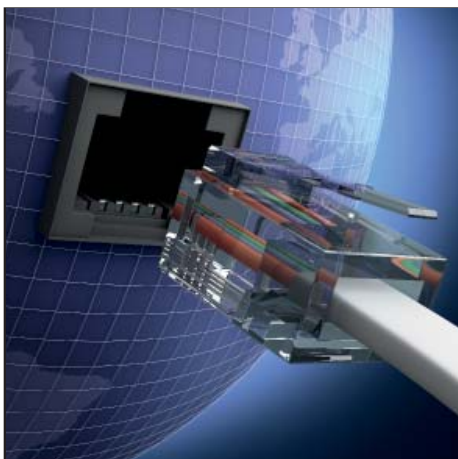


Schwerpunktthema

400 G und 400 Gigabit Ethernet: die nächste Evolutionsstufe

von Dr. Franz-Joachim Kauffels

Bedenkt man die Zeitdauer, die üblicherweise notwendig ist, bis ein Standard angemessen in Produkte umgesetzt werden kann, ist nach der Verabschiedung von 40 und 100 GbE die nächste Evolutionsstufe mit 400 GbE bereits längst überfällig. Es besteht die Gefahr, dass Produkte den Standard überholen könnten. Das hat es in der Vergangenheit schon mehrfach mit negativen Folgen für die Betreiber gegeben. In diesem Artikel betrachten wir Ziele und Überlegungen innerhalb der Standardisierung, mögliche Märkte und Anwendungsgebiete, einige technische Fragen und ... die ersten Produkte!



John d'Ambrosia, Vorsitzender der 400G Study Group von IEEE und Chef-„Ethernet-Evangelist“ bei DELL, hat es mit zwei Sätzen auf den Punkt gebracht: „Blickt man auf das Bandbreitewachstum – wir haben mobile Telefone und Server ... ja sogar schon 40G-Server – gibt es einen Tsunami an Bandbreite-Bedarf.“ „Als wir mit der Standardisierung von 10G begonnen haben, gab es noch kein iPhone!“

weiter auf Seite 7

Zweitthema

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 3

von Dipl.-Inform. Petra Borowka-Gatzweiler

Dieser Beitrag gibt exemplarische Einblicke in aktuelle Enterprise Session Border Controller Produkte etablierter Hersteller und veröffentlicht die Ergebnisse einer UBN-Evaluierung von

Q4/2015 zu den Funktionsbereichen

- Architektur
- SIP Trunking
- Sicherheits-Funktionen

Im Rahmen dieser Evaluierung wurden ca. 150 Kriterien aus den Bereichen Architektur, Sicherheit und SIP Trunking bewertet.

weiter auf Seite 20

Geleit

Fabrics kontra Bandbreite: Intelligenz kontra Kraft?

auf Seite 2

Aktueller Kongress

ComConsult Netzwerk Forum 2016

ab Seite 4

Standpunkt

Kernprozess der operativen IT-Sicherheit: Management von Sicherheitsvorfällen

auf Seite 16

Aktuelle Seminare

Neue Seminare für Nichtjuristen über die rechtlichen Herausforderungen von IT-Technologien

ab Seite 17

Neue Videos

VoIP ersetzt PSTN

auf Seite 19

Zum Geleit

Fabrics kontra Bandbreite: Intelligenz kontra Kraft?

Und wieder ist ein neuer Ethernet-Standard in der Entwicklung. 400 Gigabit/s sollen es diesmal sein, die uns alle sehr glücklich und zufrieden machen werden. Was bedeutet das? Neues Design, neue Komponenten, schon mal sparen?

In der Vergangenheit gab es darüber wenig nachzudenken. Mit jedem neuen Standard kam die 10-fache Bandbreite irgendwann einmal zum 3-fachen Preis des vorhergehenden Standards. Häufig mussten wir dazu zwei oder drei Chip-Generationen warten bis wir dieses neue Preisniveau erreicht hatten. Damit wurde der neue Standard automatisch auch die deutlich wirtschaftlichere Lösung. Gleichzeitig gab es bei den älteren Standards gerade bei den Übergängen von 100 Mbit/s auf 1 Gigabit oder später auf 10 Gigabit einen echten nachweisbaren Bedarf. Es gab nämlich einzelne Kommunikations-Verbindungen, die diese neue Bandbreite tatsächlich benötigten.

