ComConsult Research

Der Netzwerk Insider

August 2017

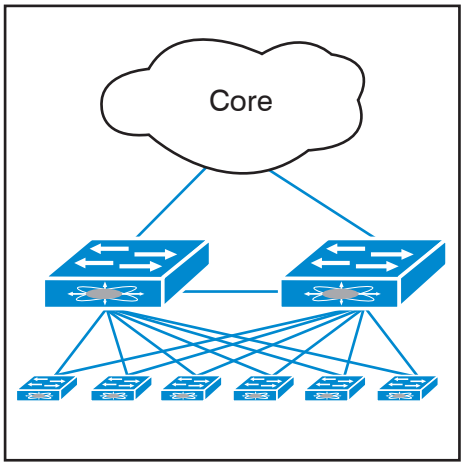
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

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

von Dipl.-Math. Cornelius Höchel-Winter

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



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

weiter ab Seite 9

Zweitthema

Cisco „Campus Fabric“ oder Software-defined Access

von Dr. Joachim Wetzlar

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

Eigentlich hätte mich dieses Thema nur am Rande interessiert, denn ich nehme bezüglich derlei Techniken grundsätzlich erst einmal eine abwartende Haltung ein. Letztlich hinter dem Ofen hervorgelockt hat mich die Tatsache, dass Cisco mit seiner „Campus Fabric“ eine spannende Anwendung des Locator/ID Separator Protocols (LISP) gelungen ist. Darüber hinaus erkenne ich auch grundsätzlichen Nutzen des SDA für einige meine Projekte. weiter auf Seite 21

Geleit

Planungs-Ansätze für die Zeit nach ISDN

auf Seite 2

Standpunkt

Informationssicherheit im Mikrokosmos von Smart Buildings

auf Seite 19

Sonderveranstaltungen

Herausforderung Informationssicherheit

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

ab Seite 18

Wireless und Mobility

ab Seite 27

Aktuelle Kongresse

ComConsult UC-Forum 2017

ab Seite 4

ComConsult Technologie-Tage 2017

ab Seite 7

Geleit

Planungs-Ansätze für die Zeit nach ISDN

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

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

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

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

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

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

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

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

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

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

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

Damit ist auch klar:

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

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

Warum ist das so?

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

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

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

Schwerpunktthema

Overlays in der Analyse

Teil 1: EVPN vs. SPBM

Fortsetzung von Seite 1

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

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

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

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

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

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

Konzepte und Bausteine

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

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

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

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

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

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

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

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

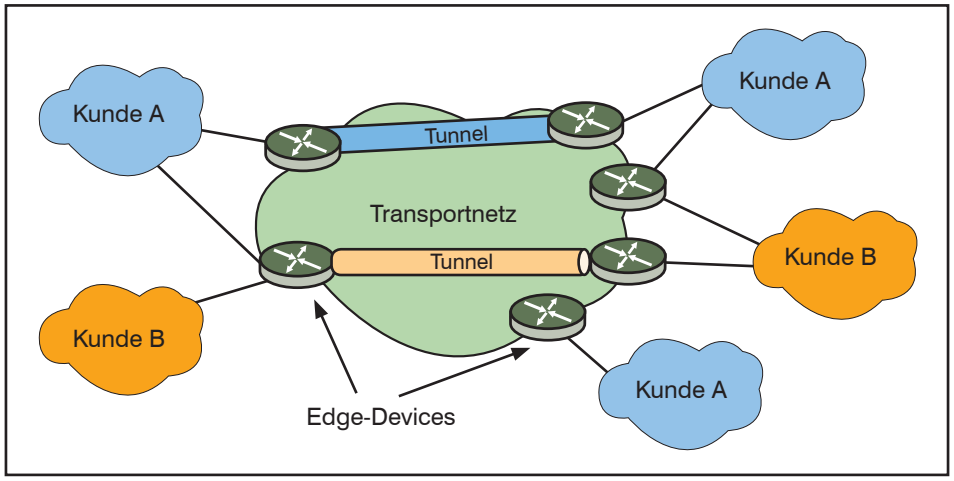


Abbildung 1: Bausteine einer Overlay-Lösung

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

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

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

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

Diese Bausteine und ihre Funktionsweisen werden im Weiteren genauer dargestellt.

Wie und warum werden Overlays überhaupt eingesetzt?

