ComConsult Research

Der Netzwerk Insider

August 2017

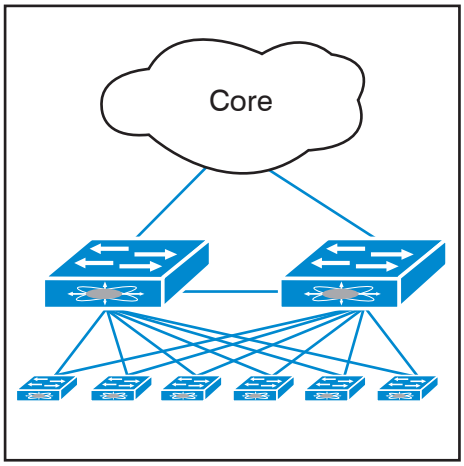
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Overlays in der Analyse - Teil 1: EVPN vs. SPBM

von Dipl.-Math. Cornelius Höchel-Winter

Die gesamte Rechenzentrumsinfrastruktur befindet sich derzeit im Umbau: weg von den klassischen Einzelboxen, die als Server, Switch, Firewall etc. individuell für einzelne Anwendungen konzipiert wurden, hin zu einer integrierten Gesamtstruktur, die gemeinhin als Cloud Computing bezeichnet wird. Die Gründe für diesen Wandel sind im Wesentlichen bekannt, im Vordergrund stehen die Bereitstellung und der Betrieb von Anwendungen. Anwendungen müssen schnell und flexibel nutzbar zur Verfügung stehen, um auf Kundenanforderungen unmittelbar und zielgerichtet reagieren zu können und um notwendige Änderungen bei den Geschäftsprozessen in kürzester Zeit umsetzen und neue Funktionen adäquat unterstützen zu können. Der Druck aus dem Markt ist in jeder Branche enorm.



Im folgenden Artikel werden zunächst die grundlegenden Konzepte und Bausteine von Overlay-Technologien und deren diversen Ausprägungen analysiert. Im zweiten Teil stellen wir dann mit SPBM und EVPN zwei verbreitete Overlay-Lösungen gegeneinander, die gleichzeitig für die beiden Basistechnologien in Unternehmensnetzen stehen: Layer 2 (Ethernet) und Layer 3 (IP).

weiter ab Seite 9

Zweitthema

Cisco „Campus Fabric“ oder Software-defined Access

von Dr. Joachim Wetzlar

Ohne das Attribut “Software-defined” lassen sich derzeit offensichtlich keine neuen Produkte mehr an den Mann bringen. Nach den Software-defined Networks (SDN) haben wir an dieser Stelle das Software-defined Data Center (SDDC) diskutiert. Sie erinnern sich, es ging um den Einsatz so genannter Overlays und um die Frage, ob man diese besser auf dem Server bzw. Hypervisor oder in den Netzkomponenten realisiert. Nun also Software-defined Access (SDA).

Eigentlich hätte mich dieses Thema nur am Rande interessiert, denn ich nehme bezüglich derlei Techniken grundsätzlich erst einmal eine abwartende Haltung ein. Letztlich hinter dem Ofen hervorgelockt hat mich die Tatsache, dass Cisco mit seiner „Campus Fabric“ eine spannende Anwendung des Locator/ID Separator Protocols (LISP) gelungen ist. Darüber hinaus erkenne ich auch grundsätzlichen Nutzen des SDA für einige meine Projekte.

weiter auf Seite 21

Geleit

Planungs-Ansätze für die Zeit nach ISDN

auf Seite 2

Standpunkt

Informationssicherheit im Mikrokosmos von Smart Buildings

auf Seite 19

Sonderveranstaltungen

Herausforderung Informationssicherheit

Cloud Computing, Security as a Service, Virtualisierung IoT, Abwehr von Angriffen, rechtliche Rahmenbedingungen

ab Seite 18

Wireless und Mobility

ab Seite 27

Aktuelle Kongresse

ComConsult UC-Forum 2017

ab Seite 4

ComConsult Technologie-Tage 2017

ab Seite 7

Geleit

Planungs-Ansätze für die Zeit nach ISDN

Als ISDN 1988 eingeführt wurde hat es mit seiner Digitalisierung die Qualität von Sprach-Kommunikation revolutioniert. Seitdem hat es sich zum absolut elementaren Kern unserer Sprach-Kommunikation entwickelt. Nun lösen wir es aus wirtschaftlichen und technischen Gründen ab. Auf der einen Seite ist sein Betrieb schlicht zu teuer geworden und passte nicht mehr in die integrierte Sprach-Daten-Landschaft. Auf der anderen Seite bestand der Bedarf nach einer technologisch offeneren Lösung, die eine größere Zahl von verschiedenen Diensten unterstützen und vor allem auch integrieren kann.

Aber was nun? Fast alle betroffenen Unternehmen stehen vor einer Reihe von Fragen:

- was kommt nach ISDN?
- wie kann eine erfolgreiche Planung für die Ablösung von ISDN aussehen?
- ISDN ist fast 30 Jahre alt und technologisch rückständig, aber wo liegt die Zukunft?

Wir greifen diese Fragen in unserer Sonderveranstaltung im Oktober und unserem UC-Forum im November auf. Dort werden viele Details und Varianten diskutiert und Empfehlungen für die Umsetzung einer neuen Kommunikations-Strategie gegeben.

Für eine erfolgreiche Projektplanung müssen eine Reihe von Fragen geklärt werden:

- wieso hat sich der Bedarf geändert und wie kann man den neuen Bedarf definieren?
- welchen Einfluss hat Effizienz-Steigerung auf die Auswahl der Lösung?
- wie kann Akzeptanz durch die Nutzer erreicht werden?
- wie gehen wir mit den permanenten Veränderungen auf der Anbieter-Seite um?
- was ist die Rolle der Cloud in zukünftigen Lösungen?

1988 war der Bedarf an Kommunikation konzentriert auf Sprache (und später Fax). Und er war als solcher einheitlich über alle Nutzer hinweg, “one size fits all”. Zwar haben wir mit einer unübertroffenen Fähigkeit zur Schaffung von überflüssiger Komplexität und Kosten selbst aus dieser scheinbar einfachen Aufgabe mit Hilfe von Leistungsmerkmalen das moderne Anlagen-Monster geschaffen (das dann auch in Konsequenz von kaum einem Benutzer tatsächlich genutzt wurde), aber im Grunde war Kommunikation weiterhin einfach und eindimensional.

Dies ist heute anders und jede neue Kommunikations-Lösung muss sich erheblichen Anforderungen stellen:

1. Es gibt nicht mehr die einheitliche Lösung für jeden. Diskutierten wir früher Leistungsmerkmale, so diskutieren wir heute Funktionsbausteine. Die für jeden Nutzer unterschiedliche Kombination aus Sprache, Daten, Video, Chat, Kollaboration usw. erzeugt ein Anforderungs-Profil für wirtschaftliche und effiziente Kommunikation, das in seiner Komplexität weit über die “alten” Lösungen hinausgeht.

2. Die Lösung heißt seit vielen Jahren Unified Communications. Dabei versteht man unter dem Begriff Unified, dass der Nutzer einen Kommunikations-Baukasten vorfindet, aus dem er die Funktionen wählen kann, die für ihn die beste und effizienteste Kommunikation ermöglichen. Dieser Ansatz geht einher mit der Schaffung eines Clients, der den vereinheitlichten Zugang zu allen Funktionsbereichen inklusive des Realzeit-Wechsels zwischen den Funktionen bringt. Darunter versteht sich zum Beispiel der lückenlose Wechsel zwischen Sprache und Video.

So weit so gut. Aber UC-Lösungen enden in vielen Fällen immer noch an der Unternehmens-Grenze. Damit laufen viele der auch wirtschaftlichen Vorteile von UC ins Leere, was wiederum dem Gesamt-Erfolg von UC in Frage stellt.

Damit ist auch klar:

- die Ablösung von ISDN muss vorrangig die Frage beantworten, wie wir in Zukunft zwischen Unternehmen / Behörden oder mit Kunden kommunizieren wollen

Was häufig unterschätzt wird und dann in Folge auch zu einem Problem werden kann, ist die Tatsache, dass in der aktuellen Technologie- und Produktsituation diese Frage zuerst (!!!) beantwortet werden muss.

Warum ist das so?

- wir müssen vermeiden, dass wir redundante Dienste entwickeln. Diese sind nicht nur ein Kosten-, sondern vor allem ein Akzeptanz-Problem. Eine höhere Kommunikations-Effizienz entsteht nicht durch Dienste, sondern durch deren Nutzung. Akzeptanz ist ein Schlüssel-Kriterium. Und kaum ein Anwender wird akzeptieren, dass er zur Kommunikation mit Externen einen anderen Dienst nutzen soll als zur internen Kommunikation

- die Kommunikation mit Externen kann (und wird) auf anderen Architekturen basieren. Statt komplexe Gateway-Lösungen für Video-Konferenzen einzusetzen, kann es sinnvoller und flexibler sein, einen Cloud-Dienst zu nutzen und den externen Kommunikations-Partner dazu einzuladen. Hier wird der Schlüssel zum Erfolg in der Installations-freien Nutzung des Dienstes durch den Externen liegen. Dies erfordert nicht nur die optimale Auswahl von Cloud-Anbietern, sondern auch die Evaluierung von Technologien wie WebRTC

Gleichzeitig generiert die Kommunikation mit Externen ein Client-Problem. UC ist mit der Vision gestartet, dass es nur einen Client gibt, der als Basis für alle Dienste gilt. Die traditionellen Anbieter haben sich hier mehr als 10 Jahre gegen entsprechende Lösungen gesperrt. Es hat der Markt-Macht von Microsoft bedarft, um diese Situation zu ändern. Die Konzentration auf einen Client geht in der Regel einher mit der Möglichkeit der Dienst-Eskalation. Ich kann eben direkt von Chat auf Sprache auf Video wechseln und dabei dynamisch immer mehr Teilnehmer einbinden. Dies funktioniert aber ggf. nur in der internen Kommunikation. Es muss nun die Frage neu gestellt werden, wie wir eine Dienst-Eskalation in der Kommunikation mit Externen handhaben wollen. Was natürlich zuvor die Antwort auf die Frage voraussetzt, welche Dienste wir überhaupt einsetzen wollen. Aber es kann an dieser Stelle blind unterstellt werden, dass die Kombination aus Chat-Sprache-Video das absolute Minimum darstellt. Das hat sich aber dummerweise noch nicht zur Telekom oder zu Vodafone rumgespro-

chen, die nach wie vor bei der Ablösung von ISDN eine reduzierte Sprach-Vision (also keinerlei Vision) haben. Allerdings gibt es dafür Gründe in der technischen Komplexität der Ablösung. Was wiederum zur Frage der gezielten Ergänzung durch Cloud-Dienste führt.

Damit sind wir bei der Frage der Anbieter-Situation und deren Zukunft. Hier gibt es keine einfache Antwort. Der Markt ist verzettelt und für viele sehr unterschiedliche Lösungen gibt es gute Gründe. So beantwortet ein Anbieter Innovaphone die Frage nach einer kostengünstigen internen UC-Lösung aus einer kleinen Box. Demgegenüber verspricht der Fokus auf Microsoft die theoretische Einbindung in alle möglichen Datendienste und eventuell in Zukunft den direkten Übergang ins PSTN und den Übergang zu anderen Unternehmen. Gleiches gilt fast für jeden anderen Anbieter, jeder hat seine spezifischen Vorteile. Trotzdem ist der Kuchen nicht mehr groß genug für alle. Ein guter Start sollte deshalb ein Projekt- und Dienste-Design sein, das möglichst neutral ist und den Wechsel des Anbieters zulässt.

Wie müssen wir an dieser Stelle Kollaboration einschätzen? Fast alle traditionellen Anbieter haben hier entsprechende Lösungen platziert (siehe Cisco Spark, Microsoft Teams, Unify Circuit). Diese Lösungen sehen toll aus, haben aber einen entscheidenden Nachteil: sie sind auf Realzeit Kollaboration reduziert und decken nicht den gesamten Bedarf ab. So gibt es Unternehmen, die ihre Lösungen auf der Basis des genutzten CRM-Produkts aufsetzen, oder Unternehmen, die File-Kollaboration in den Mittelpunkt stellen (siehe Box) oder Unternehmen, die Projekt- und Task-Management mit Kollaboration integrieren wollen (siehe Redbooth). Von daher greifen Lösungen wie Spark oder Circuit eher zu kurz. Auf der anderen Seite sind Bauchladen-Lösungen wie die von Microsoft häufig nicht gut genug im Detail oder auch einfach zu komplex. So ist es auch nicht überraschend, dass gerade viele dieser Projekte an der Akzeptanz der Benutzer scheitern. Die Umsetzung einer guten und dann auch akzeptierten Kollaborations-Lösung ist eine der größten Herausforderungen der modernen Kommunikations-Technik. Und man tut gut daran, diese Art von Projekten nicht mit einem Produkt zu starten. Dies geht mit 90% Wahrscheinlichkeit in die Hose.

Kommen wir noch einmal zum Kern dieses Geleits zurück. Die Ablösung von ISDN erfordert eine Kommunikations-Vision für die Zukunft. Diese muss zwingend mit der Frage der Kommunikation mit Externen beginnen. Bei allen in Frage kommenden Lösungen ist die Akzeptanz durch die Benutzer von entscheidender Bedeutung. Ein Dienst, den keiner benutzt, ist ein sinnloser Dienst. Eine Investition in einen derartigen Dienst ist eine gescheiterte Investition. Hier haben Cloud-Lösungen einen elementaren Vorteil, da sie erst einmal keine Investitionen binden. Dies haben auch die traditionellen Anbieter erkannt und bauen entsprechend ihr Lösungs-Portfolio aus. Dies erlaubt einen Testbetrieb von Diensten in der Cloud, auch wenn der spätere lokale Betrieb für viele Unternehmen weiterhin eine unverzichtbare Option sein kann.

Ein Geleit kann naturgemäß keine Lösungen schaffen.

Wir haben alle diese Fragen analysiert und diskutieren die verschiedenen Varianten möglicher Lösungen mit Ihnen auf unserem UC-Forum und unserer Spezial-Veranstaltung zur Ablösung von ISDN.

Ihr
Dr. Jürgen Suppan

Sonderveranstaltung

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP
9.10.2017 in Bremen

Die Deutsche Telekom hat angekündigt, bis 2018 das klassische PSTN-Netz, respektive analoge und ISDN-Anschlüsse abzuschalten. Dies betrifft alle Unternehmen, die weltweit kommunizieren wollen und müssen. Abgesehen von den rein technischen Unterschieden: bei Leitungsvermittlung vs. Paketvermittlung, E.164 Telefonnummer vs. URI gibt es erhebliche funktionale Unterschiede, denn das Dienstspektrum bei All-IP wird erheblich umfangreicher sein als es im PSTN jemals der Fall war.

Soll sich eine globale SIP / All-IP Kommunikation auf breiter Ebene etablieren, muss dies auf der Basis von genormten oder de facto Standards erfolgen. Hierfür gibt es sowohl bei ECMA als auch dem SIP Forum Ansätze. Welcher hat das größte Marktpotenzial? Gibt es Zertifizierungsmöglichkeiten? Wie sieht die aktuelle Praxis aus?

Die Perimeter-Anschaltung des SIP/All-IP Trunks zwischen Enterprise und Provider wird heute typischerweise mit einem SBC realisiert. Wir analysieren, wie die Anschaltung aussieht, welche Funktionalität von einer solchen Komponente erwartet werden sollte und wie sich der SBC-Markt präsentiert.

Im Rahmen der Veranstaltung analysieren wir, wie der Wechsel von PSTN auf All-IP im Unternehmen verläuft. Wir zeigen auf, welche Funktionalität heute erreicht werden kann und mit welchem Aufwand für Anpassung und Fehlersuche zu rechnen ist. Wie gut ist die Unterstützung durch den Enterprise-Hersteller und Provider? Wie ändert sich Betriebs- und Kostenaufwand? Nicht nur klassische PSTN-Provider werden diesen Markt unter sich aufteilen, sondern auch Kabelnetzbetreiber, Mobilfunkanbieter und ISPs werden ihr Dienstspektrum auf den All-IP Kommunikationsmarkt ausdehnen. Wir analysieren, wie das aktuelle Angebotsspektrum aussieht und welche Roadmap erkennbar ist.

Referenten: Markus Emde, Markus Geller
Preis: 1.090,-- €

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Aktueller Kongress

ComConsult UC-Forum 2017

20.11. - 22.11.2017 in Königswinter

Frühbucherphase bis 15.09.2017

Die ComConsult Akademie veranstaltet vom 20.11. bis 22.11.17 ihren Kongress "ComConsult UC-Forum 2017" in Königswinter.

Das diesjährige UC-Forum analysiert die herausragenden Trends für Unified Communications und Collaboration, VoIP sowie Videokonferenzen und gibt Empfehlungen für Projekte, Technologie-Auswahl und Investitionen in zukünftige Kommunikationslösungen. Das weiterhin dominante Thema ist „All-IP“, die Abschaltung der ISDN- und PSTN-Infrastruktur durch nationale wie internationale Provider und die sich daraus ergebenden Probleme.

Im Rahmen des Forums werden Herausforderungen rund um „All-IP“ identifiziert und Lösungsansätze aufgezeigt, angefangen bei der Frage wie es mit Fax Diensten weitergeht bis hin zu alternativen Anschlüssen für Gefahrenmeldeanlagen.

Dabei darf nicht übersehen werden, dass der Markt sich in einem dramatischen Wandel befindet. Traditionelle Hersteller kämpfen ums Überleben (oder zumindest die Produktqualität!), andere machen sich mit ihren Kollaborationsplattformen auf zu neuen Ufern. Die zunehmende Bedeutung von cloudbasierten UC-Produkten und die Verschiebung von Kommunikationsdiensten von Voice- zu Cloud-Providern werden zu weiteren Verwerfungen im Markt führen. Neue Cloud Angebote – auch von etablierten Lösungsanbietern, wie Alcatel, Cisco oder Mitel – sprechen eine eindeutige Sprache.

Aber auch die Situation rund um Microsoft

Office 365 und Skype for Business bewegt aktuell die Gemüter. Dabei wird oft die Frage aufgeworfen wo die Microsoft Lösung im Vergleich z.B. mit Cisco steht.

Dies geht einher mit einer Welle neuer Dienste und einer Neugestaltung des Mobilfunks. Gleichzeitig rücken Technologien wie Session Border Controller das SIP Protokoll wieder in den Mittelpunkt. Sie entscheiden mehr oder weniger über die Zukunftsfähigkeit moderner UC-Lösungen.

Wir analysieren dementsprechend auf dem UC-Forum 2017 für Sie:

- Wie positionieren sich Microsoft und Cisco, wer hat im Moment die bessere Lösung?
- Die TR Notruf 2.0 ist da. Was sind die wesentlichen Neuerungen?
- Mit SIP Connect und ETSI TISPAN gibt es endlich akzeptierte Peering Standards. Was bieten sie und wo werden sie eingefordert?
- Enterprise Lösungen aus der Sicht des Clients. Wohin entwickeln sich Technik und Funktionen?
- UCC auf dem Weg in die Cloud – was ist möglich und was zu beachten?
- ISDN und PSTN Abschaltung aus Sicht von Providern und Anwendern. Wo liegen die Herausforderungen?
- Fax Dienste sind tot und die mit ihnen verbundenen Arbeitsprozesse müssen sich ändern aber wie sehen die Alternativen aus?

Mit den aktuellen Änderungen der Technik ändern sich auch die Arbeitsplätze. Dies generiert neue Chancen für mehr Effizienz bei sinkenden Kosten, aber es generiert auch eine Reihe ernst zu nehmender Probleme. Gerade hier hat Microsoft in diesem Jahr eine Reihe von interessanten Ankündigungen lanciert, die wir natürlich genauer analysieren möchten.

Als zusätzliche Sonderthemen haben wir für das diesjährige Forum adressiert:

- IT-Compliance und die neue Datenschutzgrundverordnung
- Enterprise Projekterfahrungen bei einem weltweiten Rollout von Office 365 und Skype for Business
- Qualitätssicherung durch VoIP Quality Monitoring und Cloud Readiness Assessments

Seien Sie dabei und erhalten Sie die aktuellsten Trendanalysen und Informationen von ComConsult Research mit Top-Referenten, Analysen, Projektberichten und Praxiserfahrungen.

Folgende Aussteller nehmen derzeit teil (Stand 28.08.17)

In der parallel stattfindenden Ausstellung haben führende Hersteller und Dienstleister der Branche und die Kongressteilnehmer die Möglichkeit zum interaktiven Kontakt und Informationsaustausch.
Interesse? Dann schreiben Sie uns eine E-Mail an kongressorganisation@comconsult-akademie.de

Alcatel·Lucent Enterprise · AVAYA · avodaq · ComConsult BERATUNG + PLANUNG · ComConsult Research · ComConsult Study.tv

controlware communicationssysteme · EFFEXX · estos enables easy communication · innovaphone PURE IP-COMMUNICATIONS · UNIFY² Unified Communications, Accelerated

Programmübersicht ComConsult UC-Forum 2017

Montag 20.11.2017 - UCC auf dem Weg in die Cloud

9:30 Uhr
Keynote
- Cloud und nochmals Cloud
- Die ISDN Abschaltung ist da

Markus Geller, ComConsult Research GmbH

10:00 Uhr
NGN Und Cloud - UC aus dem Mobilfunknetz
Markus Emde, ComConsult Beratung und Planung GmbH

10:45 Uhr
Cloud Collaboration und die Integration von Web- und Videokonferenzen - UC aus dem Mobilfunknetz
- Cloud Lösungen und die Möglichkeiten der 3rd Party Integration
- Netzwerk und Sicherheit
- Mezzanine Produkt Suite

Thomas Brüning, Oblong Industries

11:15 Uhr Kaffeepause

11:45 Uhr
Herausforderungen Fehlersuche und Problemlösung bei Sprache, Video und Bildschirmübertragungen
- Customer Experience Management bei Echtzeitkommunikation von Sprache und Video in Cloud- und Hybridumgebungen
- Assesment/ Testing/ Assessor

Andreas Wächter, Integrated Research Germany GmbH

12:30 Uhr
Ein Client für Contact Center und andere Fälle
- Suitepad bzw. Macnetix im Hotelumfeld
- ASCOM myco 2 • TUI Meinschiff App • Contact Center Frontends
- Integrationsmöglichkeiten mit Collaboration-Lösungen

Lars Dietrichkeit, innovaphone AG

13:00 Uhr Mittagspause

14:30 Uhr
Der Client der Zukunft – Update 2018
- Cisco Spark • Avaya Zang/Equinox
- Unify Circuit • Alcatel Rainbow
- Microsoft Office 365 • Innovaphone

Markus Geller, ComConsult Research GmbH

15:15 Uhr
Cloud Collaboration und Integration von Konferenzen und Drittlösungen
- Lösungen für Cloud Collaboration
- Architektur für Unternehmen und Netzbetreiber
- Mobility, Telefonie, Konferenzen, Video und persistente „social collaboration“ • Contact Center, CRM und Groupware Integration • Global verfügbare Cloud Services als Alternative zum eigenen Betrieb

Dipl.-Ing. Stefan Patzelt, DeTeWe Communications GmbH

15:45 Uhr Kaffeepause

16:15 Uhr
Where Everthing Connects (CPaaS)
- Von der Infrastruktur agnostischen Integration von Geschäftsprozessen in Plattformen bis zur Einbindung von kundenspezifische Applikationen • Welche Technologie macht dies möglich?
- Kannibalisieren wir uns selbst?

Rene Princz-Schelter, ALE Deutschland GmbH

16:45 Uhr
DSGVO – Was passiert im Mai 2018
- Die neue EU- Datenschutz Grundverordnung im Überblick
- Was ändert sich für die Unternehmen?