Aber das ist wie schon erwähnt Vergangenheit. Betrachten wir den aktuellen 100-Gigabit-Standard, dann hat es sehr sehr lange gedauert bis der Standard auf der Produktseite so verfügbar war, dass wir von einem wirklichen Produktangebot sprechen konnten. Zwar sind wir uns vermutlich alle darüber einig, dass die 40 Gigabit-Lösungen Müll sind (wenn nein, empfehle ich die Videos von Dr. Kauffels zu diesem Thema auf ComConsult-Study.tv), aber trotzdem erfolgt die Adaption von 100 Gigabit/s nur sehr langsam. (siehe Abbildung 1)



Warum ist das so?

- für viele Installationen ist der Bedarf kaum gegeben. 10 Gigabit/s sind sehr preiswert, werden in vielen Geräteformen angeboten und reichen momentan aus.
- es gibt kaum eine Einzelverbindung, die mehr als 10 Gigabit/s erfordert. Viele Speichersysteme arbeiten bisher mit einer Anzahl von 10 Gigabit/s-Ports (auch weil der einzelne Datenstrom deutlich niedriger ist). Die Server sind auf 40 Gigabit/s zwischen Server und Top-of-Rack gewechselt, aber das ist bedingt durch Virtualisierung bereits eine Aggregierungs-Verbindung, ohne dass ein einzelner Datenstrom tatsächlich mehr als 10 Gigabit/s benötigt.

- 100 Gbit/s ist weiterhin sehr teuer und das Angebot ist durchaus als eingeschränkt zu bezeichnen.

Damit bleibt als zu diskutierendes Thema der Bereich Aggregation, also wie gehe ich damit um, wenn ich in bestimmten Teilen des Netzwerks sehr viel parallele Datenströme habe, sie in Summe deutlich mehr als 10 Gigabit/s erfordern. Und hier liegt das Hauptargument gegen neue Bandbreiten in intelligenteren Netzwerken. Sogenannte Fabrik-Architekturen verbinden Skalierbarkeit, Redundanz und optimale Wirtschaftlichkeit in einem einzigen Architektur-Ansatz. Und vor allem passen sie zu den Architekturen, die wir auf der Server und Speicher-Seite einsetzen. Wir haben im November letzten Jahres unseren Report zur Entwicklung der IT-Infrastrukturen in den nächsten 5 Jahren veröffentlicht (IT-Infrastrukturen 2020, Dr. Jürgen Suppan, ComConsult Research). Und eine der absoluten Kernaussagen des Reports war, dass Scale-Out-Architekturen bei Servern und Speichern die Zukunft bestimmen werden. Die Zeiten, zu denen wir durch Austausch von Komponenten auf die nächst neue Generation gewechselt sind, sind bei Servern und bei Speicher-Systemen vorbei. Es ist einfach zu teuer und passt auch nicht mehr zu der immer häufiger anzufindenden Software-Architektur.

Dies entspricht auch der Entwicklung, die wir bei den sehr großen Cloud-Anbietern beobachten. Abbildung 2 zeigt ein Bild von Facebook, das deren Scale-Out-Architektur im Netzwerk-Bereich beschreibt. Auch wenn es die Cloud-Rechenzentren aufgrund der sehr eingeschränkten Vielfalt ihrer Anwendungen einfacher haben und dementsprechend mehr das Problem haben eine Multiplikation einer einfachen Grundstruktur zu finden, so deckt sich das im Prinzip mit unserer Sichtweise so wie wir es in unserer Studie entwickelt haben.

Was schließen wir daraus für die Zukunft? Auf der einen Seite sind wir fest davon überzeugt, dass 10 Gigabit/s nicht ausreichen werden. Wir werden in den nächsten Jahren zunehmend den Bedarf für mehr auch auf der Ebene einzelner Verbindungen haben, zum Beispiel bei der Anbindung großer SSD-Speicher-Systeme. Da wir nicht an 40 Gigabit glauben, führt das zu der automatischen Schlussfolgerung, dass 100 Gigabit/s der natürliche Zukunfts-Standard der nächs-

