten Infrastruktur der Kanalvermittlung. Die Paketvermittlung, die heute die Basis aller Kommunikation darstellt, überzeugt durch eine Vielzahl von Vorzügen. Angefangen bei der variablen Länge einzelner Pakete bis hin zur optimalen Wege-Wahl über multiple Pfade zur Erreichung der Ziele.

Um eines direkt vorweg zu nehmen, dieser Artikel beschäftigt sich, aus Sicht vieler Netzwerkbetreiber und Administratoren, mit Randaspekten der Datenübertragung, die, trotz alledem, in Zukunft einen entscheidenden Teil der Infrastruktur bestimmen werden: das ist zum einen das 5G Netzwerk und zum anderen die sogenannten OT Netze (Operational Technology), die zukünftig die alteingesessenen Feldbussysteme oder Systeme wie SERCOS III, SafetyNET p, VARAN, Profinet, EtherNet/IP, Ethernet Powerlink oder EtherCAT in der Industrie ablösen werden.

Doch was macht diese Netze so besonders?

Die Antwort darauf lautet: Sie benötigen einen Takt.

Taktung ist aber etwas, was die Paketvermittlung nicht gewährleisten kann. Wir kennen zwar die Möglichkeit, mittels Quality of Service, ein Mindestmaß von Informationen sicher von A nach B zu transportieren. Wir können dabei Bandbreite garantieren oder die Bevorzugung einzelner Datenströme anhand von Merkmalen wie MPLS Header, DSCP, VLAN ID, IP-Adresse oder TCP/UDP-Port-Nummer in Routern und Switchen, aber es ist nicht möglich, ein festes Zeitfenster einer Anwendung zu zuordnen, zu der sie garantiert ihre Informationen versenden kann.

Ein erster Ansatz, um dieses Problem in den Griff zu bekommen, wurde vom IEEE im Jahr 2011 unternommen mit der Einführung des Standards 802.1BA:

„Dieser Standard definiert Profile zur Auswahl von Funktionen, Optionen, Konfigurationen, Standardwerten, Protokollen und Prozeduren von Brücken, Stationen und LANs, die zum Aufbau von Netzwerken erforderlich sind, die zeitkritische Audio- und / oder Videodatenströme transportieren können“ (Quelle: IEEE 802.1BA)

Dies führte im Jahr 2012 zur Bildung einer neuen Arbeitsgruppe, die sich seitdem mit der Weiterentwicklung dieser Basis beschäftigt. Diese neue Gruppe prägte den Begriff TSN, Time Sensitive Networking, um bewusst heraus zustellen dass diese Technologie nicht nur den Audio- / Video-Markt adressiert, sondern generell alle Anwendungen, die zur Ausführung eine synchrone Zeitvorgabe benötigen, sowie feste, zugesicherte Zeiten um Daten empfangen oder senden zu können.

Die Aufgabestellungen, die sich hieraus letztendlich ergeben, sehen folgendermaßen aus:

1. Zeitsynchronisation
2. Scheduling und Traffic Shaping
3. Wahl der Kommunikationspfade, Reservierungen und Fehlertoleranz

Ethernet im Takt

Hierbei sind die ersten beiden Punkte heute schon mit vorhandenen Protokollen und Ethernet Standards recht gut umzusetzen, was noch fehlt ist der dritte Punkt, der aktuell noch im Entwicklungsstadium steckt.

Die Zeitsynchronisation wird dabei folgendermaßen ermöglicht:

Damit ein zeitsensitives Netzwerk mit einer getakteten Ende-zu-Ende-Übertragung von Datenströmen funktioniert, die eine harte Echtzeitanforderungen benötigen und damit fixe Zeitobergrenzen einhalten müssen, benötigt jeder Teilnehmer im Netzwerk eine eigene, interne Uhr und damit ein Zeitverständnis. Daher müssen die Uhren aller Teilnehmer, sowohl die der Endgeräte als auch der Switche, synchron laufen. Durch diese Synchronisation wird sichergestellt, dass alle Teilnehmer stets dem gleichen Arbeitszyklus folgen und damit zum richtigen Zeitpunkt die richtige Aktion ausführen. Die Zeitsynchronisation wird dabei über das PTP (Precision Time Protocol gemäß IEEE 1588) erfolgreich abgebildet. Da dieses Protokoll jedoch über einen großen Umfang von Möglichkeiten verfügt, hat man auch hier mittels IEEE 802.1AS-2011 einen Standard eingeführt, der diese Optionsvielfalt auf das in diesem Zusammenhang benötigte Spektrum limitiert.

Der zweite Punkt, Scheduling und Traffic Shaping, macht es an dieser Stelle zwingend nötig, zum Teil neue Verfahren einzuführen, aber auch auf bewährte Mechanismen zurückzugreifen.

Eines der schon lange bekannten Verfahren, welches als Basis benötigt wird, ist der Standard IEEE 802.1Q.

VLAN Tagging und die Bereitstellung von acht Transportklassen, bzw. Prioritäten, wird genutzt, um Datenströme und Pakete zu klassifizieren. Leider garantiert dieses Verfahren jedoch nicht, dass die Daten keiner Verzögerung durch Pufferung in den Netzwerkkomponenten, wie Switche und Router, unterworfen wird. Eine maximale Ende-zu-Ende Verzögerung kann somit nicht bestimmt werden.

Somit müssen, auf Basis dieser Grundvorgaben aus dem 802.1Q Standard, weitere technische Lösungsansätze das Nichtüberschreiten einer maximalen Verzögerung sicherstellen. Dabei ist natürlich darauf zu achten, dass die Latenz nicht nur auf der Verzögerung in den Netzwerkknoten beruht, sondern auch durch die Laufzeit des Signals im Leiter bestimmt wird. Und da wird dann auch die Wegstrecke zu einem wichtigen Kriterium in der Gesamtbetrachtung.