Ulrich Emmert, esb Rechtsanwälte

ab 18:00 Uhr Happy Hour

Dienstag 21.11.2017 - Cloud ist nicht alles. Was sonst noch wichtig ist!

9:00 Uhr
Assessment von Microsoft Office 365 - Anforderungen und Konsequenzen für die IT
- Grundlagen: Lizenzmodelle, Anbindung an die Microsoft Cloud, Integration des Active Directory
- Anforderungen an die Netzinfrastruktur: WAN-Anbindung, Tools zur Überprüfung der Netzqualität, Netzdesigns zur Anbindung von Niederlassungen, Tuning Möglichkeiten
- Erfahrungen aus Kundenprojekten

Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH

10:00 Uhr
Datenschutz, Datensicherheit und Datenhoheit bei Cloud Collaboration Tools
- Intro: EU DS-GVO/GDPR und die Auswirkung auf Real Time Chat Communication Plattformen in der Cloud
- Lösungen am Markt & Cisco Spark Feature Übersicht
- Cisco Spark Hybrid Data Security – eine technische Lösung auf eine juristische Frage? • Key Federation im Detail – für sichere Zusammenarbeit zwischen Firmen • Ein vorläufiges Fazit

Sebastian Bonk, avodaq AG

10:45 Uhr Kaffeepause

11:15 Uhr
Secure productive Enterprise - So sieht moderne Zusammenarbeit heute aus – einfach, offen, sicher, mobil!
- Was für Anforderungen stellt die moderne Arbeitswelt an Unternehmen und Arbeitnehmer?
- Modernes Arbeiten mit der Microsoft Plattform inklusive Live Demonstration
- Datenschutz und Datensicherheit gewährleisten – Security im Kontext Zusammenarbeit und wie Microsoft Technologie Ihrem Unternehmen hilft GDPR konform zu werden

Dipl. Betriebsw. Jörg Petter, Microsoft Deutschland GmbH

11:45 Uhr
Cisco vs. Microsoft – Was leisten die UC-Portfolios der beiden Hersteller?
- Typische Ausgangssituationen und Zielszenarien
- Vergleich und Bewertung der UCC-Lösungsportfolios
- Welche Use-Cases werden durch die Hersteller adressiert?
- Was ist jeweils das bessere Deployment-Szenario?

Dipl.-Ing. Dominik Zöller, utilitas GmbH

12:30 Uhr Mittagspause

14:00 Uhr
Realisierung von SIP Trunking in der Projektpraxis
- Projekt-Rahmen • Standardisierung: SIPConnect, ETSI TISPAN, ATIS NNI
- Betrachtete Provider • Realisierungs-Varianten
- Evaluierte Kritierien • Kosten • Bewertungs-Ergebnisse

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

15:00 Uhr
Avaya BREEZE - Kommunikation und Zusammenarbeit im digitalen Zeitalter mit Fallbeispielen aus der Praxis
- Breeze als Beschleuniger für smarte digitale Lösungen für die Automatisierung • Turnkey und maßgeschneiderte Nutzererfahrung

Thomas, Römer, Avaya Deutschland GmbH

15:30 Uhr Kaffeepause

16:00 Uhr
Collaboration mit WebRTC (Live Chat)
- Kundenbeispiel Sparkasse Niederrhein
- Geschäftsstellen im ländlichen Bereich
- TextChat / VideoChat

Raphael Bossek, estos GmbH
Mario Wellmanns, Sparkasse am Niederrhein

16:30 Uhr
UCC und IPv6: Neues Protokoll, neue Probleme?
- Was ändert sich mit IPv6?
- Welche Tücken gibt es bei Endgeräten und Software?
- Wie verhindert man Blackholes, in denen UCC-Pakete verschwinden?
- Wie migriert man unternehmensintern sanft von IPv4 nach IPv6?

Markus Schaub, ComConsult Study.tv

Programmübersicht ComConsult UC-Forum 2017

Mittwoch 22.11.2017 - Abschaltung ISDN 2018

9:00 Uhr
Sonderanschaltungen in der Praxis
- Empfehlungen für
  - BMA, EMA, ÜMA • POS
  - Gebäudeleitechnik (Aufzugnotruf)
- VdS Empfehlungen

Markus Emde, ComConsult Beratung und Planung GmbH

9:45 Uhr
All-IP aus Carrier- und Kundensicht
- Neues Carriernetz und neue Services – was ändert sich?
- Neue Chancen für das Design von Sprach- und Datennetzen
- Praxistipps und Projekterfahrungen

Dipl.-Ing. Wilfried Meer, T-Systems International GmbH

10:30 Uhr Kaffeepause

11:00 Uhr
Notruf in Unternehmensnetzen
- AKNN Empfehlung für Provider (Notruf; Leistungsmerkmale)
- TR Notruf 2.0

Dipl.-Ing. Markus Bornheim, Avaya Deutschland GmbH

11:45 Uhr
Private Cloud IP-Telefonie Lösung mit ISDN und SIP Trunk Einbindung
- Warum Session Border Controller (SBCs)?
- ISDN-Backup mit „Trigger“ u. SIP-Trunks
- Herausforderungen bei der Implementierung
- Entwicklungsstrategie All IP

Dipl.-Ing. Rolf Nagelfeld, Techniker Krankenkasse

12:30 Uhr Mittagspause

14:00 Uhr
Migration zu SIP Trunking
- ISDN über SIP – die Evolution von reinem SIP-Trunking

N.N., Colt Technology Services GmbH

14:45 Uhr
SBC Design
- Anschaltung
- Designbeispiele
- Funktionen

Markus Emde, ComConsult Beratung und Planung GmbH

15:15 Uhr Kaffeepause

15:45 Uhr
Fax Ablösung
- T.30 Standard (Was ist T.38; Alternative T.37)
- Rechtssichere Alternativen (Zertifikatsbasierte Lösungen)

Markus Geller, ComConsult Research GmbH
Dr. Rolf Fiedler, Ferrari electronic AG

Der Veranstalter behält sich Änderungen im Programm vor

Die Referenten


Dipl.-Inform. Petra Borowka-Gatzweiler


Raffael Bossek


Dipl.-Ing. Markus Bornheim


Thomas Brüning


Lars Dietrichkeit


Markus Emde


Ulrich Emmert


Dr. Rolf Fiedler


Markus Geller


Dipl.-Math. Cornelius Höchel-Winter


Dipl.-Ing. Wilfried Meer


Dipl.-Ing. Rolf Nagelfeld


Dipl.-Ing. Stefan Patzelt


Dipl.-Betriebw. Jörg Petter


Rene Princz-Scheter


Thomas Römer


Markus Schaub


Andreas Wächter


Mario Wellmanns


Dipl.-Ing. Dominik Zöller

Anmeldung an kundenservice@comconsult-research.de

ComConsult UC-Forum 2017

Ich buche den Kongress
ComConsult UC-Forum 2017

☐ vom 20.11. - 22.11.17 in Königswinter zum Preis von 2.190,-- € netto*

*Frühbucherpreis gültig bis zum 15.09.17 dann regulärer Preis 2.390,-- € netto

☐ Bitte buchen Sie mir ein Hotelzimmer

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Aktueller Kongress

ComConsult Technologie-Tage 2017

06.11. - 07.11.2017 in Düsseldorf

Die ComConsult Akademie veranstaltet vom 06.11. bis 07.11.2017 ihren Kongress "ComConsult Technologie-Tage 2017" in Düsseldorf.

Die ComConsult Technologie-Tage 2017 wenden sich an Entscheider in Unternehmen und analysieren die Herausforderungen, denen sich IT-Infrastrukturen in den nächsten Jahren stellen müssen. Top-Experten der Branche beleuchten die Markt- und Technologie-Situation der nächsten Jahre und geben Empfehlungen für ein zukunftsorientiertes und sicheres IT-Fundament. Dieser Kongress evaluiert, welche Technologie-Bausteine aus welchen Bereichen im Moment wichtig sind und für die Planung und den Betrieb bekannt sein sollten.

Strategien für sichere Investitionen in IT-Infrastrukturen und Architekturen
Würde man heute ein Rechenzentrum oder ein Gebäude komplett neu ausstatten oder bauen, würde es sich deutlich von der Situation vor 5 Jahren unterscheiden. Skalierbarkeit und Wirtschaftlichkeit führen zu deutlich veränderten Schwerpunkten: der Wunsch, bestehende Kapazitäten schnell und preiswert in kürzester Zeit anpassen zu können, erfordert geeignete Architekturen über Technologie-Grenzen hinweg. Die Abgrenzung zur Cloud ist dabei ebenso eine treibende Kraft wie eine Chance. Zum einen haben Cloud-Rechenzentren Technologien und Architekturen marktreif und allgemein nutzbar gemacht, die es so vorher nicht gab. Zum anderen wird eine teilweise Integration von Cloud-Leistungen für die meisten Betreiber auf 5 Jahre gesehen unvermeidbar sein. Die Schlüsselfrage ist:

wie können Zukunfts-sichere Architekturen entwickelt werden, auf deren Basis mit hoher Sicherheit und Wirtschaftlichkeit investiert werden kann?

Fundamente im Technologie-Mix 2020
Die unvermeidbare Anpassung der IT-Architekturen positioniert die Basis-Technologien für Rechenzentren und das Gebäude der Zukunft neu. Zum einen gibt es Schwerpunktverlagerungen in Richtung Funk-Technologien, zum anderen erfordern moderne RZ-Architekturen eine Trennung von Netzwerk-Basis (Underlay) und Netzwerk-Nutzung (Overlay). In Summe führt dies zu einer veränderten Technologie-Auswahl für die nächsten Jahre. Gleichzeitig wird immer deutlicher, dass die Cloud als Leistungs-Baustein in einem Gesamtkonzept nicht fehlen darf. Cloud-Lösungen werden immer weniger als Gefahr für die Unternehmens-IT gesehen und bekommen immer mehr den Charakter von extrem wichtigen Ergänzungs-Bausteinen zu einem wirtschaftlichen und flexiblen Gesamtbild. Als Ergänzung müssen sie aber sauber in die bestehende Landschaft integriert werden. Dies erfordert angemessene und wohl überlegte Technologie-Entscheidungen nicht nur auf der Seite der Cloud.

Sicherheits-Strategie 2020
Das Kernproblem aller Sicherheits-Lösungen ist die schnelle Anpassung an einen veränderten Bedarf. Skalierbarkeit im Technologie-Mix wird parallel zu einer Herausforderung für Sicherheit. Sowohl die Gefahren als auch die Lasten verändern sich in so hohen Geschwindigkeiten, dass eine statische Sicherheits-Lösung auf Dauer nicht den erforderlichen Grad an Sicherheit liefern wird. Auch im Sicherheits-Bereich brauchen wir ebenfalls eine erhebliche Skalierbarkeit, die im Rahmen eines Gesamtkonzepts flexibel mit dem Bedarf wachsen kann. Dabei spielen juristische Compliance-Fragen eine immer größere Rolle. Die bekannten Ransomware-Angriffe haben nachdrücklich gezeigt, dass sowohl eine geeignete technische als auch eine den juristischen Normen entsprechende Compliance-Lösung gefordert ist. In Kombination mit der Integration der Cloud und der Komplexität, die aus Entwicklungen wie Smart-Buildings entsteht, muss Sicherheit einmal wieder neu positioniert werden.

Hier setzen die ComConsult Technologie-Tage 2017 an: wir analysieren, wie Unternehmen und Behörden erfolgreich diese Herausforderungen bestehen können. Wir evaluieren, wie ein zukunftssicheres Technologie-Fundament aussehen kann.

Anmeldung an kundenservice@comconsult-research.de

ComConsult Technologie-Tage 2017

Ich buche den Kongress
ComConsult Technologie-Tage 2017

☐ 06.11. - 07.11.2017 in Düsseldorf
zum Preis von 1.990,-- € netto

☐ Bitte buchen Sie mir ein Hotelzimmer

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

Programmübersicht ComConsult Technologie-Tage

Montag 06.11.17
Infrastruktur-Architekturen der Zukunft

9:30 Uhr
Keynote: Security by Design – Informationssicherheit als integraler Bestandteil der IT
- Cyber-Angriffe: Bedrohungen und mögliche Sicherheitsmaßnahmen
- Konsequenzen von Virtualisierung, SDN, SDDC, HCI, Container und Co. auf die Informationssicherheit
- Informationssicherheit in und aus der Cloud
- Smart Building, Smart Home, Smart Vehicle, Smart Factory, Smart …: Warum die Sicherheit hier an Grenzen stößt?
- Umdenken ist erforderlich: Notwendigkeit von Security by Design

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:30 Uhr
IT-Infrastrukturen im Gebäude der Zukunft: Bedarf, Potenziale und Gefahren
- Das Smart Building und die Auswirkung auf Infrastrukturen
- Beacon Technologien im Gebäude der Zukunft
- Das neue Gewerk IT-Security als Teil des Smart Buildings
- Vor- und Nachteil von Cloud-Diensten für Sensortechnik und BIM

Dipl.-Inform. Thomas Steil, ComConsult Beratung und Planung GmbH

11:15 Uhr Kaffeepause

11:45 Uhr
Azure kontra AWS: wer hat die bessere Cloud?
- Wie unterscheiden sich die Netzkomponenten und Designansätze von Microsoft und Amazon?
- Worauf ist bei der Auswahl der richtigen Cloud-Lösung zu achten?
- Kann man die Preise beider Anbieter miteinander vergleichen?
- Welche nativen Sicherheitsmechanismen bieten die Cloudprovider?
- Welche Verbindungsvarianten für Hybrid-Cloud-Lösungen existieren?

Markus Schaub, ComConsult Study.tv

12:30 Uhr Mittagspause

14:00 Uhr
High Performance Computing auf dem Weg zur unverzichtbaren Normalität für alle
- Technologiebausteine
- Anwendungen
- Planung

Dr. Markus Ermes, ComConsult Beratung und Planung GmbH

14:45 Uhr
Microsoft Office 365: Erfolgreiche Nutzung und Anforderungen an IT-Infrastrukturen
- Grundlagenentscheidungen: Nutzung der Office-365-Suite: Wer – Was – Wie; Lizenzmodelle; Anbindung an die Microsoft Cloud: Single Tenant vs. Multiple Tenants; Integration des Active Directory; Single Sign On
- Anforderungen an die IT-Infrastruktur: WAN-Anbindung: Bandbreite, Laufzeit, Übertragungsqualität; Tools zur Überprüfung der Netzqualität; Netzdesigns zur Anbindung von Niederlassungen; User Experience; Tuning Möglichkeiten
- Erfahrungen auf Kundenprojekten

Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH

15:30 Uhr Kaffepause

16:00 Uhr
Sicherer und effizienter Einsatz von IOS im Unternehmen, was ändert sich durch iOS11?
- DEP, VPP, MDM
- Anwender-Features mit Produktivitäts-Potential
- Fallstricke der neuen iOS11-Version
- Was wird besser mit iOS11

Mark Zimmermann, Freier Experte

16:45 Uhr
Cybersecurity: aktuelle Rechtsfragen
- Datenschutzgrundverordnung - radikale Verschärfung des Datenschutzes
- Aktuelle Entwicklungen im Bereich der betrieblichen IT-Sicherheit
- Haftung der Unternehmensleitung bei Verstößen gegen die Informationssicherheit
- Eckpunkte einer Absicherung nur Umsetzung von IT/Compliance

Dr. Jan Byok, Bird & Bird LLP

Der Veranstalter behält sich Änderungen im Programm vor

Dienstag 07.11.17
Technologien der Zukunft

9:00 Uhr
Overlays im Campus-Netz
- Kommt das Overlay nun auch ins Campus-Netz?
- Grundsätzlichen Design-Annahmen und -Ideen für den Einsatz von Overlay-Strukturen?
- Beispielbetrachtung: Campus Fabric, SPBm und weitere

Dr. Johannes Dams, ComConsult Beratung und Planung GmbH

9:45 Uhr
Software Defined Storage: Wird das traditionelle SAN überflüssig?
- Technologieübersicht - Virtualisierung bestehender Speichersysteme vs. Software Defined
- Storage Plattform auf Basis von Direct Attached Storage
- Skalierbarkeit, Management und Leistungsgrenzen
- Anwendungsszenarien

Dr. Stefan Muthmann, ComConsult Beratung und Planung GmbH

10:30 Uhr Kaffeepause

11:00 Uhr
Das Fax ist tot, aber was tritt an seine Stelle?
- Modemtechnologie in Zeiten von IP: T.30 G.711 inband Übertragung; T.37 asymmetrisches Verfahren über IP; T.38 symmetrisch Variante über IP
- Aufbau einer T.30 und einer T.38 Übertragung: Wo liegen die Probleme? (Endgerätesituation; Gateways; Was machen die SIP-Trunk / VoIP-Provider?)
- Alternative Verfahren: Was ist EDI?; Was sind digitale Signaturen? (Software Anbieter im Vergleich); Vorteile und Verfahren

Markus Geller, ComConsult Research GmbH

11:45 Uhr
WLAN, Mobilfunk und andere Funktechniken - gegenseitige Ergänzung oder Störfaktor?
- Die Grenzen des WLAN und neue Ideen zu deren Überwindung
- WLAN Offload und Konsequenzen für Betreiber
- Muss man Funkdienste gegeneinander abschirmen?
- Freiheit von Störungen sicherstellen: Funkfrequenzkataster
- Gesundheitsrisiko Funk? Muss man am Ende den Menschen abschirmen?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:30 Uhr Mittagspause

14:00 Uhr
5G: Basis für Mobilität, Disruption und Agilität
- Anforderungen moderner Anwendungsbereiche z.B. AR, VR, IoT, autonomes Fahren
- Entwicklung der Mobilfunktechnologie von LTE über LTE Advanced zu 5G
- Neue Konzepte für Small Cells, mögliche Konflikte zu WLANs, Fog Computing
- Ergebnisse aus den Feldversuchen von AT&T, Verizon, Nokia, CCI und anderen
- Die Standardisierung beginnt 2018. Was bringt die erste Welle?

Dr. Franz-Joachim Kauffels, Technologie-Analyst

14:45 Uhr
Sind die Tage der Netzneutralität gezählt?
- Was ist Netzneutralität?
- Sind die Tage der Netzneutralität gezählt?
- Auswirkungen auf Verbraucher
- Auswirkungen auf Unternehmen
- Funktioniert die Priorisierung?

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

15:30 Uhr
Herausforderung Informationssicherheit für das Gebäude der Zukunft
- Schadsoftware, Krypto-Trojaner, zielgerichtete Angriffe, Desinformation und (Distributed) Denial of Service: Bedrohungen der IT im Gebäude der Zukunft
- Welche Informationssicherheitsstandards sind für Smart Buildings relevant?
- Absicherungen von Smart Buildings mit IEC 62443
- Zonenkonzepte, mandantenfähige Infrastrukturen und Netzzugangskontrolle: Brauchen wir das wirklich?
- Absicherung von Funknetzen, Anbindung von Smartphones und Tablets: Alles wie gehabt?
- Wo sich Internetanbindung und DMZs im Smart Building vom Rest der Welt unterscheiden
- Ohne Cloud kein Smart Building: Sichere Cloud-Dienste und sichere Cloud-Nutzung für Nutzer und Betreiber
- Security by Design: Standardisierte Bausteine als Basis

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Schwerpunktthema

Overlays in der Analyse

Teil 1: EVPN vs. SPBM

Fortsetzung von Seite 1

Dipl. Math. Cornelius Höchel-Winter ist Leiter des Technologie-Labors und des Bereichs Systemintegration bei der ComConsult Research GmbH. In dem Labor werden regelmäßig Messungen und Evaluierungen neuester Hard- und Softwareprodukte durchgeführt und ausgewertet. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von RZ- und Campusnetzen und von Windows- und Linux-Umgebungen. So hat er als verantwortlicher Projektmanager die Rechenzentren und Netzwerke auf dem Gelände der EXPO2000 in Hannover aufgebaut und während der Weltausstellung betrieben. Für die ComConsult Akademie ist er außerdem seit 2001 als Autor, Trainer und Referent auf Seminaren und Kongressen schwerpunktmäßig in den Bereichen Data Center, Virtualisierung, Storage, Netzwerke und Cloud Computing tätig.

Jede Entwicklung im und um das Rechenzentrum wird derzeit getrieben von dem Anspruch, zumindest große Teile der Konfiguration von Lösungen und bereitgestellter Ressourcen automatisieren zu können. Dies gilt auch und gerade in virtualisierten Umgebungen. Zero-Touch- oder One-Stop-Provisioning lauten hier die Schlagworte.

Die Kernanforderungen lauten also: automatisierte Bereitstellung, flexible Konfiguration, geringer Administrationsaufwand, effizienter Betrieb, Fokussierung auf die Anwendungen.

Für den Netzwerkbereich haben sich hierzu zwei Technologiebereiche entwickelt: Switch-Fabrics und Overlays. Overlays trennen das Netzwerk in ein physisches Transportnetz und verschiedene logische Anwendungsnetze – oder je nach Sichtweise in ein (physisches) Providernetz und virtuelle Kundennetze (VPNs – Virtual Private Networks). Overlays adressieren also eher die Punkte Flexibilität und Effizienz bei der Bereitstellung und dem Betrieb von Anwendungen, während bei Fabrics das Underlay, das physische Transportnetz, im Vordergrund steht, verbunden mit der Fähigkeit hohen Durchsatz bei möglichst geringem Delay zur Verfügung zu stellen.

Im Folgenden werden zunächst die grundlegenden Konzepte und Bausteine von Overlay-Technologien betrachtet:

- Was bedeutet der Begriff „Overlay“, aus welchen Bausteinen setzt sich eine Lösung zusammen?
- Wieso setzen moderne Netzdesigns auf Overlay-Strukturen?
- Was leisten Overlays in Enterprise-Umgebungen?
- Wie werden die beiden Netzbereiche Overlay und Underlay gesteuert?

Konzepte und Bausteine

Der Begriff Overlay bezeichnet eine Netzwerkschicht, die über eine Abstraktionsebene von der darunterliegenden Schicht (die dann mitunter als Underlay bezeichnet wird) getrennt ist. „Overlays“ sind also eng mit „Virtualisierung“ verbunden, beide Begriff beschreiben vergleichbar Konzepte. Die technische Realisierung des Transports von Overlay-Strukturen durch das Netzwerk erfolgt dann durch Tunnelprotokolle.

Daher werden je nach Sichtweise und Standpunkt die Begriffe Overlay, Netzwerkvirtualisierung, VPN (Virtual Private Network) und Tunnelprotokoll gerne gleichbedeutend für dieselbe Technologie verwendet. Trotzdem sollte man dies alles nicht unreflektiert in einen Topf werfen.

Overlays im obigen Sinn sind jetzt wirklich Neues. Es gibt wenigstens zwei weitverbreitete Overlay-Technologien, die den meisten Lesern bekannt sein werden:

1. MPLS (Multiprotocol Label Switching):
   MPLS wird genutzt, um räumlich getrennte, meist IP- oder Ethernet-basierende Netzbereiche über große, internationale Transportnetze miteinander zu verbinden.

2. VLANs (Virtual LANs):
   VLANs werden genutzt, um Layer-2-Domänen in kleinere, voneinander unabhängige Netze zu segmentieren.