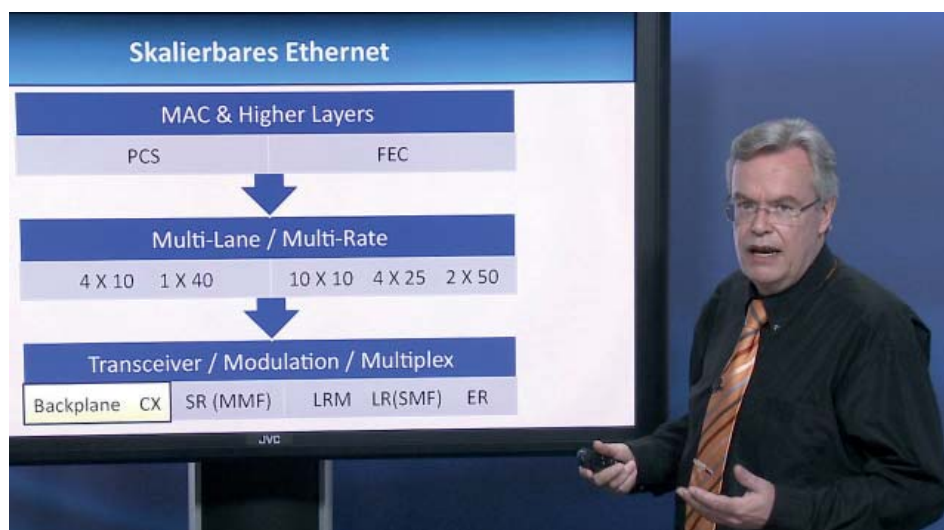


Abbildung 1: Video - Wir überspringen 40GbE

<http://www.comconsult-study.tv/de/Wir-ueberspringen-40-GbE::1419:5.htm>

SchwerpunkttHEMA

400 G und 400 Gigabit Ethernet: die nächste Evolutionsstufe

Fortsetzung von Seite 1



Dr. Franz-Joachim Kauffels ist Technologie- und Industrie-Analyst und Autor. Seit über 30 Jahren unabhängiger, kritischer und oft unbequemer Bestandteil der Netzwerkszene. Verfasser von über 20 Büchern in über 70 Ausgaben sowie über 2000 Artikeln, Videos und Reports.

Wir wissen bereits, dass die Mobilität von Endgeräten der „Knüller“ der letzten Jahre war. Während in Europa erst gegen 2020 die nächste Mobilfunkgeneration 5G eingeführt werden soll, beginnen Provider wie Verizon und AT&T in den USA mit den ersten Versuchen und haben ehrgeizige Pläne für 2018. Im Zentrum aktueller Bemühungen steht daher die Aufrüstung der Glasfaser-Backbones. Mit 10 oder 40 G pro DWDM-Kanal kann man eigentlich jetzt schon nicht mehr viel anfangen, der überwiegende Teil neu installierten Equipments ist für 100 G ausgelegt. Durch bessere Filter und andere Anordnung sowie Zusammenführung von Kanälen kann man in Verbindung mit dichterem Vordimensionierung auf Kabelsystemen, die für 40 oder 50G ausgelegt waren (teilweise sogar für 10G) multiple 100 G-Verbindungen schaffen. Der Hersteller Ciena gibt an, dass 85 % der Kunden für Neuinstallationen 200G-Lösungen wählen. Wie immer ist es der DWDM-Technik eigentlich egal, welches Übertragungsformat genutzt wird. Ethernet ist eine mögliche Alternative unter vielen.

1. Der Markt für 400 GbE

Viele werden nicht verstehen, wo es überhaupt Märkte für 400 GbE geben könnte. Aber sie sind überraschend groß und vielfältig. Nach Angaben von Markt-Beobachtern wie z.B. LightCounting Market Research haben sich die Größenordnungen bei Cloud-RZs massiv verschoben und der Anteil der Rechenzentren, die man als „Mega-DC“ bezeichnen kann, wächst mit atemberaubender Geschwindigkeit. Ähnliche Aussagen kommen auch von IDC. Für die Netzwerk-Cores in diesen RZs sind Geschwindigkeiten von 100 GbE eigentlich schon heute als Engpass zu bezeichnen. Wichtig ist, dass die Standar-

disierung mit der Kurve hinsichtlich der Anforderungen an die Datenübertragung mithalten kann und nicht zurückfällt. Das ist der erste Grund für die Trennung der Entwicklungen von 400 GbE und Terabit Ethernet.

Seit der Verabschiedung der Standards für 40 und 100 GbE hört die Ethernet Alliance laufend Klagen von Mitgliedern und der Industrie im Ganzen hinsichtlich des massiven Wachstums des globalen Netzwerk- und Internet-Verkehrs, die streng genommen keine nachhaltige systematische Weiterentwicklung der Systeme

mehr erlaubt, sondern letztlich nur ein Hinterher-Hecheln mit eher panischen Reaktionen. Man schätzt, dass alleine das Ethernet für Fahrzeuge eine Vielzahl neuer Benutzer, Ports und Anwendungen in die Systeme bringen wird, mit denen ein erheblicher Anstieg der benötigten Bandbreite einhergeht, der mit heutigen Möglichkeiten kaum zu bewältigen ist. Werfen wir zur weiteren Betrachtung einmal einen Blick auf Abbildung 1.