Für Unternehmensnetze können wir von folgender allgemeiner Situation ausgehen:

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

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

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

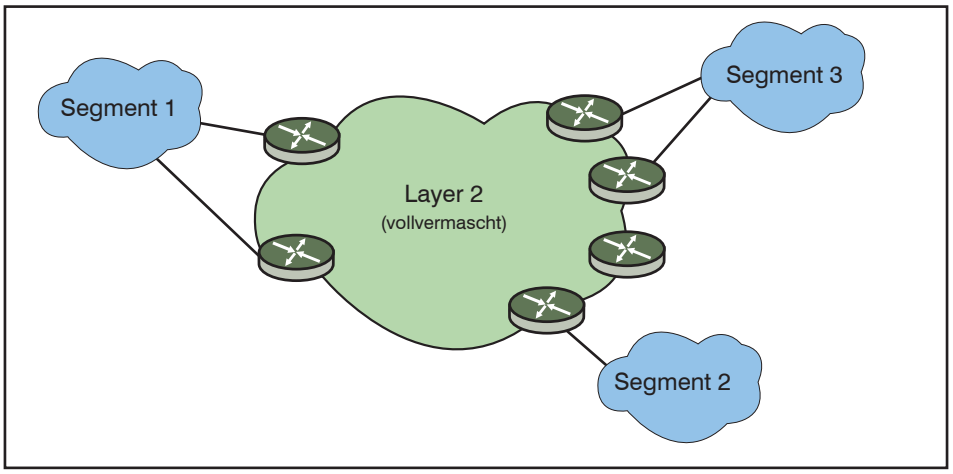


Abbildung 2: Overlay-Struktur mit Layer-2-Service aus der Sicht von Kunde A

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

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

Damit ergeben sich typische Einsatzszenarien für Overlay-Lösungen:

A) Virtuelle Anwendungsnetze:

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

B) RZ-Kopplung:

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

C) Overlays zur Nutzung flexibler Netzwerkdesigns:

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

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

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

Zweitthema

Cisco „Campus Fabric“ oder Software-defined Access

Fortsetzung von Seite 1

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

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

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

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

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

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

Grundzüge von LISP

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

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

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

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

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

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

Cisco „Campus Fabric“ oder Software-defined Access

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

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

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

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

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

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

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

Mobilität von Endpunkten mit LISP

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

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

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

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

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

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

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

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

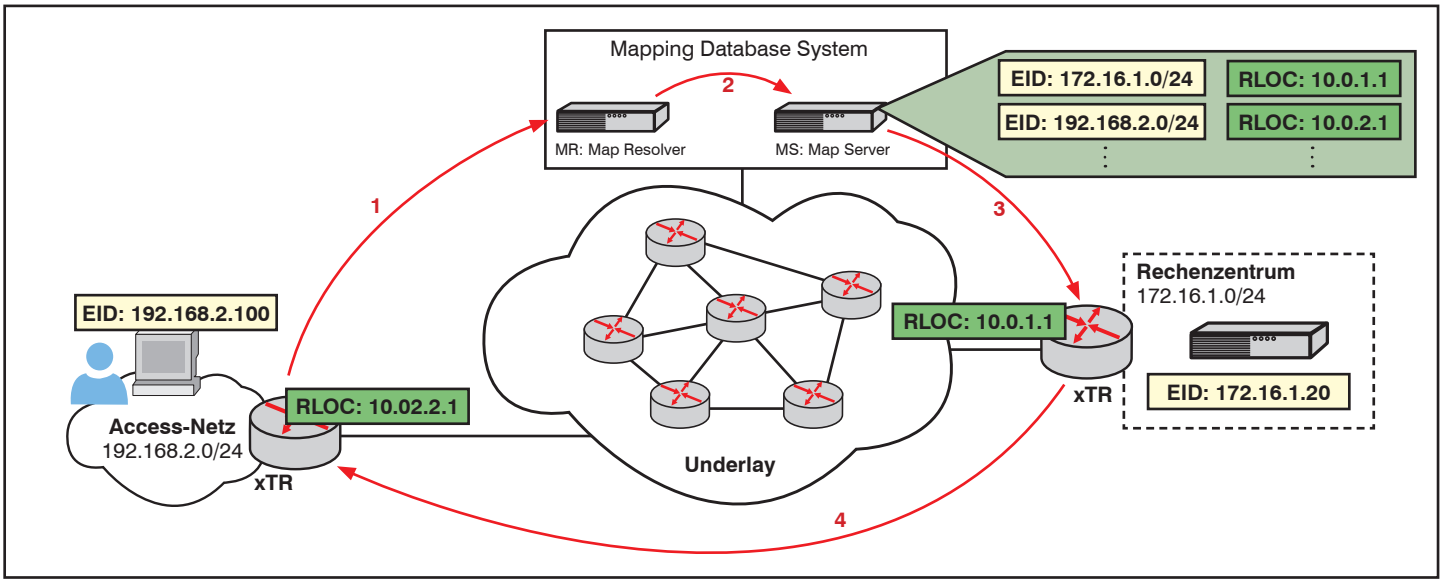


Abbildung 1: Zur grundsätzlichen Funktionsweise von LISP