ComConsult Research

Der Netzwerk Insider

Juli 2017

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Netzwerke in der AWS-Cloud

von Markus Schaub

Schaut man sich den gerade veröffentlichten Gartner Quadranten für IaaS-Cloud Services an, könnte einem der Gedanke kommen, dass Amazon Gartner gekauft hat. So einsam weit oben rechts findet man AWS im „Magic Quadrant“, dass man Microsoft, das es immerhin in denselben Quadranten geschafft hat, fast übersieht. Mit IaaS ist bei beiden aber schon lange keine reine Servermiete mehr gemeint.

Vielmehr umfasst das Angebot von Amazon, Microsoft, Google und Konsorten die komplette Infrastruktur eines Rechenzentrums, ergänzt um weitere Mehrwertdienste und das an Standorten rund um den Globus. Jeder Standort ist dabei redundant ausgelegt. Zu dieser virtualisierten Rechenzentrumsstruktur gehört naturbedingt ein Netzwerk. Denn all die Dienste und Server, die in der Cloud betrieben werden, müssen natürlich miteinander kommunizieren. Will man die Cloud mit dem eigenen Netz verbinden oder betreibt man Cloud-Lösungen an mehreren Standorten bzw. nutzt Dienste, die nicht weltweit an jedem Standort verfügbar sind, so kommen weitere Aufgaben bei der Netzwerkgestaltung hinzu. Es ist also höchste Zeit, sich dieses Themas auch als Netzwerker anzunehmen.

weiter auf Seite 9

Zweitthema

Ist BGP das bessere IGP?

von Markus Geller

In den letzten Jahren haben wir sehr oft über neue Layer 2 Verfahren gesprochen und geschrieben. Viele dieser neuen Möglichkeiten wie TRILL, SPB oder MC-LAG schienen ideal, um im Rechenzentrum die überkommenen Mechanismen des Spanning Tree oder der Link Aggregation abzulösen.

Und nicht nur wir bei der ComConsult haben das so gesehen, auch viele etablierte Hersteller setzen seit Jahren auf Layer 2 Fabrics für ihr Data Center Design.

- Cisco FabricPath
- Avaya Fabric Connect
- Juniper QFabric
- Brocade VCS Fabric

sind nur einige Beispiele, die ich hier nennen möchte. Der große Vorteil dieser neuen Technologien ist ein blockadefreies Netzwerk, in dem alle physikalischen Verbindungen optimal genutzt werden können.

Aber am Ende bleibt es immer noch eine Layer 2 Infrastruktur und somit eine Broadcastdomäne, die sich über viele Netzwerkelemente spannt mit all den Nachteilen und Problemen, die die Verarbeitung und Verbreitung von Broadcast und Multicast mit sich bringen.

weiter auf Seite 20

Geleit

iPad Pro: endlich tauglich für den Unternehmenseinsatz?

auf Seite 2

Standpunkt

Muss man Gebäude abschirmen?

auf Seite 19

Sonderveranstaltungen

Herausforderung Informationssicherheit

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

auf Seite 17

Wireless und Mobility

ab Seite 6

IT-Infrastrukturen für das Gebäude der Zukunft

ab Seite 4

Geleit

iPad Pro: endlich tauglich für den Unternehmenseinsatz?

Apple positioniert das iPad seit Jahren als Laptop-Killer und als das ideale Gerät für mobile Anwendungen. Die typischen Kunden sehen das ganz unterschiedlich, das Spektrum reicht von untauglich bis hin zu perfekt. Woran kann das liegen? Und wie sieht die Zukunft aus? Apple hat gerade eine neue Version von IOS zusammen mit einer deutlich überarbeiteten Hardware angekündigt. Kommt damit der endgültige Durchbruch?

Tatsächlich hat Apple das iPad seit Jahren bis zur aktuellen Ankündigung kaum verändert. Mit den Pro-Versionen kam vor zwei Jahren der zumindest verbale Versuch, ein Gerät speziell für den Unternehmenseinsatz zu schaffen. Das wesentliche Merkmal war dabei die Kombination mit einem "pencil" und einer Tastatur. Vereinfacht dargestellt kann man sagen als Tiger gesprungen und als Maus gelandet (ich bin seit der Markteinführung leidgeprüfter Benutzer des großen Pro). Erst der Druck durch Microsoft und das kontinuierlich verbesserte Surface Pro hat Apple nun endlich dazu gebracht alle Register zu ziehen, um endlich dem Anspruch eines professionellen Gerätes zu genügen. Dazu wurde die Hardware inklusive der Grafik auf ein Leistungsniveau gezogen, das sicher weit über dem Bedarf des normalen Benutzers liegt. Ein gutes Beispiel ist LumaFusion als Video-Editor. Die Leistung, die hier im 4k-Editing erbracht wird, erfordert ansonsten einen iMAC mit einer gehobenen Ausbaustufe. Gleiches kann man für Affinity Photo auf dem iPad sagen. Dies ist die fast volle Leistung von Photoshop auf einem Touch-Endgerät mit einer Touch-Applikation (würden doch nur meine Photoshop Actions hier funktionieren, ansonsten kann man aber sagen, dass Affinity Photo auch als Desktop-Version eine mehr als ernstzunehmende Bedrohung für Adobe ist). Wesentlichen Einfluss auf die Leistungssteigerung hat die dynamische Bildwiederholrate von bis zu 120 Bilder pro Sekunde. Diese führt bei Nutzung des Pencils zu einer Verzögerung von nur noch 20ms. Schreiben oder Malen mit dem Pencil ist vom Schreiben auf Papier bis auf die glatte Oberfläche nicht mehr zu unterscheiden (ich bin absolut begeistert und mein Wacom liegt endgültig im Schrank). Das ist die neue Hardware. Dies wird ergänzt um eine neue Version von IOS, IOS 11. Auch wenn wir es noch im Test haben und die erste Public Beta gerade erst veröffentlicht wurde, kann man jetzt schon sagen, dass dieses Upgrade aus dem iPad ein neues Gerät machen wird.

Haben die langen Jahre des Wartens auf ein professionelles iPad sich also endlich gelohnt. Haben wir jetzt endlich eine Version, die professionellen Ansprüchen genügt? Und kann Apple damit den verlorenen Boden gegenüber dem Surface Pro wieder gut machen?

iPad kontra Surface Pro: ein Vergleich, der hinkt!

Microsoft hat Windows in den letzten Jahren so erweitert, dass es sowohl eine traditionelle Bedienung mit der Maus als auch eine Touch-Bedienung erlaubt. Damit lautet das Standard-Argument für den Einsatz eines Surface Pro gegenüber einem iPad, dass es die "alten" Anwendungen weiterhin unterstützt. Das ist grundsätzlich richtig und wer den Bedarf nach einer Anwendung hat, die es nicht als Touch-Anwendung gibt, der wird auf dem Surface Pro besser aufgehoben sein. Der Nachteil dabei ist, dass es kaum sinnvolle Touch-Anwendungen auf dem Surface Pro gibt. Touch verkommt unter Windows zu einem Spielzeug ohne besonderen Mehrwert.

Der Witz und der zentrale Punkt des iPad ist, dass es nur Touch-Anwendungen unterstützt. Damit muss jede Anwendung auf dem iPad neu entwickelt werden. Dementsprechend stoßen wir auch auf dem iPad auf sehr moderne Anwendungen, die es so bisher nicht gegeben hat. Dies können bahnbrechende Anwendungen wie LumaFusion oder Affinity Photo sein oder ganz "normale" Anwendungen wie Microsoft Office oder Apple Pages.

Aus Unternehmenssicht bedeutet das: wird für einen bestimmten Einsatzzweck eine neue Anwendung benötigt und hat der Bediener einen Vorteil von einer Touch-Bedienung, dann kann das zu einem signifikanten Mehrwert führen. Beispiele für diese Art von Anwendungen finden wir in Krankenhäusern mit dem iPad als elektronische Akte, im Transportwesen, in Flugzeugen oder im Kassenbereich.

Soweit so gut, aber warum tut sich das iPad im Unternehmenseinsatz dann trotzdem so schwer? Warum kann es bisher einen Laptop eben nicht ersetzen? Und warum punktet das Surface Pro bei so vielen Anwendern?

Mangelbereich 1: Multitasking

Apple hat den Bedarf für Multitasking seit Jahren schlicht ignoriert. Alle Beschwerden oder Wünsche von Anwendern wurden einfach arrogant abgewiesen. Dem Surface Pro sei Dank, dies ist jetzt vorbei. Mit IOS 11 haben wir endlich ein deutlich flexibleres Multitasking mit der Möglichkeit von Drag-and-Drop. Endlich können wir einen Anhang aus einer Email in eine andere Anwendung ziehen oder umgekehrt. Was hier harmlos klingt, ist für die Verringerung des funktionalen Abstands zum Laptop entscheidend. Wir müssen jetzt abwarten wie der Durchschnittsbenutzer diese neue Funktionalität annimmt. Sie erfordert eine Eingewöhnung. Die ist zwar minimal, aber es wird Benutzer geben, die das nicht mehr intuitiv finden. Wie auch immer, mit IOS 11 macht Apple einen Riesenschritt nach vorne! Man muss aber anmerken, dass es eine kleine Version von Drag-and-Drop innerhalb der Anwendungen der Firma Readdle schon gibt.

Reicht das aus? Im Prinzip vielleicht, wäre da nicht der Elefant im Raum.

Mangelbereich 2: das Dateisystem, der Elefant im Raum!

Wäre es nicht toll, wenn es ein Gerät gäbe, auf dem Ransomware absolut chancenlos ist? Nun, das gibt es. Ein iPad oder ein iPhone. Ein Kernmerkmal von IOS ist das Sandboxing und der damit verbundene bewusste und gewollte Verzicht auf ein Dateisystem. Jede Anwendung läuft nur in ihrer eigenen Umgebung. Soll eine Datei bearbeitet werden, dann muss sie in dieser Umgebung sein und damit ist sie für andere Anwendungen nicht zugreifbar. Wenn ich also eine Datei in einem Cloud-Speicher habe und die-

iPad Pro: endlich tauglich für den Unternehmenseinsatz?

se mit Word bearbeiten will, dann muss ich sie in die Sandbox von Word kopieren. Damit entsteht eine neue Version dieser Datei. Dieser Zwang zur Kopie treibt iPad Anwender seit Jahren in die Weißglut. Er macht alle Nutzungsformen, die eine Bearbeitung einer Datei von mehr als einer Applikation aus erfordern, schlicht wirklichkeitsfremd. So geht es nicht. Vereinzelt gibt es Lösungen dazu. So haben Box und Microsoft eine Kooperation abgeschlossen, die es erlaubt, eine Datei von Box aus mit einer MS Office Anwendung zu öffnen und nach dem Sichern ist die Datei wieder in Box. Aber dies ist eine isolierte Initiative dieser beiden Firmen. Dies sollte rein theoretisch mit OneNote genauso gehen, aber zumindest auf unserem Testgerät was OneNote bisher eher ein Problem als eine Lösung (die neueste Version scheint besser zu sein).

Beachten Sie, dass Sandboxing auch bedeutet, dass es keine Plugins geben kann. Diese geben ja genau eine Datei an eine andere Anwendung weiter. Der gesamte Grafikmarkt mit Photoshop im Kern basiert aber auf Plugin-Architekturen. Damit ist das iPad bisher in diesem Markt trotz aller Anstrengungen von Adobe eher als Spielzeug zu sehen. Das gleiche gilt für die Video-Bearbeitung.

Tatsächlich hat das Fehlen eines Dateisystems einen weiteren wesentlichen Nachteil. Er macht die Nutzung von externen Laufwerken unmöglich. Zwar kann ein externes Laufwerk mit einer Applikation kombiniert werden (siehe SanDisk und andere), aber die Daten auf diesem Laufwerk sind für andere Applikationen nicht zugänglich.

Mit IOS 11 und den neuen iPad Pros gibt es jetzt zwei wesentliche Verbesserungen an dieser Situation:

- die iPad Pros können jetzt bis zu 512GB Speicher haben, gleichzeitig haben sie vermutete 4GB Hauptspeicher. Damit wird eine Videobearbeitung oder das Arbeiten mit großen Grafikdokumenten zum ersten Mal wirklich möglich. Bisher war es schön, die entsprechenden Apps zu haben, aber wenn man noch nicht einmal die Ergebnisse eines einzelnen Studio-Shootings als Fotos in ein iPad ziehen kann, dann ist das Ganze ein schlechter Scherz. Dies ist nun zumindest theoretisch möglich.

- es kommt mit Files endlich so etwas wie ein Dateisystem. In der ersten Public-Beta sind weiterhin alle interessanten Bereiche ausgegraut. So kann weder geprüft werden, ob ein externes Laufwerk unterstützt wird oder ein internes Dateisystem tatsächlich von mehreren Anwendungen gemeinsam genutzt werden kann. Bisher können Cloud-Dateisysteme eingebunden werden und Dateien können zwischen den verschiedenen Foldern in den verschiedenen Dateisystemen verschoben werden. Selbst wenn diese bisherigen Einschränkungen in der nächsten Public Beta aufgehoben werden, wissen wir immer noch nicht mehr, da auch die einzelnen Apps an die neuen Möglichkeiten angepasst werden müssen.

Wir testen speziell diesen Funktionsbereich für Sie und halten Sie auf dem Laufenden.

Mangelbereich 3: Augmented Reality

Apple hat in den letzten zwei Jahren zwar viel über AR gesprochen und ihm dem Vorzug gegenüber Virtuell Reality gegeben. Aber das war bisher reine Wortspielerei. Nun kommt ein komplettes Entwicklungssystem, das gerade auf dem Word Wide Developer Congress WWDC vorgestellt wurde. Und dann wird auch endlich klar, warum wir diese extreme Grafikleistung in einem iPad brauchen. Im Moment scheint es so, als ob Apple hier die Tür für das iPad in AR-Anwendungen wie im Bereich von Building Information Modeling BIM weit aufgestoßen hat. Bauherren können damit zum Beispiel in der Rohbauphase durch ihr Gebäude gehen und das iPad zeigt ihnen verschiedene Varianten der späteren Detailausstattung des Gebäudes. Damit sind eine ganze Reihe von Praxistests möglich (auch im Bereich von Brandschutz, Evakuierung, Zusammenspiel von verschiedenen technischen Gewerken), die dramatischen Einfluss auf die Entwicklung komplexer Gebäude haben (der Flughafen Berlin lässt grüßen).

Wo stehen wir jetzt?

Mit den neuen iPad-Pros und IOS 11 wird Apple zum ersten Mal in der Geschichte des iPads dem Anspruch gerecht, dass ein breites Spektrum von Unternehmens-Anwendungen wirklich ernsthaft unterstützt wird. Das iPad wird damit universell nutzbarer. Bisher dominierten einzelne Spezialanwendungen im Unternehmenseinsatz. Nun kommt der Breiteneinsatz. Ob dabei das iPad zum Laptop-Killer wird, kann weiterhin bezweifelt werden. Wer seine traditionellen Anwendungen benötigt, wird auf jeden Fall weiter den Laptop bevorzugen. Das iPad wird auch in Zukunft den Umstieg in andere Applikationen erfordern. Und damit wesentliche Änderungen in den gegebenen Arbeitsabläufen. Diese Änderungen werden sich nur durchsetzen, wenn die mit einem signifikanten Mehrwert kommen. Und dies kann je nach Anwendung eben auch der Fall sein.

Was bedeutet das für Unternehmen?

Die Nutzung von iPhone und iPad im Unternehmen ist nicht neu. Für viele Unternehmen gehört es zum Standard. Aber der Nutzungsumfang kann und sollte in den nächsten zwei Jahren deutlich zunehmen. Die Kombination aus IOS 11, neuer Hardware und einer AR-Basis schafft ein Umfeld, in dem mit schnell wachsenden Gerätezahlen gerechnet werden muss. Die IT-Abteilungen müssen darauf vorbereitet sein.

Hier setzt unser neues Seminar IOS im Unternehmen an. Wir bereiten Sie auf den professionellen Einsatz von IOS im Unternehmen vor und diskutieren die typischen Fallstricke mit Ihnen. Der Referent Mark Zimmermann ist gerade von der Apple WWDC aus Las Vegas zurück und kommt mit einem Koffer voller neuer Detailinformationen, die Ihren Einsatz von IOS im Unternehmen deutlich vereinfachen können.

Ihr Dr. Jürgen Suppan

Aktuelle Sonderveranstaltung

IT-Infrastrukturen für das Gebäude der Zukunft

16.10.2017 in Köln

Die ComConsult Akademie veranstaltet am 16.10.2017 ihre Sonderveranstaltung "IT-Infrastrukturen für das Gebäude der Zukunft" in Köln.

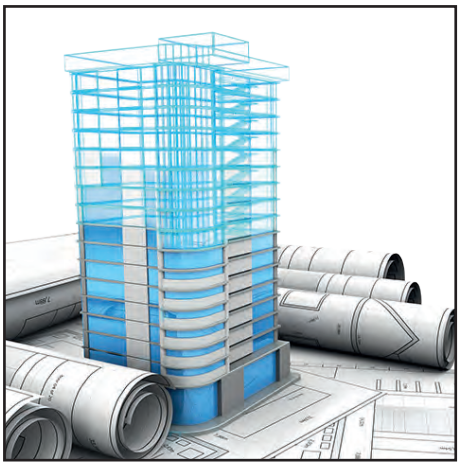
Das Gebäude der Zukunft erfordert IT-Infrastrukturen, die Gewerk-übergreifend sind, die sowohl in der Datenverarbeitung als auch in der Klimatisierung, Zugangssicherung oder allgemeiner gesprochen der Gebäude-Automatisierung eingesetzt werden können. Diese Veranstaltung wendet sich an Planer aller Gewerke 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.