In der Abbildung werden grob nur zwei Bereiche unterschieden, nämlich „Telekommunikation“, das alle Arten von Pro-

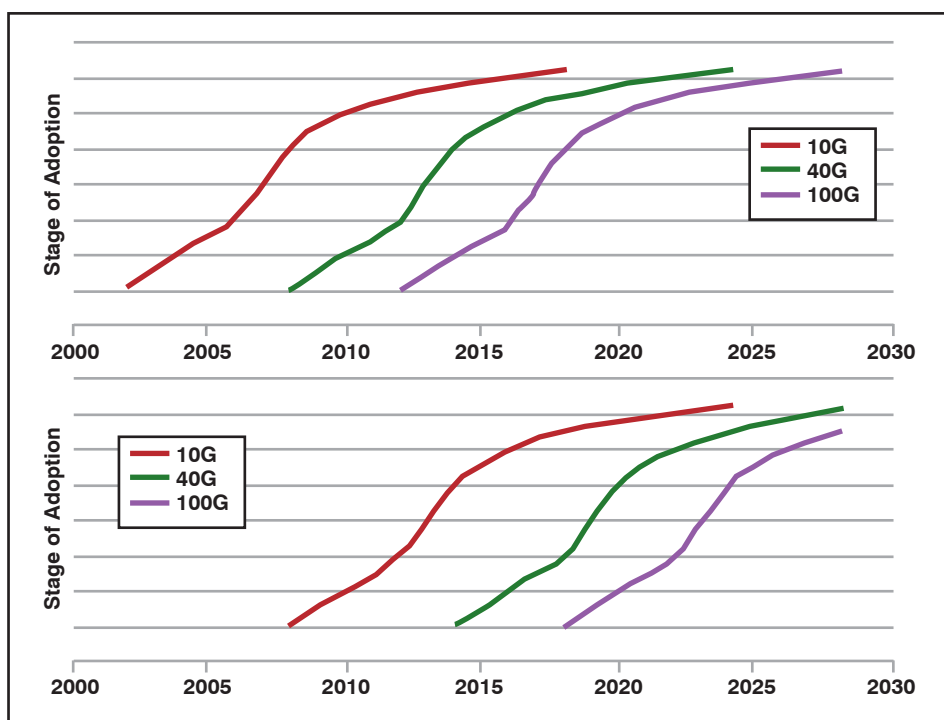


Abbildung 1: Adaption von Technologien

Quelle: LightCounting

400 G und 400 Gigabit Ethernet: die nächste Evolutionsstufe

vidern, Cloud Providern, Internet Exchanges, Unterstützungsnetzen für Wireless Infrastrukturen (LTE) usw. umfasst und „Datenkommunikation private RZs“. Was vielen bereits lange klar ist, zeigt sich hier sehr deutlich: neue Technologien kommen im Telekommunikations-Bereich viel eher „an“.

So werden die nächsten Jahre bei Providern vor allem durch eine drastische Zunahme von 100, 200 und 400 GbE-Verbindungen gekennzeichnet sein. Seit 10 GbE hat man hier allerdings auch den Effekt, dass sich neue Geschwindigkeitsstufen auch durch technische Verbesserungen bei den Modulationstechniken ergeben haben. So konnten in vielen Fällen Verkabelungs-Infrastrukturen mit SMF, die eigentlich nur für 10 GbE-Netze ausgelegt waren, auch mit 40 GbE und in Einzelfällen sogar mit 100 GbE betrieben werden, weil man von einer Modulation, die man schlicht als „Lichtmorsen“ bezeichnen könnte (technischer Name: NRZ), zu komplexeren Modulationsformen übergegangen ist, die einfach mehr Bits in einen Kanal gebracht haben, prinzipiell völlig analog zur Vorgehensweise bei WLANs, deren Leistung durch die Einführung von OFDM und Multi-Antennentechnik in den letzten 10-15 Jahren fast um den Faktor 1000 gesteigert werden konnte. Man darf dabei nie vergessen, dass wir im Fernbereich vorwiegend von Multi-Wellenlängen-Systemen, meist DWDM, sprechen, bei denen sich die Datenraten auf einzelne Kanäle beziehen, die eben mit einem bestimmten Wellenlängenbereich (einer „Farbe“) implementiert werden. In diesem Umfeld ist ein Standard für 400 GbE eine Möglichkeit, auf einer „Farbe“ eben einen Kanal mit der Übertragungsleistung von 400 Gbit/s. aufzubauen.