Ein Schritt in diese Richtung ist der Einsatz von IEEE 802.1Qbv. Dieser Standard ist ein weiterer Baustein in Richtung des Time Sensitve Networking und basiert auf Grundlagen des guten alten TDMA (Time-Division Multiple Access), also dem Zeitmultiplexverfahren aus der Telefon-Welt. Damit können Echtzeitanforderungen aus dem Industrieumfeld und der Robotersteuerung erstmalig in einem standardisierten Ethernet Netzwerk eingesetzt werden, ganz ohne Rückgriffe auf klassische Bussysteme und deren Ethernet-Ablegern.

Ein Scheduler greift dabei auf die mit 802.1Q markierten Pakete zu und sendet diese zu einem vorher definierten Takt (Zyklus). In der Praxis wird daher eine der acht Klassen mit diesem Scheduler verknüpft, damit ist sichergestellt, dass ein oder mehrere Pakete dieser Klasse immer zu einem bestimmten Zeitfenster gesendet werden können.

Eine Verknüpfung der Standards 802.1Qbv und 802.1Qav (einer Erweiterung des eingangs erwähnten 802.1BA) erlaubt daher aktuell die Einteilung in zwei fixen Zeitfenster und ein unbestimmtes:

1. Industrieanwendung nach 802.1QBV
2. Videoanwendung nach 802.1Qav
3. Restliche Daten (unbestimmt)

Die Abbildung 1 zeigt den Zugriff exemplarisch für eine Anwendung, deren Pakete mit der VLAN-Priorität 3 versehen werden. Wichtig ist hierbei, dass alle, und damit sind wirklich alle Teilnehmer eines solchen Netzwerkes gemeint, die Zeitsynchronisation unterstützen und zusätzlich wissen, welche Information zu welchem Zeitfenster gesendet werden darf.

Ein Problem, was hier nun akut werden kann, ist der Umstand, dass ein gesendetes Frame in unseren fixen Sendeslot hineinragen kann (Abbildung 2). Damit würde sich das Versenden um den Zeitbetrag verzögern, der benötigt wird, um das gerade im Versand befindliche Paket abzuschließen.

Damit kann das garantierte Zeitfenster nicht mehr eingehalten werden, und die Synchronisation geht somit verloren.

Diese Erkenntnis führt letztendlich zur Einführung von sogenannten Schutzbändern (Bild 3). Ein Schutzband ist ein Zeitfenster, das dem gesicherten Übertragungszeitraum voran geschaltet wird. Dieses Zeitfenster verhindert, dass es zu einer Überlagerung zwischen einem in Sendung befindlichen Frame und dem garantierten Zeitfenster kommt.

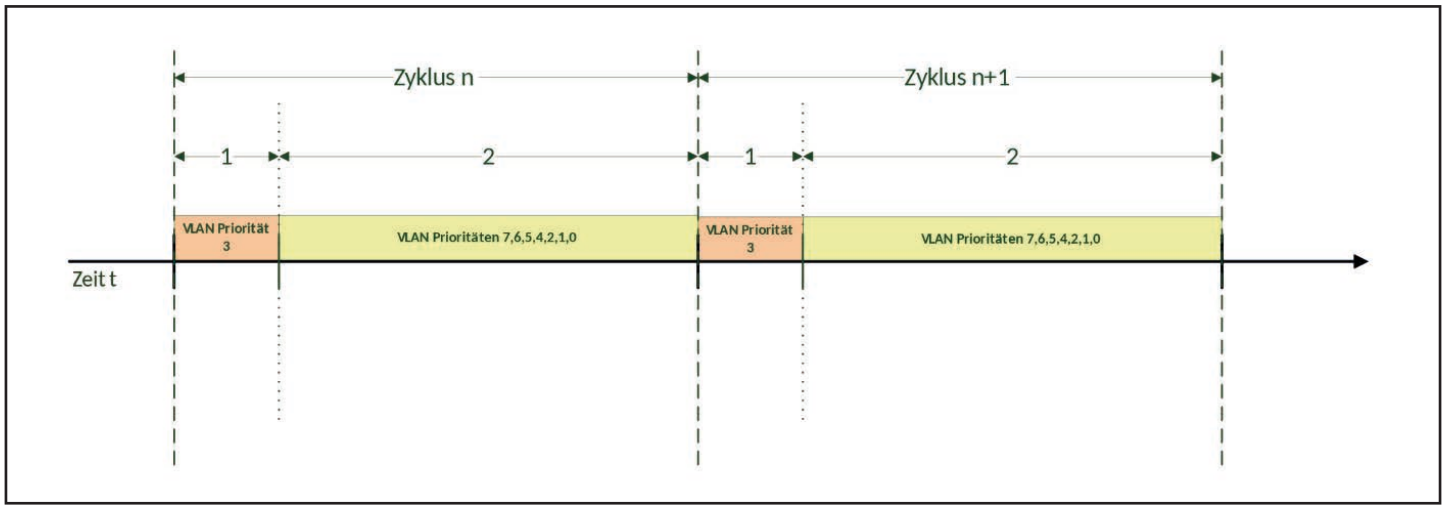


Abbildung 1: Traffic Schedule nach IEEE 802.1Qbv

Quelle: Ulgorash - Eigenes Werk, CC BY-SA 4.0, **https://commons.wikimedia.org/w/ index.php?curid=50281258**