Die IT-Infrastrukturen der Gebäude der Zukunft umfassen:

- eine Anwendungs-unabhängige Verkabelung
- eine Anwendungs-unabhängige Vorbereitung für unterschiedliche Funknetze
- flächendeckende Funknetze
- eine flächendeckende Gleichstrom-Versorgung auf der Basis Power-over-Ethernet

Auf den genannten Infrastrukturen setzen die verschiedensten Anwendungen in den unterschiedlichen Gewerken auf. Beispiele dafür sind Gebäude-Automatisierung mit Bluetooth, Zigbee, EnOcean oder Beacon-Technologien.

Damit entsteht ein hierarchisches Schichtenmodell von Infrastruktur-Diensten, das



eine Reihe von signifikanten Vorteilen hat:

- es ist wirtschaftlich, es wird nur installiert, was wirklich gebraucht wird und wesentliche Teile der Infrastruktur können von verschiedenen Gewerken gemeinsam genutzt werden
- es ist langlebig und am Nutzungszeitraum des Gebäudes ausgelegt
- es vermeidet Kollisionen oder Überlappungen zwischen Gewerken
- es ist flexibel und gestattet eine schnelle Reaktion auf Bedarfsänderungen im Betrieb des Gebäudes

Dieses Schichtenmodell steht im Einklang mit Building Information Modeling BIM. Es kann in ein BIM-Modell integriert werden, es kann aber auch autonom gesehen werden.

Diese Sonderveranstaltung diskutiert mit Ihnen:

- welchen Infrastruktur-Bedarf das Gebäude der Zukunft erzeugt
- wie eine effiziente, flexible und Gewerke-übergreifende Infrastruktur-Planung erfolgt
- wie Mehrwert-Dienste in einzelnen Gewerken auf diese Basis-Schicht von Infrastruktur aufsetzen

Wir gehen dabei auf eine Reihe von Spezialfragen ein, die helfen, den Aspekt der langfristigen Investitionssicherung abzudecken:

- wie sieht der Arbeitsplatz der Zukunft aus und welche Infrastruktur erfordert er?
- welchen Stellenwert hat eine WLAN-Infrastruktur im Gebäude der Zukunft und wie dicht wird sie geplant?
- was bedeutet Smart Building und wie kann es sauber auf eine Basis-Infrastruktur aufgesetzt werden?
- wie sieht die Anwendungs-neutrale Verkabelung eines Gebäudes aus? Bis wohin sollte sie gebracht werden und ab wann startet der Gewerke-spezifische Teil?
- wo steht Power-over-Ethernet technisch, was ist in den nächsten Jahren zu erwarten und wie kann es Gewerke-übergreifend und flexibel genutzt werden?
- wie effizient können Mehrwertdienste wie Beacon-Technologien integriert werden?
- welche Rolle wird Mobilfunk mit 5G spielen? Inwieweit muss es mit den anderen geplanten Funktechnologien als Einheit gesehen werden?

Anmeldung an kundenservice@comconsult-research.de

IT-Infrastrukturen für das Gebäude der Zukunft

Ich buche die Sonderveranstaltung
IT-Infrastrukturen für das Gebäude der Zukunft

☐ 16.10.2017 in Köln
zum Preis von 1.090,- € 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 IT-Infrastrukturen für das Gebäude der Zukunft

Beginn 09:30 Uhr

09:30 - 10:15 Uhr
Keynote: SMART Commercial Building - Die Digitalisierung verändert die Anforderungen an unsere Gebäude
- Trends und Beispiele
- Digitalisierungsbausteine Hardware/Software
- Use Cases für die Bauherren/Investoren
- Vorgehensweise (Anforderungsmanagement)
- Entscheidervorlage Digitalisierung
- Neues Leistungsbild Digitalisierung „Digital Transformation Manager“

Dipl.-Ing. Klaus Dederichs, Drees & Sommer GmbH

10:15 - 11:00 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)
- Soll man ausgewählte Daten sammeln oder alles, was man bekommen kann?
- Schutzbedarf der Daten
- Gefahr der Scheinkorrelation (Storks deliver Babies von Matthews (2000))
- 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

11:00 - 11:30 Uhr Kaffeepause

11:30 - 12:15 Uhr
Der Arbeitsplatz der Zukunft – Anforderungen an die Infrastruktur
- Kabeltechnik
- Netzwerktechnik
- Endgerätetechnik
- Applikation
- Edge Data Center bringen die Rechenleistung näher zum Nutzer

Dipl.-Ing. Thomas Simon, ComConsult Beratung und Planung GmbH

12:15 - 13:00 Uhr
WLAN und andere Funktechniken
- Stand der Technik bei WLAN
- Wie viele Access Points werden benötigt und wie verkabelt man sie?
- „WLAN-Verteiler“ werden marktfähig, sind sie für das Smart Building geeignet und lassen sich dadurch Kabel sparen?
- Jedem sein eigenes WLAN oder zentrale WLAN-Infrastruktur für alle Mieter?
- Welche Rolle spielen Mobilfunk und andere Funkdienste in Gebäuden?
- Braucht man Abschirmungen gegen Funkwellen von außen?
- Wie lassen sich gegenseitige Störungen zwischen Funkdiensten in einem Smart-Building vermeiden?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

13:00 - 14:00 Uhr Mittagspause

14:00 - 14:45 Uhr
Verkabelung als Gewerke-übergreifende Basis für die Gebäude-IT
- Kann es eine Gewerke-übergreifende Universal-Verkabelung für ein Gebäude geben? Wenn ja, wo ist die Schnittstelle zu den Gewerken und was umfasst der Gewerke-übergreifende Teil?
- Wie unterscheidet sich die EN 50173-6 von den bisherigen Verkabelungsnormen?
- Wie viele Unterverteiler werden benötigt, um eine saubere Basis für alle Gewerke zu legen?
- Was bringt die Berücksichtigung der Norm an Vorteilen?
- Was sind die Besonderheiten einer anwendungsneutralen Verkabelung bei Nutzung durch die Gebäudeleittechnik?
- Welche grundsätzlichen technischen und organisatorischen Entscheidungen müssen getroffen werden?
- Warum lassen sich die bekannten Verkabelungs-Technologien und Materialien nicht immer 1:1 für Netze der Gebäudeleittechnik verwenden?
- Warum kann man aus den Erfahrungen beim Aufbau von lokalen Netzen im Industrie-Umfeld lernen?

Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

14:45 - 15:30 Uhr
Power-over-Ethernet: Gewerke übergreifende Stromversorgung im Gebäude der Zukunft

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

15:30 - 16:00 Uhr Kaffeepause

16:00 - 17:00 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 und Netzzugangskontrolle: Brauchen wir das wirklich?
- Mandantenfähige Infrastrukturen für Nutzer und Betreiber von Smart Buildings
- Absicherung von Funknetzen, inkl. WLAN, 5G und Co., 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: Skalierbare Sicherheitsarchitekturen

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Ende der Veranstaltung 17:15 Uhr

Der Veranstalter behält sich Änderungen im Programm vor

Aktuelle Sonderveranstaltung

Sonderveranstaltung Wireless und Mobility 18.10. - 19.10.2017 in Bonn

Die ComConsult Akademie veranstaltet vom 18.10. - 19.10.2017 in Bonn 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 Referenten


Dr. Jan Byok


Dipl.-Ing. Stefan Bien


Dr. Johannes Dams


Christian Gauer


Dipl.-Ing. Olaf Hagemann


Dr. Simon Hoff


Dr. Franz-Joachim Kauffels


Reinhard Lichte


Dipl.-Ing. Michael Schneiders


Dipl.-Inform. Thomas Steil


Dr. Joachim Wetzlar

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 den Report "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 – 60 GHz-Bänder). Hier können leicht Multigigabit-Leistungen erreicht werden, aber eben ver-

2. aktualisierte und deutlich erweiterte Auflage Oktober 2017

bunden 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 _____

Programmübersicht Wireless und Mobility

Mittwoch 18.10.17

9:30 - 10:30 Uhr

Wireless: Basis für Disruption und Agilität

- Mobilität als Grundlage neuer Arbeitsplatzmodelle
- Disruption und Agilität als wesentliche Triebkräfte
- Neue Anwendungen und Anforderungen an Multi-Gigabit WLANs
- IoT und die enge Verbindung zu Mobilfunktechnologie (5G)
- Strukturelle Aspekte unterstützender Infrastrukturen

Dr. Franz-Joachim Kauffels, Technologie-Analyst

10:30 - 11:30 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 - 13:00 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

14:00 - 15:00 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 und Dr. Johannes Dams, ComConsult Beratung und Planung GmbH

15:00 - 15:45 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

15:45 Uhr Kaffeepause

16:15 - 17:00 Uhr

Cisco Virtual Beacon Solution und Hyperlocation Lösung

Christian Gauer, Cisco Systems GmbH

17:00 - 18:00 Uhr

Von LTE Advanced zu 5G

- Mobilfunk: Stütze der nächsten digitalen Revolution
- Koexistenz von LTE / 5G und WLANs
- 5G: Konzepte, Technologien, Feldversuche, Standardisierung
- Die Eckpfeiler des ITU-Standards für 5G vs. Pre-Standard-Lösungen

Dr. Franz-Joachim Kauffels, Technologie-Analyst

18:00 Uhr Happy Hour

Donnerstag 19.10.17

9:00 - 10:30 Uhr

Wireless / Mobile / Cloud Security: Ganzheitliche Konzepte sind gefragt

- Sicherheit im WLAN: Ein alter Hut?
- Warum es trotz Hotspot 2.0 kaum sichere Hotspots gibt
- Absicherung von iOS und Android
- Sichere Integration mobiler Endgeräte
- Schlüsselelement sichere Cloud-Dienste
- Rolle von MDM und WLAN Management aus der Cloud

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:30 Uhr Kaffeepause

11:00 - 11:45 Uhr

Mobile Netzwerke sind mehr als nur WLAN – Lokationsabhängige Interaktionen mit Anwender 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
- Neu 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

11:45 - 12:30 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

12:30 Uhr Mittagspause

14:00 - 15:00 Uhr

AR-gestütztes Building Infrastructure Management für flächendeckende WLAN-Lösungen

N.N.

15:00 - 16:00 Uhr

Rechtliche Aspekte des Betriebs privater WLAN-Infrastrukturen

Dr. Jan Byok, Bird & Bird LLP

16:00 Uhr der Veranstaltung

Schwerpunktthema

Netzwerke in der AWS-Cloud

Fortsetzung von Seite 1

Markus Schaub ist seit 2009 Leiter von ComConsult-Study.tv. Er verfügt über umfangreiche Berufserfahrung in den Bereichen Netzwerken und VoIP und ist seit mehr als 13 Jahren bei ComConsult beschäftigt. Seine Schwerpunkte liegen im Netzwerk-Design, IP-Infrastrukturdiensten und SIP, zu denen er viele Vorträge auf Kongressen hielt, erfolgreich Seminare durchführte und zahlreiche Veröffentlichungen schrieb.

In diesem Artikel werden zunächst die Basiselemente der Cloud-Netze bei Amazon vorgestellt. Danach wird erklärt, wie Systeme zwischen verschiedenen Subnetzen innerhalb der Cloud kommunizieren und wie man Dienste anbindet, die aus dem Internet heraus erreichbar sein sollen. Zum Abschluss wird noch auf die Koppelungsvarianten der Cloud mit dem eigenen Netz eingegangen. Auf spezifische Sicherheitsaspekte wird zwar eingegangen, sie stehen jedoch nicht im Fokus, da das den Umfang eines Artikel sprengen würden.

Gestaltungselemente

Wer Netzwerke in der Cloud verstehen will, muss sich zunächst einmal mit neuen und alten Begriffen und deren Funktion auseinandersetzen: Region, Availability Zone, VPC, Subnetz. Hat man verstanden was diese bedeuten und wie sie zusammenhängen, ist es eigentlich ganz einfach, ein Netzdesign aufzusetzen.

Region

Eine „Region“ ist bei AWS recht wörtlich, nämlich geographisch gemeint. Aktuell gibt es 14 Regionen: 4 in den USA, eine in Kanada, 3 in der EU (noch: eine ist nämlich „London“), 5 in Asien und eine weitere in Süd Amerika. Diese Regionen sind zumeist Städten oder Bundesstaaten zugeordnet, manchmal geht es aber auch durcheinander. Für die europäischen gibt es London, Frankfurt und Irland.

Diese Regionen sind weitestgehend autark: man kann zwar Verbindungen zwischen zwei Regionen konfigurieren, jedoch ist das vergleichsweise aufwendig und nicht sonderlich performant. Im Grunde ist es vergleichbar mit einem VPN-Tunnel zwischen zwei Rechenzentren an unterschiedlichen, weit entfernten Rechenzentren. Damit gilt für die meisten Cloud-Dienste, dass man sie möglichst in derselben Region betreibt, wenn zwischen ihnen viele Daten ausgetauscht werden müssen.

Was Regionen noch auszeichnet, sind die dort verfügbaren Dienste: nicht alle Dienste sind überall verfügbar. So gibt es die Amazon-eigene Datenbank „Aurora“ beispielsweise nicht in Frankfurt, wohl aber in Irland. Dasselbe gilt auch für den Mail-Dienst SES. Wenn man ein Projekt aufsetzt, sollte man also vorher klären, welche Dienste man benötigt und danach die Region auswählen. Ist einem jedoch der Standort wichtiger, so muss man ggf. andere Dienste nutzen, also mySQL statt Aurora oder diese, wenn möglich, selbst betreiben, wie beim Email-Dienst.

Availability Zones

Innerhalb einer Region gibt es „Availability Zones“. Das sind verschiedene, jedoch nah beieinanderliegende Rechenzentren. Die Availability Zonen einer Region sind mit hoch-performanten Verbindungen miteinander gekoppelt, so dass das Delay kaum ins Gewicht fällt und Bandbreite keine Rolle spielt. Alle Dienste einer Region sind in allen Availability Zones verfügbar.

Bei diesen Zonen geht es also um Verfügbarkeit: fällt in einer Zone bspw. der Strom aus, so gilt das nicht (zwangsläufig) für die andere. In jeder Region gibt es mindestens zwei Availability Zonen. In Frankfurt gibt es seit kurzem sogar drei davon.

Bei den Zonen ist zu beachten, dass sie anders heißen können als die Region, in der sie liegen. So heißt die Region „EU (Frankfurt)“, die Zonen dort eu-central-1 und nicht eu-ffm oder eu-fra, wie man hätte meinen können. Die drei Zonen sind von „a“ bis „c“ durchnummeriert, also bspw. eu-central-1a.

Bei Pro Account (Account = Vertrag, nicht User) entspricht eine Zone immer einem Standort: für alle User dieses Accounts liegt die Availability Zone eu-central-1a also im selben Rechenzentrum und eu-central-1b in einem anderen. Das ist für die Planung hochverfügbarer Anwendungen schon mal gut zu wissen. Man muss aber auch wissen, dass für einen anderen Account eu-central-1a ein anderes Rechenzentrum gemeint sein kann. Wenn bei dem Vertrag ComConsult Research bspw. eu-central-1a das Rechenzentrum 1 gemeint ist, kann eu-central-1b bei dem Vertrag ComConsult Akademie ebenfalls das Rechenzentrum 1 gemeint sein. Hat ein Unternehmen also mehr als einen Account, so kann man über die Availability Zones nicht sicherstellen, dass Anwendungen im selben bzw. in unterschiedlichen Lokalitäten laufen.

Virtual Private Cloud (VPC)

Eine „Virtual Private Cloud“ wird fast durchgängig nur abgekürzt als VPC bezeichnet. Eine VPC kann man sich als das eigene Rechenzentrumskonstrukt innerhalb einer AWS-Region vorstellen. D.h. eine VPC kann alle Availability Zonen einer Region überspannen, also ganz so als würde man an einem Standort zwei Rechenzentren betreiben. Jedoch ist eine VPC immer auf eine Region beschränkt.

Alternativ kann man VPCs aber auch als Sicherheitszonen betrachten. Denn wie später im Artikel erklärt wird, kann man zwei VPCs mit Middleboxen, wie Firewalls oder IDS/IPS, gegeneinander abschotten, innerhalb einer VPC ist das hingegen nicht möglich.

Die Verbindung zwischen zwei VPCs nennt man Peering. Um zwei VPCs peeren zu können, müssen sie in derselben Region sein und die IP-Bereiche dürfen sich nicht überlappen.

Netzwerke in der AWS-Cloud

Subnetze

Subnetze sind genau das, was sie schon immer waren. Bei der Amazon-Cloud ist ein Subnetz immer auf eine Availability Zone beschränkt. Zwischen Subnetzen wird geroutet, dabei ist es jedoch egal, ob die beiden unterschiedlichen Subnetze in derselben Availability Zone sind oder nicht.

Abbildung 1 zeigt den Zusammenhang zwischen den verschiedenen Komponenten, aus denen ein Amazon-Netz besteht.

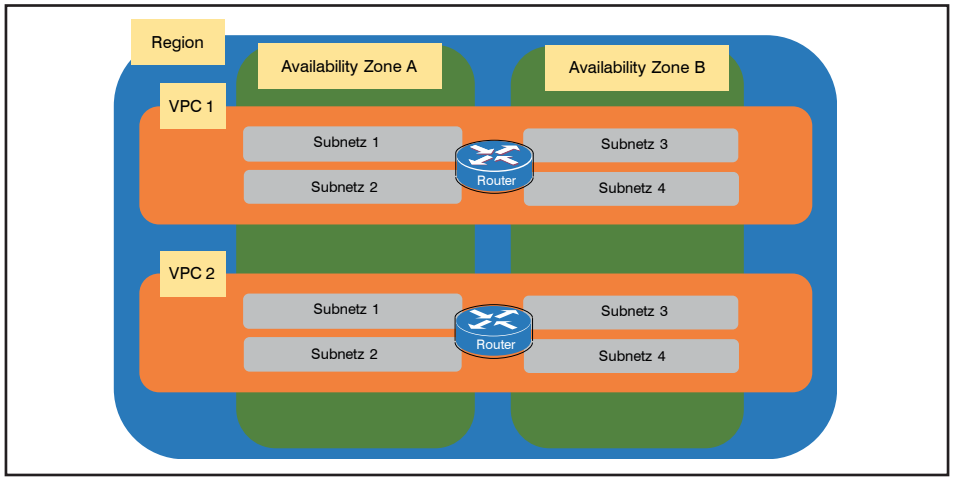


Abbildung 1: Zusammenwirken von Region, Availability Zone, VPC und Subnetze

IPv4-Adressen in der Cloud

Das Zusammenwirken von Regionen, VPCs und Subnetzen hat unmittelbare Konsequenzen für das IP-Design. Dabei müssen für IPv4 zwei verschiedene IP-Adressräume unterschieden werden:

1. Private IP-Adressen (RFC1918)
2. Elastic IP Adressen (öffentliche Adressen von Amazon)

VPCs und Subnetzen ordnet man bei der Anlage private IP-Adressen zu. Systeme, die an die Subnetze angeschlossen werden, bekommen aus diesem Bereich automatisch Adressen zugewiesen. Schließt man also bspw. einen EC2-Server an, so bekommt er eine private IP-Adresse, ebenso gilt das für einige Dienste, wie beispielsweise Datenbanken.