Jedes Mal, wenn Provider die Leistung von Kanälen erhöhen können, sparen sie bares Geld, weil das ja eigentlich die Zusammenlegung von mehreren Kanälen zu einem einzigen bedeutet. Dadurch hat man wieder weniger Einzelteile, weniger Wartungspunkte und benötigt letztlich sogar weniger Personal. Voraussetzung ist eigentlich nur, dass die neue Technik nicht zu teuer wird.

Die untere Hälfte der Graphik zeigt, dass es die Betreiber von privaten RZs langsamer angehen lassen. Sie haben in der Breite grade damit angefangen, 40 GbE zu installieren. Es gibt aber durchaus die Ansicht, dass viele „Strategen“ an dieser Stelle einen schwerwiegenden Fehler machen: sie setzen nämlich voraus, dass das notwendige Leistungswachstum in einem privaten RZ relativ langsam ist und keine Sprünge macht. Dabei übersehen

sie aber eine Anzahl von Möglichkeiten, die zu einem eher sprunghaften Anwachsen des Leistungshungers auch in einem privaten RZ führen können:

- Einführung völlig neuer Dienste
- Einführung eines neuen betrieblichen Konzepts
- Einführung einer neuen Prozessor-Generation
- Ernsthafte Konzentration
- Ernsthafte Konvergenz

Hinsichtlich der möglichen Einführung neuer Dienste von BYOD über UC bis hin zu IoT haben wir schon viele Quadratmeter Informationen zusammengetragen und das sollte soweit bekannt sein, dass wir es hier nicht weiterverfolgen.

Ein neues betriebliches Konzept ist z.B. die Virtualisierung. „Das Netz wird zum Systembus“ war die Parole der Berater, die sich bis heute bewährt hat. Hier kann man aber sehr schnell in ein Massenproblem laufen und es ist sicher kein

halten. Mit entsprechenden Erweiterungen wie Ivy Bridge und Jordan Creek entsteht ein Bandbreite-Monster. Siehe dazu ohne weitere Erläuterungen die Abbildungen 2. Hersteller können mit diesem Prozessor Server-Systeme bauen, die bis zu 120 Threads unterstützen und selbst wenn man bequem ist, kann man pro Thread eine VM installieren. Eine heute bei weniger anspruchsvollen Installationen gerne genannte Daumenregel ist, dass man pro VM 1 GbE Kommunikationsleistung vorsehen soll. Das umfasst natürlich nur VMs, die recht einfache Aufgaben haben. Wir erinnern uns, dass vier Prozessoren zusammen auf einem Sockel sitzen, das heißt im Klartext, es gibt auch nur einen einzigen Server, auf den z.B. zehn bisherige Server konsolidiert werden können, die jeweils rund 12 VMs hatten.

Also muss man selbst wenn man zwei wirklich kritisch vereinfachende Annahmen, nämlich die Beschränkung auf 1 GbE pro VM und eine Überbuchung von

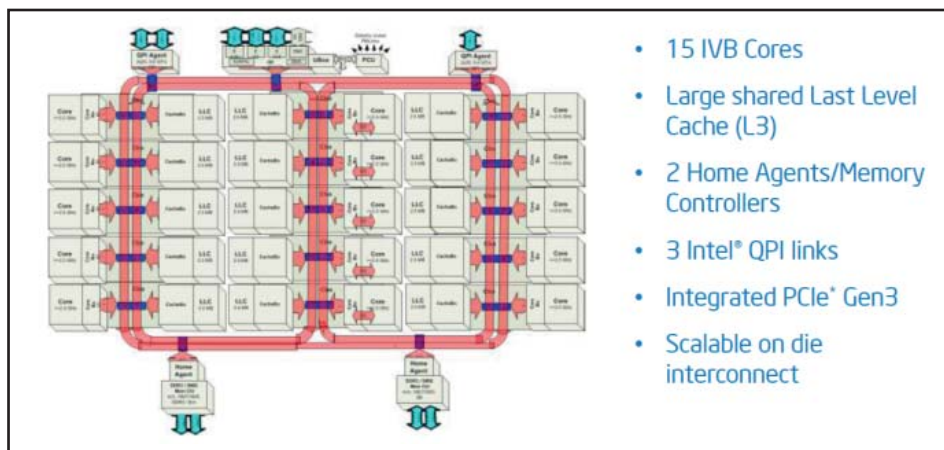


Abbildung 2: Der Server-Hammer: Intel Xeon E7 V2: bis zu 60 Cores/120 Threads Quelle: Intel

Zufall, dass jetzt wieder die Thematik von QoS und Priorisierung aufkommt. Eigentlich benötigt man beides in einem RZ wie Bauchweh, wenn die zugrundeliegende Leistung des Netzes wirklich stimmt. Die Hersteller bringen aber die Diskussion erneut auf, weil sie schon befürchten, dass das nicht der Fall sein wird.