Schon anhand dieser beiden Beispiele können zwei wesentliche Funktionsmerkmale von Overlay-Lösungen festgehalten werden:

1. Angebundene Netzsegmente, die zusammengehören, werden transparent miteinander verbunden.

2. Netzsegmente, die zu verschiedenen Kunden oder Sicherheitszonen etc. gehören, müssen jedoch sicher voneinander getrennt werden, ohne dass Kunde

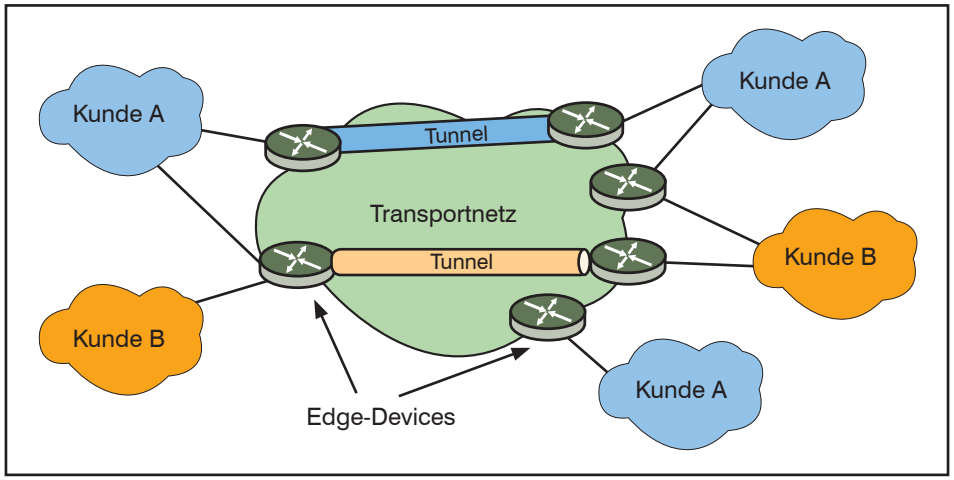


Abbildung 1: Bausteine einer Overlay-Lösung

A Verkehrsströme von Kunde B sehen oder beeinflussen kann. (siehe Abbildungen 1 und 2)

Eine technische Gesamtlösung, die Overlays zur Verfügung stellt, besteht also mindestens aus folgenden Bausteinen:

- einem physischen Transportnetz und
- mehreren daran angebundenen Kundensegmente (das können Einzelsysteme oder Teilnetze sein), die zu einem oder mehreren Kunden (Benutzergruppen, Services, Sicherheitszonen etc.) gehören,
- einem Tunnelprotokoll und
- Steuerungsebenen (Control Layer) für Overlay und Underlay.

Darüber hinaus ist gerade in Unternehmensrechenzentren in der Regel auch eine Virtualisierungsplattform mit Hypervisor und Management-Software integriert bzw. involviert.

Diese Bausteine und ihre Funktionsweisen werden im Weiteren genauer dargestellt.

Wie und warum werden Overlays überhaupt eingesetzt?

Für Unternehmensnetze können wir von folgender allgemeiner Situation ausgehen:

1. Es besteht ein verbreiteter Bedarf das Gesamtnetz in unabhängige Teilnetze zu unterteilen, in der Regel geschieht dies durch VLANs. Die Gründe hierfür sind vielfältig und reichen von der Notwendigkeit, die Broadcast-Last und der Größe von Fehlerdomänen zu beschränken, bis zu dem Wunsch, Benutzergruppen, Dienste, Anwendungen, Sicherheitsbereiche etc. unabhängig voneinander administrieren und steuern zu können.

2. Um trotzdem Kommunikationsbeziehungen auch zwischen diesen Teilnetzen zulassen zu können, werden hierauf Layer-3-Strukturen abgebildet und diese IP-Subnetze über Routing-Instanzen wieder miteinander verbunden.

3. Im Rechenzentrum sind Virtualisierungslösungen insbesondere für Compute- und Storage-Ressourcen im Einsatz. Der effektive Betrieb dieser Lösungen erfordert es, dass speziell virtuelle Server flexibel und dynamisch auf Virtualisierungshosts platziert und bei Bedarf verschoben werden können – letzteres auch während des aktiven Betriebs. Soll dies unterbrechungsfrei aus Sicht der Anwendung geschehen, darf sich bei den meisten der derzeit genutzten Anwendungen die IP-Adresse nicht ändern.

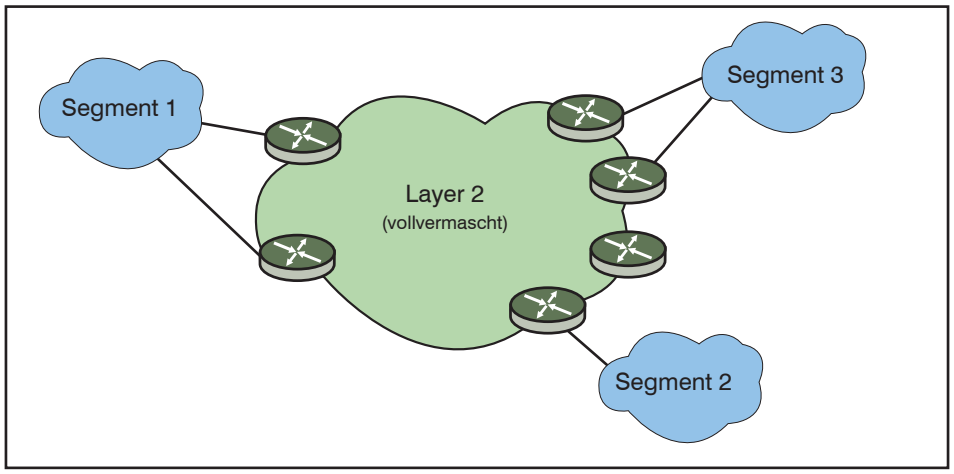


Abbildung 2: Overlay-Struktur mit Layer-2-Service aus der Sicht von Kunde A

4. Im Rechenzentrum werden IP-Subnetze meist nach räumlichen Kriterien verteilt, also pro Rack oder pro Rackzeile ein Subnetz. Das ist natürlich für eine flexible Verteilung virtueller Maschinen und die dynamische Bereitstellung von Anwendungen äußerst ungünstig.

5. Georedundante Rechenzentren werden im WAN in der Regel über unterschiedliche IP-Adressbereiche erreicht. Wie eben erwähnt, widerspricht dies der flexiblen Verteilung virtueller Maschinen und ihrer Anwendungen, aber auch einer schnellen Bereitstellung zustätzlicher Ressourcen.

Damit ergeben sich typische Einsatzszenarien für Overlay-Lösungen:

A) Virtuelle Anwendungsnetze:

In oder direkt hinter den Virtualisierungshosts (zum Beispiel im Top-of-Rack-Switch) werden Overlay-Netze aufgesetzt, die die virtuellen Maschinen, die gerade auf diesem Host oder diesem Rack platziert sind, mit ihren jeweiligen Layer-2-Domänen transparent verbinden. Damit können virtuelle Maschinen und Anwendungen unabhängig von einem speziellen Virtualisierungshost oder Server-Rack irgendwo im Rechenzentrum platziert und verschoben werden. Letzteres wird auch gerne mit dem Begriff „MAC Mobility“ bezeichnet. (siehe Abbildung 3)

B) RZ-Kopplung:

Georedundante Rechenzentren werden über Providernetze miteinander verbunden. Hierbei stellt in der Regel der Provider die Overlay-Technologie (nach wie vor meist MPLS). Für den Kunden ist es nur wichtig zu entscheiden, ob (aus seiner Sichtweise, also innerhalb der Tunnel) die Rechenzentren über Layer 2 oder Layer 3 verbunden werden sollen. Der erste Fall ist sicherlich einfacher und flexibler gerade für RZ-interne Kommunikationsbeziehungen, im zweiten Fall erscheint das gesamte Providernetz wie ein einziger Router, der die beiden Rechenzentren über IP verbindet.

C) Overlays zur Nutzung flexibler Netzwerkdesigns:

Das entscheidende Hemmnis zur Nutzung flexibler Designs wie Maschen, Ringe, Spine-Leaf und gegebenenfalls von Lastausgleich über parallele Wege (Equal Cost Multipathing - ECMP) ist der Spanning Tree bzw. die Unfähigkeit von Ethernet Schleifen zu verhindern. Klassischerweise wird dieses Manko durch ein Layer-3-Design und die Nutzung von Routingprotokollen wie OSPF (die ECMP unterstützen) überwunden. Solche Lösungen sind ohne zusätzlichen Automatisierungslayer jedoch administrativ sehr aufwändig und daher nur für kleine Netzbereiche (z. B. Übergang Core – Backbone) sinnvoll.

Wie oben erwähnt, haben Overlays aber nicht nur die Fähigkeit zu verbinden, sondern auch zu trennen. Daher werden einige Lösungen wie beispielsweise SPB auch dazu genutzt, um die Funktionalität klassischer VLANs einfach nur zu erweitern und Beschränkungen, die Layer-2-Netze mit sich bringen, aus dem Weg zu räumen. Hierzu gehören:

- die gegebenenfalls zu geringe Anzahl von maximal gut 4.000 VLANs,
- die Notwendigkeit, für jedes VLAN ein eigenes virtuelles Interface anlegen zu müssen,

Overlays in der Analyse - Teil 1: EVPN vs. SPBM

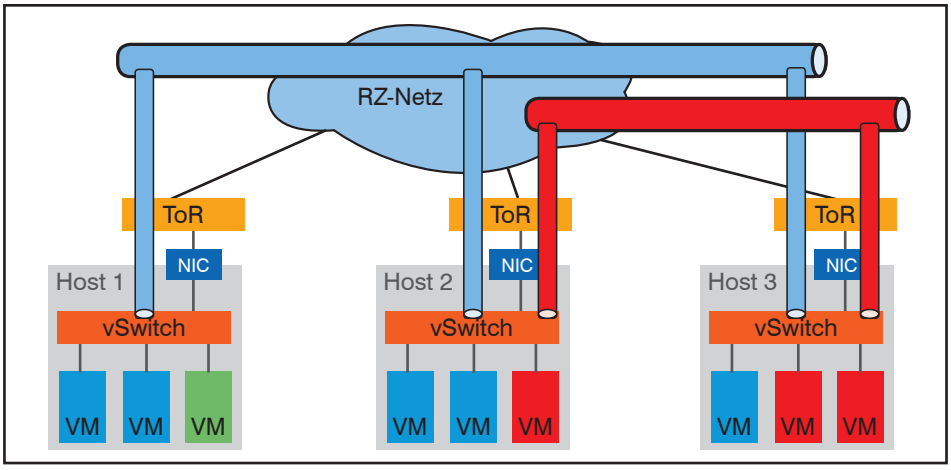


Abbildung 3: Tunnellösung im Hypervisor

- die Beschränkung auf eine einzige Baumstruktur (Spanning Tree).

Kommen wir zu den Bausteinen einer Gesamtlösung.

Transport-Edge (Provider-Edge)

Die für das Gesamtkonzept wichtigsten und auch technisch aufwändigsten Komponenten sind offensichtlich die Systeme, die den Rand des Transportnetzwerks bilden:

- Sie sind mit zwei Welten verbunden sind, dem Transportnetz und den angebundenen Anwendungs- bzw. Kundennetzen (siehe Abbildung 4), die sich unter Umständen sogar in der Zugangstechnologie voneinander unterscheiden.
- Sie müssen die Topologien und Netzwerktechnologien auf beiden Seiten unterstützen, das heißt sie müssen auf beiden Seiten Frames empfangen und senden können.
- Hier werden die Tunnel bzw. die Overlays aufgesetzt, um die auf der Kundenseite empfangenen Frames durch das Transportnetz zu leiten.
- Hier werden die Tunnel auch terminiert und die ausgepackten Inhalte an die richtigen Empfänger weitergeleitet.
- Hier stoßen Underlay und Overlay aufeinander! Das heißt, sollen Informationen aus dem Overlay (wie beispielsweise QoS-Tags) auf das Underlay übertragen werden, dann hier.

Abbildung 4 zeigt den generischen Aufbau eines Edge-Systems.

Die Verbindung zwischen Kundennetz und Transportnetz erfolgt über eine Abstraktions- und Steuerungsschicht sowie ein Overlay-Modul. Letzteres bildet den Tunnelendpunkt und ist für das Einpacken und Entpacken der Verkehrsflüsse in ein geeignetes Tunnelprotokoll zuständig, während auf der Abstraktions- und Steuerungsschicht (gerne auch als *Virtualisierungsschicht* bezeichnet) alle Funktionen implementiert sind, die einerseits unterschiedliche Kundennetze voneinander trennen und andererseits räumlich getrennte Netzsegmente, die zum selben Overlay gehören, miteinander verbinden. Hierzu gehören insbesondere die Wegewahl und Informationen über die Erreichbarkeit entfernter Endgeräte.

Diese Edge-Systeme werden im Allgemeinen als „Provider Edge“ gezeichnet, weil gerade bei Provider-Produkten die gesamte Technologie des Transportnetzes inklusive der Tunnelendpunkte meist im Netzwerk des Providers installiert ist. Das muss aber nicht zwingend so sein. Gerade bei Layer-2-VPNs zum Beispiel mit VXLAN kann es günstiger sein, die IP-Tunnel auf der Kundenseite aufzubauen und beim Provider ein einfacheres Layer-3-Produkt einzukaufen.

Wir bleiben daher im Folgenden bei der neutralen Bezeichnung Edge. Die zusätzliche Betrachtung eines „Customer Edge“ als letztes reguläres System im Kundennetz macht aus konzeptioneller Sicht eh keinen Sinn.

Ein solches Edge-System kann sowohl als Teil eines virtuellen Switches innerhalb eines Hypervisors als auch innerhalb eines physischen Switchs oder Routers oder auch in einer separaten Netzwerk-Appliance (Tunnel-Gateway) implementiert sein.

Servicetypen

Typischerweise können über eine Overlay-Struktur zwei Arten von Netzwerkservices transportiert werden: Layer-2-Services und Layer-3-Services.

Ein Layer-2-Service verbindet Ethernet-basierende Netzsegmente entweder auf einer Punkt-zu-Multipunkt- oder Multipunkt-zu-Multipunkt-Topologie. Typische Beispiele für Layer-2-Services sind MPLS L2VPN, SPB (Shortest Path Bridging nach 802.1aq), VXLAN oder EVPN (Ethernet VPN). Das Overlay stellt dabei also ein kundenspezifisches Layer-2-Switching zwischen den angebundenen Segmenten zur Verfügung. Als Transporttechnologien kommen sowohl Ethernet, IP als auch MPLS zum Einsatz.

Ein Layer-3-Service stellt dagegen kundenspezifisch eine IP-Routing-Funktionalität zwischen den angebundenen IP-Subnetzen zur Verfügung. Das hat zur Folge, dass zwischen diesen Subnetzen Routing-Informationen ausgetauscht werden müssen, die auch auf den Edge-Devices (Tunnelendpunkten) zur Verfügung stehen müssen. Mit anderen Worten, die Edge-Devices sind in das übergreifende Routing der Kundennetze eingebunden. Insbesondere wenn die Edge-Device zum Providernetz gehören, ist das nicht immer gewünscht.

Im Underlay kommen hierbei bevorzugt Layer-3-Technologien wie MPLS oder IP zum Einsatz.

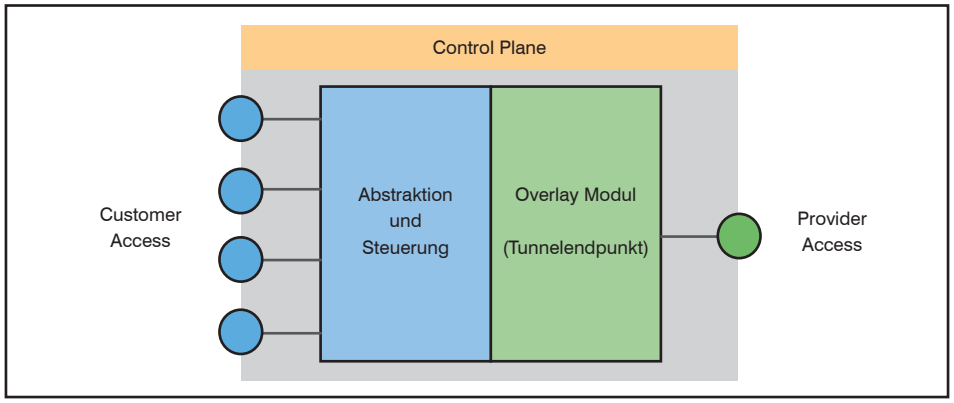


Abbildung 4: Generischer Aufbau eines Edge-Systems

Overlays in der Analyse - Teil 1: EVPN vs. SPBM

Tunnelprotokolle

Der Frame-Aufbau von Tunnelprotokollen folgt im Wesentlich folgendem Schema (siehe Abbildung 5):

- Vor den zu transportierenden Protokoll-Frame wird ein verfahrensspezifischer Tunnelheader gesetzt – mitunter wird auch das gesamte innere Protokoll in einen Tunnelrahmen eingebettet.
- Das so neu verpackte Paket wird dann um die standardmäßigen Header des jeweiligen Transportnetzes erweitert und entsprechend transportiert.

Als Tunnelprotokolle kommen sowohl spezifische Protokolle, die dediziert auf ein inneres Protokoll zugeschnittenen sind, als auch generische Protokolle, die unterschiedliche Kommunikationsprotokolle transportieren können, zum Einsatz.

Es gibt also jeweils einen äußeren Header, der für den Transport durch das Transportnetz zuständig ist, gefolgt von einem Tunnelheader und den inneren Header des transportierten Pakets. Tunnelprotokolle gibt es wie Sand am Meer, einige populäre Beispiele sehen Sie in Tabelle 1.

Für Overlay-Lösungen kommen natürlich nur Protokolle infrage, die Layer-2- oder Layer-3-Frames transportieren. Die beiden Storage-Protokolle sind lediglich mit aufgeführt, um das grundlegende Prinzip zu verdeutlichen.

Wesentliches Merkmal solcher Protokolle ist, dass sie Endgeräte oder Netzbereiche transparent miteinander über das jeweilige Transportnetzwerk verbinden. Transparent bedeutet hierbei, dass aus Sicht der angebundenen remote Systeme das Transportnetz als solches gar nicht existiert. Die angebundenen Netze, Systeme oder Dienste „wissen“ nicht, dass sie sich durch einen Tunnel bewegen / bewegt haben, das Transportnetz verhält sich wie ein großer Switch oder Router.

Dieser Punkt beschreibt das generelle Virtualisierungskonzept:

> Die in der virtuellen Welt bereitgestellten Ressourcen und Dienste funktionieren genauso wie in der physischen Welt. Dienste und Anwendungen müssen nicht an die konkrete Ausgestaltung des Transportnetzes oder des Tunnelprotokolls angepasst werden.

Die damit einhergehende logische Trennung in Overlay und Underlay hat zwei wichtige Konsequenzen:

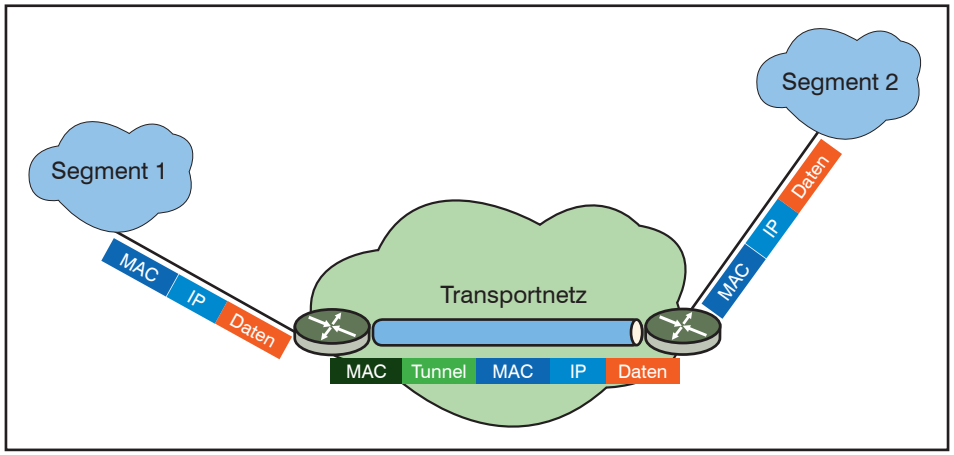


Abbildung 5: Tunnelframes

1. Struktur und Aufbau der virtuellen Overlay-Netze sind unabhängig von der Hardware und der Technologie des Underlays.

   Dies ist ein äußerst wichtiger Aspekt für den Aufbau flexibler Netzinfrastrukturen, für die schnelle, automatisierte Bereitstellung von Anwendungen – und natürlich für die nahtlose Integration von Cloud-Infrastrukturen, wo mir als Kunde die Technologie des Betreibers ja gegebenenfalls überhaupt nicht bekannt ist. Denn nur dank der durchgehenden Abstrahierung von allen physischen Ressourcen können virtuelle Overlays, inklusive deren virtuellen Workloads und Netzwerkdiensten in die Cloud verschoben und auch wieder zurückgeholt werden! Entscheidend hierfür ist die Virtualisierungsplattform, aber eben nicht die Hardware.

2. Umgekehrt ist aber auch das Underlays befreit von allen Spezialitäten der angebundenen Kunden- und Anwendungsnetze.

Die Weiterleitung innerhalb des Transportnetzes erfolgt ausschließlich anhand einfach auszuwertender Felder, die direkt im äußeren Transportheader stehen (wie MAC-Adresse, VLAN-ID, MPLS-Label). Aufwändige Lookups in tiefere Schichten des Pakets, insbesondere in den getunnelten kundenspezifischen Frame entfallen. Das macht die Weiterleitung schnell und den Betrieb einfach.

Darüber hinaus sind auch die Weiterleitungstabellen in den Geräten deutlich kleiner und damit schneller zu bearbeiten, da nur die Netzwerkadressen aus dem Transportnetz bekannt sind. Die gegebenenfalls deutlich umfangreichere Zahl an MAC- und IP-Adressen sowie VLAN-Tags ist für den Kern des Transportsnetzes transparent.

Umgangssprachlich heißt das, auch das Underlay muss nicht „wissen“, dass es Kundennetze in Tunnelprotokollen transportiert. Wiewohl dies nicht für die Tunnelendpunkte zutrifft, sondern nur für die

Verfahren	Äußerer Transportheader	Tunnelheader	Innerer Header
VLANs	MAC	**VLAN**	IP
MPLS L3VPN **)	Layer 2	**MPLS**	IP
MPLS L2VPN **)	Layer 2	**MPLS**	MAC
FCoE	MAC	**FCoE**	FC – SCSI
iSCSI	IP – TCP	**iSCSI**	SCSI
VXLAN	IP – UDP	**VXLAN**	MAC
PBB (802.1ah) *)	MAC	**PBB**	MAC
TRILL **)	MAC	**TRILL**	MAC
*) Wird von SPBM (IEEE 802.1aq) genutzt.			
**) Bei MPLS und TRILL erfolgt der Transport zusätzlich Hop-by-Hop anhand der Angaben im jeweiligen Tunnelheader.			

Tabelle 1: Tunnelprotokolle

Overlays in der Analyse - Teil 1: EVPN vs. SPBM

Switche im Kern des Transportnetzes – und auch diese könnten, wenn es das Verfahren erfordert, durch einen tieferen Lookup die Tunnel natürlich sehen.

3. Für Provider ist es sicherlich noch interessant, dass hiermit MAC-Adressen, IP-Adressen und VLAN-IDs kundenspezifisch bleiben und es bei Überschneidungen zu keinen Kollisionen kommt. In Unternehmensnetzen spielt dies eine eher untergeordnete Rolle, allenfalls die Möglichkeit, VLAN-IDs wiederzuverwenden, ist eine Option.

Der zwischen Transportheader und Header des transportierten Pakets eingeschobene Tunnelheader ist wesentlich dafür zuständig, dass in mandantenfähigen Designs Tunnel für unterschiedliche Kunden oder Services über dieselbe Infrastruktur transportiert und trotzdem sauber voneinander getrennt werden können. Hierfür muss im Tunnelheader der jeweilige Sicherheitskontext kodiert werden, damit am Tunnelende der entpackte Frame auch dem richtigen Kunden bzw. Netzsegment zugeordnet werden kann.