Mit diesen privaten IP-Adressen können die Systeme aus dem Internet nicht erreicht werden und ebenso wenig von sich aus mit dem Internet kommunizieren. Natürlich will man bestimmte Dienste und Server aber aus dem Internet erreichbar machen. Es kann auch die Anforderung geben, dass die Server selbst auf das Internet zugreifen können, bspw. für Systemupdates oder beim Betrieb von Mailservern.

Dazu gibt es drei Möglichkeiten:

1. NAT-Gateway

   Das NAT-Gateway funktioniert im Grunde wie der DSL-Router zuhause. Die Systeme können von sich aus Verbindungen ins Internet aufbauen. Verbindungen aus dem Internet hingegen benötigen eine Forwarding-Tabelle, die auf dem NAT-Gateway hinterlegt müsste. Das geht, Stand heute, jedoch nicht. Man kann jedoch selbst so genannte NAT-Instanzen betreiben, mittels derer das möglich ist. Dazu später mehr.

2. Loadbalancer

   Will man bspw. mehr als einen Web-Host betreiben, kann man einen Loadbalancer dafür nutzen.

3. Elastic IP

   Elastic IP Adressen sind öffentliche IP Adressen aus dem Vorrat von Amazon selbst. Diese kann man anfordern und einzelnen Systemen zuordnen. Die sind dann unter der Elastic IP Adresse erreichbar.

   Elastic IP-Adressen sind so lange kostenfrei, wie sie an laufende Systeme gebunden sind. Sobald sie nur vorgehalten werden, kosten sie Geld.

Es bietet sich an, das NAT-Gateways für Systeme anzubieten, die nur als Clients auf das Internet zugreifen und nur innerhalb der VPC Serverdienste anbieten. Also bspw. Datenbank-Server, die nur gelegentlich Update aus dem Internet benötigen, vom Internet aus jedoch nicht erreichbar sein sollen.

Elastic IP-Adressen wiederum nutzt man, um Serverdienste aus dem Internet erreichbar zu machen, bspw. Frontend-Web-Server.

Sämtlicher VPC-interne Datenverkehr wird über die privaten IPv4 Adressen abgewickelt, sodenn er über IPv4 transportiert wird.

Damit wären wir bei der Frage nach den

IPv6-Adressen in der Cloud

Bei Amazon gibt es die Möglichkeit, einer VPC auch einen IPv6 CIDR-Block zuweisen zu lassen (vgl. Abbildung 2). Pro VPC bekommt man dabei einen /56er Block zugewiesen. Die Größe dieses Blockes kann auch nicht geändert werden.

Damit hat man pro VPC rechnerisch also nur 256 Präfixe zur Verfügung. Für ein Rechenzentrum, was ja einem VPC entspricht, könnte das knapp werden. Für eine Sicherheitszone sollte das jedoch allemal ausreichen. Warum Amazon hier herum geizt, bleibt Amazons Geheimnis. Andererseits: wer mehr als 256 Subnetze benötigt, überweist wahrscheinlich jeden Monat so viel Geld an Amazon, dass die mit sich reden lassen, sodass diese Begrenzung nur für das Gros der Kunden gilt und denen sollten 256 Netze pro VPC genügen.

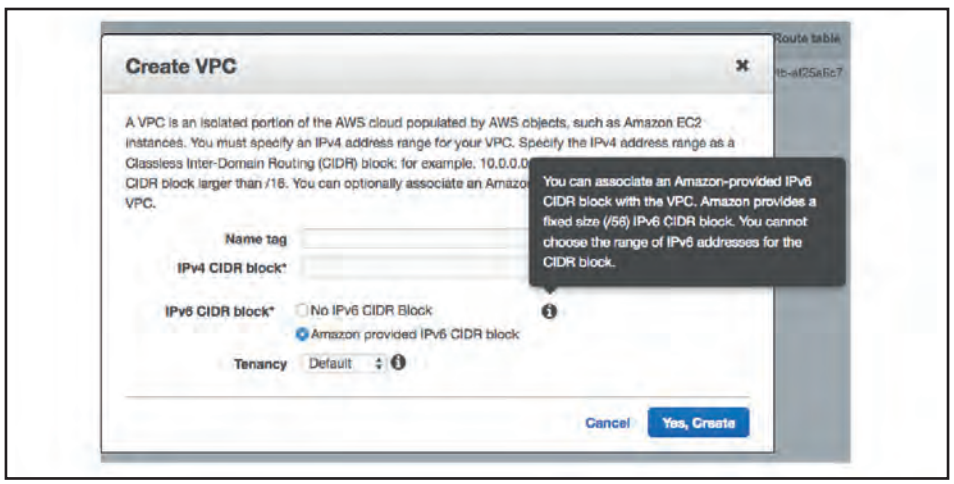


Abbildung 2: IPv6-CIDR Block für VPC bei AWS

Bei den IPv6-Netzen ist zu bedenken, dass es sich um öffentliche IP-Adressen handelt. D.h. alle Systeme können aus dem Internet heraus unter diesen Adressen erreicht werden, vorausgesetzt man hat das Routing so eingerichtet. Will man nur bestimmte Hosts erreichbar machen, so muss man das entweder über Access-Listen oder über Security Groups sicherstellen. Damit die Systeme von sich aus für Updates trotzdem auf das Internet zugreifen können, existieren so genannte „Egress Only Internet Gateways“. Diese kann man bei Bedarf als Default Gateway bei den Servern eintragen.

IP-Design in und mit der Cloud

Um sicher zu stellen, dass man seine Systeme in der Cloud auch erreichen kann, müssen sich die IP-Adressen in der Cloud natürlich von denen des eigenen Netzes unterscheiden. Entsprechend muss der IP-Bereich bei V4 gewählt werden. Weitere, wesentliche Fragen bei dem IP-Design sind:

- In wie vielen Regionen wird man langfristig tätig werden?
- Wird man langfristig mit mehr als einer VPC pro Region auskommen?
- Wie viele Subnetzte pro VPC werden benötigt?
- Wie viele Systeme wird es in einem Subnetz geben?

Bei Beantwortung dieser Fragen sollte man VPCs wie Rechenzentren/Sicherheitszonen betrachten und die IP-Adressen entsprechend planen. Man kann die Erfahrungen aus dem Eigenbetrieb also durchaus übernehmen.

Eine generelle Lösung gibt es dafür nicht. Da das 10er Netz von vielen Unternehmen genutzt wird, wird ein Design wie in Abbildung 3 nur in den wenigsten Fällen möglich sein. Stattdessen wird man auf kleinere CIDR-Blöcke oder andere private IPv4-Blöcke wie den 172.16er zurückgreifen müssen. Das schränkt die Flexibilität bei der Planung unter Umständen erheblich ein.

Auf der anderen Seite dürften nur wenige Unternehmen in vielen Regionen unterwegs sein und/oder mehrere VPCs pro Region betreiben, weshalb ein Design wie in der Abbildung dargestellt weit über das Ziel hinausschießen dürfte.

Was man jedoch anhand dieses idealisierten Designs schön sehen kann, ist, dass bei der Planung zusammenhängende Adressblöcke genutzt werden sollten, die dann nach dem dargestellten hierarchischen System aufgeteilt werden. Auf diese Weise entsteht ein sauberes IP-Design, das man später einfach wird pflegen können. Außerdem erkennt man so auch

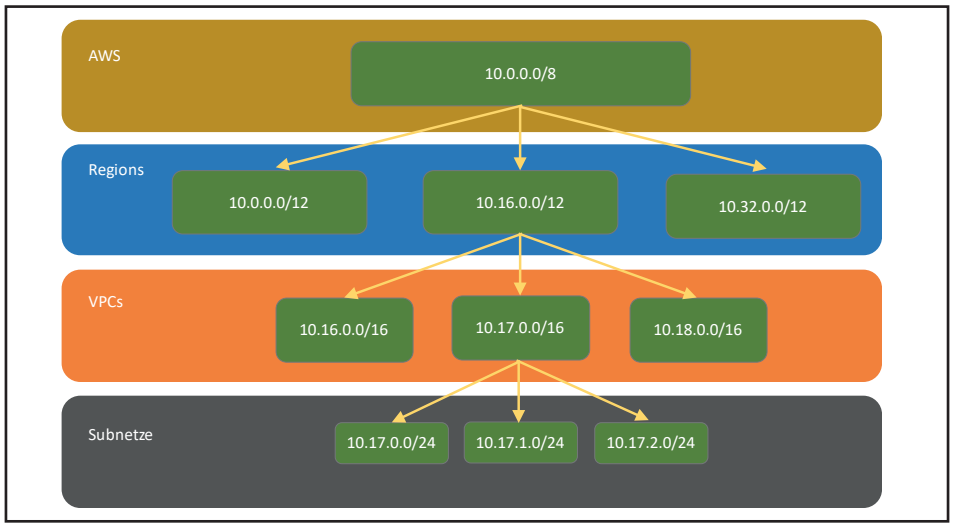


Abbildung 3: Idealisiertes IPv4 Design für den Cloud-Betrieb

beim Troubleshooting anhand der IP-Adresse schnell, ob es sich um Cloud- oder interne Systeme handelt. Schon allein aus diesem Grund sollten die Netzwerkverantwortlichen eines Unternehmens von vorn herein in die Planung jeglicher Cloud-Aktivitäten eingebunden werden.

Bei IPv6 steht man vor anderen Herausforderungen. Da die IP-Adressen aus dem Bereich stammen, der Amazon in der entsprechenden Region zugewiesen wurde, hat man das Problem der Adressüberschneidungen mit den eignen Adressen schon mal nicht. Hinzu kommt, dass man pro VPC einen nicht wählbaren /56er Bereich von Amazon zugewiesen bekommt, nicht pro Region.

Damit reduziert sich die Planung dramatisch, wie in Abbildung 4 dargestellt. Statt mit immer granularer werdenden Subnetzmasken zu jonglieren, reduziert sich das Design auf die /64-Maske für die Subnetze.

Da es sich um öffentliche IP-Adressen handelt, die auch zu den entsprechenden Rechenzentren von Amazon geroutet werden, muss man bei dem Anschluss der Cloud an das eigene Netz jedoch beachten, dass diese Netze über die Default-Route, also über das Internet angesteuert würden, wenn man kein entsprechendes Routing einträgt. Trägt man das Routing jedoch ein, so werden die Systeme über die Direct Connect Verbindungen und zukünftig auch über VPN-Verbindungen angesprochen. Access-Listen würden so u.U. umgangen. So kann es zu einem anderen Verhalten kommen, als es ein User erlebt, der irgendwo im Internet sitzt. Da zudem IPv6 gegenüber IPv4 bevorzugt wird, sollte man Tests grundsätzlich auch mit Rechnern machen, die nicht über das Firmennetz auf die Cloud-Systeme zugreifen, um sicher zu stellen, dass alles, was erlaubt ist, auch funktioniert und alles, was verboten ist, wirklich nicht aus dem

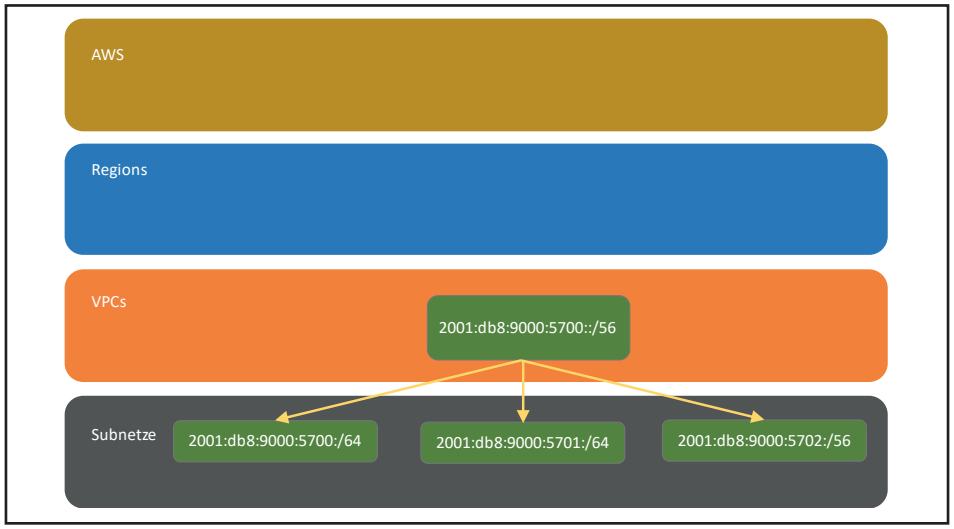


Abbildung 4: IPv6-Design in der AWS-Cloud

Internet heraus erreichbar ist. Die Tests müssen natürlich mit beiden Versionen von IP durchgeführt werden.

Verbindungen

Cloud-interne Verbindungen

Router

Innerhalb eines VPCs dient ein virtueller Router als Gateway zwischen den Subnetzen einer VPC. Dabei ist es egal, ob die Subnetze sich in derselben Availability Zone befinden oder in unterschiedlichen. Abbildung 5 zeigt beispielhaft einen Aufbau einer VPC mit Availability Zonen mit je einem Subnetz. Über den virtuellen Router können die Hosts in den Subnetzen miteinander kommunizieren.

Prinzipiell kann es beliebig viele Routing-Tabellen geben. Aber es macht natürlich keinen Sinn, mehr Routing-Tabellen als Subnetze zu haben. Generell gilt, dass man entweder wirklich für jedes Subnetz eine eigene Tabelle anlegt, oder besser noch versucht mit möglichst wenigen aus zu kommen, bspw. einer für Subnetze mit Zugriff auf bzw. vom Internet und einer ohne diesen Zugriff. Abbildung 6 zeigt eine Routing-Tabelle mit Zugriff auf/vom Internet und auch die Zuordnung zweier Subnetze zu dieser speziellen Routing-Tabelle.

Dabei ist zu beachten, dass die ersten beiden Zeilen nicht editierbar sind und auch nicht gelöscht werden können. D.h. eine Routing-Tabelle stellt immer die Kommunikation zu allen anderen Subnetzen einer VPC bereit. Da jedem Subnetz eine Routing-Tabelle zugeordnet werden muss, können Systeme eines VPCs immer miteinander über den Default-Router kommunizieren. Weder ist es möglich, die Kommunikation zu unterbinden noch eigene Middleboxen (Firewall, IDS/IPS) dazwischen zu positionieren.

Die letzten beiden Zeilen aus Abbildung 6 mit den Default-Routen für IPv4 und IPv6 müssen hingegen manuell hinzugefügt werden. Damit kann man also problemlos eine Routing-Tabelle anlegen, die zwar den VPC-internen Verkehr erlaubt, ins Internet hingegen nicht. Später in diesem Artikel werden noch Verknüpfungen der Corporate-Netze mit der VPC vorgestellt, auch für diese können bzw. müssen eigene Einträge in den Routing-Tabellen angelegt werden.

Je nach Sicherheitsbedürfnis und Anwendungsfall für die VPC sollten verschiedene Arten von Routing-Tabellen angelegt und den Subnetzen zugeordnet werden:

- Internet Access
  Wenn man den Hosts Zugriff auf das Internet gewähren will, muss man natürlich eine Routing-Tabelle anlegen, die auch eine Default-Route enthält. Arbeitet man mit beiden Versionen von IP, müssen auch für V4 und V6 Default-Routen angelegt werden.

  Beim Einsatz von IPv6 ist zu beachten, dass damit alle Hosts nicht nur auf das Internet zugreifen können, sondern auch umgekehrt, da Amazon öffentliche IPv6 Adressen vergibt.

  Bei IPv4 hingegen gilt, dass nur solche Hosts die Elastic IP Adressen haben, auch auf und vom Internet.

- Reiner VPC Traffic
  Für komplexe Anwendungen in der Cloud wird es eine ganze Anzahl von Hosts geben, die nur „interne“ Aufgaben erledigen. Beispielsweise bei einer mehrstufigen Web-Anwendung müssen nur die Frontend-Server wirklich vom Internet aus erreichbar sein, nicht jedoch die Anwendungsserver oder Datenbanken.

  Ist die Anwendung so geschrieben, dass ein Zugriff vom Corporate-Netzwerk direkt nicht notwendig ist, kann man dafür ein eigene Routing-Tabelle anlegen, die nur den internen Verkehr erlaubt.

  Dabei ist jedoch zu beachten, dass in diesem Fall auch kein Zugriff für die Wartung und Pflege möglich ist.

  Man sollte sich also gut überlegen, ob man das wirklich will. Aus Sicht der Sicherheit kann das jedoch Sinn machen, wenn man den administrativen Zugriff auf Cloud-Systeme dadurch kontrollieren möchte, dass diese nur über einen speziellen Host in der Cloud erreichbar sind.