Die Einführung einer neuen Prozessor-Generation alleine wäre vielleicht nicht weiter aufregend, wenn sie nicht gleichzeitig mit neuen strukturellen Konzepten verbunden würde. Betrachten wir einfach nur den neuen Xeon® E7 V2-Prozessor von Intel. Dieser Prozessor setzt alle bisherigen Maßstäbe außer Kraft. Ein einzelner Prozessor hat 15 Cores, aber mit einer speziellen Sockelkonstruktion kann man bis zu vier Prozessoren zusammenschalten, die sich wie ein einzelner ver-

20% hinnimmt, für diesen Server einen Vollduplex-100 GbE-Anschluss vorsehen. Die Hoffnung, hier mit einem Bündel von 10 GbE-Anschlüssen auszukommen, entspricht nicht mehr dem Stand der Technik. So, und wenn man auf der Server-Ebene bereits bei 100 GbE angekommen ist, wird man im Aggregations-Bereich 400 GbE dringend benötigen.

Wenn man es streng auslegt, hat IEEE ziemlich tief geschlafen. Die Entwicklung bei den Prozessoren ist recht gut vorhersehbar und der E7 V2 hätte gut und gerne auch schon im Jahr 2014 kommen können. Wenn das Spektrum der Möglichkeiten bei 100 GbE endet, ist das für Prozessoren dieser Art, von denen es bald mehr geben wird, nicht adäquat. Nach wie vor wird es auch private RZ-Netze geben, die sehr verzweigt sind und nicht mit

Zweitthema

Session Border Controller: Die Perimeter-Komponente für All-IP

Fortsetzung von Seite 1



Dipl.-Inform. Petra Borowka-Gatzweiler leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

Die nachfolgende Übersicht in Abbildung 5.2 zeigt die Einzelbereiche sowie die vorgenommene Gewichtung.

Die Session Border Controller Produktlinie des Herstellers Oracle (Acme) wurde nicht in die Evaluierung einbezogen, da wir nach dem Aufkauf von Acme durch Oracle eine stark schwindende Marktbedeutung der Acme SBCs für den allgemeinen Markt erleben.

5.1 Produktbeispiel: OpenTouch von Alcatel-Lucent Enterprises

Die ALE Lösung zur Realisierung der Session Border Funktionen kommt im Dreierpack, das heißt sie kombiniert drei Elemente als Paket (siehe Abbildung 5.3): Den OpenTouch Session Border Controller, den OpenTouch Edge Server und einen (OpenTouch) Reverse Proxy. Die Lösung wird im Bereich MLE (mittlere und große Unternehmen) unter dem UC-Brand OpenTouch vermarktet.

Die Architektur ist eine Overlay Lösung, die eine bereits vorhandene Sicherheits-Infrastruktur wie FW und Authentisierung voraussetzt, welche weiterhin zum Einsatz kommt. Die Lösung unterstützt SIP Trunking Funktionen, webbasierte Kollaboration für Gäste via Internet und UC Multipunkt-/Multimedia-Dienste für Remote Nutzer, die sich von zu Hause oder von unterwegs aus einloggen (natürlich im Rahmen der ALE-eigenen UC-Lösung OpenTouch).

Der OpenTouch Session Border Controller leistet SIP Perimeter Schutz für SIP Trunking und SIP remote Zugriff von PCs, Tablets oder Smartphones aus.

Der OpenTouch Edge Server agiert als Front End Server für den Web-Zugang. Im Zusammenspiel mit dem SBC leistet er:

Hauptgruppe	Prozent	Untergruppe	Prozent	Punkte	Normierte Punkte	Wichtungsfaktor
Architektur	25%			158	98,50	0,62
Sicherheit	40%					
		Authentisierung, Zugangskontrolle	15%	21	23,64	1,13
		Topology Hiding, Angriffsschutz	85%	133	133,96	1,01
SIP Trunking, Leistungsmerkmale	35%					
				82	137,90	1,68
Summe	100%			394	394,00	

Abbildung 5.2: Enterprise Session Border Controller Evaluierung

- die Authentisierung von Gästen mittels Web-Zugangscodes
- Screening und Weiterleiten von legitimen Konferenzen zum internen Konferenzserver (dies bedeutet zum Beispiel, dass er gefälschte URLs blockiert)
- abhängig von der konfigurierten Policy: Unterstützung der eingehenden oder ausgehenden Einwahl in eine Konferenz über PSTN