Zu diesem Zweck wird in der Regel eine netzwerkweit eindeutige Tunnel- oder Service-ID im Tunnelheader genutzt. Die Größe dieses Felds entscheidet darüber, wie viele Kontexte im Netz unterschieden werden können. Nachdem sich die 12 Bit große VLAN-ID schon in mittleren Umgebungen als zu klein herausgestellt hat, ist in den meisten neueren Tunnelprotokollen ein doppelt so großes ID-Feld vorgesehen. Damit können fast 17 Millionen virtuelle Netze unterschieden werden.

Abbildung 6 zeigt das Frameformat von PBB (Provider Backbone Bridges), dem Format, das von Shortest Path Bridging – MAC-Mode (SPBM) genutzt wird. Die Tunnel-ID heißt hier Service-Identifier (im Bild das Feld I-SID) und ist 24 Bit lang.

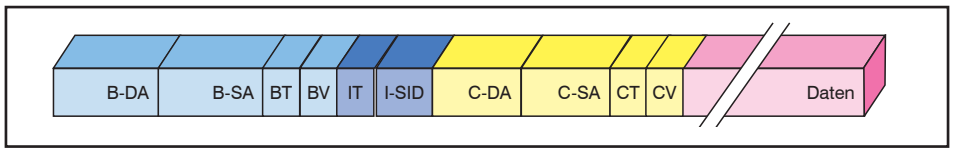


Abbildung 6: Frameformat von PBB und SPBM

Steuerungsebene/Control Plane

Die wichtigsten Aufgaben der in Abbildung 4 dargestellten Control Plane betreffen die korrekte Zustellung von durchgeleiteten Frames. Hierzu muss jedes Edge-System Regeln verwalten, welche Kundensegmente zusammengehören, welche getrennt werden müssen, wie sie unterschieden werden, welche Endsysteme über lokal angebundene Segmente erreicht werden und wie entfernte Endsysteme erreicht werden können.

Die Zuordnung von ankommenden Frames zu „ihrem“ virtuellen Overlay und umgekehrt erfolgt über Regeln, die meist administrativ verwaltet oder von einem übergeordneten Managementsystem übermittelt werden. Typische Kriterien für solche Zuordnungen sind neben dem Eingangsport des Frames die üblichen Netzwerkadressen von Layer 2 bis Layer 4 inklusive der VLAN-ID des Frames.

Die Weiterleitung der Frames selbst erfolgt dann anhand von Weiterleitungstabellen der Form:

- Netzwerkadressen des Endsystems
- zugehörige Tunnel-ID
- Erreichbarkeit (Das ist entweder der lokale Switch-Port oder der entfernte Tunnelendpunkt, hinter dem das Endsystem zu erreichen ist.)

Bei der Frage nach der konkreten Weiterleitung des Tunnel-Frames kommen wir zu einem sehr grundlegenden Punkt der jeweiligen Lösung:

Wie sehr sind die Control Layer von Overlay und Underlay miteinander verquickt? Und natürlich hängt diese Frage eng mit der geforderten Hardware-Unabhängigkeit der Lösung zusammen.

Hypervisor-basierende Lösungen wie NSX verwalten zu entfernten Endsystemen ausschließlich die Netzwerkadresse des entfernten Tunnelendpunkts und halten sich damit aus der Wegewahl durch das Transportnetz komplett raus.

Befindet sich dagegen der Tunnelendpunkt auf einer aktiven Netzwerkkomponente, die ihrerseits bereits Teil des Underlays und gegebenenfalls eines Routingprozesses im Underlay ist, dann entscheidet dieses Edge-System nicht nur zu welchem entfernten Tunnelendpunkt der verpackte Frame geschickt wird, sondern eben auch auf welchem Weg durch das Underlay dies geschieht. Vergleichen Sie hierzu Abbildung 7 mit Abbildung 3.

Dies bringt zusätzliche Komplexität in das Edge-Device und verquickt die Weiterleitungsentscheidungen im Overlay mit denen im Underlay.

Der Aufbau dieser Tabellen kann ganz klassisch durch Lernen von eingehenden Frames auf der Data Plane erfolgen (Data Plane Learning). Dieses „Lernen“ von Netzwerkadressen hat aber einen großen Nachteil: Unbekannte Zieladressen müssen im virtuellen Overlay geflutet, das heißt, an alle potentiellen Endpunkte, die zum gleichen Overlay gehören, ausgeliefert werden. Im Overlay geschieht dies wie gewohnt durch Broadcasts oder Anycasts, was schon aufwändig genug ist. Im Underlay bedeutet das aber unter Umständen die Unterstützung von Multicasts mit allen unangenehmen Begleitumständen wie Multicast-Routing etc.

Um dies zu vermeiden, setzen moderne Overlay-Lösungen auf eine übergeordnete Control Plane, die Netzwerkadressen und Erreichbarkeitsinformationen unter allen beteiligten Systemen austauscht. Dieses „Control Plane Learning“ hat außerdem den Vorteil, dass man besser kontrollieren kann, wer welche Adressen lernt, und

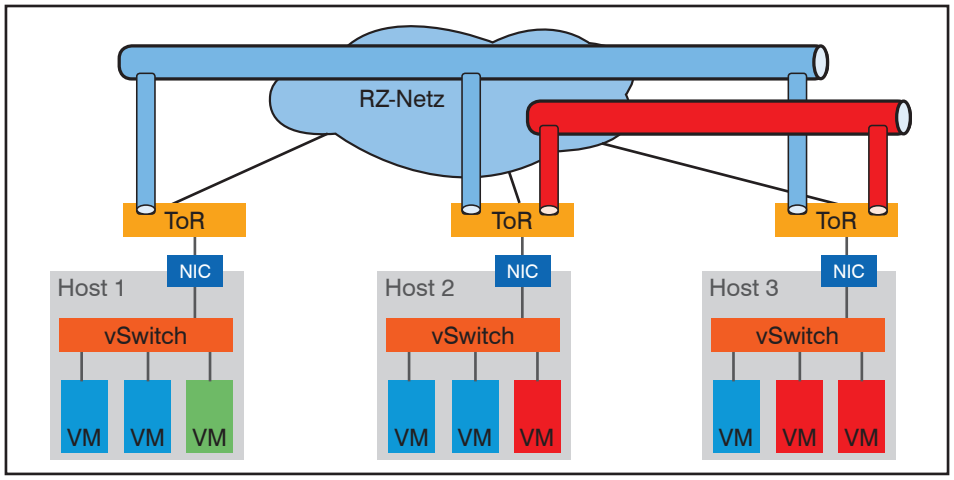


Abbildung 7: Wo endet das RZ-Netz?

Overlays in der Analyse - Teil 1: EVPN vs. SPBM

den Prozess über geeignete Policies steuern kann, was gerade in mandantenfähigen Umgebungen wichtig ist.

Falls die Lösung zu angebundenen Endgeräten sowohl MAC- als auch IP-Adressen verwaltet, können darüber hinaus die Edge-Devices ARP-Anfragen zu entfernten System lokal beantworten (Proxy-ARP).

Am Edge-Port selbst werden die angebundenen Netze und deren Adresse natürlich weiterhin ganz klassisch gelernt:

- über eingehende Frame (Data Plane),
- über IEEE 802.1X („Port Based Network Access Control“),
- via LLDP (Link Layer Discovery Protocol),
- über manuell konfigurierte Einträge (Management Plane),
- sonstige Protokolle.

Diese übergeordnete Control Plane kann entweder als zentraler SDN-Controller oder als verteilte Steuerebene (Distributed Control Plane) umgesetzt werden. Im ersten Fall werden wie bei dem Overflow-Modell alle relevanten Informationen an einer zentralen Instanz zusammengezogen und entweder proaktiv oder auf Anfrage den Tunnelendpunkten mitgeteilt. Beispiele für diesen zentralen Ansatz sind VMware NSX und Cisco ACI, aber auch MPLS-Netze nutzen in der Regel zentrale Instanzen, um Pfaddefinitionen zu verteilen.

Im zweiten Fall wird ein Control-Protokoll genutzt, um die Informationen an alle Endpunkte zu verteilen. Hierbei ist es wichtig sicherzustellen, dass alle Weiterleitungssysteme denselben Informationsstand haben. Typischerweise wird hierbei auf eines der etablierten Routing-Protokolle gesetzt, deren Aufgabe es ja klassischerweise ist, Routing-Informationen in einer Routing-Domäne zu verteilen und für eine gemeinsame Datenbasis zu sorgen.

Da die Steuerungsschicht in Overlay-Lösungen, die Layer-2-VPNs zur Verfügung stellen (was ja gerade in Unternehmens- bzw. Rechenzentrumsnetzen notwendig und gewünscht ist), aber mehr Informationen braucht als „einfache“ Layer-3-Routing-Informationen (z. B. die MAC-Adressen von Endsystemen), sind diese Routing-Protokolle verfahrensspezifisch erweitert. Wir werden weiter unten auf zwei Beispiele genauer eingehen.

Weitere Funktionen, die je nach Verfahren von der Steuerungsschicht der Edge-Devices wahrgenommen werden, sind:

- lokales Bridging,
- lokales Routing,
- Integration des Underlay zur Wegewahl durch das Transportnetz

Im Folgenden werden zwei Beispiele von verbreiteten Overlay-Lösungen und deren Control Plane im Überblick vorgestellt: BGP-EVPN und SPB.

EVPN

EVPN (Ethernet VPN) wurde standardisiert von der mittlerweile geschlossenen IETF Working Group L2VPN (Layer 2 Virtual Private Networks). Ziel dieser Arbeitsgruppe war die Entwicklung von Lösungen, die Layer-2-Verbindungen über Providernetze ermöglichen. Untergeordnet wurde auch untersucht, welche Anforderungen Cloud-Lösungen und große Rechenzentren an diese Protokolle haben.

Dabei stand von Anfang an die klare Trennung zwischen Overlay und Underlay fest. L2VPN-Lösungen sollten keine Kontrolle über das Underlay haben, falls nötig, sollen existieren QoS-Mechanismen oder Funktionen zur Wegewahl des Underlay genutzt werden.

EVPN selbst ist im RFC 7432 „BGP MPLS-Based Ethernet VPN“ definiert, Ziel ist alle Servicetypen wie E-LAN, E-LINE, E-TREE, L3-VPN und RZ- und Cloud-Kopplungen durch eine einheitliche Technologie betreiben zu können. (siehe Abbildung 8)

In dem Dokument wird ein Verfahren beschrieben, um Ethernet-basierende Services über MPLS zu verbinden – also eine Alternative zu den „klassischen“ MPLS L2VPNs wie VPLS (Virtual Private LAN Service). Adressiert werden insbesondere:

- Multihoming und Redundanz (und zwar sowohl active-passive Anbindungen als auch active-active),
- Optimierungen für Multicasts,
- einfache Provisionierung (Auto-Discovery),
- flowbasierendes Load-Balancing und
- Multipathing.

Die beschriebenen Mechanismen beziehen sich jedoch ausnahmslos auf die Control Plane in den Edge-Devices. Das Dokument betont daher auch explizit, dass EVPN nicht auf MPLS-Transportnetze beschränkt ist, sondern auch mit IP-basierenden Transportprotokollen umgesetzt werden kann – also beispielsweise mit VXLAN (VXLAN BGP EVPN). Solche Implementierungen gibt es von einer ganzen Reihe von Herstellern (Cisco, Juniper, Brocade u. a.).

Darüber hinaus gibt es auch Implementierungen, die PBB als Encapsulation-Protokoll und darüber MPLS als Transportprotokoll nutzen („MPLS PBB-EVPN“). Hierbei werden im Edge die Funktionen einer PBB-Edge-Bridge und eines EVPN-Edge-Devices kombiniert: Angebundenen Segmenten wird eine Service-ID (I-SID) für PBB zugeordnet (Cisco nennt das auch „PBB Bridge Domain“) und jeweils einer oder mehreren dieser Bridge Domains wird eine EVPN-ID zugeordnet, die ihrerseits mit einem MPLS-Label verbunden ist, um die so verpackten Frames über das MPLS-Netz zu transportieren. Der Vorteil dieser vorgeschalteten PBB-Encapsulation ist im Wesentlichen die weitere Reduzierung der Größe der MAC-Tabellen.

Kernpunkte von EVPN sind:

- Es werden virtuelle Ethernet-Services über Layer 3 (MPLS oder IP) bereitgestellt. Das heißt, die Edge-Devices verbinden Layer-2-Segmente über Layer-3-Tunnel transparent miteinander.
- Das Verfahren ist mandantenfähig, das heißt, das genutzte Tunnelprotokoll muss eine Tunnel-, Service- oder Kunden-ID transportieren.

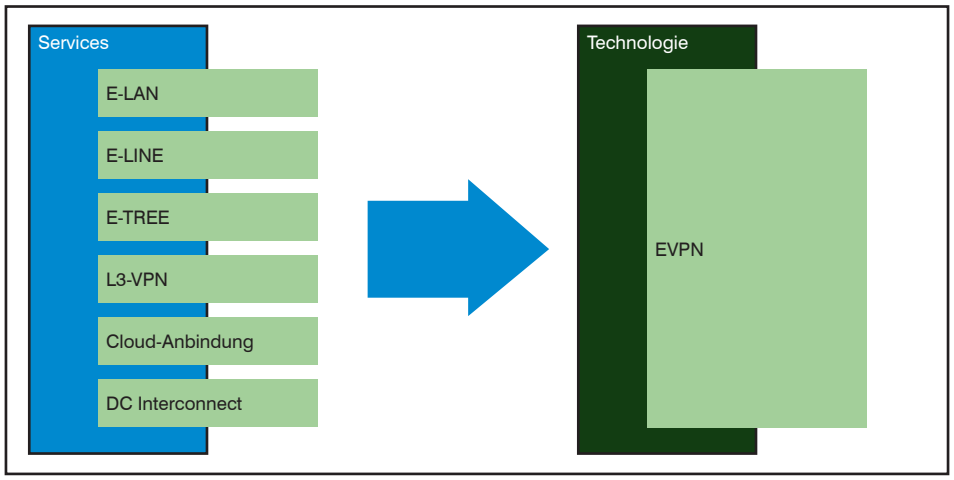


Abbildung 8: Einheitliche Technologie für verschiedene Services durch EVPN

Overlays in der Analyse - Teil 1: EVPN vs. SPBM

- BGP wird als Control-Protokoll zum Austausch von Netzwerkadressen und Erreichbarkeitsinformationen genutzt.
- MAC-Learning von entfernten Segmenten erfolgt nicht über die Data Plane, sondern über die Control Plane, also BGP.

Damit diese Anforderungen von BGP unterstützt werden können, sind einige Erweiterungen zur ursprünglichen Standardisierung nötig. Die wichtigste ist MP-BGP (Multiprotocol Border Gateway Protocol, standardisiert in RFC 4760 „Multiprotocol Extensions for BGP-4“), da BGP klassischerweise nur für IPv4 definiert ist. Mit Multiprotocol-BGP werden sogenannte „Address Family Identifier“ eingeführt, um unterschiedliche Netzwerkadresstypen wie IPv4, IPv6, MAC, Frame Relay, L2VPN, MPLS etc. pp kennzeichnen zu können. Somit können mit MP-BGP Netzwerk-Routen für völlig unterschiedliche Adresstypen verteilt werden.

Gleichwohl braucht weiterhin jeder BGP-Router, genauer jedes System, das BGP spricht, eine IPv4-Adresse! (siehe Abbildung 9)

Für EVPN wurde eine neue, eigene „Address Family“ definiert, mit der fünf verschiedene Routen kodiert werden können:

- Ethernet Auto-Discovery (A-D) route
  um schnellere Konvergenz im Fehlerfall und Load Balancing zu unterstützen
- MAC/IP Advertisement route
  für Unicast MAC-Adressen und Zuordnung der Tunnel-ID (oder MPLS-Label) optional können zusätzlich eine oder mehrere IP-Adressen des Endgeräts übermittelt werden, womit am lokalen Edge ARP-Requests beantwortet werden können (Proxy ARP)
- Inclusive Multicast Ethernet Tag route
  für Multicast-Unterstützung, inklusive Broadcast und Unknown Unicasts
- Ethernet Segment route
  zur Unterstützung von Multihoming und Auto-Discovery von mehrfach angebundenen Ethernet-Segmenten, sowie zur Wahl des Designated Forwarders
- IP Prefix route zur Integration von Layer-3-Routing

Das hierauf aufbauende Verfahren zur Weiterleitung von Frames ist dem von IP-VPNs (wie im RFC 4364 „BGP/MPLS IP Virtual Private Networks (VPNs)“) sehr ähnlich:

- Jedem Kundensegment wird eine eigene Weiterleitungstabelle, jetzt jedoch für Layer-2-Adressen, (MAC-VRF - Virtual Routing and Forwarding Table for MAC Addresses) zugeordnet.
- Routen zu diesen Segmenten werden über einen „Route Distinguisher“ eindeutig gemacht. Somit erreicht man einerseits, dass gleiche IP-Adressen in verschiedenen VPNs genutzt werden können, und andererseits können unterschiedliche Routen zum selben physischen Segment (oder Endgerät) unterstützt werden (Multihoming).
- Edge-Devices, die an dasselbe zusammenhängende Ethernet-Segment angebunden sind, wählen einen „Designated Forwarder“, der für Broadcasts, Multicasts und Unknown Unicasts zuständig ist.

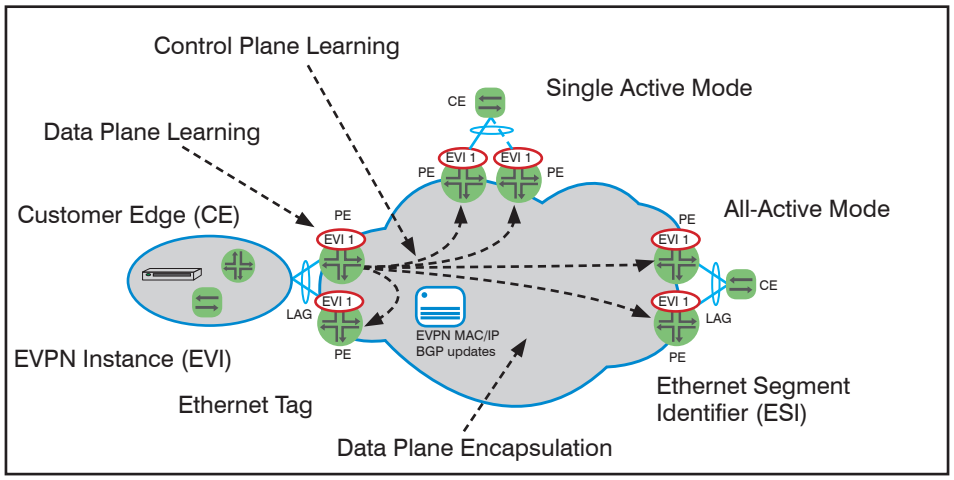


Abbildung 9: EVPN Konzepte

Ergänzend zu diesem standardmäßigen „intra-subnet forwarding“ auf Layer 2, behandelt EVPN auch „inter-subnet forwarding“, also die Weiterleitung von Frames über Subnetzgrenzen hinweg und wo infolge dessen IP-Routing erfolgen muss.

Traditionell wird hierfür der Verkehr über ein zentrales Layer-3-Gateway (Default Gateway) geführt. Das bedeutet aber eben, dass die Kommunikation zwischen zwei virtuellen Maschinen, die beispielsweise auf demselben Host laufen, erst den Host verlassen muss, gegebenenfalls quer durch das Rechenzentrum zum Gateway geführt, dort geroutet und dann zum Host zurückgeführt wird. Gerade in großen Umgebungen ist das sehr ineffektiv.

Seminar

Netzwerk-Design für Enterprise Netzwerke
27.11. - 29.11.2017 in Berlin

LAN-Technik unterliegt einem permanenten Wandel, neue Anforderungen erfordern neue Lösungen. Gerade im Rechenzentrum zeigen Trends wie die Konvergenz von Daten- und Storage-Netzen, die Einbindung von Netzwerkdiensten in ein virtualisiertes Gesamtdesign und die Integration von Cloud-Computing-Prinzipien, dass uns klassische Technologien und Designs nicht mehr weiterbringen. Das Seminar erklärt, was im Moment passiert und wie Sie sich auf die Zukunft vorbereiten können. Es geht auf Designalternativen im RZ und Campus im Zeitalter neuer Layer-2-Technologien wie Fabrics, Multichassis-Link-Aggregierung, Shortest Path Bridging und Hochgeschwindigkeits-Datenraten von 10/40/100 Gigabit ein. Darüber hinaus werden Priorisierungstechniken wie AVB und DCB besprochen sowie aktuelle Entwicklungen rund um die Themen Overlay-Designs, Netzwerkvirtualisierung, Software-Defined Data Center und Cloud Computing.

Referent: Dipl.-Math. Cornelius Höchel-Winter
Preise: 1.890,-- € netto

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Um dieses „hair pinning“ zu vermeiden, soll daher das Routing zwischen Systemen, die hinter demselben Tunnelendpunkt liegen, lokal erfolgen, also ohne dass der Verkehr verpackt wird und den Tunnel überhaupt erreicht. Das heißt, jedes Edge-System wird zum Default-Gateway für die angebundenen Subnetze und hat eine Schnittstelle in alle anderen angebundenen Subnetze. Diese Schnittstellen spielen dann ihrerseits Default Gateway für jede Netze.

Da die IP-Adressen von Default-Gateways innerhalb eines Subnetzes eindeutig sind, müssen diese IP-Adressen als IP-Anycast-Adressen allen Edge-Systemen zugewiesen werden, wo ein entsprechendes Segment angebunden ist. Ob zusätzlich auch einheitlich MAC-Anycast-Adressen genutzt werden, ist je nach Implementation unterschiedlich. Einheitliche MAC-Anycasts haben jedenfalls den Vorteil, dass im Netz keine Routen zu den MAC-Adressen der Default Gateways verteilt werden müssen – die Edge-Systeme agieren an dieser Stelle völlig autark voneinander.

Der IETF Entwurf „Integrated Routing and Bridging in EVPN“ (draft-ietf-bess-evpn-inter-subnet-forwarding – letzte Version 3 vom 8.2.17) schlägt ergänzend vor, optional auf allen Edges Schnittstellen für alle möglichen EVPN-Overlays bereitzustellen (siehe Abbildung 3). In diesem Szenario würde dann jeglicher subnetzübergreifende Verkehr direkt am Ingress-Edge in das Zielnetz geroutet und dann erst über die Tunnel zum jeweiligen Tunnelendpunkt geleitet.(siehe Abbildung 10)

Das Konzept sieht es dabei durchaus vor, dass beide Verfahren, zentrales Gateway und verteiltes Gateway, nebeneinander genutzt werden können. Beispielsweise könnte Verkehr, der zum selben Kunden oder zur selben Sicherheitszone gehört, lokal geroutet werden, während Verkehr, der die Grenzen von Kundennetzen oder Sicherheitszonen überquert, extern über eine dedizierte Firewall geführt wird.