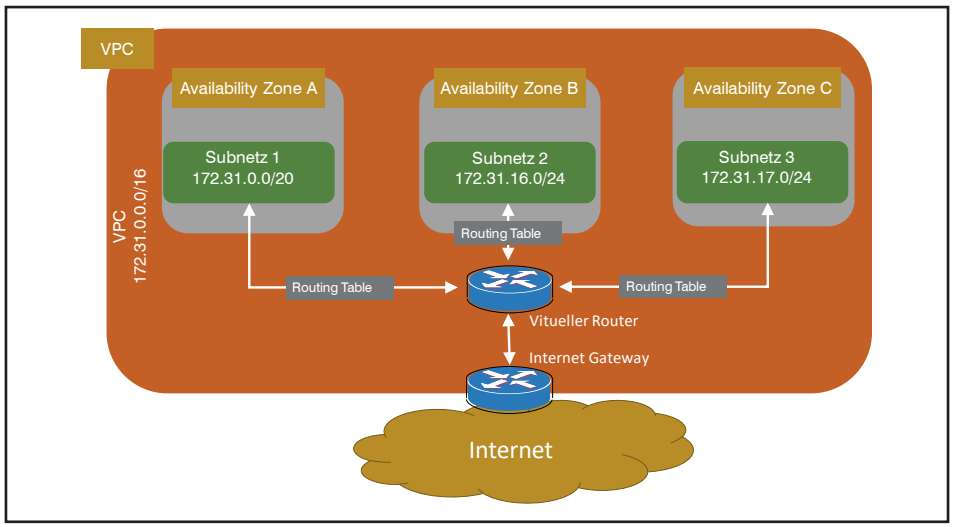


Abbildung 5: Schematischer Aufbau einer gerouteten VPC

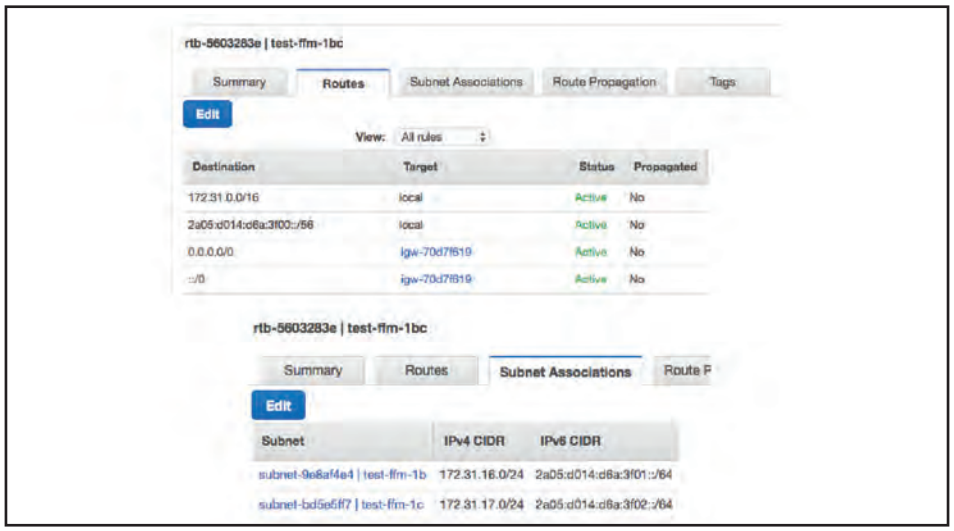


Abbildung 6: Routing-Tabelle und Subnetz-Zuordnung

Übrigens muss diese Liste nicht angelegt werden, es handelt sich um die default Routing-Table, die man zwar editieren kann. Aber, wie bereits gesagt, kann sie nur um weitere Einträge ergänzt und nicht gelöscht werden. Das interne Routing selbst lässt sich keinesfalls verhindern.

- Corporate/VPC Zugriff
  Will man Systeme zwar nicht öffentlich erreichbar machen, jedoch aus Wartungs-/Entwicklungs-/etc.-Zwecken vom Firmennetzwerk, kann man eine Routing-Tabelle erstellen, die die Firmennetze in Richtung eines VPN-Gateways bzw. Direct Connect Gateways lenkt. Dasselbe gilt natürlich auch für hybride Cloud-Lösungen.

In den meisten Fällen dürften diese Routing-Tabellen ausreichen. Jedoch gibt es noch weitere, speziellere Einsatzmöglichkeiten. Beispielsweise ist es möglich so genannte Endpoints zu definieren: damit kann man aus seinen Subnetzen heraus AWS Dienste erreichen, ohne dass man den Systemen, die das tun, öffentliche IP Adressen zuweisen muss. Ein anderes Beispiel wäre, wenn man mittels Peering zu anderen VPCs Verbindungen aufgebaut hat. Dazu später mehr.

Routing Hosts

Nun ist es im eigenen Rechenzentrum aber schon lange nicht mehr ungewöhnlich, mit Sicherheitszonen zu arbeiten. Dabei werden Firewalls bzw. IDS/IPS genutzt, den Traffic zwischen den Zonen zu kontrollieren.

Die Idee liegt nahe, das auch zwischen Subnetzen in der VPC zu tun. Da allerdings stößt man auf Widerstand. Zwar gibt es durchaus Firewall-/IPS-/IDS-Lösungen für AWS, diese unterliegen jedoch den Einschränkungen der VPC und sind nicht so einsetzbar, wie man es vom eigenen Rechenzentrum her gewohnt ist.

Die einfachste Lösung wäre es, einem Host zumindest zwei Netzwerkinterfaces zu spendieren, die in unterschiedlichen Subnetzen sind. Darauf installiert man eine Firewall seiner Wahl und nutzt diesen Host als Router. Das ist wegen des nicht editierbaren Defaul-Routings innerhalb einer VPC jedoch nicht sinnvoll. Zwar wäre es grundsätzlich möglich, die IP Adressen auf den Servern statisch zu konfigurieren, anstatt mit dem VPC eigene DHCP zu arbeiten, dabei muss man jedoch bedenken, dass es Dienste gibt, die eigene Interfaces in den Subnetzen haben können. Dazu gehören beispielsweise Datenbanken. Diese bekommen ihre IP Adressen jedoch unmittelbar von Amazon. Dasselbe gilt bei der Neu-Anlage eines Servers,

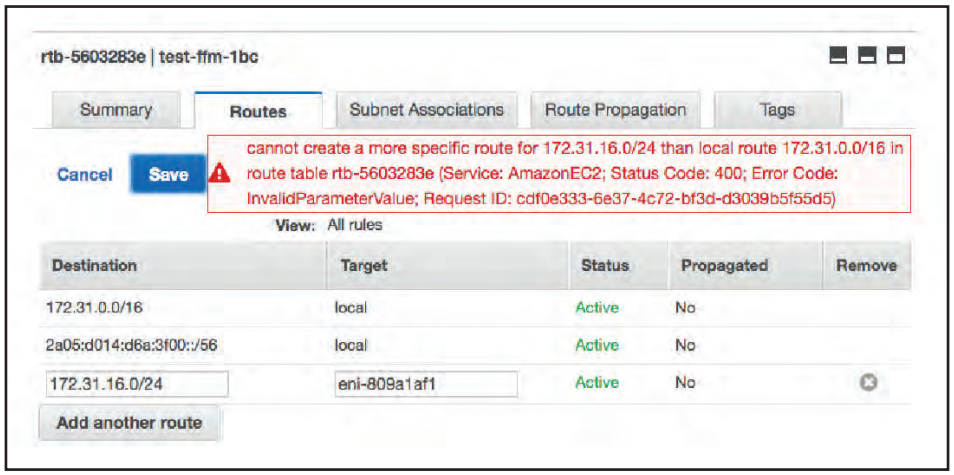


Abbildung 7: Kein Routing zu Teilnetzen

auch dabei werden zunächst IP Adressen per DHCP vergeben, die man erst nachträglich ändern kann.

Man kann darauf pokern, dass es zu keinen Überschneidungen kommt, aber es ist ein Risiko. Da man VPCs wie Rechenzentren/Sicherheitszonen behandeln sollte, sollte man dieses lieber nicht eingehen, sonst schießt man sich versehentlich einen Server wegen doppelter IP Adressen ab.

Es käme noch eine weitere Lösung in Frage: man platziert die Middleboxen in einem anderen Subnetz und ändert das Routing so, dass alles über dieses Subnetz geroutet wird. Als Netzwerker ist man gewohnt, dass Routing-Tabellen mittels „Longest Match“ bzw. „Most Specific“ ausgewertet werden. Es ist in der klassischen Routing-Tabelle also kein Widerspruch für das Netz 10.0.0.0/0 einen Next-Hop zu pflegen und für das spezifischere Netz 10.0.1.0/24 einen anderen. Wie Abbildung 7 zeigt, ist dieser Lösungsansatz leider nicht möglich.

Somit bleibt noch eine letzte Möglichkeit über: anstatt eine VPC als Rechenzentrum zu betrachtet, betrachtet man sie als Sicherheitszone. Das wiederum funktioniert. Die Fehlermeldung in Abbildung 7 besagt, dass eine spezifischere Route nicht möglich ist, wie Abbildung 8 zeigt, ist eine weniger spezifische Route – hier Default-Route – jedoch möglich. Ebenso kann man Routen zu Netzen definieren, die in einer anderen VPC liegen.

Diesen Trick nutzen die Firewallhersteller wie Sophos, Checkpoint oder Palo Alto, um ihre virtuellen Firewalls in AWS zu platzieren. Abbildung 9 zeigt wie so etwas aussehen kann.

Da sämtlicher Verkehr durch die Firewalls läuft, können diese den natürlich filtern. Allerdings fallen für die Firewalls Lizenzkosten an.

Eine andere Anwendung für diese Routing Hosts ist der Schutz der eigenen Server vor dem Internet. Will man einen Webauftritt aus der Cloud anbieten, möchte man unter Umständen auf eine Next Generation Firewall zurückgreifen, die weit mehr Schutzmöglichkeiten bietet, als es die zur Zeit doch eher bescheidenen An-

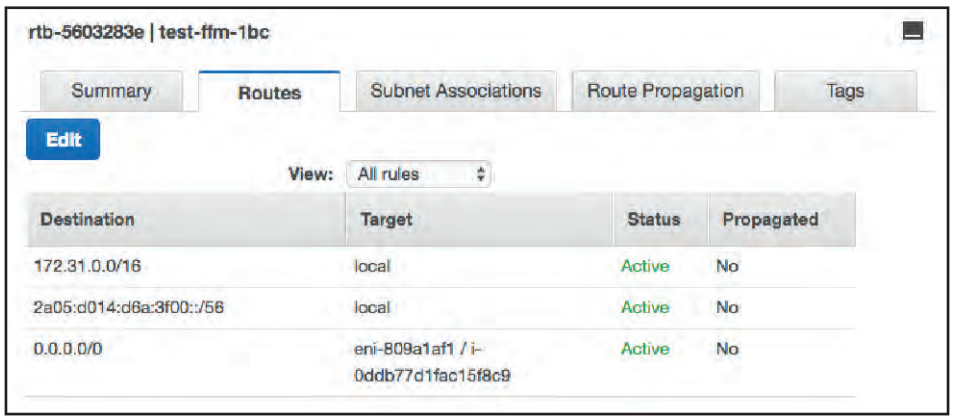


Abbildung 8: Default Route über eigene Firewall

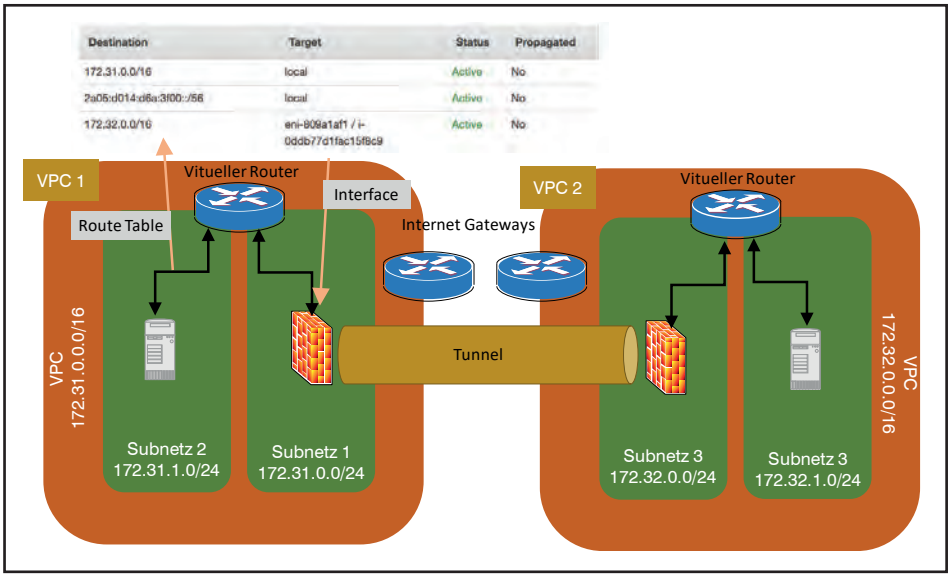


Abbildung 9: Tunnel zwischen VPCs

gebote von Amazon tun. Viele namhafte Hersteller bieten deswegen ihre Firewalls auch im AWS-Marketplace als virtuelle Lösungen eben dafür an.

Abbildung 10 zeigt wie so ein Aufbau aussieht. Auf den ersten Blick scheint diese Lösung schlüssig zu sein. Sie hat jedoch einen Pferdefuß. Denn was man auf den ersten Blick schnell übersieht, ist das Fehlen von IPv6 Adressen. Und richtig! Dieser Aufbau funktioniert nur mit IPv4 oder NAT66, was eigentlich niemand will.

Der Grund ist einfach:
Bei IPv4 gibt man die Elastic IP Adresse der Firewall im DNS als Webserver-Adresse an. Die Clients schicken ihre Pakete somit direkt an die Firewall. Die macht dann NAT-Forwarding, sprich leitet alle Pakete für Port 80 an den Webserver weiter. Dessen Antwortpakete werden entlang der Default-Route des Subnetzes 1 gesendet, die wie bei Abbildung 9 auf die Firewall zeigt. Diese macht wieder NAT und die Antwort erreicht anschließend über das Internet Gateway, das bei der Default Route von Subnetz 2 eingetragen ist, ihr Ziel im Internet. Wer mag kann sogar Loadbalancing zwischen verschiedenen Webservern machen, entweder über die Firewall-Funktion oder den AWS-Dienst.

Bei IPv6 funktioniert der Trick nur, wenn man NAT66 auf der Firewall macht, was eigentlich nicht gewollt ist. Macht man das nicht, so landet die Anfrage aus dem Internet direkt bei dem Webserver, da der virtuelle Router das Subnetz des Webservers kennt und man in diesem Fall keine Route zur Firewall definieren kann. Die Antwortpakete könnte man zwar über die Firewall schicken, das jedoch würde die Firewall „verwirren“, sprich sie würde blocken, da sie nur Antworten, aber keine Fragen sieht. Ein Fall, auf den sich keine Firewall einlässt.

Peering Groups
Man kann auch VPCs miteinander kombinieren, ohne dass man darauf auf Thrid-Party-Lösungen zurückgreifen muss. Amazon stellt dafür die Funktion „Peering“ zur Verfügung. Anders als die Tunnellösung zwischen Thrid-Party-Firewalls ist Peering jedoch nur innerhalb einer Region möglich. Neben der Verknüpfung eigener VPCs kann Peering auch genutzt werden, um eine Verbindung zu anderen Accounts herzustellen, also bspw. Partnerfirmen.

Die IP-Bereiche der VPCs sollten sich unterscheiden. Zwar gibt es auch Lösungen für den Fall, dass das nicht der Fall ist, diese sind aber aufwendiger und mit denselben Restriktionen behaftet, die man auch hat, wenn man versucht, mit einer Partnerfirma eine Verbindung herzustellen, die denselben privaten IP-Bereich nutzt wie man selbst.

Ist das Peering zweier VPCs noch sehr übersichtlich, wird es bei mehreren VPCs schnell komplex. Als Design-Lösungen bieten sich dieselben Varianten an, die man von der Standort-Standort-Kopplung des eignen Unternehmens her kennt: Stern oder Full-Meshed. Bei Letzterem fällt sehr viel Konfigurationsaufwand an. Bedenkt man, dass der Traffic zwischen VPCs anders als VPC interner Traffic nicht kostenfrei ist und dass das Peering auf eine Region beschränkt ist, so sollte man sich mit der Anzahl von VPCs pro Region möglichst zurückhalten.

Verbindungen in die Cloud
Da Cloud-Computing kein Selbstzweck ist und die Geräte sich auch nicht selbst aufsetzen und warten, benötigt man neben den Verbindungen zwischen Subnetzen, VPCs und Regionen natürlich auch noch Verbindungen in und aus der Cloud. Abhängig von der Art des Zugriffs stehen verschiedene Möglichkeiten zur Verfügung.

Zugriff aus dem Internet
Typisch für Cloudanwendungen ist, dass man damit Dienste für eine breite Öffentlichkeit oder viele Kunden anbieten möchte. Ein Zugriff aus dem Internet muss also möglich sein. Um die Verbindung zwischen den Cloudnetzen und dem Internet herzustellen, gibt es die Internet Gateways. Bei AWS beginnen die Namen mit „igw-“.

Um mit dem Internet kommunizieren zu können, benötigen die Systeme öffentliche IP Adresse aus dem Adressraum vom Amazon, die bereits erwähnte Elastic IP Adressen. Diese können den Servern zugeordnet werden. Einige Dienste wie Datenbanken oder der Mailservice SES bringen von Hause aus eigene öffentliche IP Adressen mit.