OpenTouch Edge Server wandelt eingehende WebRTC Sessions in reinrasige SIP Sessions, das heißt insbesondere: er entfernt die HTML5 Container. Der OpenTouch Edge Server implementiert hierfür einen back-to-back WebRTC und SIP Agenten. Das versetzt ihn in die

Lage, WebRTC ↔ SIP Gateway zu spielen. Erst nach Durchlaufen der Gateway-Funktion des Edge Servers kommen Signalisierung und Media Stream(s) einer Session am OpenTouch Enterprise Session Border Controller an und werden hier kontrolliert und bearbeitet; somit ist der SBC in der Lage, alle SIP und RTP Streams kontrollieren, die zwischen den Enterprise SIP Applikationen und der WebRTC Applikation ausgetauscht werden. Eine Übersicht zum Zusammenspiel von Edge Server und SBC zeigt Abbildung 5.4.

Der OpenTouch Reverse Proxy authentisiert und terminiert die TLS Verbindungen, die die Web Dienste absichern, welche von OpenTouch Client Anwendungen auf PCs, Tablets und Smartphones genutzt werden

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 3

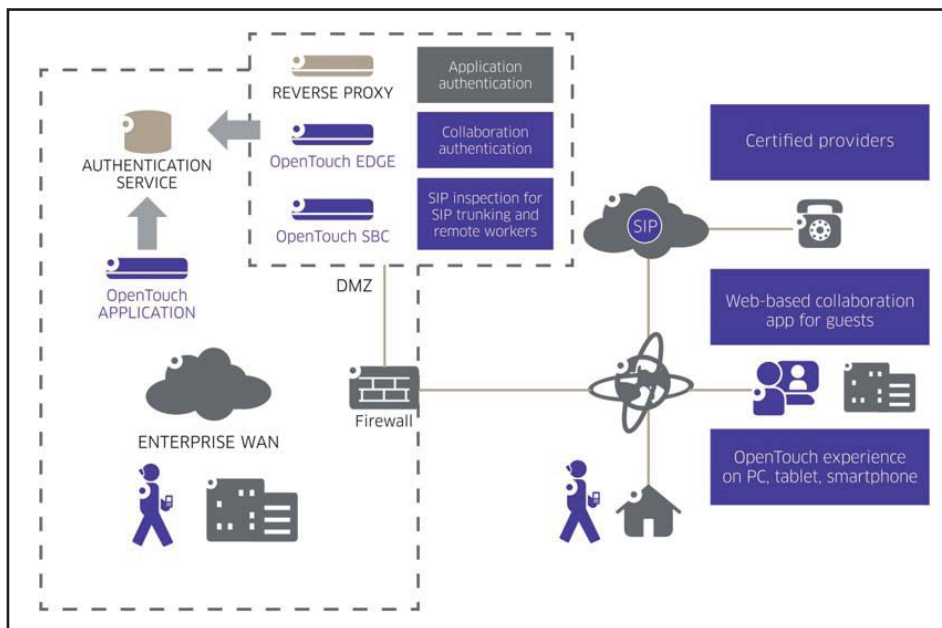


Abbildung 5.3: Session Border Control Lösung von Alcatel-Lucent Enterprises Quelle: Alcatel-Lucent