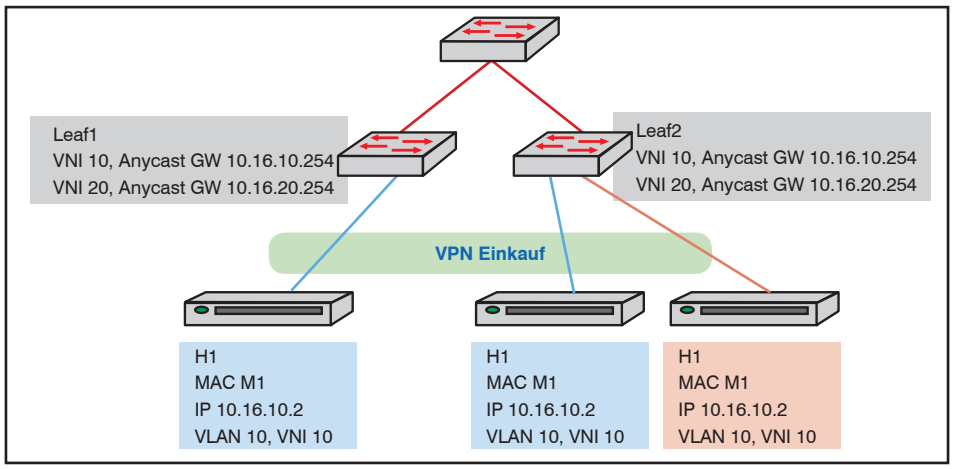


Abbildung 10: Lokales Routing bei EVPN

Shortest Path Bridging

Shortest Path Bridging (SPB) ist von der IEEE in der Erweiterung 802.1aq zum VLAN-Standard 802.1Q standardisiert. Die Ziele dieses Standards sind:

- Berechnung kostengünstiger Wege für Unicasts und Multicasts,
- Überwindung der Beschränkung auf nur einen einzigen Spanning Tree pro VLAN,
- Steigerung der Bandbreite und Senkung der Laufzeiten im Netzwerk,
- bessere Ausnutzung aller Netzwerk-Ressourcen und Ermöglichung von Lastausgleich über kostengleiche Wege.

Basis des Verfahrens ist IS-IS. IS-IS steht für „Intermediate System to Intermediate System Protocol” und ist von der ISO als Routingprotokoll für OSI-Systeme standardisiert (ISO 10589). IS-IS wurde ausgewählt, weil das Protokoll einige interessante Eigenschaften mit sich bringt:

- IS-IS ist als OSI-Protokoll unabhängig von einem speziellen Adressformat. Es werden also beispielsweise keine IP-Adressen benötigt wie etwa bei OSPF, sondern es läuft auch direkt auf Layer 2.
- IS-IS ist ein „Link State“-Protokoll (wie auch OSPF). Link-State-Protokolle konvergieren üblicherweise sehr schnell, sie sind weniger anfällig gegen Routing-Loops und unterstützen größere Netze.
- IS-IS kann ohne Konfiguration (sogenannte „Zero Configuration“) betrieben werden.
- IS-IS verwendet eine TLV-Kodierung (Type, Length, Value); dies vereinfacht die Definition und den Transport von neuen Arten von Daten.

Letzteres wurde dann auch von der IEEE genutzt, um einige neue, SPB-spezifische TLVs zu definieren.
Auf dieser Control Plane setzen zwei verschiedene Tunnelverfahren auf:

- SPBV: Shortest Path Bridging VID (VLAN-ID) Mode und
- SPBM: Shortest Path Bridging MAC Mode.

SPBV nutzt das in IEEE 802.1ad spezifizierte Q-in-Q-Verfahren „Provider Bridges“, während SPBM das in IEEE 802.1ah spezifizierte MAC-in-MAC-Verfahren „Provider Backbone Bridges (PBB)“ einsetzt (Frameformat siehe Abbildung 6).

SPBV hat praktisch keine Marktrelevanz, einzig SPBM ist in einer Implementierung der Firma Avaya (mittlerweile/demnächst Extreme) in nennenswerten Umfang installiert.

Vergleich EVPN und SPBM

Mit beiden Verfahren werden moderne Overlay-Lösungen gesteuert, die Layer-2-Services zur Verfügung stellen, und damit gibt es auf den ersten Blick eine ganze Reihe von Gemeinsamkeiten:

- Die IP- und MAC-Adressräume unterschiedlicher Kunden bzw. Services werden vollständig voneinander und vom Transportnetz getrennt. Damit werden überlappende Adressräume zwischen Kunden unterstützt.
- Es gibt nur ein sehr reduziertes MAC-Learning auf der Data Plane, nämlich beim Lernen von Adressen aus lokal angebundenen Layer-2-Segmenten. Alle MAC-Adressen aus entfernten Segmenten und alle MAC-Adressen der Tunnelendpunkte werden über die Control Plane gelernt. (Bei SPB außerdem die Adressen aller anderen Transportswitches ebenfalls.)
- Neue Endpunkte von Servicenetzen werden automatisch erkannt und über die Control Plane verteilt.
- Shortpathing und Multipathing werden von beiden Verfahren unterstützt.

Nichtsdestotrotz unterscheiden sich die Verfahren gewaltig, der wesentlichste Unterschied ist, dass SPBM im Gegensatz zu EVPN auf ein Layer-2-basierendes Underlay setzt. Hieraus leiten sich

Overlays in der Analyse - Teil 1: EVPN vs. SPBM

insbesondere für die Administration und das Operating solcher Netze wichtige Funktionsunterschiede ab:

1. Adressvergabe

Layer 2 ist per se selbstkonfigurierend, da keine Layer-2-Adressen manuell oder automatisiert vergeben werden müssen.

Für ein Layer-3-Design, wie es EVPN BGP erwartet, müssen dagegen an alle Tunnelendpunkte und alle Routingschnittstellen einzeln IP-Adressen vergeben werden. Dies wird in der Regel manuell erfolgen und ist mit entsprechendem Aufwand verbunden. Eine automatisierte Vergabe erfordert zusätzliche Tools und Schnittstellen, die zum einen die Komplexität der Lösung erhöhen und zum anderen ebenfalls konfiguriert werden müssen.

So oder so müssen außerdem im Vorfeld geeignete IP-Adresspläne entwickelt werden.

Hierzu ein kurzes Rechenbeispiel:

In einem mittleren Spine-Leaf-Design mit 2 Spines mit 30 Leafs benötigt man:

- 32 IP-Adressen für die Systeme selbst (Loopback Interfaces)
- 30 IP-Adressen für die Tunnelendpunkte auf den Leaf-Switches
- 2 Spines * 30 Leafs = 60 Punkt-zu-Punkt-Verbindungen * 2 für /31-Netze ergibt 120 IP-Adressen
- In Summe also 182 IP-Adressen, sinnvollerweise verteilt auf drei Adressgruppen.

2. Netzwerkerweiterung

SPB ist vom Konzept her eine Erweiterung des STP (Spanning Tree Protocol) und nutzt daher ebenfalls MAC-Multicasts (so genannte BPDUs – Bridge Protocol Data Units) zur Kommunikation mit den direkten Nachbarn. Das bedeutet, dass sich SPBM-Switches automatisch finden und eine SPBM-Fabric ohne Konfiguration erweitert werden kann. Einziger Nachteil: Eine SPB-Area muss immer zusammenhängend aufgebaut werden, jeder Switch, der kein SPB unterstützt, begrenzt der Area.

Die Nachbarschaftsbeziehungen von BGP laufen dagegen prinzipiell immer über TCP und müssen daher konfiguriert werden, bevor irgendeine BGP-Kommunikation beginnen kann. Es gibt einige erste Produkte (z. B. von Extreme), bei denen sich *direkt benachbarte* Layer-3-Switches über LLDP (Link Layer Discovery Protocol) finden und so auch für BGP-basierende Designs eine Art Auto-Discovery realisieren.

3. Netzwerktopologie

Eines der wichtigsten Ziele bei der Entwicklung von SPB war es, die Einschränkungen des Spanning Trees zu überwinden. Daher ist SPB vom Design her dazu prädestiniert, beliebige Topologien vom Ring bis zur Vollvermaschung zu unterstützen. SPB-Fabrics können ohne Rücksichtnahme auf irgendwelche Designvorschriften nach Bedarf aufgebaut und erweitert werden.

BGP setzt per Design auf Punkt-zu-Punkt-Verbindungen, wobei iBGP eine Vollvermaschung aller Router eines autonomen Systems voraussetzt, was in der Regel durch den Einsatz von Route Reflectors umgangen wird. Die Topologie einer hoch performanten BGP-Fabric mit redundanter Mehrwege-Ausbreitung ist somit alles andere als trivial, Spine-Leaf-Topologien sind hierfür noch am besten geeignet. Von den meisten Herstellern gibt es daher sehr detaillierte Leitfäden zum Aufbau von EVPN-basierenden Fabrics mit sehr wenig Spielraum für individuelle Sonderwünsche.

4. Skalierbarkeit

Das Underlay einer SPB-Lösung ist ein flaches Layer-2-Netz. Auch wenn in dieser gemeinsamen Broadcast-Area praktisch keine Broadcasts verwendet werden, beschränkt dies natürlich die Skalierbarkeit von SPBM deutlich. Hinzukommt, dass auch das Control-Protokoll IS-IS in einer einzigen Area läuft, was bedeutet, dass alle Switches die gleiche Topologie-Datenbank verwalten. Den Aufbau einer hierarchischen Lösung lässt SPB nicht zu. Damit ist eine SPB-Area realistischer Weise auf wenige Hundert Switches beschränkt.

Wie erwähnt, setzen die meisten EVPN-Designs auf eine Spine-Leaf-Topologie. Spine-Leaf wird gerne als Wundermittel für hoch skalierbare Netze verkauft, aber gerade eine reinrassige Spine-Leaf-Topologie hat klare Skalierungsgrenzen dort, wo alle Ports an den Spines belegt sind. Der entscheidende Vorteil von EVPN liegt darin, mit BGP klassische hierarchische Clos-Architekturen aufbauen zu können.

Zusammenfassung

Braucht ein Unternehmensnetz zwingend Overlays?

Kurz gesagt: Ja. Overlays sind das Mittel der Wahl, um skalierbare Netze zu bauen. Das ist nicht neu, mit VLANs machen wir das schon seit Jahrzehnten, aber VLANs und daraus aufbauende Netze unterliegen einer Reihe von Einschränkungen, die in modernen Netzen nicht länger tolerierbar sind:

- Gut 4.000 VLAN-IDs sind in vielen Umgebungen zu wenig.
- Die Virtualisierung und Automatisierung im RZ erfordert das Verschieben virtueller Maschinen über Layer-3-Grenzen hinweg (MAC Mobility).
- Der Spanning Tree als Mittel zur Schleifenunterdrückung ist indiskutabel.

Gleichzeitig kommen gerade im Rechenzentrum weitere Anforderungen nach Flexibilität und Automatisierung hinzu. Damit kommt insbesondere der Control Plane einer Overlay-Lösung große Bedeutung zu.

Wir haben in diesem Artikel zwei Overlay-Lösungen verglichen, deren Control Plane noch ganz klassisch im Netzwerk, verteilt auf alle teilnehmenden Netzwerkkomponenten liegt und die gleichzeitig stellvertretend für die beiden Basistechnologien Ethernet und IP im physischen Underlay sind.

Die Unterschiede sind erwartungsgemäß so groß, dass eine Entscheidung zwischen beiden Modellen nicht schwerfällt:

SPBM basiert auf Layer 2 und konfiguriert sich damit praktisch von alleine. Es werden beliebige Topologien unterstützt, solange die Fabric zusammenhängend bleibt, was die Lösung insbesondere auch für den Campus und die Access-Bereich interessant macht. Multicast-Support ist quasi eingebaut. Einzig die Zuordnung zu den virtuellen Netzen am Edge muss konfiguriert werden.

Der Wermuttropfen von SPBM liegt in der Skalierbarkeit, für wirklich große Netze ist die Lösung nicht geeignet.

Und genau hier liegt die Stärke von BGP-EVPN: Durch die Möglichkeit hierarchische Netzstrukturen zu bauen und einer Vielzahl weiterer Konfigurationsparameter kann man sehr präzise steuern, wer wie viele Routen verwaltet muss, und erreicht so deutlich größere Netze bis hin zu Hyperscalern wie Facebook, Microsoft und Co.

Von einem Zero-Touch-Provisioning oder One-Stop-Provisioning sind wir hierbei jedoch meilenweit entfernt. EVPN ist letztlich eben doch Provider-Technologie. Oder wie sehen Sie das? Ich freue mich auf Ihre Rückmeldungen.

Im nächsten Teil werden wir uns mit der Frage beschäftigen, welche Auswirkungen die Wahl eines bestimmten Overlay-Protokolls (wie beispielsweise VXLAN) oder einer bestimmten Control Plane (wie beispielsweise EVPN) eigentlich auf das Underlay hat.

Aktuelle Sonderveranstaltungen

Herausforderung Informationssicherheit

Cloud-SaaS-Virtualisierung 25.09.17 in Bonn

IoT-Abwehr-Recht 26.09.17 in Bonn

Sparen Sie 590,-- € im Paket

Die ComConsult Akademie veranstaltet am 25.09. und am 26.09.2017 ihre Sonderveranstaltungen "Herausforderung Informationssicherheit - Cloud Computing, Security as a Service, Virtualisierung" und "Herausforderung Informationssicherheit - IoT, Abwehr von Angriffen, rechtliche Rahmenbedingungen" in Bonn.

Die Informationssicherheit muss stets flexibel, schnell und ausgesprochen kreativ auf neue Angriffsformen, Schwachstellen in IT-Systemen und neuen oder sich ändernden Informationstechnologien reagieren. Wir müssen einerseits mit immer trickreicheren zielgerichteten Angriffen, DDoS-Attacken (inzwischen der Terabit-Klasse) und Schadsoftware kämpfen, andererseits haben sich mit Cloud Computing, Mobile Computing, Software-defined Networking, RZ-Automatisierung und dem Internet of Things entscheidende Änderungen in der IT materialisiert, auf die sich die Informationssicherheit offensichtlich noch nicht gut genug vorbereitet hat, wie entsprechende Sicherheitsvorfälle eindrucksvoll bewiesen haben.

Dies haben wir zum Anlass für diese Sonderveranstaltung genommen, die wir in zwei aufeinander folgende Thementage unterteilt haben, die einzeln oder zusammen gebucht werden können.

An **Tag 1** analysieren und bewerten wir für Sie: Cloud Computing: Wie kann eine sichere Nutzung der Cloud ohne signifikanten Kontrollverlust erfolgen? Wie sehen die technischen Lösungsbausteine für Cloud-Sicherheit aus? Security as a Service: Wo ist der Mehrwert von Cloud-basierten Sicherheitslösungen? Wo sind die Grenzen? Wie kommt man zu einer integrierten Gesamtlösung? Risikobereich Virtualisierung: Wo sind die Angriffspunkte – Hypervisor, Container, VM, Speicher, Netzwerk? Wie sehen die Lösungen aus? Was bedeutet das für Zonenkonzepte?

An **Tag 2** analysieren und bewerten wir für Sie: Albtraum Internet of Things: Wie kritisch sind ungesicherte Endgeräte? Welche Sicherheit bieten neue Technologien wie 5G? Welche Handlungsmöglichkeiten bestehen? Zielgerichte Angriffe, die Kür des Sicherheits-Managements: Wie erfolgen Sie? Wie können Sie verhindert werden? Wie können sie isoliert werden, wenn sie erfolgreich sind? Juristische Rahmenbedingungen: Was erzwingt die aktuelle Rechtslage? Wie werden Verstöße bestraft? Wann können Sicherheitsmaßnahmen mit dem Gesetz in Konflikt gerate?

Wenn Sie beide Seminare zum Thema "Herausforderung Informationssicherheit" buchen, bieten wir Ihnen einen Rabatt von 590,-- € an.

Sie zahlen für beide Kurse nur 1.590,-- € statt regulär 2.180,-- €.

Dr. Simon Hoff wird Sie durch beide Veranstaltungen begleiten.

Dr. Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Anmeldung an kundenservice@comconsult-research.de

Herausforderung Informationssicherheit

Ich buche die Sonderveranstaltung(en)
Herausforderung Informationssicherheit

☐ 25.09.2017 in Bonn - 1.090,-- € netto
☐ 26.09.2017 in Bonn - 1.090,-- € netto
☐ 25.-26.09.17 in Bonn - 1.590,-- € netto

☐ Bitte buchen Sie mir ein Hotelzimmer

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

Standpunkt

Informationssicherheit im Mikrokosmos von Smart Buildings

Der Standpunkt von Dr. Simon Hoff greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

Moderne Gebäude sind in vielen Fällen längst Bestandteil des Cyber-Raums geworden, d.h. die Komponenten der Gebäudetechnik von der Heizungsanlage bis zur Beleuchtung sind vernetzt und benötigen zur Fernwartung nicht selten auch einen Internet-Zugang. Zur Vernetzung werden dabei natürlich immer häufiger auch drahtlose Techniken wie z.B. Enocean, ZigBee, Bluetooth und WLAN sowie Mobilfunk eingesetzt. In diesem Sinne sind moderne Gebäude längst im Internet of Things (IoT) angekommen. Dies bildet die Grundlage für den nächsten entscheidenden Schritt: Das Gebäude der Zukunft ist intelligent, kann autonom auf Umwelteinflüsse reagieren und mit dem Nutzer des Gebäudes auf vielfältigste Art interagieren. Dabei wird natürlich auch die Integration mobiler Endgeräte wie Smartphones und Tablets eine besondere Rolle spielen.

Ein solches Smart Building beinhaltet also letztendlich nichts anderes als eine spezielle IP-vernetzte IT-Infrastruktur, die einen höchst interessanten Mikrokosmos bildet:

- IP-vernetzte Sensoren, Aktuatoren, Steuerungen, Mensch-Maschine-Schnittstellen, Maschine-Maschine-Schnittstellen und natürlich Server für die (hoffentlich intelligente) Verarbeitung von Daten und die Kontrolle des Smart Building
- Nutzung von Standard-Betriebssystemen, von Windows, Linux über iOS zu Android
- Access Points für die verschiedenen lokalen Funktechniken, Ethernet Switches für die interne Vernetzung
- Firewalls und Gateways für Zonenübergänge und Internetanbindungen

Das ist scheinbar nichts Neues, denn praktisch jede moderne industrielle IT basiert auf einer solchen Infrastruktur. Was ist also anders? Ganz einfach: Was vorher „teuer und edel“ sein durfte, muss jetzt (vergleichsweise) günstig, sehr schnell und standardisiert aufbaubar, natürlich extrem leicht replizierbar und mit geringstem Aufwand betreibbar sein.

Und es kommt noch etwas Besonderes hinzu: ohne Cloud kein Smart Building! Während in der industriellen IT die notwendige Intelligenz häufig noch im eigenen Rechenzentrum bereitgestellt werden kann, ist für ein Smart Building die Cloud gefragt. Dies ist insbesondere der Fall, wenn gebäudeübergreifend Daten für Auswertungen z.B. mit Big-Data-Techniken erfolgen sollen und wenn für Nutzer und Betreiber der Smart Buildings eine einheitliche Benutzeroberfläche über Web-Anwendungen zur Verfügung werden soll. Eine über das Internet erreichbare „Smart Building Cloud“ ist also quasi das Rechenzentrum für ggf. eine große Zahl von Smart Buildings.

Worin besteht nun die Gefahr? Ganz einfach: Ein Smart Building ist Bestandteil des IoT, und bislang hat sich das IoT bedingt durch unsichere und damit leicht kompromittierbare Things als eine der größten Bedrohungen im Internet erwiesen. Dank des IoT konnte beispielsweise das Mirai Botnet Attacken vom Typ Distributed Denial of Service (DDoS) der Terabit-Klasse erreichen [1]. In der Praxis stellt man dabei immer wieder fest, dass die Entwickler (und die Nutzer) der Things im IoT selbst die elementarsten Grundregeln der Informationssicherheit verletzen. Solange es sich um vollständig isolierte Systeme handelt, mag das noch unkritisch sein, nur haben wir hier aber Systeme, die über das Internet kommunizieren und ggf. sogar vom Internet aus erreichbar sein müssen. Diese Situation lässt sich natürlich sofort auf ein Smart Building übertragen. Nehmen wir einfach mal ein paar Angriffsszenarien an:

- Ein DDoS auf spezielle im Internet erreichbare Dienste kann dazu führen, dass nicht nur der Dienst, sondern auch dahinter befindliche Anlagen im Smart Building ihren Geist aufgeben. Nebenbei, so etwas ist schon längst vorgekommen: Wenn eine Heizung in Finnland durch eine DDoS-Attacke nicht mehr funktioniert, kann es richtig kalt werden, wie im November 2016 berichtet wurde [2].
- Wenn Schwachstellen in Web-Anwendungen / Web-Services bestehen, die in einem Smart Building oder einer Smart Building Cloud zur Verfügung angeboten werden, können hierüber Server kompromittiert werden oder auch Schadsoftware auf Endgeräte injiziert werden, die diese Dienste nutzen. Im schlimmsten Fall kann ein tausende Kilometer entfernter Angreifer das gesamte Smart Building unter seine Kontrolle nehmen.
- Ein Angreifer könnte einen PC oder ein Smartphone eines Nutzers oder Administrators eines Smart Building z.B. per Spear Phishing angreifen und dort ein sogenanntes Remote Administration Tool injizieren, d.h. eine spezielle Schadsoftware, über die der Angreifer z.B. den Nutzer belauschen und Aktivitäten mindestens mit den Berechtigungen des Nutzers ausführen kann [3]. Wenn über dieses Endgerät auf ein Smart Building zugegriffen werden kann, ist das Kind in den Brunnen gefallen, und auch hier könnte am Ende schlimmstenfalls das komplette Smart Building unter der Kontrolle des Angreifers sein.
- Höchst spannend ist auch die Manipulation von Sensorwerten entweder durch einen internen Angriff oder durch einen externen Angriff, bei dem der Angreifer z.B. der Smart Building Cloud vorgaukelt, ein Sensor in einem Smart Building zu sein. Die Folge könnte eine Fehlentscheidung der Intelligenz des Smart Building mit weitreichenden Konsequenzen sein.

Es ist klar, dass eine solche IT-Infrastruktur nach dem Stand der Technik abgesichert werden muss. Informationssi-

cherheit muss integraler Bestandteil von Produktentwicklung, Planung, Implementierung und Betrieb von Smart Buildings sein. Alles andere ist mehr als fahrlässig. Was kann man also tun? Man könnte beispielsweise sicherstellen, dass

- ein Smart Building konsequent über den gesamten Lebenszyklus nach dem Standard IEC 62443 „Industrial communication networks - Network and system security“ abgesichert ist und, dass dabei nur Produkte eingesetzt werden, die im Sinne von IEC 62443 sicher oder sogar zertifiziert sind,
- der Betreiber eines Smart Building nach ISO 27001 zertifiziert ist,
- eine Smart Building Cloud nach ISO 27001 und nach ISO 27017 „Code of practice for information security controls based on ISO/IEC 27002 for cloud services” zertifiziert ist oder ein Testat gemäß Cloud Computing Compliance Controls Catalogue (C5) des Bundesamts für Sicherheit in der Informationstechnik (BSI) vorweisen kann.

Nur: Das kostet richtig Geld! Speziell der erste Punkt hat es in sich, denn nicht nur die Kosten für Planung, Umsetzung und Betrieb steigen signifikant, sondern auch die Kosten für die Entwicklung und nachhaltige Pflege von Produkten im Sinne von IEC 62443. Das wesentliche Schlagwort ist hier Security by Design, d.h. Informationssicherheit als integraler Bestandteil der Produktentwicklung und Maintenance. Das Ergebnis wären dann im Idealfall Komponenten, die aus sich selbst heraus angemessen abgesichert sind. Ein Kunde von mir hat hierzu für den Bereich der Absicherung der industriellen Fertigung sehr treffend den Begriff der Eigensicherheit von Komponenten verwendet.

Die interessante Frage ist nun: Würde es ausreichen, wenn wir ausschließlich eigensichere Komponenten in einem Smart Building verwenden würden? Dann könnten wir doch auf den ganzen anderen Rest an schrecklichen Sicherheitsmaßnahmen verzichten! Die Antwort auf diese Frage ist leider: Nein. Erstens sichert auch Security by Design keine Fehlerfreiheit einer Komponente zu (und wir wissen nun einmal, dass Software - fast – nie fehlerfrei ist). Zweitens würde dies nur dann funktionieren, wenn die Betriebsprozesse stets hundertprozentig sicherstellen könnten, dass diese Eigensicherheit über den gesamten Lebenszyklus der Komponente weiter besteht.