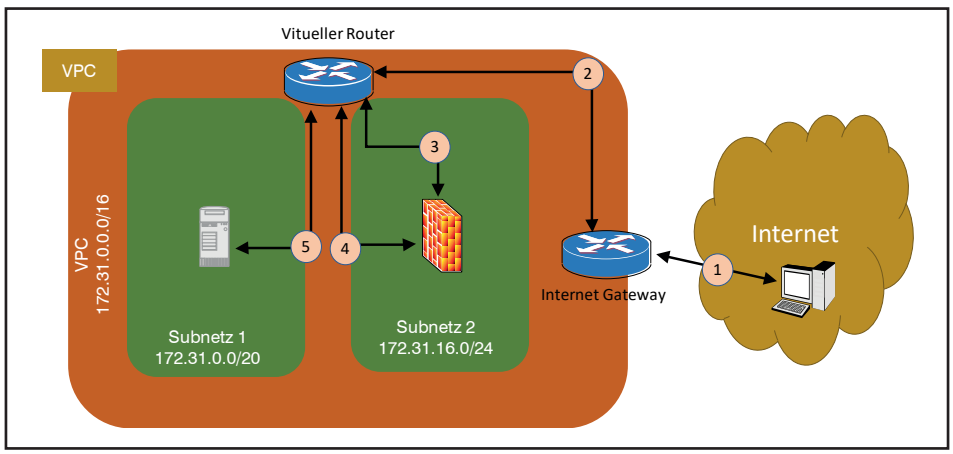


Abbildung 10: Firewall als Schutz für Server

Neben der Möglichkeit, die Systeme mit öffentlichen IP Adressen auszustatten, gibt es zwei Varianten NAT zu nutzen:

1. NAT Instanzen
   Eine NAT-Instanz ist nichts anderes als ein EC2-Server mit einem speziellen Amazon-eigenen Linux-Image, das die notwendigen NAT Funktionen bereits beinhaltet.

   Einmal installiert muss das NAT selbst eingerichtet werden. Auch die entsprechenden Routing-Tabellen, Security Groups und Access Listen muss man selbst anpassen. Da eine NAT Komponente naturbedingt vom Internet her angreifbar ist, muss man auch entsprechende Routinen schaffen, um das Software-Image aktuell zu halten.

   Die Netzwerk-Einstellungen entsprechen denen von Abbildung 10, was wenig überraschend ist, da eine Firewall, wie in der Abbildung dargestellt, natürlich ebenso als NAT-Instanz betrieben werden kann.

2. NAT Gateway
   Alternativ zur selbst betriebenen NAT-Instanz bietet Amazon die Möglichkeit der NAT-Gateways. Wie die NAT-Instanzen bieten diese Cloud-Systeme ebenfalls die Möglichkeit auf das Internet zuzugreifen. Der Vorteil der NAT-Gateways ist, dass man sich um deutlich weniger kümmern muss, als bei selbst betriebenen Lösungen. Der Nachteil ist, dass der Funktionsumfang eingeschränkt ist:

   NAT-Instanzen und virtuelle Firewalls bieten die Möglichkeit, interne Systeme aus dem Internet heraus erreichbar zu machen. Das geschieht mittels NAT Forwarding, also einer portbasierte Weiterleitung von Paketen. Diese Möglichkeit gibt es bei den Amazon-NAT-Gateways nicht. Ebenso wenig kann man einen Bastion Host hinter einem NAT-Gateway betreiben, also einen Host, zu dem aller eingehende Verkehr geroutet wird. NAT-Instanzen und die meisten Firewalls bieten eine solche Möglichkeit.

   Ein typisches Einsatzszenario für NAT-Gateways ist es, Servern für Systemupdates eine Verbindung ins Internet zur Verfügung zu stellen, die selbst nicht aus dem Internet erreichbar sein sollen. Server, die aus dem Internet erreichbar sein sollen, gibt man Elastic IP Adressen und kann so auf NAT verzichten.

Der Zugriff aus dem Internet kann natürlich genutzt werden, um die Systeme per ssh oder Ähnlichem zu warten. Ebenso könnte man diesen Zugang auch nutzen, um eine hybride Cloud aufzusetzen. Allerdings ist beides aus Sicherheitsgründe wenig empfehlenswert, da man so alle Dienste zum Internet hin entblößt. Grundsätzlich gilt, dass man nur die Dienste zum Internet hin öffnet, die auch allen zur Verfügung gestellt werden sollen.

VPN

Für den erweiterten Zugang zu den Cloud-Diensten und -Servern gibt es neben selbst gebastelten Lösungen zwei AWS Dienste: VPN und Direct Connect.

Die VPN-Lösung setzt auf Seiten des AWS Kunden mindestens ein dediziertes VPN-Gateway voraus. Eine VPN-Lösung zur Einwahl von Endgeräten existiert nicht. Amazon gibt eine Liste von Geräten an, die für die VPN-Verbindung getestet sind. Richtet man die VPN-Verbindung mittels Web-Oberfläche ein, gibt es für viele dieser Geräte auch eine Konfiguration zum Download, die man nach kleinen Anpassungen auf seinem Gateway einspielen kann. Neben diesen empfohlenen Geräten können aber auch andere VPN-Lösungen auf Kundenseite eingesetzt werden, vorausgesetzt sie erfüllen die notwendigen Voraussetzungen und unterstützen die geforderten Protokolle und Algorithmen.

Abbildung 11 zeigt die einfachste Variante eines VPN zwischen Kundennetz und AWS:

Auf Seiten des Kunden steht in diesem Fall ein VPN-Gateway. Auf Seiten von AWS werden zwei virtuelle Router als VPN-Endpunkte eingerichtet. Entsprechend müssen vom eigenen Gateway ausgehend auch zwei Tunnel konfiguriert werden. Amazon gibt an, dass von Zeit zu Zeit Wartungsarbeiten an den Routern durchgeführt werden. Die zweite Tunnellösung ist somit notwendig, um für diesen Fall, ebenso wie im Fehlerfall, eine unterbrechnungsfreie Verbindung zwischen Kundennetz und Cloud zu gewährleisten. Es ist jedoch immer nur einer der beiden Tunnel aktiv.

Die Tunnel werden stets von Seiten des Kunden-Gateways aufgebaut und auch nur bei Bedarf und nicht persistent. Das bedeutet, dass Systeme in der Cloud keine Verbindung zu Systemen im Unternehmensnetz aufbauen können, wenn die Verbindung gerade mal nicht geöffnet ist. Benötigt man eine dauerhafte Verbindung zwischen den Netzen, so empfiehlt es sich, diese Verbindung mittels Keep-Alives oder Monitoring-Tools offen zu halten.

Die Tunnel sind mit IPsec verschlüsselt. Als Schlüsselaustausch-Protokoll wird Internet Key Exchange (IKE) eingesetzt.

Neben dieser einfachen Lösung können natürlich auch komplexere nach diesem Muster gebaut werden. Will man bspw. auch auf Kundenseite mit zwei Gateways arbeiten, so verdoppelt man im Grunde das Bild aus Abbildung 11. Ebenso kann man sein Gateway natürlich nutzen, um VPNs zu verschiedene Regionen des AWS aufzubauen.

Für das Routing zwischen Unternehmensnetz und Cloud werden zwei Lösungen angeboten: entweder man routet statisch oder nutzt BGP. Vorausgesetzt man hat aggregierbare Routen für alle genutzt Regionen und auch das eigene Netz hat ein nicht allzu chaotisches IP-Design, so wird in den meisten Fällen statisches Routing ausreichen.

Direct Connect

Die VPN-Lösung ist sicherlich reizvoll, wenn es um die reine Wartung der AWS-Syste-

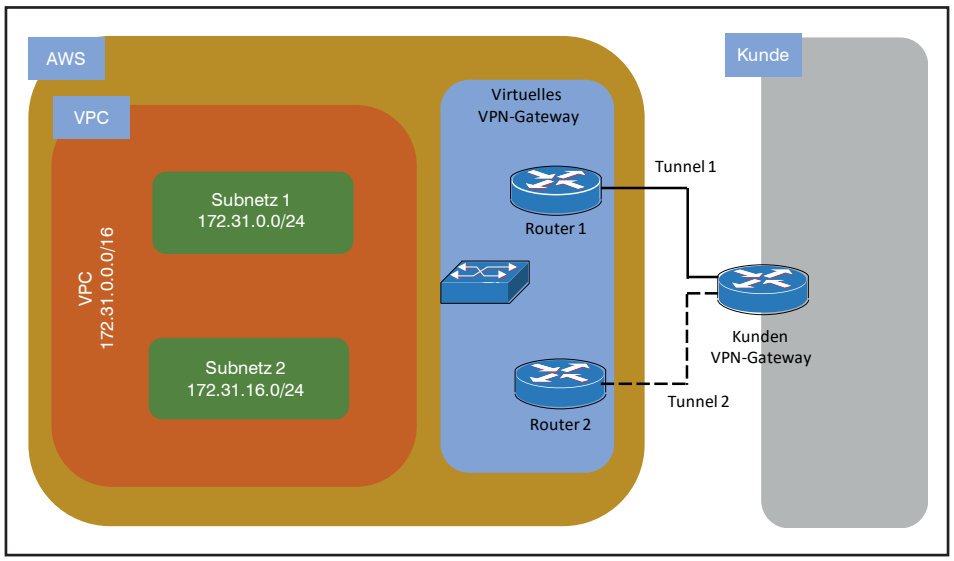


Abbildung 11: Einfache VPN-Verbindung zwischen Kundennetz und AWS

me und das Aufspielen der Anwendungen geht. Auch für kleinere bis mittlere Cloud-Lösungen dürfte sie im Regelfall ausreichen. Will man AWS als hybride Cloud nutzen, bei der viele Daten zwischen dem eigenen und dem Cloud-Netz ausgetauscht werden, so bieten VPN-Verbindungen über das Internet nicht die notwendige Bandbreite und geforderte Performance.

Für diesen Fall gibt es AWS Direct Connect. Abbildung 12 zeigt des Aufbau eines Direct Connect Zuganges in die AWS Cloud.

Amazon unterhält eine Reihe von so genannten Direct Connect Locations auf der ganzen Welt. Diese Standorte sind jeweils den Regionen zugeordnet. Die AWS Direct Connect Locations sind typischerweise Rechenzentren, in denen man auch selbst Reckspace anmieten kann wie bspw. Equinix.

Zwischen diesen Standorten und der AWS Region können die Kunden breitbandige, hochperformante Glasfaser-Verbindungen mieten. Die Verbindungsgeschwindigkeiten sind wahlweise 1 oder 10 Gigabit, wobei mehrere Glasfaser aggregiert werden können. Über diese physikalischen Verbindungen werden virtuelle Interfaces definiert, die in zwei Kategorien unterschieden werden: public und private. Über die private Interfaces erreicht man seine eigenen VPCs und die dort gehosteten Server. Die public Interfaces dienen dazu, öffentliche AWS Dienste wie S3 ansprechen zu können, ohne den „Umweg“ über das Internet nehmen zu müssen.

Für den Kunden bleibt somit die Frage, wie man denn das eigene Rechenzentrum genau so performant mit den Direct Connect Locations verbindet. Dafür stehen einem zwei Möglichkeiten offen: entweder man mietet sich Rackspace in dem entsprechenden Rechenzentrum und betreibt dort seine eigenen Server oder man wendet sich an einen Direct Connect Partner, der einem die gewünschte Verbindung vom eigenen Rechenzentrum in die Direct Connect Location zur Verfügung stellt. Amazon listet die Partner auf seiner Homepage getrennt nach Regionen auf.

Es muss einem klar sein, dass diese Lösung eine Stange Geld kosten wird: nicht nur der AWS Direct Connect Link muss bezahlt werden, sondern auch die Partner, egal ob es nun die Miete für Platz in Serverracks oder die Verbindung zu den AWS Locations über Service Provider ist. Beides dürfte nicht günstig sein. Bevor man sich für diese Lösung entscheidet, sollte man also sehr sicher sein, dass Amazon mit seinem AWS Angebot der richtige Partner ist.

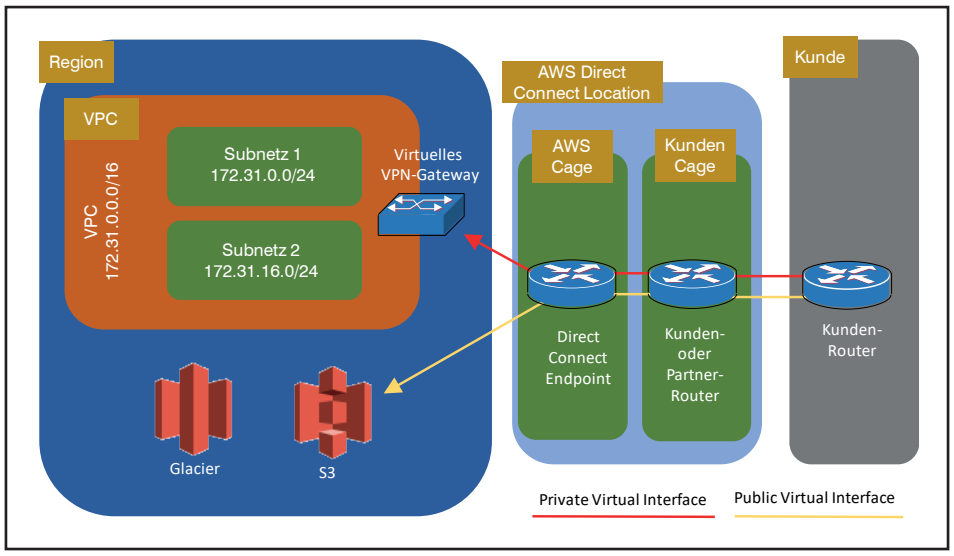


Abbildung 12: AWS Direct Connect

Fazit

Dieser Artikel hat die Kernkomponenten von Cloud-Netzen im Fokus gehabt. Darüber hinaus gibt es noch viele weitere Aspekte, die für Netzwerker relevant sind. Dazu gehören u.a. Sicherheit, Access Listen, Service Groups, Content Delivery Networks (CDN), DHCP in VPCs etc. Aber schon diese Auswahl zeigt, dass Netzwerker die Cloud nicht als ein Problem anderer Leute betrachten können, sondern dass die Gestaltung der Cloud ebenso zu ihren Aufgaben gehört, wie das Design eines Rechenzentrumsnetzes. Denn im Grunde ist eine Cloud-Lösung der Marke Amazon ebenso wie Azure von Microsoft nichts anderes als ein gehostetes Rechenzentrum, oder im Falle einer hybriden Cloud die virtuelle Erweiterung desselben.

Netzwerker sind also gut beraten, das Thema nicht auf die lange Bank zu schieben, sondern sich von Anfang an, an der Gestaltung der Cloud-Lösung des eigenen Unternehmens zu beteiligen.

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 1590,- € statt regulär 2180,- €.

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 _____

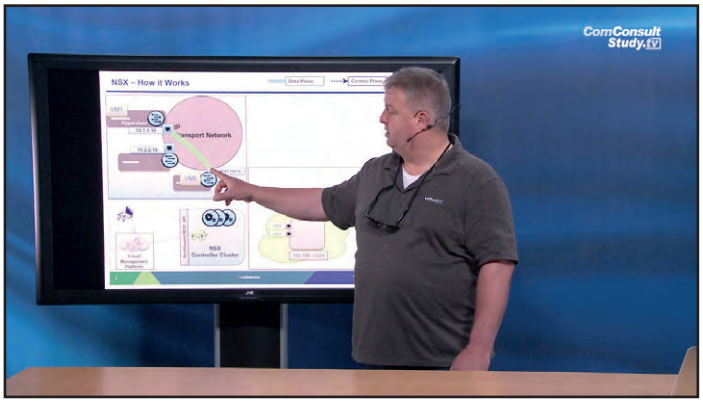
Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

ComConsult-Study.tv

Aktuelle Video-Neuerscheinungen

Die Virtualisierung ist in den Rechenzentren von heute Standard. Dazu gehört auch die Virtualisierung der Netzwerke. Allerdings hängen die virtuellen Netze nicht im luftleeren Raum. Vielmehr benötigt jedes Overlay- auch ein Underlaynetzwerk. Zur Zeit gibt es ein Ringen um die Vorherrschaft über die Netzadministration: Virtualisierer und Hardwarehersteller positionieren ihre Administrationstools neu, um dieses Ringen für sich zu entscheiden. Hinzu kommt, dass Server letzten Endes auch mit Clients kommunizieren. Dazu müssen die virtuellen Netze mit dem Rest der Welt verbunden werden. Die Frage, welches Routingprotokoll dafür genommen werden soll, wird heiß diskutiert. Zu diesen Themen gibt es eine Reihe von neuen Videos bei ComConsult Study.tv. Hier eine kleine Auswahl:



VMware NSX Basics

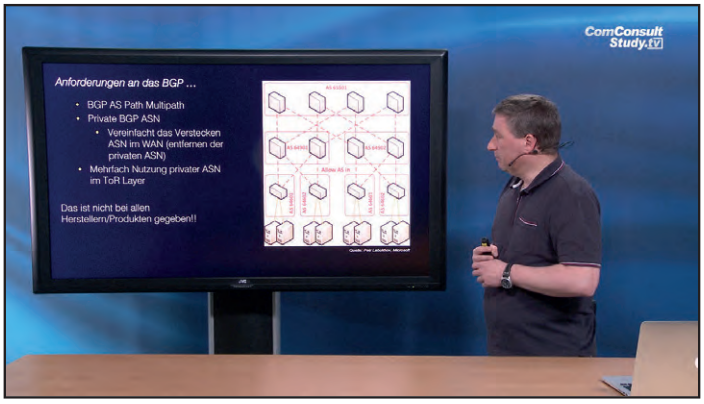
Referent: **Gerd Pflüger**
Zeit: 00:20:26
Preis: kostenlos

Der kurze Vortrag zeigt die Grundfunktionen von VMware NSX. Zudem werden die Begrifflichkeit der Datacenter-Virtualisierung erklärt. Ausgehend von der Virtuellen Maschine (VM) und dem IP-Transport-Netz werden Enkapsulierung und die notwendigen Services angesprochen. Der Inhalt des Vortrages ist technisch einfach aufgebaut und spricht sowohl den Netzwerk-Techniker als auch den technischen Entscheider an.

Die Zukunft von Netzwerk-Hardware

Referent: **Markus Harbeck**
Zeit: 00:28:11
Einzelpreis: 49,00 € netto
Im Abo: kostenlos

Warum entwickelt Cisco eigene Hardware und eigene ASICs, wenn doch alle auf „Software only" setzen? In dieser Session wird erklärt, warum man spezifische Hardware und ASICs braucht und darüber hinaus welche Möglichkeiten Ihnen Cisco trotzdem liefert, offen mit der zur Verfügung gestellten Hardware umzugehen. U.a. Network Function Virtualization, Container und Guestshell.