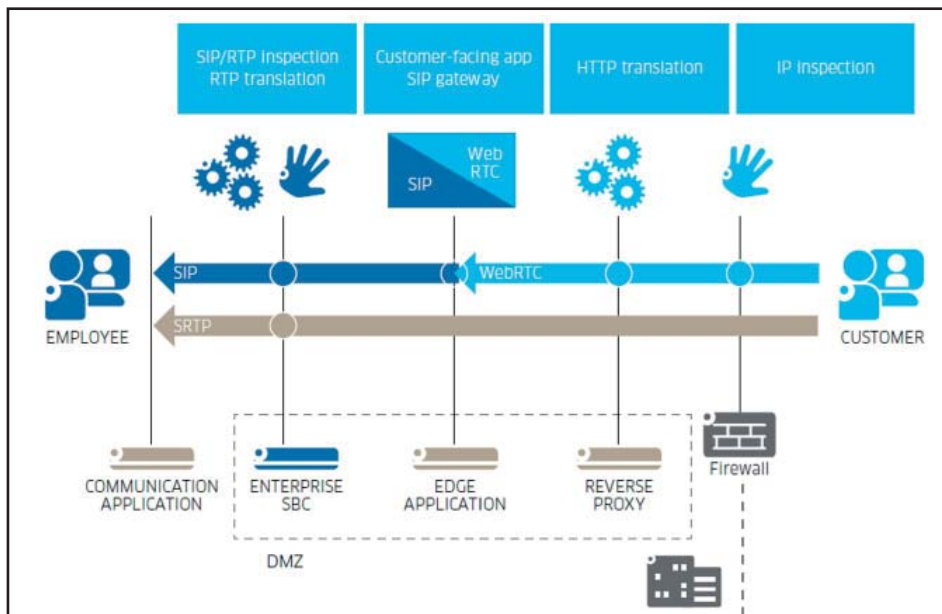


Abbildung 5.4: Kommunikation von WebRTC Anwendungen mit internen SIP UC Diensten

Quelle: Alcatel-Lucent

- Er baut für sich selbst eine Verbindung zum Authentifizierungsdienst des Unternehmens auf
- Ein bereits vorhandener Reverse Proxy für HTTP Translation und Authentifizierung von Web Applikationen lässt sich auch für die OpenTouch Webdienste nutzen

OpenTouch Session Border Controller

Der OpenTouch Session Border Controller ist ein OEM von Audiocodes. Als dedizierte Hardware-Lösung (HP Proliant DL320,

HP Proliant DL120) unterstützt er Implementierungen von 50 bis maximal 5000 registrierten Teilnehmern und bis zu 4000 Sessions. Als virtualisierte Lösung ist die Leistung sehr viel niedriger: mit der Virtual Edition auf Basis VMware ESXi 5.1 (2 Cores, 2 GB RAM, 10 GB HDD) sind maximal 1000 registrierte Teilnehmer / TLS Sessions und maximal 250 SIP Sessions möglich.

Aber auch bei der Anzahl SIP Sessions stellt 4000 eine Obergrenze dar, die nicht immer gilt: Unterstützt werden zwar maximal 4000 SIP/SIPS Audio Sessions, aber

nur 2000 Video Sessions. Eine gleichartige Einschränkung gilt für Verschlüsselung: während 4000 RTP Sessions möglich sind, werden max. 2000 SRTP Sessions unterstützt.

Im Sicherheitsbereich unterstützt der OpenTouch Session Border Controller Funktionen, die der Betreiber im Unternehmen typischerweise erwartet

- SIPS, SRTP für Audio und Video, parallel SRTP und RTP
- DDoS Prevention L3/L4, SIP stateful Inspection, SIP Topology Hiding
- SIP IDS und SIP Black Listen
- dynamisches Audio und Video Port Firewall Pinholing
- SIP Authentisierung (HTTP digest) für Clients und Gateways
- SIP Authentisierung durch externen RADIUS Server
- Erweitertes Media Latching (für NAT Traversal)

Die Evaluierung zeigt einen Gesamt-Erfüllungsgrad von knapp 77 Prozent, wobei der Erfüllungsgrad im Bereich Architektur mit 64,6 Prozent am schwächsten ausgeprägt ist, SIP Trunking hat mit einem Erfüllungsgrad von knapp 83 Prozent den höchsten Umfang. (siehe Abbildung 5.5 und Abbildung 5.6)

5.2 Produktbeispiel: Avaya Session Border Controller for Enterprise

Der Avaya Session Border Controller for Enterprise (ASBCE) ist innerhalb der üblicherweise vorhandenen Sicherheits-Infrastruktur, also zwischen dem internen und externen Firewall positioniert und führt dort die für eine gesicherte SIP Kommunikation notwendigen Kontroll- und Schutz-Funktionen durch (siehe Abbildung 5.7 und Abbildung 5.8). So werden die UC-Applikationen sowohl allgemein durch die Enterprise (IT) Firewalls als auch speziell durch den ASBCE mit seiner "SIP-Awareness" geschützt. Diesen schicht-orientierten Sicherheits-Ansatz empfiehlt Avaya als anerkannte Best Practice Lösung.

In dieser Arbeitsteilung blockieren Firewall und IDS / IPS die Layer-3 und Layer-4 Angriffe sowie Angriffe auf Betriebssysteme und IT Applikationen, der Session Border Controller verhindert im Standard-Lieferumfang Angriffe des SIP Protokolls sowie Angriffe über das SIP Protokoll, insbesondere DoS und DDoS mit SIP Spoofing und SIP Kompromittierung als Toll Fraud (Dienste-Nutzung auf Kosten des Angegriffenen). Für Remote Nutzer Zugriff, Media Replizierung und Verschlüsselung von Signalisierung und/oder Media Streams wird eine erweiterte Lizenz benötigt.