Was passiert beispielsweise, wenn man einen Web-Service in einem IoT-Gerät nach den Regeln der Kunst implementiert, hierzu aber Software-Komponenten eines Dritt-Herstellers verwendet, die bisher unbekannte Schwachstellen haben und die sich erst bei detailliertester Analyse zeigen würden? Die Wahrscheinlichkeit ist recht hoch, dass der Fehler auch nach intensiven Produkttests übersehen wird und man mit der Schwachstelle auf den Markt geht. Und das würde dann auch für alle Produkte gelten, die die entsprechende Software-Komponente einsetzen (und damit ggf. millionenfach verbreitet sein). Dass genau so etwas tatsächlich vorkommt, zeigt eine Meldung aus dem Juli 2017, die zunächst eine Überwachungskamera des Herstellers Axis betraf, jedoch letztendlich für alle Produkte galt, die gSOAP einsetzen [4]. Hierbei handelt es sich um ein verbreitetes Open-Source-Werkzeug für SOAP/XML Web Services in C/C++.

Die logische Konsequenz ist: Was für die „normale“ IT gilt, gilt auch für Smart Buildings: Geräte im Smart Building dürfen nicht für Hinz und Kunz direkt aus dem Internet erreichbar sein, sondern nur für spezifische, angemessen authentisierte Systeme in einer entsprechend abgesicherten Umgebung, die letztendlich von der Smart Building Cloud bereitgestellt werden muss. Es bleibt also dabei: Auch wenn die (IoT-) Komponenten im Smart Building vielleicht immer sicherer werden, das gesamte Smart Building muss nach den Regeln der Kunst nachhaltig abgesichert werden, auch wenn es erheblichen Aufwand verursacht. Nebenbei: Alles scheint ja im Moment „smart“ oder intelligent zu werden und die Diskussion in diesem Artikel lässt sich natürlich 1-zu-1 auf alle anderen „smarten“ Bereiche übertragen.

Verweise

[1] Siehe: „Alle Räder stehen still, wenn dein starker Arm es will“ oder das unterschätzte Angriffspotential von DDoS, aus "Der Netzwerk Insider" vom Oktober 2016

[2] Siehe: **http://www.spiegel.de/netzwelt/web/finnland-hacker-schalten-heizungen-aus-a-1120234.html**

[3] Siehe: „Abwehr zielgerichteter Angriffe - die Paradedisziplin der Informationssicherheit“ aus "Der Netzwerk Insider" vom Mai 2017

[4] Siehe **http://blog.senr.io/blog/devils-ivy-flaw-in-widely-used-third-party-code-impacts-millions**

Sonderveranstaltung

IT-Infrastrukturen für das Gebäude der Zukunft
16.10.2017 in Köln
17.10.2017 in Bonn

Das Gebäude der Zukunft erfordert IT-Infrastrukturen, die Gewerk-übergreifend sind, die sowohl in der Datenverarbeitung als auch in der Klimatisierung, Zugangssicherung oder allgemeiner gesprochen der Gebäude-Automatisierung eingesetzt werden können. Diese Veranstaltung wendet sich an Planer aller Gewerke und bietet den idealen Blick über den Tellerrand, um zu einer erfolgreichen und wirtschaftlichen Gewerke-übergreifenden Planung zu kommen und einen langfristig flexiblen Betrieb eines neuen Gebäudes zu erreichen.

Moderation: Dipl.-Inform. Thomas Steil
Preis: 1.090,-- € netto

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Zweitthema

Cisco „Campus Fabric“ oder Software-defined Access

Fortsetzung von Seite 1

Dr.-Ing. Joachim Wetzlar ist seit mehr denn 20 Jahren Senior Consultant der ComConsult Beratung und Planung GmbH und leitet dort das Competence Center „Data Center“. Er verfügt über einen erheblichen Erfahrungsschatz im praktischen Umgang mit Netzkomponenten und Serversystemen. Seine tiefen Detailkenntnisse der Kommunikations-Protokolle und entsprechender Messtechnik haben ihn in den zurückliegenden Jahren zahlreiche komplexe Fehlersituationen erfolgreich lösen lassen. Neben seiner Tätigkeit als Troubleshooter führt Herr Dr. Wetzlar als Projektleiter und Senior Consultant regelmäßig Netzwerk- WLAN- und RZ-Redesigns durch. Besucher von Seminaren und Kongressen schätzen ihn als kompetenten und lebendigen Referenten mit hohem Praxisbezug.

Stellen Sie sich also die folgende Aufgabenstellung vor: Die Access-Netze eines Kunden basieren auf den typischen drei Stufen „Access“, „Distribution“ und „Core“. Es handelt sich um einen weit verzweigen Campus mit zahlreichen Gebäuden und entsprechend mehr als einer Handvoll Distribution-Bereichen. Insgesamt gibt es eine dreistellige Anzahl Access Switches und eine entsprechend große Anzahl von Access-Subnetzen. Ein IP-Adressierungskonzept berücksichtigt die geographische Aufteilung der Subnetze und erwartete Client-Anzahlen. Sie können sich sicher vorstellen, wie ein solches IP-Adressierungskonzept nach einigen Jahren praktischem Netzbetrieb mit „Moves, Adds und Changes“ aussieht.

Nun wird gefordert, Network Access Control (NAC) einzuführen. Clients werden verschiedenen Sicherheitszonen zugeordnet. Die Einteilung erfolgt bezogen auf Benutzergruppen, also etwa „Standard-Arbeitsplatz“, „Personalabteilung“, „Vorstand“, „Entwicklung“ und „Gäste“. Selbstverständlich werden Sie zu diesem Zweck nicht mehrere physische Netze parallel aufbauen und betreiben wollen. Stattdessen wählen Sie eine Technik zur Netzwerk-Virtualisierung, wie beispielsweise Virtual Routing and Forwarding (VRF) und Virtual LAN (VLAN). Oder sie machen es per Overlay, z.B. mittels Multi-Protocol Label Switching (MPLS).

Ein Problem bleibt jedoch bei den meisten Techniken: Sie müssen unterschiedlichen Benutzergruppen unterschiedliche IP-Subnetze zuweisen. Man kann sich die Sache einfach machen und das IP-Adressierungskonzept vervielfachen. Wo es bisher ein Access VLAN gab, sind es nun fünf. Welch ein Aufwand, vor allem weil die meisten Benutzergruppen nur wenige Anwender umfassen. Also könnte man deren Subnetze auf bestimmte Bereiche begrenzen. Aber was passiert bei Umzügen? Wählen wir also unterschiedliche geographische Ausdehnungen: Standard-Arbeitsplätze bleiben wie gehabt und zusätzlich je ein Campus-übergreifendes Netz für Entwicklung, Personalabteilung, etc. Aber auch das hat wohlbekannte Nachteile.

Sie erkennen, dass eine wie auch immer geartete neue Technik nützlich wäre, Access-Netze von der örtlichen Bindung an das IP-Subnetz der Switching-Infrastruktur zu entkoppeln. Anders ausgedrückt, man braucht eine Switching-Infrastruktur, mit der sich der Zugang zu bestimmten IP-Subnetzen ortsunabhängig realisieren lässt. Dies lässt sich mit spezieller Hardware realisieren, wie beispielsweise mittels Bridge Port Extension. Access Switches mutieren dabei zu abgesetzten Line Cards eines großen modularen „Access Core“. Oder man greift (mal wieder) auf ein Overlay zurück, wie beispielsweise Shortest Path Bridging MAC (SPBM).

Cisco hat nun eine neues Overlay für diesem Zweck erfunden, die „Campus Fabric“. Das Overlay ist hierbei eine Kombination aus LISP und Virtual Extensible LAN (VXLAN). Schauen wir uns zunächst die Funktionsweise vom LISP an; ich vereinfache so weit wie möglich.

Grundzüge von LISP

LISP, das Locator/ID Separator Protocol, wurde im Januar 2013 als RFC 6830 veröffentlicht. Die in der Überschrift zu dem als „experimental“ eingestuften Dokument genannten Autoren stammen allesamt von Cisco Systems. Bereits im Sommer 2011 hat Cisco in unserem Hause eine Implementierung auf Basis der Serie Nexus 7000 vorgeführt und wir konnten erste Tests der Funktionsweise im ComConsult-Labor durchführen. Kurz gesagt, unterscheidet LISP zwei Ebenen der IP-Adressierung:

- Ebene der Endpunkte, die miteinander kommunizieren: Jeder Endpunkt verfügt über eine Adresse, den so genannten End Point Identifier (EID). Dieser kann entweder eine IPv4 oder eine IPv6-Adresse sein. Die EIDs sind Teil lokaler IP-Netze, wie beispielsweise Access-Netze oder Rechenzentren.

- Ebene des „Underlay“: Hierbei handelt es sich um ein beliebiges geroutetes IPv4- oder IPv6-Netz. Die Netze der EIDs sind daran über spezielle Router angeschlossen, die eine Enkapsulierung bzw. Dekapsulierung der Pakete von EIDs vornehmen. Aus dem Underlay werden diese Router über so genannte Routing Locators (RLOC) adressiert. Der RLOC ist also die IP-Adresse des LISP-Routers aus der Sicht des Underlay.

Die Übertragung von Paketen erfolgt im Underlay getunnelt. IP-Pakete werden in IP-Paketen verpackt, wobei alle vier Varianten denkbar sind, also IPv4 in IPv4, IPv4 in IPv6, usw. Dementsprechend heißen diese Router auch „Tunnel Router“. Es werden zwei grundsätzliche Funktionen beim Tunnel Router unterschieden:

- Ingress Tunnel Router (ITR): Der ITR enkapsuliert Pakete der EIDs und sendet sie über das Underlay an einen ETR.

- Egress Tunnel Router (ETR): Der ETR nimmt enkapsulierte Pakete aus dem Underlay entgegen, dekapsuliert sie und sendet den Inhalt per „normalem“ IP Routing an den entsprechenden EID.

Jeder Router unterstützt im Allgemeinen beide Funktionen, damit den Paketen ein Rückweg offensteht. Die Router werden daher gerne mit dem Kürzel xTR bezeichnet. Die Abbildung 1 zeigt ein einfaches Beispiel für LISP. Neben einem Access-Netz und dem Rechenzentrum erkennt man das Underlay und die beiden xTR mit ihren IP-Adressen (RLOC). Außerdem sind ein Client und ein Server mit ihren IP-Adressen (EID) zu erkennen.

Eine Funktion fehlt noch, damit die Pakete letztlich ihr Ziel erreichen. Es muss eine Abbildung von EID auf die RLOC geben. Der ITR muss irgendwo nachschlagen können, an welchen ETR er das enkapsulierte Paket senden soll. Dazu spezifiziert LISP die beiden Funktionen „Map Resolver“ und „Map Server“. Im Map Server hinterlegen die ETR alle über sie erreichbaren EID bzw. deren IP-Netze. Die entsprechende Tabelle ist in Abbildung 1 angedeutet. Man sieht dort zwei Einträge, einen für das Access-Netz und einen für das Rechenzentrum. Mit Pfeilen angedeutet ist, wie der ITR die Adresse des passenden RLOC erfährt:

1. Der Client im Access-Netz sendet sein Paket an den ITR. Die IP-Adresse des ITR auf der Seite des Access-Netzes (z.B. 192.168.2.1) könnte am Client als Default Gateway eingerichtet sein. Der ITR bittet nun den Map Resolver, den zum Ziel-EID passenden RLOC zu suchen.

2. Der Map Resolver gibt die Anfrage an den Map Server weiter.

3. Der Map Server findet den gesuchten Eintrag und leitet die Anfrage an den RLOC weiter. Dabei handelt es sich um den bzw. einen gesuchten ETR.

4. Dieser ETR informiert nun den anfragenden ITR über seine IP-Adresse im Underlay (RLOC). Der ITR legt die Adresse in seinem Cache ab. Er sendet nun das enkapsulierte Paket an den ETR.

Dieser etwas komplizierte Ablauf stellt einerseits sicher, dass der ETR tatsächlich eine Verbindung zum ITR besitzt (und nicht z.B. inzwischen ausgefallen ist). Zum anderen besteht so die Möglichkeit, abhängig von der Verkehrssituation stattdessen den RLOC eines zweiten Interfaces oder eines redundanten ETR zu bekanntzugeben und damit letztlich den Datenfluss zu steuern.

Mobilität von Endpunkten mit LISP

Sie werden bemerkt haben, dass die Frage, wo sich ein Endpunkt (also Client oder Server) befindet, unabhängig von der Netzwerk-Adresse in den jeweiligen Access-Netzen ist. Diese Übereinstimmung von EID und Netzwerk-Adresse wird nur für das Routing innerhalb der Access-Netze benötigt.

Machen wir also folgendes Gedankenspiel: Die Access-Netze umfassen jeweils nur ein /24-Subnetz und der xTR ist für dieses Subnetz der Default Gateway. Nun nehmen wir einen Client aus einem Access-Netz heraus und stecken ihn auf ein Switch Port, das sich in einem zweiten Access-Netz befindet. Die IP-Adresse des Client bleibt jedoch unverändert, es kommt also insbesondere kein DHCP zum Einsatz. Abbildung 2 illustriert dieses Szenario. Jetzt passiert folgendes:

- Der umgezogene Client versucht den Server zu erreichen und sendet ein entsprechendes Paket an den ITR (wie das einzelnen geht, lassen wir hier unberücksichtigt).

- Der ITR erfährt über den Map Resolver den RLOC des passenden ETR und sendet das Paket enkapsuliert über das Underlay, wie oben beschrieben.

- Der ITR hat bei dieser Gelegenheit bemerkt, dass sich nun ein Client in seinem Access-Netz befindet, der nicht zu ihm gehört, dessen IP-Adresse aus einem anderen IP-Netz stammt.

- Nun registriert der ITR die IP-Adresse des Client am Map Server. Er verwendet dazu die /32-Subnetzmaske, die nur genau die eine IP-Adresse bezeichnet. Es entsteht ein neuer Eintrag im Map Server, den Sie in der Abbildung 2 erkennen können. Gleichzeitig erzeugt der ITR eine Host Route für den Client, die in das angeschlossene Access-Netz zeigt.

- Der Map Server informiert nun den ITR des ursprünglichen Access-Netzes (192.168.2.0/24) darüber, dass sich der Client nicht mehr in seinem Bereich befindet. Er macht sich einen entsprechenden Eintrag in einer „Abwesenheits-Liste“.

Nach diesen Maßnahmen würde das Antwortpaket des Servers zunächst am ursprünglichen RLOC ankommen. Dieser xTR führt den Client in der Abwesenheits-Liste und wird den absendendenden ITR im Rechenzentrum anweisen, seinen entsprechenden Cache-Eintrag zu löschen. Dieser führt dann die Standard-LISP-Pro-

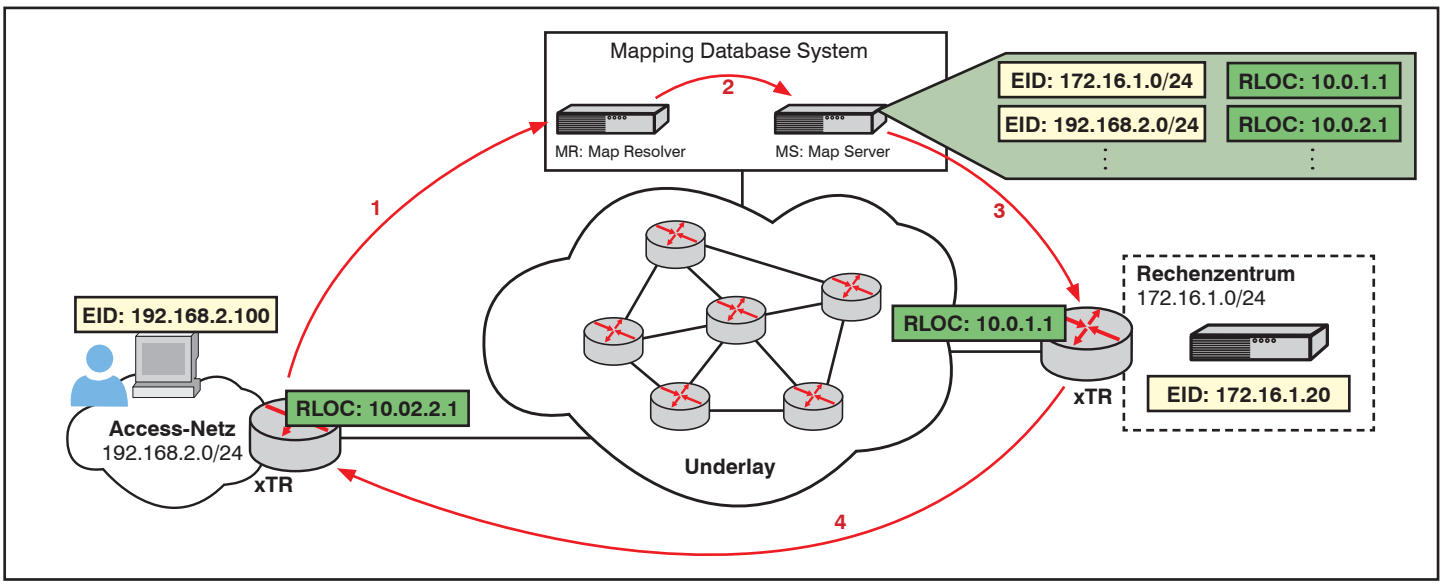


Abbildung 1: Zur grundsätzlichen Funktionsweise von LISP

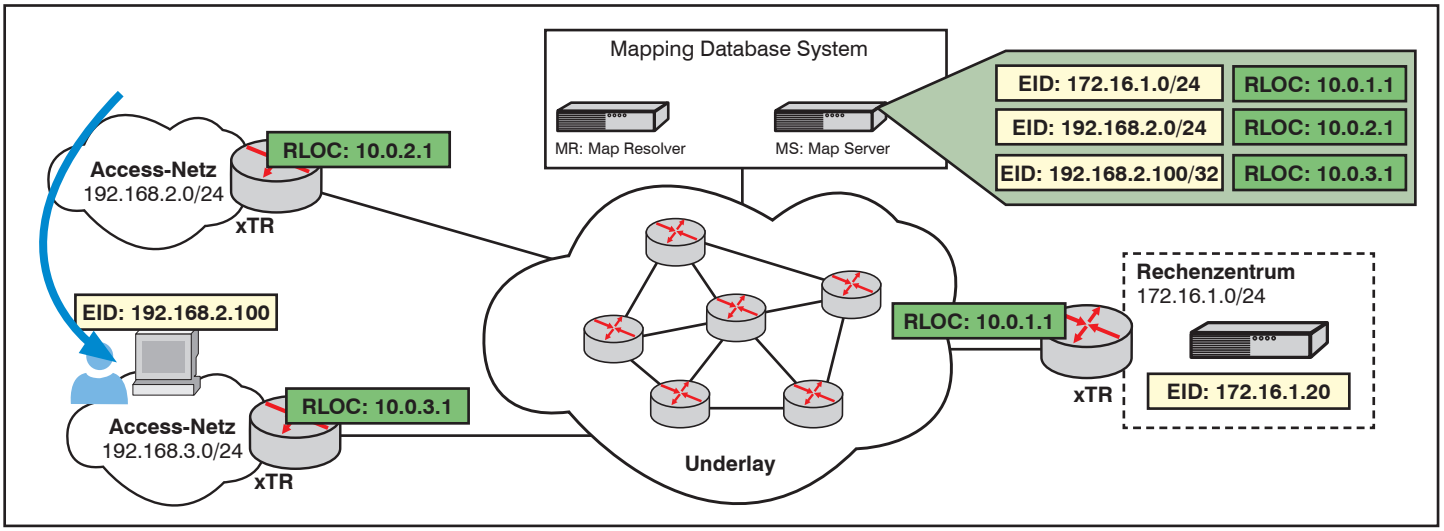


Abbildung 2: LISP unterstützt die Mobilität von Endpunkten

zedur mit Anfrage am Map Resolver durch und erhält nun als neuen RLOC die IP-Adresse 10.0.3.1 genannt.

Verwendung von LISP in Cisco Campus Fabric

Sie merken, dass die Sache mit der Mobilität von Endpunkten so nicht ganz rund ist. Es mutet irgendwie komisch an, dass sich Endgeräte in Subnetzen aufhalten sollen, in die sie eigentlich nicht hineingehören. An dieser Stelle würde man doch lieber auf DHCP vertrauen und den Endpunkten neue IP-Adressen und auch das passende Default Gateway zuweisen. In diesem Fall kann man sich fragen, wozu man dann noch den Umweg über das Underlay braucht. Ganz Genau!

Cisco hat nun einen entscheidenden Kunstgriff gewagt: Alle Access-Netze haben dieselbe IP-Adresse und Subnetzmaske. Wie bitte? Richtig: Es sieht nach einem „Split Brain“ aus. Dadurch würde eigentlich jegliche Kommunikation mit dem entsprechenden Subnetz unmöglich. Nicht so dank der Fähigkeiten von LISP. Schauen Sie sich hierzu die Abbildung 3 an.

Alle Access-Netze tragen dieselbe IP-Netzwerkadresse und Subnetzmaske. Mehr noch: Die xTR haben aus Sicht der Clients alle dieselbe IP-Adresse (z.B. 192.168.2.1) und MAC-Adresse. In dieser Hinsicht ähnelt das Verfahren also den Protokollen zur Router-Redundanz, wie dem Virtual Router Redundancy Protocol (VRRP) oder seinem Cisco-Pendant HSRP (Hot-Standby Router Protocol). Aus Sicht der Clients ist die Sache also einfach. Egal, in welchem physischen Netz sie sich befinden, das Default Gateway wird immer erreicht. Cisco bezeichnet das als „Anycast Gateway“.

Da nun alle Access-Netze dieselbe Adresse tragen, kann es für diese Netze keine Einträge mehr im Map Server geben. Es lässt sich kein eindeutiger RLOC für ein Netz bestimmen. Es gibt nur noch Host-Einträge, denn Hosts lassen sich eindeutig einem Access-Netz und seinem ETR bzw. RLOC zuordnen. Auf der Seite des Rechenzentrums könnte das grundsätzlich genauso sein, wenn der xTR unmittelbar mit dem Layer-2-Segment in Verbindung stünde, an dem sich auch die Server befinden. Wird dazwischen geroutet, erscheinen wie gehabt ganze Netze im Map Server, wie in Abbildung 3 dargestellt. Zur Unterscheidung der Funktionsweise, werden ETR bzw. ITR hier mit dem Zusatz „Proxy“ belegt, kurz also PxTR.