Netzdesigns für Data Center im Vergleich

Referent: **Markus Geller**
Zeit: 00:37:41
Einzelpreis: 49,00 € netto
Im Abo: kostenlos

Aktuelle Netzwerk Infrastrukturen in Data Center basieren in der Regel auf zwei Säulen: einem Layer 2 Netz mit etablierten Verfahren wie RSTP und Link Aggregation und einem Layer 3 Netz mit OSPF oder IS-IS für die IP Kommunikation.

Zukünftige Rechenzentren orientieren sich aber an neuen Layer 2 Mechanismen oder einem reinen Layer 3 Design mittels BGP als Steuerungsprotokoll.

Standpunkt

Muss man Gebäude abschirmen?

Der Standpunkt von Dr. Joachim Wetzlar 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.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat vor einigen Jahren eine technische Richtlinie mit dem Titel „Elektromagnetische Schirmung von Gebäuden“ (BSI TR-03209) veröffentlicht. Darin finden sich neben allerlei theoretischen Grundlagen zur Wellenausbreitung und deren Schirmung insbesondere auch umfangreiche Messreihen zur Dämpfung verschiedenster Baumaterialien (im Teil 2). Sie können sich vorstellen, dass ich die Lektüre sehr interessant fand.

Mit welchem Ziel beschäftigt sich ausgerechnet das BSI mit diesem Thema? Ganz einfach: Es geht um das Vermeiden „bloßstellender Abstrahlung“, letztlich um den Schutz der in IT-Systemen verarbeiteten Informationen vor Abhören durch Unbefugte. Das ist sicher nicht mein Anliegen. Ich komme dennoch gleich noch einmal darauf zurück. Zunächst berichte ich Ihnen jedoch von einem interessanten Fall, mit dem ich mich vor kurzem beschäftigen durfte.

Ein Kunde hat vor einiger Zeit ein neues Gebäude bezogen. Dieses Gebäude ist flächendeckend mit WLAN versorgt. Außerdem wurde Mobilfunk eingebracht. Alle drei deutschen Provider strahlen 2G- sowie 3G-Mobilfunk auf verschiedenen Frequenzen innerhalb des Gebäudes ab.

Daneben gibt es noch verschiedene weitere Funkdienste im Gebäude: Mikrophone für die Veranstaltungstechnik, Digitalfunk für Feuerwehr und Sicherheitsdienste, Mikrowellenherde in Teeküchen und nicht zuletzt – simple Lichtschalter. Die Trennwände zwischen Büros und Fluren wurden nämlich als (Milch-)Glasscheiben ausgeführt. Lichtschalter mussten also aufgeklebt werden, natürlich drahtlos! Desgleichen alle Raumthermostaten. Die beim Druck auf den Lichtschalter vom Finger abgegebene Energie ist für ein kurzes Funksignal ausreichend. Überall an den Decken verteilte Empfangsantennen leiten diese Signale an die Lichtsteuerung weiter. Raumthermostaten senden regelmäßige Lebenszeichen an diese Antennen. Sie sind mit Batterien ausgestattet, die mehrere Jahre Lebensdauer versprechen.

In einigen Bereichen des Gebäudes gibt es immer wieder Probleme mit den Raumthermostaten. Die regelmäßigen Lebenszeichen bleiben von Zeit zu Zeit aus. Der Hersteller ist ratlos. Schließlich habe ich mir die Sache vor Ort angesehen und Messungen mit dem Spektrumanalysator vorgenommen. Funkschalter und Thermostaten arbeiten bei 868 MHz. WLAN ist also „weit entfernt“. Aber vielleicht sendet ein anderes Funksystem in diesem Frequenzbereich.

Und wirklich: Immer wieder zeigte der Analysator starke Signale in unmittelbarer Nachbarschaft der Funkschalter an. Zum Teil mit 1000fachem Pegel und mit 10 MHz Bandbreite. Offensichtlich eine schnelle Datenübertragung. Gut möglich, dass die empfindlichen Empfänger der Funkschalter von diesen Signalen zeitweise „zugestopft“ werden. Die Suche nach der Signalquelle erwies sich als unerwartet schwierig. Wohin ich auch Analysator und Richtantenne bewegte, die Signale blieben gleich stark.

Am Ende entdeckte ich die Signalquelle in meiner Hosentasche: mein eigenes Smartphone! Die Überraschung war groß: Das Smartphone nutzte nämlich 4G-Mobilfunk, obwohl dieses im Gebäude gar nicht bereitsteht. Es hatte sich stattdessen mit einem Mobilfunkmast außerhalb des Gebäudes verbunden. Da dessen Signale durch Fenster, Wände, etc. stark gedämpft werden, musste das Smartphone offensichtlich mit hoher Leistung senden.

Einige Smartphones verhalten sich also wie manche WLAN Clients: Sie verbinden sich mit dem „schnelleren“ Netz, selbst wenn dieses erheblich schwächer empfangen wird als eine nur wenige Meter entfernte Basisstation älterer Technik. Meine Empfehlung für den Kunden lautete, baldmöglichst auch 4G im Gebäude bereitstellen zu lassen – auf anderen Frequenzen als ausgerechnet in unmittelbarer Nachbarschaft der empfindlichen Funkschalter.

Was lernen wir daraus: Erstens ist es überaus nützlich, einen Überblick über alle im Gebäude oder einer Liegenschaft genutzten Funkdienste zu haben. Ein Funkfrequenzbeauftragter, der ein entsprechendes „Kataster“ verwaltet, ist meines Erachtens ein Muss. Entsprechende Prozesse stellen sicher, dass Funktechnik nur mit Wissen und Genehmigung dieser Instanz in Betrieb geht. Die Wahrscheinlichkeit von Störungen lässt sich so frühzeitig minimieren.

Zweitens wird zukünftig die Abschirmung von Gebäuden eine Bedeutung erlangen. Nicht gegen bloßstellende Abstrahlung. Nein, vielmehr gegen störende Einstrahlung. Eine weitgehende Trennung der Funkwellen zwischen drinnen und draußen ermöglicht die Mehrfachnutzung der wertvollen Ressource „Spektrum“. Der Kampf um diese Ressource hat gerade erst begonnen!

Zweitthema

Ist BGP das bessere IGP?

Fortsetzung von Seite 1

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

Ein zusätzliches Problem, welches alle genannten Produkte gleichsam trifft, ist zudem der Umstand, dass die Lösungen zueinander inkompatibel sind. Da sich mit TRILL und SPB gleich zwei Standards zur Bildung von loop- und blockadefreien Layer 2 Strukturen etabliert haben, führte dies im Markt zu einer Aufspaltung in zwei Lager, so dass kaum eine Möglichkeit der Interoperabilität zwischen den Herstellern gegeben ist.

Aber auch Lösungen, die mit Multi-Chassis Link Aggregation arbeiten, haben ihre Probleme. Zum einen gibt es hierfür keine Standards im Rahmen von IEEE 802.3ad, und auch die Frage, wie viele Chassis sich zu einer virtuellen Fabric zusammenschließen lassen, ist bei jedem Hersteller anders implementiert.

Parallel zu der Entwicklung im Layer 2 Networking gab es aber auch Überlegungen, ob man die bekannten Probleme mit dem klassischen Data Center Design nicht auch mit Layer 3, also mittels Routing, lösen kann.

Vorreiter dieser Überlegungen waren die Hyperscale Rechenzentren von Microsoft und Facebook. Allen voran muss man hier Petr Lapukhov nennen, der sowohl bei Microsoft als auch bei Facebook diesen Designansatz etablierte und bei der IETF den RFC 7938 federführend betreute.

Dieser RFC 7938 beschreibt im Detail, wie ein Layer 3 Netzwerk mittels eBGP aufgebaut werden sollte. Doch dazu kommen wir etwas später.

Die primären Fragen, die wir zunächst klären sollten, lauten daher:

1. Welche Vorteile hat eigentlich ein Layer 3 Design?
2. Welche Data Center Anwendungen profitieren davon?
3. Welche Auswirkung hat die Wahl des Routing Protokolls?
4. Wie sieht die Topologie eines eBGP Layer 3 Data Center aus?
5. Lässt sich das Design auch auf den Campus übertragen?

Kommen wir damit direkt zu Frage 1:

„Wo liegen die Vorteile?“

Diese unterscheiden sich erstmal gar nicht so sehr von den Vorzügen einer Layer 2 Designs mit TRILL oder SPB.

Auch hier können wir eine Struktur aufbauen, die sowohl eine Link-, als auch eine Node-Protection ermöglicht. Dies bedeutet: Sowohl der Ausfall einer Leitung als auch eines Netzwerkknotens kann kompensiert werden, da immer mindestens ein alternativer Pfad (Link bzw. Next Hop) zur Verfügung steht. Auch die Vorzüge des ECMP (Equal Cost Multi-Path), die sowohl TRILL als auch SPB dank des zugrundeliegenden IS-IS Routing mitbringen, lassen sich in einem Layer 3 Design umsetzen.

Ebenso sind die Umschaltzeiten mehr als ausreichend. Im Vergleich zu klassischen Verfahren wie dem RSTP oder dem STP geht es sogar rasend schnell. Je nach eingesetzter Hardware können diese in Bereichen von 20 bis 50ms liegen. Schneller geht es auch bei einem MPLS Provider nicht.

Die eigentlichen Vorteile liegen vielmehr in der Beschneidung der Broadcastdomänen, da in einem solchen Designansatz das Routing bis in den Top of Rack bzw. End of Row Switch gezogen wird.

Im Ergebnis bildet jeder ToR Switch sein eigenes Subnetz, welches mittels Routing bekannt gegeben wird. Dadurch entfällt die Verarbeitung und Weiterleitung von Broadcast über den Access-Switch hinaus.

Diese Beschneidung von Layer 2 Broad- und Multicast führt uns zu einem Design, welches viel stärker skaliert als alle bisherigen Ansätze, da alle hiermit verbundenen Probleme nur singulär auf einem ToR/EoR Switch gelöst werden müssen.

In einem Designbeispiel der Firma Facebook führt dies zu einem möglichen Ausbau mit 48 ToR Switchen pro PoD (Point of Delivery oder auch Modul) und dem Zusammenschluss von 48 dieser PoDs zu einem Data Center. Gehen wir von einem 48 Port Switch im Access (ToR) aus und nutzen 4 Anschlüsse für den Uplink, so ergibt sich eine maximale Anzahl von über 100.000 Ports zur Anschaltung von Servern innerhalb eines einzigen Rechenzentrums. Eine, wie ich finde, beeindruckende Anzahl. (siehe Abbildung 1)

Da hierzu jedoch kein proprietäres Verfahren benötigt wird und auch keine Entscheidung für oder gegen ein Layer 2 Verfahrens wie TRILL oder SPB bzw. MC-LAG getroffen werden muss, ist diese Vorgehensweise auch in einer heterogenen Umgebung einsetzbar.

Denn die Entscheidung für oder gegen TRILL bzw. SPB, also einer Layer 2 Fabric, bedeutet auch, sich in die direkte Abhängigkeit eines Herstellers und seiner Lösung zu begeben.

Erstes Zwischenfazit: Ein standardisiertes Routing Verfahren erlaubt ein Netzwerk

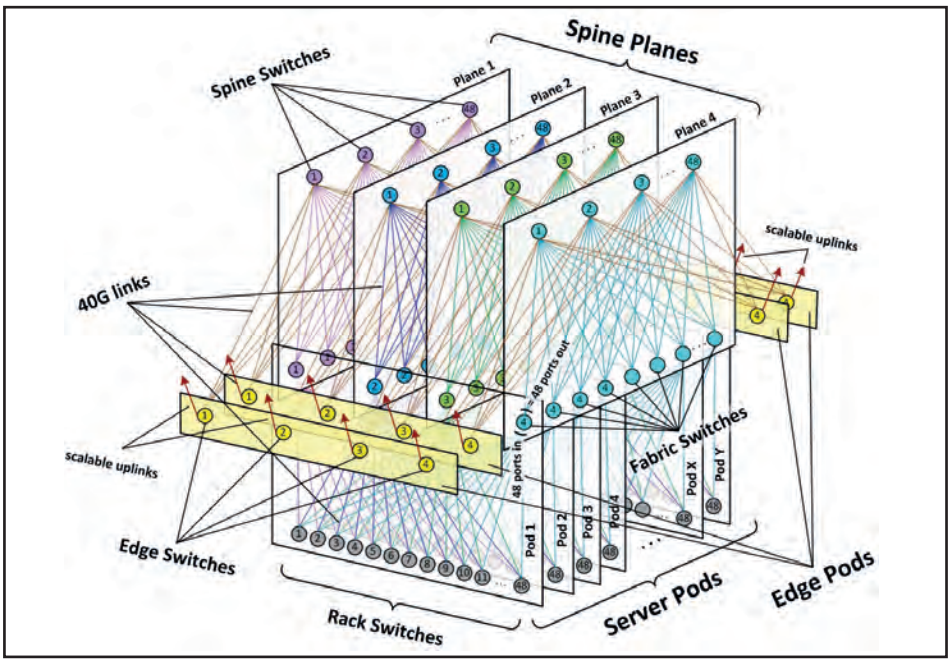


Abbildung 1: Spine-Leaf Data Center Quelle: Facebook

Design ohne Broadcastprobleme, hoher Skalierung und Herstellerunabhängigkeit.

Kommen wir somit zur 2. Frage:

„Welche Data Center Anwendungen profitieren davon?“

Zunächst einmal müssen wir natürlich feststellen, wer mit einem solchen Design ins Hintertreffen gerät, nämlich alle Anwendungen, die auf Broadcast oder Layer 2 Multicast basieren.

Ist das heute noch ein Problem? Ausschließen sollte man solche Situationen nie. Gerade bei der Migration älterer Anwendungen muss man vorsichtig agieren und sich genau darüber informieren wie eine Anwendung kommuniziert.

Betrachten wir jedoch moderne Anwendungen gerade im Web Umfeld, so sehen wir hier ausschließlich eine IP basierte Verständigung. Diese kommt naturgemäß sehr gut mit einer Layer 3 Fabric aus.

Dieser Grundgedanke der web-basierten Server Infrastruktur ist es denn auch, der den neuen Design Ansatz erst ermöglicht und vorangetrieben hat. Facebook und Microsoft setzen gezielt auf Routing und haben damit sämtliche Layer 2 Aktivitäten, soweit es geht, aus ihren Rechenzentren verbannt. Dies bedeutet: Keine Server Kommunikation mittels Broadcast oder Layer 2 Multicast, keine Layer 2 Redundanzverfahren zur Absicherung des Netzwerkes.

Ein weiterer großer Nutznießer des Routingansatzes ist die Server-Virtualisierung. Wie sicher viele von Ihnen wissen, basieren die gängigen Virtualisierungslösungen wie VMware NSX, Microsoft Hyper-V oder Cisco ACI auf einem Tunnelmechanismus. Hierzu wird auf einem bestehenden, physikalischen Netzwerk ein sogenanntes virtuelles Overlay Netzwerk gelegt.

Dieses wird zwischen den sogenannten Tunnelendpunkten, den VTEP, mittels eines Protokolls wie VXLAN, NVGRE oder Geneve gebildet. Die Tunnelendpunkte können sowohl auf einem Netzwerkknoten (z.B. Switch) als auch auf einem Serverhost liegen. Einzige Voraussetzung ist, dass sich die VTEP über IP erreichen können um, in IP gekapselt, Layer 2 Domänen zu bilden.

Und auch hier bietet uns das Layer 3 Design eine bestmögliche Lösung.

Zusammengefasst kann man also sagen, dass moderne Server Architekturen und die damit oft verbundene Virtualisierung sehr stark von einem gerouteten Netzwerkdesign profitieren.

Natürlich funktioniert Server Virtualisierung auch mit einer TRILL oder SPB Fabric, aber die Nachteile überwiegen. Da wäre zum einen der Umstand, dass neben den Overlay Tunnel zusätzlich Layer 2 Tunnel innerhalb der Layer 2 Fabric gebildet werden, was zu verschachtelten Tunnel führt und damit das Troubleshooting verkompliziert und zum anderen, dass Broadcast und Multicast sich innerhalb der Fabric wieder ungehemmt ausbreiten können.

Kommen wir damit zum nächsten Punkt:

„Welche Auswirkung hat die Wahl des Routing Protokolls?“

Diese Frage ist zugegeben ein wenig heikel und erfordert zunächst einmal einen Blick zurück in die Vergangenheit. Am Ende der Betrachtung sollte aber klargeworden sein, warum statt eines IGP Routings BGP aktuell so beliebt ist.

Die ersten Routing Protokolle, die entwickelt wurden, waren die Distance Vector Protokolle (RIP oder auch IGRP). Diese haben jedoch einige unangenehme Eigenschaften.

Da wäre zum einen der Umstand, dass sie nur sehr langsam periodische Updates zur Anzeige der Erreichbarkeit übermitteln und daher auch nur verzögert auf Netzwerkfehler reagieren können.

Ein weiteres Manko ist die nicht vorhandene Struktur. Anders als OSPF mit seinem Area-Konzept bilden alle Router, die untereinander RIP Informationen austauschen, „ein“ Netzwerk. In Kombination mit dem langsamen Verhalten bei der Erkennung von Netzwerkproblemen hat man daher die maximale Größe eines Netzes begrenzt (z.B. bei RIP auf 15 Hops). Zudem ist die Metrik meist sehr beschränkt, d.h. man betrachtet nur die Anzahl der Hops, über die ein Zielnetzwerk zu erreichen ist und beachtet dabei nicht, ob es sich um einen guten Pfad (z.B. mit hoher Bandbreite) handelt.

Außerdem haben sie die unangenehme Eigenschaft, neue Informationen schnell zu lernen, aber Fehler nur sehr langsam zu erkennen. Dies liegt daran, dass sie nicht erkennen, dass sie Teil des Problems sind. Die folgenden zwei Grafiken in Abbildung 2 sollen dies verdeutlichen.

Wie man sieht lernt der Router R1, dass sein ausgefallenes Netz über den Nachbar Router R2 scheinbar erreichbar ist. Damit nun der Hop Count nicht ins Unendliche läuft, hat man die Anzahl auf 15 Hops begrenzt. Erst beim Erreichen des max. Hop Counts verwerfen die Router das gelernte Netzwerk. Dies, in Kombination mit den langsamen Update-Intervallen, führt zu einer sehr stark verzögerten Konvergenz des gesamten Netzes.

Als Gegenentwurf zu den Distance Vector Protokollen wurden daher die Link State Protokolle entwickelt. Ihre bekanntes-

Ist BGP das bessere IGP?

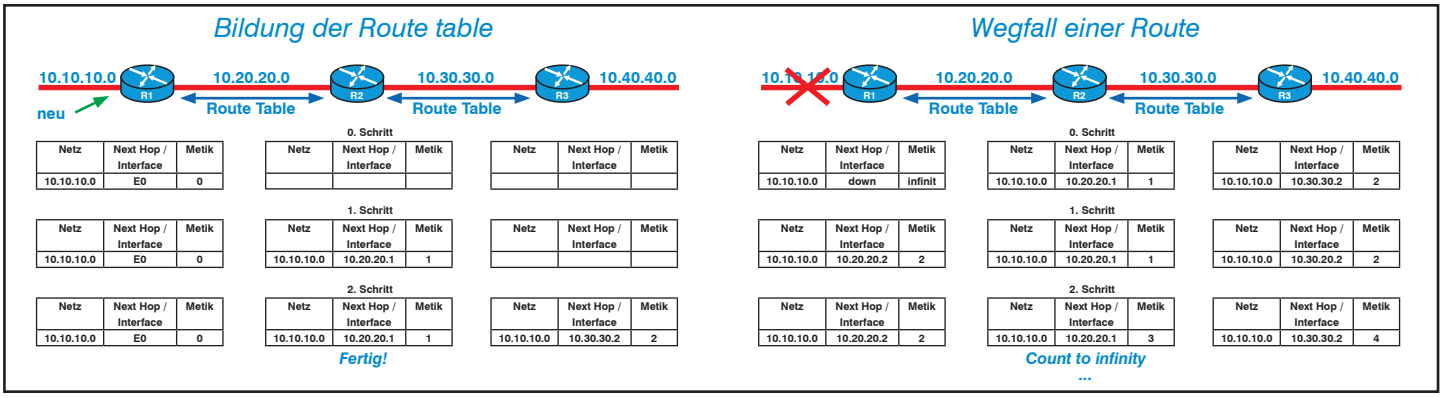


Abbildung 2: Lernen eines Netzes / Löschen eines Netzes

ten Vertreter sind OSPF und IS-IS. Ziel der Entwicklung war es, die Probleme des Distance Vektor Routings zu eliminieren. Dazu wurde eine komplexe Metrik eingeführt, die verschiedene Paramater zur Wegewahl berücksichtigt und das Updateverhalten umgestellt. Wurde vorher intervallmäßig immer die komplette Route-Table übertragen, beschränkte man sich jetzt auf den Austausch von Keepalive-Informationen bzw. Update Nachrichten bei Änderungen.

Eine weitere Neuerung war die Einführung eines Strukturmodells mittels des Area-Designs, speziell bei OSPF.

Die Funktionsweise dieser Link State Protokolle ist einfach erklärt. Zunächst sammelt ein Router alle Informationen seiner Umgebung (interne und externe von benachbarten Routern) und bildet daraus einen Topologie Datenbank, die ihm die Möglichkeit bietet, das Netzwerk als Ganzes zu erkennen. (siehe Abbildung 3)

Aus diesem Wissen über den Aufbau des Netzes kann jetzt jeder Router für sich bestimmen, wie er ein Zielnetzwerk auf dem besten Weg (Pfad mit der günstigsten Metrik) erreichen kann. Hat er seine Routing-Tabelle gebildet, versendet er nur noch Status-Änderungen und sogenannte Hello Pakete, um seine Nachbarn über seine Erreichbarkeit zu informieren.

Die Vorteile dieses Ansatzes sind:

- verschiedene „gleichwertige“ Pfade parallel zu nutzen (ECMP)
- dabei sehr schnell zu konvergieren
- bei einem gleichzeitig geringen Verkehrsaufkommen zum Informationsabgleich

Allerdings wird hierfür ein höherer Speicherbedarf benötigt (Vorhaltung einer Routing-Tabelle „und“ einer Topologie-Datenbank) und mehr CPU Leistung zur selbständigen Berechnung bei Topologieänderungen.

Aber wie immer im Leben erfolgt auf jede Reaktion auch eine Gegenreaktion. In unserem Fall wurde versucht, die Unzulänglichkeiten der Distance Vector Protokolle zu kompensieren bzw. zu minimieren. Zum einen gab es Bestrebungen, das Konvergenzverhalten zu verbessern. Dies gelang durch die Einführung von:

- Split Horizon
- Route Poisoning
- Holddown Timers
- und Triggered Updates

(siehe hierzu auch Abbildung 4)

Und zum anderen durch die Entwicklung eines neuen Routing Protokolls, des Enhanced Interior Gateway Routing Protokoll (EIGRP), durch Cisco.

Dieses Protokoll sollte die Metrik Probleme z.B. von RIP beheben, aber gleichzeitig weniger komplex als OSPF sein.

Die Situation, die wir daher heute in unseren internen Netzen antreffen, zeigt dann auch, dass sowohl das Distance Vektor Protokoll EIGRP als auch das Link State Verfahren OSPF sehr weit verbreitet sind.

Bleibt noch eine wichtige Frage in diesem Zusammenhang, die geklärt werden muss.

Welche Auswirkung hat das Wissen um die Topologie des Netzes?

Wie wir gesehen haben, kennt OSPF unser Netz ziemlich genau und könnte aus diesem Wissenvorsprung vielleicht weitere Schlüsse ziehen. Aber genau hier ergibt sich leider, trotz der vorhandenen Informationen, kein Mehrwert. Das Wissen wird nur herangezogen, um den Next Hop für ein Ziel zu ermitteln und somit verhält sich OSPF nicht anders als RIP oder EIGRP. Das Grundprinzip bleibt weiter „Hop-by-Hop Destination Only“.

Daher zunächst ein kleines Fazit zum „internen“ Routing:

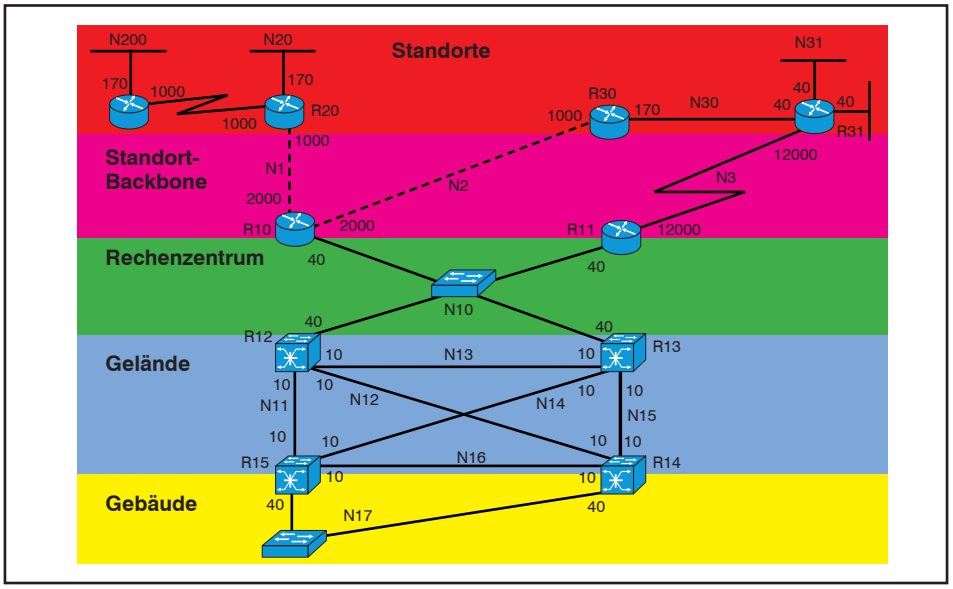


Abbildung 3: Topologie Datenbank

Ist BGP das bessere IGP?

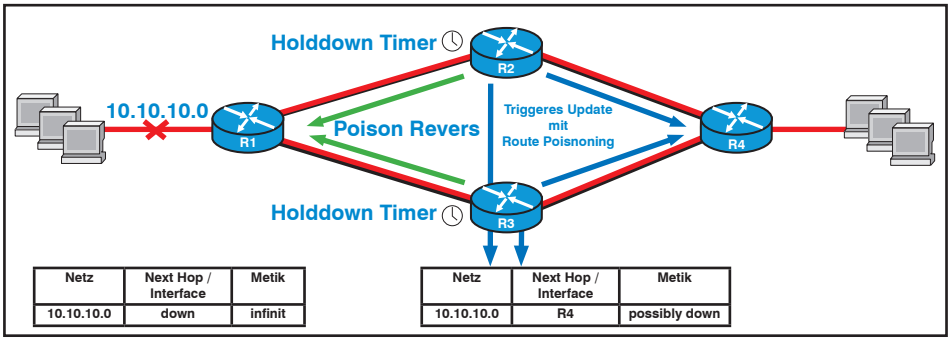


Abbildung 4: Konvergenz Beschleunigung

- Der Einsatz der unterschiedlichen Verfahren macht heute kaum noch einen Unterschied

- Dank der Erweiterungen für das Distance Vektor Verfahren erreicht man heute eine ähnlich gute Konvergenz

- Der eigentliche Unterschied bei den Protokollen beruht auf:
  - Flooding-and-computing bei Link State
  - Computing-and-propagating bei Distance Vector

- Die Nutzung der Topologie Kenntnisse fällt nicht ins Gewicht

- Routing funktioniert immer noch nach dem „Next-Hop“ Prinzip

- Erst der Einsatz von Traffic Engineering würde von der Topologie DB profitieren (z.B. durch Fast Re-Route auf der Basis bekannter, alternativer Pfade)

Warum aber jetzt zusätzlich zu den doch schon recht gut funktionierenden IGP Verfahren „das“ Exterior Gateway Protokoll namens BGP einsetzten?

Zunächst auch hier erstmal ein paar grundlegenden Gedanken zu BGP, um die entscheidenden Unterschiede im Anschluss herausarbeiten zu können.

Die Funktionweise des BGP fundiert auf dem sogenannten Path Vector und ist daher eng verwandt mit den Distance Vector Verfahren. Ziel der BGP Entwicklung war es, den Datenaustausch zwischen unterschiedlichen Computernetzen zu ermöglichen.

Ein solches Netz definiert sich als ein „Autonomes System (AS)“ und wird mit einer eindeutigen Nummer versehen.

Aufgabe des BGP ist es nun, zwischen verschiedenen autonomen Systemen Informationen auszutauschen. Damit ist BGP „das“ Internet Routing Protokoll.

Um nun den Verkehrsfluss effizient zu steuern, Bedarf es natürlich einer stark ausgeklügelten Metrik, die ein Distance Vektor Protokoll so nicht mitbringt. Diese Metrik wird im BGP als eine Reihe von Attributen definiert. Diese beinhalten, anders als bei den IGP Verfahren, technische und strategische Gesichtspunkte zur Ermittlung des Next Hop und zur Bildung der Routing Tabelle.

Wichtig für unsere Betrachtung an dieser Stelle:

- Wir schauen nur auf den Anwendungsfall für das interne RZ Netzwerk

- Externes Verhalten, wie das Internet oder Provider Routing funktioniert, wird hier nicht erläutert

- Auch BGP Funktionen für die Informationsverteilung in Overlay Netzen (Server Virtualisierung) sind außen vor, als Beispiel sei hier genannt MP-BGP EVPN VXLAN (Multiprotocol Extensions for Border Gateway Protocol with Ethernet Virtual Private Network and Virtual Extensible Local Area Network)

Die Besonderheit, die BGP an dieser Stelle mitbringt, ist der Umstand, dass es zwei Arten der Implementierung vorsieht. Da wäre zum einen der Einsatz als iBGP, also internes BGP, um:

- von eBGP-Routern gelernten Routen innerhalb des eigenen autonomen Systems zu propagieren.

Dies wäre auch mit Hilfe eines IGP möglich, jedoch sind diese nicht dafür ausgelegt, die BGP-Attribute zu übermitteln. Auch müssen alle iBGP-Router, die zusammen Routen austauschen, dieselbe AS-Nummer verwenden.

Die zweite Variante wäre das eBGP, also externes BGP, sowie wir es aus dem Internet kennen und zum Austausch von Routing Informationen zwischen autonomen Systemen benötigen.

Um weitere Nachteile des Distance Vector Verfahren zu eliminieren, gibt es zusätzliche Mechanismen zum Informationsaustausch, die eine schnelle Konvergenz ermöglichen:

- OPEN -> Message Type 1
  Wird nur zu Beginn einer Verbindung gesendet und muss mit einer KEEPALIVE-Nachricht beantwortet werden. Bei der OPEN-Nachricht werden die folgenden Parameter versendet: BGP-Version, AS-Nummer, Hold Timer, BGP Identifier sowie optionale Parameter. Im Anschluss werden die Routing Tabellen zwischen den Routern ausgetauscht.

- UPDATE -> Message Type 2
  Teilt eine Pfadänderung mit. Es können dabei pro UPDATE-Nachricht mehrere Pfade gleichzeitig hinzugefügt und/oder mehrere entfernt werden. UPDATE-Nachrichten sind daher das Kernstück von BGP.

- NOTIFICATION -> Message Type 3
  Beendet eine Verbindung und gibt Fehler- bzw. Statuscodes an. Alle Pfade, die über diese beendete Verbindung empfangen wurden, müssen gelöscht werden. Über ein BGP-Update muss dann verbreitet werden, dass diese Route nicht mehr verfügbar ist.

- KEEPALIVE -> Message Type 4
  Bestätigt die OPEN-Anfrage. Zur regelmäßigen Überprüfung, ob der verbundene Router noch online ist oder ob die Verbindung unterbrochen ist und die Pfade über den verbundenen Router somit ungültig geworden sind.

Die Auswahl eines Pfades wird dabei über die übermittelten Attribute gesteuert:

1. Bevorzugt wird der Wert mit der größten Local Preference.

2. Wenn die Werte für Local Preference gleich sind, wird der Pfad bevorzugt, der mittels BGP auf diesem Router generiert wurde.

3. Wenn kein Pfad auf diesem Router generiert wurde, bevorzuge den Pfad mit dem kürzesten AS_PATH-Attribut.

4. Wenn alle AS_PATH-Attribute die gleiche Länge haben, bevorzuge den niedrigsten Origin-Typ (IGP ist niedriger als EGP, EGP ist niedriger als Incomplete).

5. Wenn alle Origin-Typen gleich sind, bevorzuge den Pfad mit dem niedrigsten MED-Attribut.

Voraussetzungen	OSPF	IS-IS	BGP
Prefix Verteilung	Ja	Ja	Ja
Prefix Filterung	Limitiert	Limitiert	Voll umfänglich
Traffic Engineering	Limitiert	Limitiert	Voll umfänglich
Verkehrsmarkierung	Einfach	Einfach	Sehr variabel
Multi-Vendor Stabilität	Ja	Ja	Ja (siehe Internet)

Tabelle 1: Vergleich der Routing-Protokolle

6. Wenn alle Pfade den gleichen Wert für MED haben, bevorzuge externe Pfade gegenüber internen Pfaden.

7. Wenn immer noch alle Pfade die gleiche Priorität haben, bevorzuge den Pfad zum nächstgelegenen IGP-Nachbarn.

8. Sollten alle Pfade gleich sein, bevorzuge den Pfad mit der niedrigsten IP Adresse des BGP-Peers bezogen auf die Router-ID.

Wie man unschwer erkennen kann, ist die Auswahl sehr komplex und führt im Endergebnis zu „einem“ bevorzugten Pfad für ein Ziel-Netzwerk.

Wenn man jedoch eine Layer 3 Fabric baut, sind neben den reinen Weiterleitungsregeln weitere Funktionen zu berücksichtigen. Da wäre zum einen die Prefix Verteilung und Filterung, sowie die Verkehrserkennung und -markierung und besonders wichtig ein stabiles Netzverhalten auch über Herstellergrenzen hinweg. Vergleichen wir hierzu einmal die bekannten Routing Protokolle. (siehe Tabelle 1)

Die geforderten Punkte können also durchaus mit Hilfe des BGP Protokolls umgesetzt werden. Jedoch sollte man ein paar Rahmenbedingungen für das LAN im Hinterkopf haben.

So ist es natürlich zwingend notwendig, bei einem Data Center Design darauf zu achten, dass alle zur Verfügung stehenden Leitungen ausgenutzt werden (ECMP). Außerdem würde man im RZ das Thema Traffic Engineering sehr viel weniger komplex angehen als in einem Provider Backbone. Hier reichen im allgemeinen Funktionen wie:

- Graceful Shutdown oder
- Graceful Degradiation

um Server, Links oder Netzwerkknoten außer Betrieb zu nehmen bzw. das Netzwerk bei Störungen zu stabilisieren. Auch hierzu ein Vergleich, jetzt aber bezogen direkt auf den Einsatz von BGP. (siehe Tabelle 2)

Und auch hier kristallisiert sich schnell eine Variante heraus, die alle Voraussetzungen erfüllt, nämlich eBGP.

Nebenbei bemerkt verursacht der Einsatz iBGP noch weitere Probleme, denn eine iBGP Layer 3 Fabric arbeitet wie folgt:

Jeder Switch benötigt ein iBGP Peering mit jedem andern Switch innerhalb seines AS. Dies setzt aber eine Voll-Vermaschung aller Switche voraus oder aber den Einsatz von Route-Reflektoren.