Wenn Sie nun die oben beschriebene Standard-LISP-Prozedur durchspielen, werden Sie nachvollziehen können, dass Clients in Access-Netzen erfolgreich

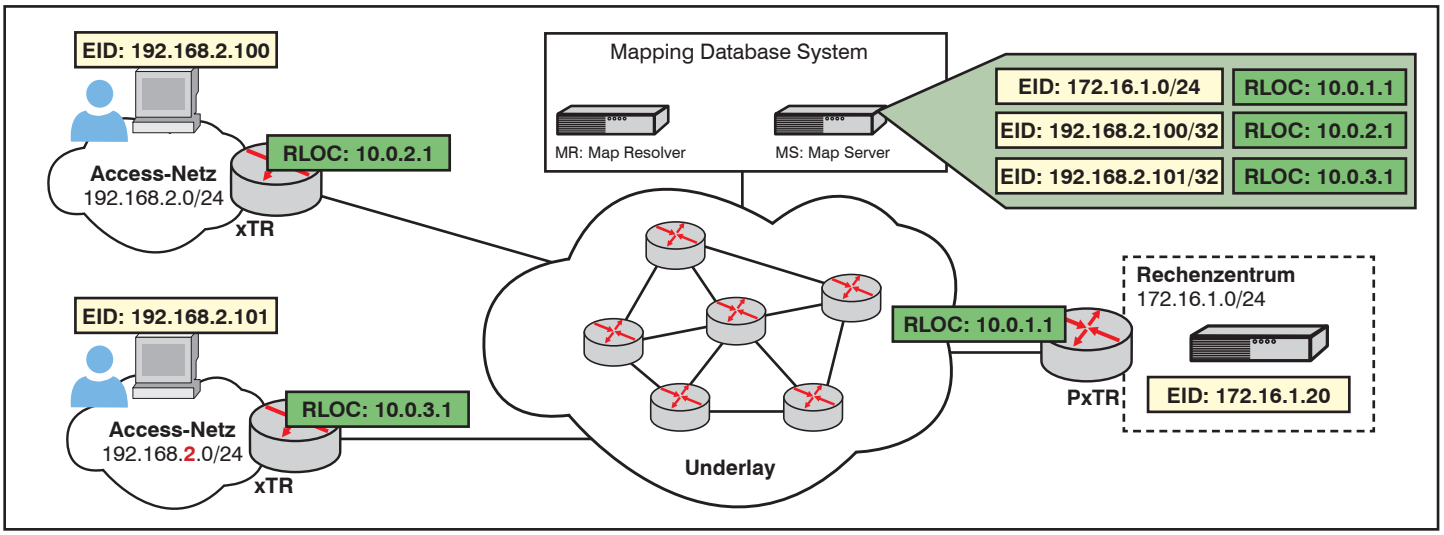


Abbildung 3: Grundzüge der Realisierung von LISP in der Cisco Campus Fabric

mit Servern im Rechenzentrum kommunizieren können und umgekehrt. Und wir haben nun eine Lösung für das Problem des Kunden, der die 100 auf zwei Gebäude und sechs Etagen verteilten Mitarbeiter der Anwendungs-Entwicklung in einem einzigen Subnetz zusammenfassen möchte.

Ein wichtiger Aspekt fehlt jedoch noch: Was ist, wenn zwei Clients in unterschiedlichen Access-Netzen direkt miteinander kommunizieren wollen? Wie funktioniert Peer-to-Peer-Kommunikation, wie z.B. bei Voice und Video? Hier würde der Client nicht das Default Gateway ansprechen, sondern stattdessen per ARP (Address Resolution Protocol) oder mit dem IPv6-Pendant Neighbor Discovery Protocol (NDP) direkt nach der IP-Adresse des Kommunikationspartners suchen, um dessen MAC-Adresse herauszufinden. In diesem Fall muss der lokale xTR an Stelle des Client antworten, wollte man nicht ARP Requests oder Neighbor Solicitations in alle anderen Access-Netze übertragen oder mit Hilfe des Map Resolvers auflösen. Der Router wird damit zum ARP bzw. NDP Proxy. Das Feature heißt bei Cisco „Local Proxy ARP“, da hierbei auf die IP-Adressen des angeschlossenen Subnetzes geantwortet wird und nicht auf alle anderen (wie normalerweise bei Proxy ARP). Cisco Campus Fabric emuliert also Layer-2-Netze, was die Wahl des Begriffs „Fabric“ erklärt. Damit bezeichnen Hersteller Gebilde aus Switches, die übergreifend eine Layer-2-Konnektivität bereitstellen, als handele es sich um einen einzigen ausgedehnten Layer-2 Switch. Genau genommen handelt es sich zwar nur um “Private VLANs”, die dank Local Proxy ARP am Ende doch miteinander kommunizieren können, aber das tut letztlich nichts zur Sache.

LISP an sich ist jedoch eine Routing-Technik. Insbesondere lassen sich in LISP nur IP-Pakete enkapsulieren. Der RFC 6830 nennt explizit die beiden Adress-Familien IPv4 und IPv6 und nicht mehr. Insbesondere keine MAC-Pakete. Das mag der Grund dafür sein, dass Cisco sich gegen das Enkapsulieren in LISP entschieden hat und stattdessen VXLAN gewählt hat. Abbildung 4 verdeutlicht den Unterschied. Enkapsuliert man ein Paket in LISP, geht der MAC Header verloren. In VXLAN bleibt er erhalten.

Allerdings wird der ursprünglich MAC Header bereits dadurch verändert, dass der ITR das Paket entgegennimmt. Jeglicher IP-Router überträgt eben nur IP-Pakete, ohne MAC Header. Für die Enkapsulierung hätte Cisco also grundsätzlich auch LISP wählen können, ohne die Funktionsweise der Campus Fabric zu beschränken – jedenfalls soweit ich sie bis hierher dargestellt habe. Vielleicht liegt der Grund für die Wahl der VXLAN-Enkapsulierung darin, dass im VXLAN Header etliche Bits als „reserved“ markiert sind. Sie sind also frei für spätere Nutzung. Und tatsächlich trägt Cisco dort eigene Informationen ein. Vielleicht liegt der Grund auch einfach in der Hardware begründet. Damit eine hohe Performance erzielt wird, sollten Switches Pakete mit ihrer Hardware weiterleiten und entsprechend modifizieren. Und für VXLAN, also die VXLAN Tunnel Endpoints (VTEP), hat Cisco bereits aus anderen Projekten entsprechende Implementierungen, die sich nun ohne weiteres für Campus Fabric nutzen lassen.

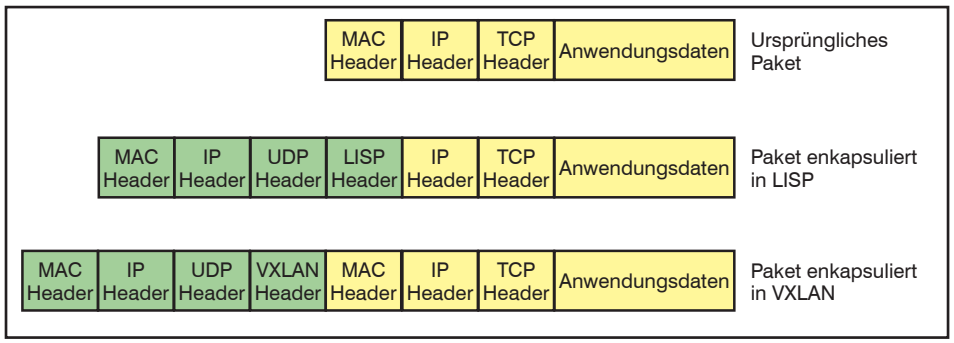


Abbildung 4: Enkapsulierung eines Pakets in LISP und VXLAN

Implementierung von Cisco Campus Fabric

Cisco unterstützt Campus Fabric auf seinen bekannten LAN Switches und Routern. Wesentliche Elemente der Lösung konnten also offensichtlich in Software realisiert werden, so dass in relativ kurzer Zeit eine recht breite Produktunterstützung gegeben ist. Folgende Elemente gibt es in der Campus Fabric (siehe Abbildung 5):

- Edge Nodes sind die Access Switches, mit denen die Access-Netze realisiert werden. Edge Nodes enthalten die LISP Router xTR und sind letztlich auch Teil des gerouteten Underlay. Es handelt sich also um typische Access Switches mit Layer-3-Funktionalität. Darüber hinaus ist die Fähigkeit der Port-basierten Zugangskontrolle (Network Access Control, NAC) für Campus Fabric nützlich, dazu später mehr. Als Edge Nodes eignen sich einige modulare und nichtmodulare High-End Access Switches von Cisco.
- Intermediate Nodes sind Standard Layer-3 Distribution und Core Switches ohne zusätzliche Anforderungen.

Sonderveranstaltung

Wireless und Mobility
18.10. - 19.10.2017 in Bonn

Das IoT, autonome Mobilität und neue Arbeitsplatzmodelle verändern die Anforderungen an flächendeckende Wireless Infrastrukturen dramatisch. Neue WLAN-Techniken und 5G Mobilkommunikation führen zu einem neuen Universum für die Versorgung von menschlichen und maschinellen Teilnehmern. Die Sonderveranstaltung widmet sich mit herausragenden Referenten diesem hoch dynamischen Problemkreis.

Moderation: Dr. Franz-Joachim Kauffels
Preis: 1.990,-- € netto

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

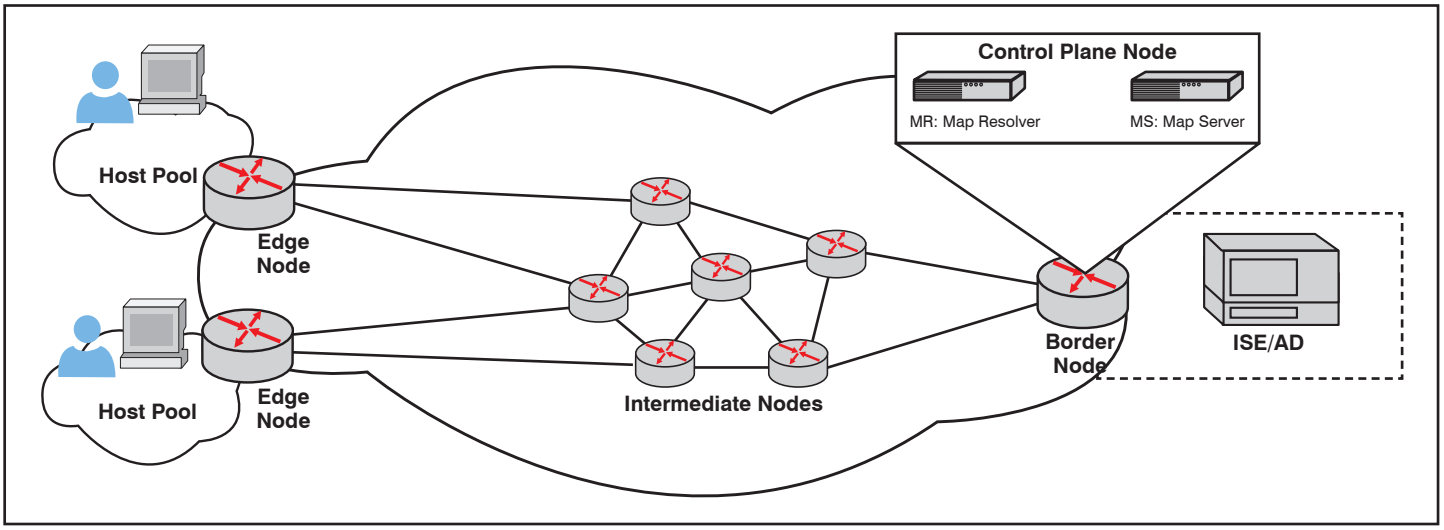


Abbildung 5: Elemente der Cisco Campus Fabric

- Die Kopplung der Campus Fabric in Richtung von Rechenzentrums-Netzen wird von den so genannten Border Nodes realisiert. Als Border Nodes sind die großen modularen Switches aus dem Campus- und RZ-Portfolio geeignet. Aber auch bestimmte Router und nicht-modulare High-End Access Switches können diese Funktion wahrnehmen.

- Map Resolver und Map Server werden als Control Plane bezeichnet. Diese Funktionen sind in der Switch Software realisiert. Die meisten der als Border Nodes geeigneten Switches können auch Control Plane Nodes sein.

- Die von der Control Plane verwaltete Datenstruktur bezeichnet Cisco als Host Tracking Database (HTDB).

Wie bereits erwähnt, wird NAC im Zusammenhang mit Campus Fabric unterstützt. Das wird sogar als der wesentliche Vorteil der Lösung angesehen. Nach Authentisierung am Switch Port wird der Client einem Host Pool zugewiesen. Darunter versteht Cisco die Access-Netze, die zu einer Benutzergruppe gehören. Alle Clients einer Benutzergruppe teilen sich also eine Fabric. Der Border Node routet die Pakete der Fabric in ein entsprechendes virtuelles Netz (VRF), über das letztlich die Server erreicht werden.

Der Charme daran ist aus meiner Sicht die einfache Konfiguration. Alle Edge Nodes können nämlich gleich konfiguriert werden. Wird ein zusätzlicher Edge Node benötigt, kopiert man die Konfiguration von einer Vorlage und passt die Loopback-Adresse für das Routing im Underlay an. Es brauchen keine VRF oder VLANs eingerichtet zu werden. Switch Virtual Interfaces (SVIs) haben auf allen Switches dieselben IP-Adressen (Anycast Gateway).

Sozusagen als Gegenleistung für diese Einfachheit muss man die Security-Lösung „TrustSec“ von Cisco implementieren, die auf der Identity Services Engine (ISE) als zentralem Element basiert. TrustSec nutzt zur Klassifizierung von Daten unter anderem ein proprietäres Informations-Element, das Scalable Group Tag (SGT), das im VXLAN Header mit übertragen wird. Letztlich ermöglicht die Tatsache, dass Pakete durch das Underlay getunnelt werden, also erst die Übertragung des SGT und somit die Qualifizierung des Datenverkehrs an zentralen Firewall-Elementen, ohne dass man wie bisher IP-Adressen und TCP-Portnummern dafür heranziehen müsste. Und damit sich das alles noch verwalten lässt, bietet Cisco mit dem DNA Center [1] gleich die passende Management-Lösung mit an.

Weitere Aspekte

Campus Fabric ist, wie gesagt, ein Overlay. Pakete werden enkapsuliert über ein Underlay übertragen. Durch die Enkapsulierung werden die Pakete länger (vgl. Abbildung 4). Diesen Effekt kennen Sie von allerlei VPN-Techniken. Normalerweise bekommt man davon wenig mit, weil die enkapsulierenden Elemente Router sind. Übliche Betriebssysteme unterstützen zu diesem Zweck das Verfahren der Path MTU Discovery (RFC 1191 bzw. RFC 8201 für IPv6) , welches die maximale Paketlänge (Maximum Transmission Unit) auf dem Weg zum Ziel bestimmt. Hierzu wird das Don’t Fragment Bit im IP Header gesetzt, und der Router teilt dem Absender mit, wenn er das Paket verwerfen musste.

Im Gegensatz dazu emuliert die Campus Fabric eine Layer-2-Technik. Dennoch scheint Path MTU Discovery unterstützt zu werden, schließlich sind alle Edge Nodes auch Router. Cisco empfiehlt jedoch, dass im Underlay eine größere MTU eingestellt wird als die im Ethernet normalerweise verwendeten 1500 Bytes. Es sollten also auf allen Switches des Underlay wie auch auf den Border und Edge Nodes Jumbo Frames aktiviert werden.

Das Emulieren von Layer-2-Netzen impliziert eigentlich auch die Unterstützung von Broadcasts und Multicasts. Damit sieht es bei LISP schlecht aus, denn es gibt keine Funktion, zur Verteilung solcher Pakete (LISP ist eine Layer-3-Technik). Cisco ermöglicht es dennoch, Multicasts für bestimmte Host Pools zu aktivieren. Die Verteilung von Multicasts erfolgt durch den ITR an alle ETR. Damit das Paket hierfür im Underlay nicht wiederholt ausgesandt werden muss, wird es per IP Multicast an die ETR verteilt. Das Underlay muss also über die Fähigkeit des Multicast Routing verfügen.

Eine weitere Einschränkung muss bezüglich DHCP hingenommen werden. Normalerweise gibt es in gerouteten Netzen die Funktion des DHCP Relay Agent, die in Routern implementiert ist, die als Default Gateways für Clients wirken. Empfängt der Relay Agent einen DHCP Request als Broadcast, wandelt er ihn in ein Unicast-Paket um, das an die IP-Adresse des DHCP Servers gesandt wird. Gleichzeitig trägt der Relay Agent die IP-Adresse des Interface, auf dem er den Broadcast empfangen hatte, in ein entsprechendes Feld im DHCP Header ein. An dieser Adresse erkennt der DHCP Server, aus welchem Topf („Scope“) er eine IP-Adresse herausnehmen und dem Client anbieten soll.

Dieses Verfahren funktioniert laut Cisco im Zusammenhang mit Campus Fabric nicht. Als Grund wird angegeben, dass als Ab-

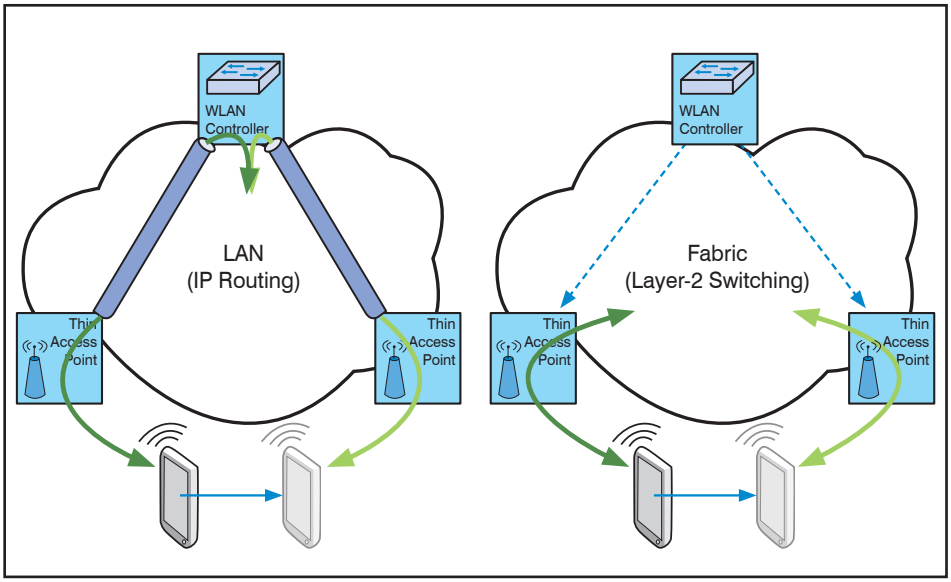


Abbildung 6: WLAN Roaming in Layer-2 Fabrics

senderadresse für DHCP nur die Loopback-Adresse des Edge Node in Frage kommt, die bekanntlich in keinem Zusammenhang zum IP-Netz des Host Pool steht. Stattdessen muss hier die DHCP Option 82 verwendet werden, in die der Relay Agent eine sogenannte Circuit ID einträgt. Damit wird das VLAN bzw. Subnetz bezeichnet, für das der DHCP Server eine IP-Adresse anbieten soll. Selbstverständlich muss dieses Verfahren von Ihrem DHCP Server unterstützt werden, und Sie müssen es entsprechend einrichten.

Zuletzt weise ich noch auf einen interessanten Nebeneffekt des Einsatzes von Cisco Campus Fabric auf WLAN hin. Bekanntlich werden WLAN seit Jahren auf Basis von WLAN Controllern aufgebaut. Die Access Points tunneln alle Pakete zum Controller. Damit realisiert der WLAN Controller sozusagen eine WLAN Fabric, also ein virtuelles Layer-2-Netz über alle Access Points. Mobile Endgeräte können sich von Access Point zu Access Point hangeln, ohne ihre IP-Adressen anpassen zu müssen. Ich habe mich zur Darstellung eines Bildes aus meinem Insider-Artikel vom September 2013 bedient (Abbildung 6). Auf der linken Seite erkennt man das Prinzip des WLAN Controllers mit zentraler Data Plane. Der gesamte WLAN Traffic läuft über den Controller, was diesen an die Grenze seiner Performance bringen kann.

Zur Abhilfe dieses Problems bieten die Hersteller schon seit langem die Option des Local Bridging [2] an. Hierbei leitet der Access Point den Datenverkehr direkt ins LAN. Der WLAN Controller dient einzig noch dem Management der Access Points. Der Nachteil dieses Verfahrens war bisher der Verzicht auf Mobilität, denn WLAN-Endgeräte mussten beim Wechsel zu einem anderen Access Point im Allgemeinen eine neue IP-Adresse anfordern. Nicht so mit einer Fabric (Abbildung 6 rechte Seite). Hier wird das Layer-2 Overlay durch die Fabric bereitgestellt. Alle Access Points können den mobilen Endgeräten dasselbe IP-Subnetz anbieten. Die volle Performance der über das Underlay vermaschten Fabric steht damit auch dem WLAN zur Verfügung. Leider wird diese Variante von Cisco Campus Fabric offensichtlich nicht unterstützt – wie schade. Über die Gründe kann nur spekuliert werden. Möglicherweise dauert der Vorgang der Client-Registrierung durch den ITR zu lange oder man fürchtet eine Überlastung der Control Plane durch häufiges WLAN Roaming.

Zusammenfassung

Cisco stellt mit dem Produkt Campus Fabric eine Technik vor, mit der sich Access-Netze und die zugehörigen IP-Subnetze auf beliebigen Access-Ports eines Campus bereitstellen lassen. Die Bereitstellung lässt sich statisch einrichten oder dynamisch mit Hilfe der Möglichkeiten von Cisco TrustSec. Zur Implementierung können viele Switches des bereits existierenden Cisco-Portfolios eingesetzt werden. Jedoch benötigen die Switches – insbesondere auch die Access Switches – erweiterte Routing Funktionen. Es steht also nicht zu erwarten, dass Campus Fabric eine Low-Cost-Lösung sein wird.

Die Fähigkeit, IP-Subnetze auf beliebigen Access-Ports eines Campus bereitstellen zu können, ist für Netze, bei denen Endgeräte verschiedener Benutzergruppen bzw. Sicherheitszonen sich ein LAN teilen, hilfreich. Die Konfiguration der Netzkomponenten wird dadurch vereinfacht. So lassen sich bei Umzügen benötigte Anschlüsse in kurzer Zeit über ein zentrales Management bereitstellen, was Cisco veranlasst, diese Technik als Software-defined Access (SDA) zu titulieren.

Redundanzfunktionen des der Campus Fabric unterliegenden Netzes basieren auf den bekannten und bewährten Routing-Algorithmen. Entsprechende Konfiguration vorausgesetzt, lassen sich im Fehlerfall schnelle Wiederherstellungszeiten garantieren. Probleme, die in ausgedehnten Layer-2-Netzen durch Schleifenbildung entstehen können, werden durch das Routing-basierte Tunnelprinzip vermieden.

Basis der Datenübertragung (Data Plane) ist Virtual Extensible LAN (VXLAN). Als Control Plane der Campus Fabric hat Cisco das ansonsten recht unbekannte Label/ID Separator Protocol (LISP) gewählt. Genau genommen ist das meines Erachtens die erste wirklich sinnvolle Anwendung von LISP überhaupt. Dennoch stellt sich die Frage, wieso Cisco ausgerechnet dieses Protokoll verwendet. Im Data Center wird mit Ethernet VPN (EVPN) eine Technik mit vergleichbaren Zielen angeboten, die einerseits ebenfalls auf VXLAN basiert, andererseits das Border Gateway Protocol (BGP) als Data Plane verwendet. Außerdem verfügt Cisco mit Fabric Path über eine weitere Layer-2 Fabric. So läge es nahe, eine dieser Techniken auch im Access anzubieten. Cisco wendet ein, dass im Access-Bereich das LISP geeigneter sei, weil hierfür letztlich weniger Rechenleistung auf den Komponenten benötigt werde.

Wie dem auch sei, ich finde die Lösung technisch interessant. Ob allerdings die damit einhergehende enge Bindung an den Hersteller Cisco Systems und seine umfassenden Management- und Security-Lösungen am Ende gerechtfertigt ist, muss von Fall zu Fall abgewogen werden. Ich bin jedenfalls gespannt, ob der Campus Fabric eine breite Akzeptanz gegönnt sein wird.

Erläuterungen

[1] Das DNA Center ist der Nachfolger des Application Policy Infrastructure Controller Enterprise Module (APIC-EM). „DNA“ steht hier für Digital Network Architecture.

[2] Bei Cisco als Flex Connect bezeichnet

Aktuelle Sonderveranstaltung

Sonderveranstaltung Wireless und Mobility 18.10. - 19.10.2017 in Bonn

Die ComConsult Akademie veranstaltet vom 18.10. bis 19.10.2017 ihre Sonderveranstaltung "Wireless und Mobility" in Bonn.