Der Grund für eine vollständige Vermaschung liegt darin, dass iBGP innerhalb eines autonomen Systems empfangene BGP-Informationen von benachbarten BGP-Routern selber nicht an andere iBGP-Router weitergibt („Split-Horizon-Prinzip"). Dieses wiederum unterstützt die Vermeidung von Routing-Schleifen.

Eine weitere Einschränkung bezieht sich auf die Kommunikation der BGP Peers, denn diese basiert nicht, anders als bei eBGP, auf der IP Adresse der Routerinterfaces. Hier wird meist die Loopback Adresse für das Peering genutzt.

Hierdurch wird vermieden, dass bei Ausfall einer physikalischen Router-Schnittstelle die iBGP-Verbindung abbricht, obwohl der Router über redundante Interfaces verfügt, auf die innerhalb des autonomen Systems umgeschwenkt werden könnte.

Voraussetzungen	iBGP	iBGP
ECMP	Setzt die Erweiterung BGP AddPath voraus	Setzt die Erweiterung Multi-AS Pathing voraus
Peering	Mit Hilfe von Route Reflectoren um eine Voll-Vermaschung zu vermeiden	BGP Session zwischen unterschiedlichen AS
Traffic Engineering	Nicht unterstützt	Voll umfänglich

Tabelle 2: Vergleich beim Einsatz von BGP

Ohne Loopback-Adressen wären die iBGP-Router untereinander also an physikalischen Schnittstellen gebunden. Da BGP keinen Automatismus zum Lernen seiner Peers kennt, müssen diese immer erst eingerichtet werden.

Bei einem Ausfall eines Interface wäre somit auch ein BGP Peering unterbrochen und eine dauerhafte Verteilung von Routen innerhalb eines autonomen Systems selbst dann nicht mehr sichergestellt, wenn die interne Netzwerkinfrastruktur redundant aufgebaut ist.

Die sich daraus ableitende Voraussetzung ist: Die Verteilung der Loopback-Adressen erfolgt über ein zusätzliches IGP innerhalb des AS, da diese nicht an ein Interface gebunden sind und das IGP in der Lage ist, über seinen Automatismus die Router Nachbarn zu erkennen.

Kommen wir aber jetzt zur Bewertung, ob BGP tatsächlich das bessere OSPF ist.

Ein Layer 3 Fabric Design mit OSPF hat sicher einige Nachteile gegenüber dem Einsatz von eBGP:

- Kein Traffic Engineering

- Single Area Design skaliert nicht
  - Max 100 Router pro Area
  - Mit steigender Anzahl der Router steigt mit $n\hat{}2$ der Protokoll Overhead

- Höherer HW Aufwand
  - Speicher: Für Topologie DB
  - CPU: Berechnung der Routing Tabelle

Auf der Habenseite finden wir jedoch auch einige Vorzüge:

- Automatischer Aufbau der Nachbarschaftsbeziehungen
- ECMP ist implementiert per Default
- Mittels Multi Area-Design ist eine für den Enterprisebereich ausreichende RZ Skalierung möglich

Der Einsatz von eBGP geht daher meist auch einher mit der Einführung von SDN bzw. einem Controller, der u.a. die Datenströme innerhalb des RZs steuert. Allein die Konfiguration der BGP Peers ist ohne Automatisierung eine Aufgabe für jemanden, der Vater und Mutter erschlagen hat, denn wie schon gesagt kennt BGP keinen Automatismus zum Erkennen seiner Nachbarn.

Letztendlich ergeben sich vier Faktoren, die in einem bestimmten Fall, nämlich dem Aufbau eines Hyperscaler RZ, den Einsatz von eBGP forcieren:

- Stabilität
- Interoperabilität
- durchgehendes BGP Routing intern wie extern zum WAN oder Internet Provider
- sowie Traffic Enginnering

Sollten Sie jedoch verstärkt auf Server Virtualisierung setzen, so kann zumindest ein Teil der Verkehrssteuerung im Overlay Netzwerk durch die Virtualisierungslösung erbracht werden. Aus der Sicht eines solchen Netzwerk ist es am Ende egal, wie das Ende zu Ende IP Routing im Underlay für die VTEPs zustande kommt, Hauptsache die Tunnelendpunkte können miteinander kommunizieren.

Diese Bewertung wird sicher nicht von jedem geteilt, jedoch findet man auch in Data Center Design Guides etablierter Hersteller wie z.B. Arista den Hinweis, dass auch ein OSPF Design gerade für kleinere RZ Strukturen nicht völlig abwegig ist.

Fazit daher an dieser Stelle: Sowohl OSPF als auch eBGP eignen sich zum Aufbau einer Layer 3 Fabric, jedoch sind die Steuerungsmöglichkeiten sowie die Skalierbarkeit ein klarer Pluspunkt für den Einsatz von BGP.

Dies bringt uns dann zum nächsten Punkt auf unserer To Do Liste:

„Wie sieht die Topologie eines eBGP Layer 3 Data Center aus?“

Aus den bisherigen Ausführungen zum Thema BGP geht hervor, dass eBGP das bessere Verfahren zum Aufbau einer sehr großen Layer 3 Fabric ist. Und genau mit diesem Aufbau beschäftigt sich auch der RFC 7938 - Use of BGP for Routing in Large-Scale Data Centers.

Wie der Titel des RFC schon beschreibt, geht es in erster Linie um Routing und Skalierbarkeit. Weitere Funktionen werden natürlich ebenso berücksichtigt, allen voran die Möglichkeit, einen überbuchungsfreien Backbone im RZ zu errichten. Dieser soll sowohl den klassischen Nord-Süd Verkehr (Client-Server Request) als auch den immer häufiger anzutreffenden Ost-West Traffic (Server-Server Kommunikation) gleichermaßen bedienen können. Dazu wurde ein Scale Out Design mit Spine Leaf Ansatz gewählt.

Daher zunächst die Frage: Was bedeutet das?

Dieser Ansatz wird auch als Clos Design bezeichnet und ist zurückzuführen auf Charles Clos, der in den 1950er Jahren in den Bell Laboratories sich mit der Frage beschäftigte, wie ein theoretisch idealisiertes, mehrstufiges, damals noch Telefonnetzwerk aussehen könnte.

Um das Design zu erklären, möchte ich nochmal auf Abbildung 1 verweisen, welche genau diesen Aufbau bei Facebook zeigt. Es handelt sich um ein dreistufiges, überbuchungsfreies Netzwerkdesign, welches auf dem ToR Layer eine geringe Anzahl von Switchports vorsieht (max. 48 Ports). Diese ToR Switche können bei Bedarf überbuchungsfrei an den Leaf angeschaltet werden. Hierzu stehen Bandbreiten zwischen mehrfach 10 oder 40 Gbit/s zur Verfügung. Jeder ToR Switch wird mit mindestens zwei Leaf Switchen verbunden. Dies können Switche eines Leaf AS oder, zur Erhöhung der Verfügbarkeit, Switche aus unterschiedlichen Leaf AS sein. Sollen mehr ToR Switche für die Serveranbindung bereitgestellt werden, so kann auch die Anzahl der Switche pro Leaf erhöht werden, um die erforderliche Konnektivität zu gewährleisten. Dabei bildet jeder ToR Switch ein eigenes AS und somit auch ein eigenes IP-Subnet mit bestenfalls 64 Netzadressen (26er Subnetmask). Eine Rack-Reihe mit ToR Switchen bildet dabei einen sogenannten PoD (Point of Delivery, abweichend auch Modul oder Container).

Die Leaf Ebene fasst ebenfalls eine Reihe von Switchen zu einem AS zusammen. Wichtig: auf dieser Ebene gibt es kein eBGP Peering zwischen den Switchen eines AS bzw. zwischen den Switchen verschiedener AS. Die Leaf Ebene dient nur der Vermittlung zwischen ToR und Spine und stellt ausreichend Bandbreite und parallel Pfade für den Netzwerkverkehr zur Verfügung. Hier werden keine Sever angebunden. Sie bildet die eigentliche Layer 3 Switch Fabric. Die Anzahl der Leaf Ebenen kann variieren je Anzahl der Spine AS.

Der Spine stellt den Übergang zwischen den verschiedenen Leaf AS bereit und dient zur Anbindung aller externen Übergänge oder auch Border Leafs genannt. Auch hier bilden die Spine Switche ein eigenes AS, welche ebenfalls kein internes eBGP Peering vollziehen. Die Spine Ebene kann bei Bedarf mehrfach ausgelegt sein je nach benötigter Bandbreite und Verfügbarkeit. Dabei bildet jede weitere Spine ebenfalls ein eigens AS.

Es bietet sich an, AS Nummern zu verwenden, die im RFC 1930 bzw. 6996 (for Private Use) beschrieben sind. Danach stehen laut RFC 1930 die Nummern 64512 bis 65535 und nach RFC 6996 die Nummern 4200000000 bis 4294967294 zur Verfügung. Dies vermeidet Probleme beim Übergang zum Internet oder WAN Provider, da private AS Nummern, ähnlich wie RFC 1918 IP-Adressen, im Internet ignoriert werden. (siehe Abbildung 5)

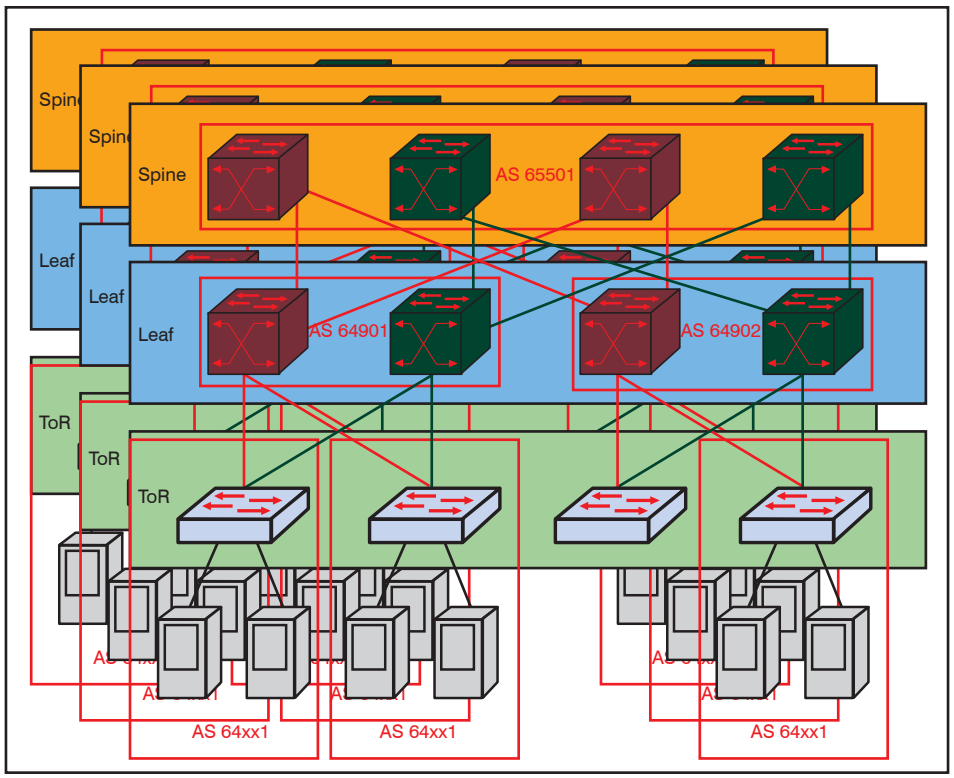


Abbildung 5: AS Nummern im RZ

Um ein solches Design steuern und konfigurieren zu können, bedarf es aber zwingend eines Controllers, der im Regelfall am Spine angeschlossen wird.

Allerdings gilt es in diesem Zusammenhang noch eine weitere Frage zu klären, nämlich: Wie schnell konvergiert eigentlich so ein BGP gesteuertes Netzwerk?

Nun, im Regelfall benötigt BGP laut RFC ein 7 Sekunden Intervall zur Fehlererkennung, wird jedoch ein schnelleres Umschaltverhalten erwartet, so kann zusätzlich BFD (Bidirectional Forwarding Detection) eingesetzt werden.

BFD (RFC 5880 & 5881) etabliert eine Session zwischen zwei Endpunkten über einen zu überwachenden physikalischen Link oder Pfad. Da BFD ähnlich wie BGP keinen Automatismus zur Erkennung eines Nachbarn besitzt, muss auch hier jeder Endpunkt entsprechend konfiguriert werden. Da BFD ein IP basiertes Verfahren ist, kann es jede Art von Layer 2 Link überwachen.

Es gibt zwei Varianten der Implementierung.

- *asynchronous mode*
- *und demand mode*

Im *asynchronous mode* senden die Endpunkte periodische Hello Pakete. Können diese nicht mehr empfangen werden, wird die Session als verloren angesehen.

Im *demand mode* werden dagegen keine Hello Informationen ausgetauscht, nachdem eine BFD Session aufgebaut wurde. Es wird daher vorausgesetzt, dass die Endpunkte ein anderes Verfahren zum Austausch der Keepalive Informationen einsetzen.

Unabhängig vom eingesetzten Modus kann das Verlieren einer BFD Session als Trigger genutzt werden, um auf einen alternativen Pfad umzuschalten, so dass die Downtime auf 200 bis 500ms begrenzt werden kann. Sollten Sie Ultra Low Latency Switche einsetzten, sind sogar Umschaltzeiten zwischen 20 und 50ms möglich.

Kommen wir damit zur letzten Frage unserer Liste:

„Lässt sich das BGP Design auch auf den Campus übertragen?“

Aktuell gibt es mit Extreme Networks einen Anbieter, der diesen Ansatz verfolgt. Die sogenannte Extrem Fabric ist ein auf iBGP beruhendes Konzept. Das bedeutet, dass alle Switche innerhalb der Fabric zu einem Autonomen System gehören.

Da auch iBGP seine Nachbarschaftsbeziehungen nicht automatisch aufbauen kann, greift man zur Peer Bildung auf das LLDP (Link Layer Discovery Protokoll) zurück. Über den Austausch von erweiterten MIB Informationen können die Switche untereinander die genutzte AS Nummer übermitteln und somit BGP Peers bilden. Alternativ kann diese Funktion aber auch von einem SDN Controller übernommen werden. Hierbei erhalten die Switche während ihrer Bootphase mittels DHCP eine IP Adresse und über eine DHCP Option die Information, wie sie den Controller erreichen können. Diese stellt dann die erforderliche Konfiguration für jeden Switch innerhalb der Fabric zur Verfügung. Dieser Ansatz ist im Moment nur mit Extreme Switchen möglich und auch innerhalb des Produktportfolios auf aktuell wenige Modelle beschränkt, welches aber zügig ausgebaut werden soll. Das Ziel ist ganz klar eine BGP Fabric über Campus und Core bis in den Access Bereich hinein.

Die Vorteile des Ansatzes:

- Automatischer Aufbau der Fabric (Plug'n Play)
- SDN basiertes Traffic Engineering
- Ein durchgehendes Routing Protokoll über den Campus, zum Rechenzentrum bis zum Internet/WAN Provider

Ob dieses Konzept auch von anderen Anbietern adaptiert wird, bleibt im Moment noch abzuwarten.

Fazit: Ist BGP jetzt das bessere IGP?

Zunächst kann man einmal festhalten, dass sich durch die Änderung des Routing Protokolls das Forwarding-Verhalten nicht verändert. Es gilt immer noch das Hop-by-Hop Prinzip. Was man jedoch erhält ist ein vereinfachtes Netzwerkdesign, was sowohl intern wie extern auf einem Routingverfahren beruht. Zudem haben wir mit eBGP die Möglichkeit, erstmalig Traffic Engineering im Rechenzentrum einzusetzen. Ob dies aber wirklich benötigt wird, ist wiederum abhängig vom Design Ihrer Applikationen:

- Nutzen Sie hauptsächlich webbasierte Verfahren, so ergeben sich große Vorteile durch den Einsatz von BGP bei der Verkehrssteuerung.

- Arbeiten Sie jedoch verstärkt mit Server Virtualisierung auf Basis von VMware und Co, verpufft ein Großteil dieser Steuerungsmöglichkeiten, da die Paketverteilung durch das eingesetzte VXLAN Overlay dominiert wird.

Im Ergebnis können wir festhalten:

- Benötigen Sie ein stark skalierendes RZ-Konzept mit bis zu 100.000 Switchports oder mehr, führt kein Weg an eBGP vorbei.

- Geht es auch eine Nummer kleiner und ist Traffic Engineering für Sie kein Thema, trägt auch ein Konzept was, wie bisher auch, auf OSPF beruht.

ComConsult Veranstaltungskalender

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

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

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: UCC-Lösungen im Wettbewerb – Cisco versus Microsoft, 19.09.2017 in Bonn

Seit Jahren führen die Hersteller Cisco und Microsoft mit ihren Produkten „Skype for Business“ (ehem. Lync) und „Unified Communications Manager“ sowie dem zugehörigen Client- und Lösungsportfolio diverse nationale und internationale Benchmarks zum Thema Unified Communications & Collaboration (UCC) an. Doch was macht diese UCC-Lösungen so besonders? Was unterscheidet diese Lösungen von ihren Mitbewerbern? Welche Unterschiede ergeben sich im direkten Vergleich? Und vor allem: wer hat sich im Kampf um Marktanteile einen echten Vorteil erarbeiten können?

Preis: € 1.090,-- *

Neuerungen und Entwicklungen im Recht der Informations- und Kommunikationstechnologie, 25.09.2017 in Bonn

Rabattaktion

Nutzen Sie als Nichtjurist die jährlich stattfindende Veranstaltung, um sich in dem schnelllebigen und unübersichtlichen Bereich der Informations- und Kommunikationstechnologien an nur einem Tag hinsichtlich der wesentlichen Entscheidungen und Entwicklungen der letzten 12 Monate auf den neuesten Stand bringen zu lassen.

Preis: € 1.090,-- *

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

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

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

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 für Nichtjuristen, 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,-- *

* 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 Aachen
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