Das IoT, autonome Mobilität und neue Arbeitsplatzmodelle verändern die Anforderungen an flächendeckende Wireless Infrastrukturen dramatisch. Neue WLAN-Techniken und 5G Mobilkommunikation führen zu einem neuen Universum für die Versorgung von menschlichen und maschinellen Teilnehmern.

Die Sonderveranstaltung widmet sich mit herausragenden Referenten diesem hoch dynamischen Problemkreis.

Die Positionierung von Wireless-Netzwerken ist in einem starken Wandel von einer Ergänzungs- hin zu einer Haupt-Kommunikationsstruktur. Die Auslöser dieser Entwicklung kommen aus verschiedenen Bereichen ausgehend von IoT, Gebäude-Automatisierung bis hin zu flexiblen und mobilen Arbeitsplätzen.

Dementsprechend ändern sich die Standards und die Planungsansätze. Und gleichzeitig müssen wir Wireless immer mehr als Spektrum sich ergänzender Technologien sehen. Von Bluetooth über ZigBee zum WLAN und von da zum Mobilfunk.

Das Ergebnis: eine Zukunfts-taugliche Wireless-Infrastruktur erfordert eine abgestimmte Gesamtplanung, die zudem auf den zukünftigen Bedarf ausgelegt ist.

Hier setzt unsere Sonderveranstaltung Wireless und Mobilty an. Wir analysieren und diskutieren mit Ihnen:

- Mit welchen Verkehrsvolumina müssen wir rechnen? Was ändert sich? Wie können wir den Zukunftsbedarf erfassen und beherrschen?
- Wie wird sich die Zahl zu vernetzender Endpunkte verändern? Welche Anwendungen werden damit verbunden sein?
- In welchem Umfang ist das traditionelle WLAN darauf vorbereitet? Was kann getan werden, um seine Zukunfts-Tauglichkeit zu verbessern?
- Wie kann WLAN in Zukunft gegenüber dem Mobilfunk abgegrenzt werden? Oder gibt es einen integrierten Planungsansatz?
- Welche Konsequenzen bringt Gebäudeautomatisierung mit Anwendungen wie Beacons und zusätzlichen Netzwerktypen wie ZigBee oder Bluetooth mit sich?
- Gibt es eine Chance für eine flächendeckende Wireless-Infrastruktur mit einem Technologie-Mix für ein Gebäude?
- Welche neuen Perspektiven bieten neue Technologien wie die Übertragung im Millimeterbereich? Brauchen wir derartige Mikrozellen?

Die Zellen-Technologien sind aber nur die eine Seite der Medaille. Wichtige Themen zur Infrastruktur sind also mindestens:

- Struktur und Betrieb angemessener Backbones
- Sicherheit als Gesamtkonzept für Wireless
- Taktische und rechtliche Sicherheit
- Wirkung der Technologien auf Menschen

Die ComConsult Sonderveranstaltung „Wireless und Mobility“ ermöglicht Ihnen die Diskussion all dieser Themen mit hochkarätigen, erfahrenen Spezialisten.

Die Referenten


Dr. Jan Byok


Dipl.-Ing. Stefan Bien


Dr. Johannes Dams


Christian Gauer


Dipl.-Ing. Olaf Hagemann


Dr. Simon Hoff


Reinhard Lichte


Dipl.-Ing. Michael Schneiders


Dipl.-Inform. Thomas Steil


Dr. Joachim Wetzlar

Moderation

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 sowie über 2000 Artikeln, Videos und Reports.

Programmübersicht Wireless und Mobility

Mittwoch 18.10.17

9:30 Uhr

Wireless: Basis für Disruption und Agilität

- Mobilität: Grundlage neuer Arbeitsplatzmodelle
- Neue Anwendungsbereiche und ihre Anforderungen
- IoT und die enge Verbindung zum Mobilfunk
- Der Weg zu 5G über LTE und LTE Advanced
- Wichtige Elemente von 5G schon 2018: 5G-LTE
- Koexistenzfragen von LTE/5G und WLANs als Mikrozellen

Dr. Franz-Joachim Kauffels, Technologie-Analyst

10:30 Uhr

WLANs zwischen Altlasten und Hoffnung

- IEEE 802.11ac in den verschiedenen Geschmacksrichtungen
- Ist mit 10 Gbit/s auf 2,4 und 5 GHz Schluss oder geht zukünftig noch mehr?
- WLAN im 60-GHz-Band: Es gibt Standards, aber kaum Anwendungen
- Was sagt die IEEE zur Mobilfunk-Integration?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:30 Uhr Kaffeepause

12:00 Uhr

Netz-Architekturen für (High Speed) WLANs

- Welche Anforderungen bestehen an die Netzarchitektur für den Aufbau von WLANs? • Der WLAN-Controller: Flaschenhals oder Mittel der Wahl?
- Alternativen zum WLAN Controller: Was bieten die Hersteller?
- IEEE 802.3bz: Seit dem 27.09.2016 gibt es „Breitreifen“ für Access Points

Dipl.-Ing. Michael Schneiders, ComConsult Beratung und Planung GmbH

13:00 Uhr Mittagspause

14:30 Uhr

WLAN-Zellplanung auf dem Prüfstand

- Welchen Stellenwert hat die WLAN-Zellplanung bei der Konzeptionierung einer WLAN-Infrastruktur?
- Welche Parameter sind bei einer professionellen WLAN-Zellplanung zu berücksichtigen?
- Ausleuchtungsmessung vs. Simulation
- Häufige Fehler, die Sie unbedingt vermeiden sollten. Dos and Don‘ts

Dipl.-Ing. Stephan Bien, ComConsult Beratung und Planung GmbH

15:15 Uhr

Kritisches Infrastrukturelement:
PoE für höhere Geschwindigkeiten

- Was leistet PoE nach dem heutigen Stand der Technik?
- Neue Einsatzgebiete erobern den Markt. Welche Herausforderungen sind damit verbunden und wie können wir sie gewinnbringend nutzen?
- Welche planerischen Maßnahmen ergeben sich aus dem flächendeckenden und Gewerke übergreifenden Einsatz von PoE? • Hohe Datenraten vs. PoE. Was nicht passt, wird passend gemacht
- IEEE 802.3bt: Die Revolution für den Arbeitsplatz der Zukunft?

Dipl.-Ing. Stephan Bien, ComConsult Beratung und Planung GmbH

16:00 Uhr Mittagspause

16:30 Uhr

Intelligenz im Gebäude: Sensoren, Beacons, Cloud - macht das Sinn?

- Aktuelle Situation bei modernen Gebäuden - Protokolle und Hardware
- Indoor Navigation und Asset Tracking (Technologien dafür z.B.: Beacons)
- Datensammlung und Schutzbedarf der Daten
- Scheinkorrelation und Beispiele für sinnvolle Datenkorrelationen --> Heatmaps • Cloud Dienste und Mehrwert
- Fazit und Ausblick: MetaCloud --> eine zentrale Anlaufstelle für den Betrieb, eine API für die App

Dipl.-Inform. Thomas Steil, ComConsult Beratung und Planung GmbH

Genaue Lokalisierung mobiler Endgeräte mit WLAN oder Bluetooth LE Beacons

- Unterscheidung zwischen Lokalisierung mittels WLAN und BLE Beacons
- WLAN: Welche Genauigkeit lässt sich bei der Lokalisierung von WLAN Endgeräten erreichen?
- WLAN: Cisco Hyperlocation – Angle-of-Arrival Auswertung von Datenframes erlaubt eine Steigerung der Genauigkeit auf 1-3m
- BLE: Cisco Virtual Beacon Solution – weniger Hardware Beacons und wie Machine Learning den RF-Fingerprint ersetzt.

Christian Gauer, Cisco Systems GmbH

Donnerstag 19.10.17

9:00 Uhr

Sicherheit im WLAN:
Es gibt immer noch Herausforderungen!

- Warum traditionelle Hotspots so gefährlich sind
- Sichere Hotspots mit Hotspot 2.0: Wie funktioniert EAP-SIM in der Praxis?
- Lücken in IEEE 802.11i / WPA2
- Fallstricke bei der kombinierten Maschinen- und Nutzerauthentisierung mit IEEE 802.1X
- Neue Entwicklungen bei EAP: TEAP und Co.
- Was kommt nach WPA2?
- WLAN Security im IoT braucht neue Konzepte: DPP, Passpoint, ...

Dipl.-Inform. Daniel Prinzen, ComConsult Beratung und Planung GmbH

9:45 Uhr

Mobile Netzwerke sind mehr als nur WLAN –
Lokationsabhängige Interaktionen mit
Anwendern durch Einsatz von Beacons und Apps

- Eine Infrastruktur, ein Management für WLAN und BLE Beacons
- Verschiedene Wege zur eigenen Unternehmens App mit Lokationsdiensten - von einfach bis komplex
- Neue Services für Anwender durch den Einsatz von Beacons live gezeigt
- Asset Tracking als integrierter Bestandteil einer Beaconlösung
- Branchenbezogene Beispiele: Gesundheitswesen, Retail, Unternehmensnetze

Reinhard Lichte, HPE Aruba Germany

10:30 Uhr Kaffeepause

11:00 Uhr

WLAN als Teil eines Software Defined Enterprise Networks

- Einheitliches Management und Zugangskontrolle für LAN und WLAN
- Automatische Kontrollmechanismen bis auf Applikationsebene
- On-Premise vs. Cloud
- Wireless IDS/IPS
- Wie sieht die Zukunft aus?

Dipl.-Ing. Olaf Hagemann, Extreme Networks GmbH

11:45 Uhr

WLAN und Mobilfunk als Gesundheitsrisiko?!

- Begriffe erklärt: SAR-Wert und Leistungsflussdichte
- Wovor schützt uns der Gesetzgeber?
- Gefahren der Funkwellen jenseits amtlicher Grenzwerte
- Messtechnik und Nachweis
- Empfehlungen zum Schutz der Mitarbeiter

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:15 Uhr Mittagspause

13:45 Uhr

Rechtliche Aspekte des Betriebs privater WLAN-Infrastrukturen

- Grundlagen der deutschen Störerhaftung
- Neueste Entwicklungen im Bereich der Störerhaftung
- Zukunft der deutschen Störerhaftung
- Praxistipps zum Betrieb privater WLAN-Infrastrukturen

Dr. Jan Byok, Bird & Bird LLP

14:30 Uhr

5G: Anforderungen, Architektur, Standardisierung

- Mobilfunk: Stütze der nächsten digitalen Revolution
- Anwendungsszenarien und Minimalanforderungen nach ITU IMT-2020
- Stand der Standardisierung und Ergebnisse aus den Feldversuchen
- Network-Slicing und Software-basiertes Architekturmodell
- AI für automatisierte Funktionen in Network Management und Operations

Dr. Franz-Joachim Kauffels, Technologie-Analyst

15:30 Uhr Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor

Report- Neuerscheinung (2. Auflage) zur Sonderveranstaltung

Wireless-Systeme der nächsten Generation

Anwendungen, Systeme, Anforderungen

von Dr. Franz-Joachim Kauffels

Mit Ihrer Seminarbuchung der Sonderveranstaltung "Wireless und Mobility" können Sie die Neuauflage (August 2017) des Reports "Wireless-Systeme der nächsten Generation" zum vergünstigten Paketpreis erwerben.

Dieser Report ist ein unverzichtbares Hilfsmittel für alle, die sich mit der Schaffung von Wireless Versorgungsstrukturen für die Anforderungen der digitalen Zukunft zu rüsten. Die Studie hilft, die neuen drahtlosen Übertragungstechniken und ihre Wechselwirkungen besser einzuschätzen und die passende Infrastruktur vorzubereiten.

Die Neuauflage befasst sich zusätzlich ausführlich mit der kommenden 5G-Technologie, möglichen Varianten, Anwendungsfeldern und Implikationen. Durch 5G bleibt letztlich kein Stein mehr auf dem anderen. Zusätzlich gibt es ein neues Kapitel, welches den aktuellen Erkenntnisstand hinsichtlich möglicher Wechselwirkungen der vielen neuen Funksysteme auf den menschlichen Organismus darstellt.

Der Report ist dadurch von fünf auf sieben Kapitel angewachsen.

Im ersten Kapitel betrachten wir die Entwicklung von Anwendungen und Anforderungen. Das zweite Kapitel ist der aktuell neu verfügbaren WLAN-Technik, primär IEEE 802.11ac ab „Wave 2“ gewidmet. Kapitel drei beleuchtet die Entwicklung kleinerer Funkzellen und Mikrozellen im Millimeterwellen-Bereich (50 bis 60 GHz-Bänder).

2. aktualisierte und deutlich erweiterte Auflage August 2017

Hier können leicht Multigigabit-Leistungen erreicht werden, aber eben verbunden mit recht geringen Ausdehnung der Zellen. IEEE 802.ad „WiGig ®“ ist der erste Repräsentant dieser Systemklasse.

Die Zukunft wird allerdings durch die Entwicklung der Mobilfunksysteme deutlich stärker geprägt als durch die der WLANs. Ausgehend von LTE gibt es eine Reihe von Weiterentwicklungen in neuen Releases, einschließlich der Möglichkeit des Vordringens von Providern in lizenzfreie Bereiche, die bislang den WLANs vorbehalten waren. Kapitel vier stellt diese Entwicklungen dar. Es wird klar, dass hier die Messlatte für die mobile Kommunikation deutlich höher gelegt wird.

Neben LTE auf dem Weg zu 5G wird es neue WLAN-Techniken mit deutlich mehr Leistung und höherer Qualität geben, wie IEEE 802.11ax und IEEE 802.11ay. In Kapitel 5 beleuchten wir, was das in Zukunft für die unterstützenden Infrastrukturen, besonders in Unternehmen, bedeutet. Mittelfristig ist mit einer notwendigen Versorgungsleistung für WLAN-Zellen von mindestens 10 Gbit/s. zu rechnen.

5G ist nicht nur einfach eine weitere Mobilfunktechnologie, sondern spannt ein völlig neues Universum der Mobilkommunikation und ihrer Möglichkeiten auf. Natürlich wird es auch eine „verbesserte“ Handy-Kommunikation geben, aber die eigentliche Herausforderung ist die Versorgung von Milliarden neuer Mobilstationen im Rahmen von IoT. Ein autonomes Auto erzeugt bis zu 60 GByte Daten pro Stunde, ein Wärmezähler vielleicht 1000 Bit/Monat. Tauchen Sie mit diesem Report in die Welt der Anwendungen, Möglichkeiten und technischen Lösungen dafür ein. Übrigens: die Standardisierung wird in wichtigen Teilen von 2020 auf 2018 vorgezogen. Seit es Funksysteme mit größerer Ausbreitung gibt, machen sich viele Menschen Sorgen um die möglichen Schäden für ihre Gesundheit. In letzter Zeit ist es vermehrt zu einer Ballung und Verdichtung solcher Systeme gekommen, die bei Manchen sogar Angst oder andere psychologische Wirkungen hervorgerufen hat, die sie in Leben und Arbeit negativ beeinflusst haben. Der Report blickt auf den aktuellen Stand der Forschung und gibt Anhaltspunkte zur weiteren Recherche.

Anmeldung an kundenservice@comconsult-research.de

Wireless und Mobility

Ich buche die Sonderveranstaltung
Wireless und Mobility

☐ 18.10. - 19.10.2017 in Bonn
zum Preis von 1.990,-- €

☐ inklusive Report "Wireless-Systeme der nächsten Generation"
zum Teilnehmer Sonderpreis von 298,-- €

☐ Bitte buchen Sie mir ein Hotelzimmer

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

ComConsult Veranstaltungskalender

IP-Wissen für TK-Mitarbeiter, 18.09. - 19.09.2017 in Düsseldorf

Garantietermin

Dieses Seminar vermittelt TK-Mitarbeitern ohne Vorkenntnisse im Bereich LAN und IP das erforderliche Wissen zur Planung und zum Betrieb von VoIP-Lösungen. Die Inhalte sind so gegliedert, dass Sie die Grundlagen schnell verstehen. Es werden die wichtigsten VoIP-spezifischen Aspekte vorgestellt und unter praxisrelevanten Gesichtspunkten beleuchtet. Die Themen erstrecken sich von IP und LAN-Grundlagen hin zu praxisrelevanten Themen wie QoS, Jitter und Bandbreiten-Fragen. Ziel ist es dem IP-Unkundigen die wichtigen Grundlagen der Netzwerktechnik kompakt und praxisnah zu vermitteln.

Preis: 1.590,-- €*

Lokale Netze für Einsteiger, 18.09. - 22.09.2017 in Aachen

Garantietermin

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Der Intensiv-Kurs vermittelt die notwendigen theoretischen Hintergrundkenntnisse, vermittelt den praktischen Aufbau, den Betrieb eines LANs und vertieft die Kenntnisse durch umfangreiche, gruppenbasierende Übungsbeispiele. Ausgehend von einer Darstellung von Themen der Verkabelung und Übertragungsprotokolle wird die Arbeitsweise von Switch-Systemen, drahtloser Technik, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: 2.490,-- €*

Sonderveranstaltung: Herausforderung Informationssicherheit – Cloud Computing, Security as a Service, Virtualisierung, 25.09.2017 in Bonn

Garantietermin

In diesem Seminar analysieren und bewerten wir für Sie: Cloud Computing: Wie kann eine sichere Nutzung der Cloud ohne signifikanten Kontrollverlust erfolgen? Wie sehen die technischen Lösungsbausteine für Cloud-Sicherheit aus? Security as a Service: Wo ist der Mehrwert von Cloud-basierten Sicherheitslösungen? Wo sind die Grenzen? Wie kommt man zu einer integrierten Gesamtlösung? Risikobereich Virtualisierung: Wo sind die Angriffspunkte – Hypervisor, Container, VM, Speicher, Netzwerk? Wie sehen die Lösungen aus? Was bedeutet das für Zonenkonzepte?

Preis: 1.090,-- €*

Sonderveranstaltung: Herausforderung Informationssicherheit – IoT, Abwehr von Angriffen, rechtliche Rahmenbedingungen, 26.09.2017 in Bonn

Garantietermin

In diesem Seminar analysieren und bewerten wir für Sie: Albtraum Internet of Things: Wie kritisch sind ungesicherte Endgeräte? Welche Sicherheit bieten neue Technologien wie 5G? Welche Handlungsmöglichkeiten bestehen? Zielgerichte Angriffe, die Kür des Sicherheits-Managements: Wie erfolgen Sie? Wie können Sie verhindert werden? Wie können sie isoliert werden, wenn sie erfolgreich sind? Juristische Rahmenbedingungen: Was erzwingt die aktuelle Rechtslage? Wie werden Verstöße bestraft? Wann können Sicherheitsmaßnahmen mit dem Gesetz in Konflikt gerate?

Preis: 1.090,-- €*

Troubleshooting in vernetzten Infrastrukturen, 26.09. - 29.09.2017 in Aachen

Garantietermin

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator-Software kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: 2.290,-- €*

Sonderveranstaltung: Das PSTN stirbt: Die neue Kommunikation mit SIP/IP, 09.10.2017 in Bremen

Die Deutsche Telekom hat angekündigt, bis 2018 das klassische PSTN-Netz, respektive analoge und ISDN-Anschlüsse abzuschalten. Dies betrifft alle Unternehmen, die weltweit kommunizieren wollen und müssen. Diese Sonderveranstaltung analysiert, wie der Wechsel von PSTN auf All-IP im Unternehmen verläuft. Sie zeigt auf, welche Funktionalität heute erreicht werden kann und mit welchem Aufwand für Anpassung und Fehlersuche zu rechnen ist.

Preis: 1.090,-- €*

Vertragsgestaltung und rechtssichere Organisation von Cloud Services, 09.10. - 10.10.2017 in Bremen

Rabattaktion

Dieses Seminar erklärt, was Sie bei der Vertragsgestaltung mit Cloud Service Anbietern oder deren Resellern (z.B. für Microsoft oder Amazon Cloud Dienste) alles beachten müssen.

Preis: 1.590,-- €*

Netzzugangskontrolle: Technik, Planung und Betrieb, 09.10. - 11.10.2017 in Bremen

Dieses Seminar vermittelt den aktuellen Stand der Technik der Netzzugangskontrolle (Network Access Control, NAC) und zeigt die Möglichkeiten aber auch die Grenzen für den Aufbau einer professionellen NAC-Lösung auf. Schwerpunkt bildet die detaillierte Betrachtung der Standards IEEE 802.1X, EAP und RADIUS. Dabei wird mit IEEE 802.1X in der Fassung von 2010 und mit IEEE 802.1AE (MACsec) auch auf neueste Entwicklungen eingegangen.

Preis: 1.890,-- €*

TCP/IP-Netze erfolgreich betreiben, 09.10. - 11.10.2017 in Bremen

IP ist die Grundlage jeglicher Rechnerkommunikation. Neben IPv4 gewinnt IPv6 zunehmend an Bedeutung. Für den erfolgreichen Betrieb von IP Netzen ist es unabdingbar beide Protokolle zu verstehen und zu beherrschen. Die Protokolle TCP und UDP bilden die Basis jeder Anwendungskommunikation. Der Kurs vermittelt praxisnah das notwendige Wissen und grundsätzliche Kenntnisse über Routingprotokolle DHCP und DNS.

Preis: 1.890,-- €*

* alle ausgewiesenen Preise sind Netto-Preise

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze für Einsteiger
18.09. - 22.09.17 in Aachen
19.02. - 23.02.18 in Aachen
14.05. - 18.05.18 in Aachen

TCP/IP-Netze erfolgreich betreiben
09.10. - 11.10.17 in Bremen
12.03. - 14.03.18 in Berlin
04.06. - 06.06.18 in Bonn

Internetworking
13.11. - 16.11.17 in Aachen
09.04. - 12.04.18 in Aachen
18.06. - 21.06.18 in Aachen

Paketpreis für ein 5-tägiges, ein 4-tägiges, ein 3-tägiges Intensiv-Seminar € 6.000,--* (Einzelpreise: € 2.490,--*, € 2.290,--*, 1.890,--*)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
26.09. - 29.09.17 in Aachen
24.04. - 27.04.18 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
07.11. - 10.11.17 in Aachen
15.05. - 18.05.18 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.280,--*
(Seminar-Einzelpreis € 2.290,--* , mit Prüfung € 2.470,-- *)

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
16.10. - 18.10.17 in Frankfurt
12.03. - 14.03.18 in Bonn
14.05. - 16.05.18 in Köln

Session Initiation Protocol Basis-Technologie der IP-Telefonie
08.11. - 10.11.17 in Stuttgart
11.04. - 13.04.18 in Düsseldorf
04.06. - 06.06.18 in Bonn

Umfassende Absicherung von Voice over IP und Unified Communications
27.11. - 29.11.17 in Berlin
23.04. - 25.04.18 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
18.09. - 19.09.17 in Düsseldorf
19.02. - 20.02.18 in Bonn
03.05. - 04.05.18 in Köln

Wir empfehlen die Teilnahme an diesem Seminar **"IP-Wissen für TK-Mitarbeiter"** all jenen, die die Prüfung zum ComConsult Certified Voice Engineer anstreben, ganz besonders aber den Teilnehmern, die bisher wenig bis kein Netzwerk Know How, insbesondere TCP/IP, DNS, SIP usw., vorweisen können.

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 5.100,--* statt € 5.670,--*
Optionales Einsteigerseminar: Aufpreis € 1.190,--* statt € 1.590,--*

* alle ausgewiesenen Preise sind Netto-Preise

Impressum

Verlag:
ComConsult Research Ltd.
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline of ComConsult-Research:
02408-955300

E-Mail: kundenservice@comconsult-research.de
http://www.comconsult-research.de

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungsweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen
Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages
© ComConsult Research